BADAN SIBER DAN SANDI NEGARA



PANDUAN PEMENUHAN KONTROL KEMATANGAN KEAMANAN SIBER

Instrumen Pengukuran Kematangan Keamanan Siber

IKAS

DIREKTORAT KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI

2025

TLP:CLEAR

PANDUAN PEMENUHAN KONTROL KEMATANGAN KEAMANAN SIBER

Panduan Pemenuhan Kontrol Kematangan Keamanan Siber ditujukan untuk meningkatkan pemahaman tentang gambaran kondisi penerapan keamanan siber pada pemangku kepentingan (stakeholders) dan sebagai panduan pengisian Instrumen Penilaian Kematangan Keamanan Siber (IKAS)

Disusun oleh:
Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi
Deputi Bidang Strategi dan Kebijakan
Badan Siber dan Sandi Negara

SUSUNAN REDAKSI

Panduan Pemenuhan Kontrol Kematangan Keamanan Siber
Versi 1.0 : Desember 2025

Penanggung Jawab : Nunil Pantjawati, B.Sc.,M.E.

Ketua Tim : Yuri Prihantono, S.S.T.TP., M.T.

Tim Penyusun :

1. Sefiulki Weni Sari, S.ST., M.T.
2. Satrio Wicaksono N.P., S.ST.
3. Fitria Sekarwulan Risdhafany, S.ST.
4. Aji Setiyo Sukarno, S.ST.
5. Qusyairi Ridho S.F., S.S.T.TP., M.T.
6. Yuri Prihantono, S.S.T.TP., M.T.
7. Ahmad Baihaqi, S.Tr.TP.
8. Desy Ravitasani, S.Tr.MP.
9. Hasan Yahya, S.Kom.
10. Istuningtiyas, S.Tr.TP.
11. Nurwahidin Syu'ib, S.Tr.TP.
12. Wuri Handayani, S.Tr.TP., M.M.
13. Reriswandha Putra H., S.Tr.MP.
14. Aulia Nurul Azizah, S.Tr.Kom.
15. Ahmad Alinnoor U. Alby A., S.Tr.Kom.
16. Almas Fauzia Wibawa, S.Kom.
17. Anastasia Oktaviany Putri, S.Tr.Kom.
18. Andrian Rizky Moranta, S.Hum.
19. Mohammad Raffli F., S.Tr.Kom.
20. Ryan Muhammad A. K., S.Tr.Kom.

Tim Reviu :

1. Dian Novemia Perdana, S.Kom.
2. Maria Putri Handayani, S.Kom., M.AP.
3. Enggar Ndaru Prasojo, S.ST.
4. Ummu Fauziah Fitri, S.ST.
5. Fadly Achmad, S.ST., M.AP.
6. Kartika Pertiwi, S.S.T.MP., M.H., M.Sos.

Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi
Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar No. 70, Bojongsari, Depok, Jawa Barat 16516

KATA PENGANTAR

Seiring dengan berkembangnya teknologi informasi yang semakin pesat, ancaman terhadap keamanan siber pun semakin kompleks dan beragam. Untuk itu, perlu ada upaya yang terstruktur dan berkelanjutan dalam memastikan bahwa setiap pemangku kepentingan dapat menjaga dan meningkatkan kesiapsiagaan mereka terhadap potensi ancaman siber yang ada.

Sebagai bagian dari upaya tersebut, Badan Siber dan Sandi Negara (BSSN) telah mengeluarkan Peraturan BSSN Nomor 10 Tahun 2023 yang mengatur tentang penilaian kematangan keamanan siber. Penilaian ini sangat penting untuk mengukur sejauh mana penerapan kontrol keamanan siber di berbagai organisasi dapat menjamin perlindungan terhadap informasi dan sistem yang ada.

Panduan Pemenuhan Kontrol Kematangan Keamanan Siber ini disusun dengan tujuan untuk memberikan pemahaman yang lebih komprehensif mengenai gambaran kondisi penerapan keamanan siber pada berbagai pemangku kepentingan. Selain itu, panduan ini juga dimaksudkan sebagai pedoman bagi pemangku kepentingan dalam mengisi Instrumen Penilaian Kematangan Keamanan Siber (IKAS), yang menjadi bagian integral dalam proses penilaian kematangan yang diatur dalam peraturan ini.



Nunil Pantjawati, B.Sc., M.E.

Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi

Dengan adanya panduan ini, diharapkan setiap organisasi dapat memahami dan mengidentifikasi area-area yang memerlukan perhatian lebih dalam penerapan keamanan siber, serta dapat mengambil langkah-langkah perbaikan yang tepat untuk meningkatkan ketangguhan sistem keamanan siber organisasinya. Hal ini sejalan dengan komitmen kami untuk menciptakan ekosistem siber yang aman, terjamin, dan siap menghadapi tantangan di masa depan.

Kami berharap panduan ini dapat memberikan manfaat yang besar bagi seluruh pemangku kepentingan dalam mewujudkan keamanan siber yang lebih baik dan lebih tangguh, serta memberikan kontribusi signifikan terhadap terciptanya dunia maya yang lebih aman bagi seluruh masyarakat.

Depok, 12 Desember 2025

Dokumen ini ditandatangani secara elektronik oleh:
Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi

NUNIL PANTJAWATI, B.Sc., M.E.
Pembina Utama Madya (IV/d)

DAFTAR ISI

PANDUAN PEMENUHAN KONTROL KEMATANGAN KEAMANAN SIBER 1

DAFTAR ISI 5

DAFTAR ISTILAH 9

KRITERIA PEMENUHAN KONTROL KEMATANGAN KEAMANAN SIBER 10

PENDAHULUAN 16

A. LATAR BELAKANG 16

B. TUJUAN 16

KEMATANGAN KEAMANAN SIBER 18

A. KONSEPSI PELINDUNGAN IIV 18

B. INSTRUMEN PENILAIAN KEMATANGAN KEAMANAN SIBER (IKAS) 20

C. TAHAPAN PENGISIAN DAN PELAPORAN IKAS 22

D. PENJELASAN INDEKS 24

E. RUMUS 25

F. INDIKATOR PADA INSTRUMEN PENGUKURAN IKAS 27

DOMAIN I IDENTIFIKASI 28

1.1. Mengidentifikasi Peran dan tanggung jawab organisasi 29

1.1.1. Menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi 30

1.1.2. Mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya 36

1.1.3. Mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor IIV 40

1.2. Menyusun strategi, kebijakan, dan prosedur Pelindungan IIV 46

1.2.1. Menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan penyelenggara IIV 47

1.2.2. Mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV 55

1.2.3. Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan 60

1.2.4. Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga 64

1.3. Mengelola aset informasi 68

1.3.1. Mengelola daftar inventaris aset informasi 69

1.3.2. Memetakan jalur komunikasi dan alur data pada organisasi 76

1.3.3. Menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi 80

1.3.4. Menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya 87

1.3.5. Mengendalikan aset informasi milik organisasi 91

1.4. Menilai dan mengelola risiko Keamanan Siber 98

1.4.1. Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi. 99

1.4.2. Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal 103
1.4.3. Mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut 110
1.4.4. Menganalisis nilai risiko terhadap IIV 113
1.4.5. Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko 128
1.4.6. Menentukan dan mengomunikasikan toleransi risiko organisasi 134
1.4.7. Mengelola hasil penerapan manajemen risiko yang telah ditetapkan 139
1.4.8. Melakukan reviu terhadap hasil penerapan manajemen risiko 146

1.5. Mengelola risiko rantai pasok 149
1.5.1. Mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok .. 150
1.5.2. Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV 156
1.5.3. Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV 161
1.5.4. Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya 167
1.5.5. Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut 174

DOMAIN II PROTEKSI 181

2.1. Mengelola identitas, autentikasi, dan kendali akses 182
2.1.1. Mengelola identitas dan kredensial yang menggunakan layanan IIV 183
2.1.2. Mengelola akses jarak jauh terhadap layanan IIV 186
2.1.3. Mengelola izin akses dan otorisasi layanan IIV 191
2.1.4. Memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya 196

2.2. Melindungi aset fisik 199
2.2.1. Menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV 200
2.2.2. Memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur 207
2.2.3. Memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur 212
2.2.4. Memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman 217
2.2.5. Memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman 220

2.3. Melindungi data 223
2.3.1. Pelindungan terhadap data yang tersimpan pada Penyelenggara IIV 224
2.3.2. Pelindungan terhadap data yang terkirim dari Penyelenggara IIV 231
2.3.3. Memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai 237
2.3.4. Mengimplementasikan pelindungan dari kebocoran data 244
2.3.5. Mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data 250
2.3.6. Memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala 261
2.3.7. Menyediakan kebijakan pemusnahan data 264

2.4. Melindungi aplikasi 267

2.4.1. Menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi 268
2.4.2. Mengembangkan dan mengimplementasikan rencana manajemen kerentanan 281
2.4.3. Memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional 286
2.4.4. Mengimplementasikan prosedur pengembangan sistem yang aman 291

2.5. Melindungi jaringan 296
2.5.1. Menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum 297
2.5.2. Menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali 303
2.5.3. Menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan 309
2.5.4. Memastikan integritas jaringan senantiasa dilindungi 316
2.5.5. Menerapkan prosedur dan teknologi pencegahan malware 320
2.5.6. Memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi 331
2.5.7. Memastikan bahwa informasi mengenai pelindungan terhadap teknologi dibagikan hanya kepada pihak tepercaya 334

2.6. Melindungi sumber daya manusia 337
2.6.1. Menerapkan prosedur pengelolaan keamanan terhadap personel 338
2.6.2. Menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber 354
2.6.3. Menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di Penyelenggara IIV 363

DOMAIN III DETEKSI 371

3.1. Mengelola deteksi Peristiwa Siber 372
3.1.1. Menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber 373
3.1.2. Melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku 380
3.1.3. Menguji prosedur pendeteksian Peristiwa Siber secara berkala 385
3.1.4. Menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak 388

3.2. Menganalisis anomali dan Peristiwa Siber 393
3.2.1. Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data 394
3.2.2. Melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi 398
3.2.3. Menentukan dampak dari Peristiwa Siber yang terdeteksi 405
3.2.4. Mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi 410

3.3. Memantau Peristiwa Siber berkelanjutan 414
3.3.1. Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin 415
3.3.2. Memonitor kegiatan personel yang berada di dalam lingkup sistem IIV 425
3.3.3. Memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV 429
3.3.4. Menerapkan teknologi pemindaian kerentanan terhadap sistem IIV 433

DOMAIN IV PENANGGULANGAN DAN PEMULIHAN 440

4.1. Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber 441

4.1.1. Menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi 442
4.1.2. Menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi 455
4.1.3. Memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala 468
4.1.4. Memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan 472
4.1.5. Memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang 483

4.2. Menganalisis dan melaporkan Insiden Siber 486
4.2.1. Mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal maupun sumber informasi eksternal 487
4.2.2. Mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber 492
4.2.3. Memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan 496
4.2.4. Memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait 499

4.3. Melaksanakan penanggulangan dan pemulihan Insiden Siber 504
4.3.1. Memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber 505
4.3.2. Mengumpulkan dan memelihara bukti Insiden Siber dari IIV terdampak 514
4.3.3. Menginvestigasi dan eradikasi penyebab Insiden Siber 517
4.3.4. Mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber 523
4.3.5. Memastikan setiap aset informasi diperiksa keamanannya setelah penanganan Insiden Siber 527
4.3.6. Melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan 530
4.3.7. Menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan 549
4.3.8. Pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi 558
4.3.9. Memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber 562
4.3.10. Penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait 569

4.4. Meningkatkan keamanan setelah terjadinya Insiden Siber 573
4.4.1. Meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan 574
4.4.2. Mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala 578
4.4.3. Mengumpulkan dan memelihara hasil forensik digital 583
4.4.4. Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala 588

PENUTUP 593

TAKSONOMI ANCAMAN 594

DAFTAR ISTILAH

1	Infrastruktur Informasi Vital (IIV)	Sistem Elektronik yang memanfaatkan teknologi informasi dan/ atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan Sistem Elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/ atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.
2	IKAS	Instrumen Penilaian Kematangan Keamanan Siber
3	Kematangan Keamanan Siber	Kondisi yang menggambarkan kapabilitas dan kemajuan organisasi dalam menerapkan, meningkatkan, dan menjalankan Keamanan Siber secara efektif dan efisien.
4	Kementerian atau Lembaga	Instansi penyelenggara negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.
5	*Malware*	Perangkat lunak berbahaya yang dirancang untuk merusak Sistem Elektronik.
6	Penyelenggara IIV	Instansi penyelenggara negara, badan usaha, dan/atau organisasi yang memiliki dan/atau mengoperasikan IIV
7	Sistem Elektronik	Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
8	Teknologi Informasi	Sistem Elektronik yang digunakan untuk menyimpan, mengolah, dan menyebarkan informasi.
9	Teknologi Operasional	Sistem Elektronik yang digunakan untuk mengontrol perangkat fisik.
10	Tim Tanggap Insiden Siber	Sekelompok orang yang bertanggung jawab menangani insiden siber dalam ruang lingkup yang ditentukan terhadapnya.

KRITERIA PEMENUHAN KONTROL KEMATANGAN KEAMANAN SIBER

1 Kontrol 1.1.1.a: 31
2 Kontrol 1.1.1.b: 34
3 Kontrol 1.1.2.a: 37
4 Kontrol 1.1.3.a: 41
5 Kontrol 1.1.3.b: 44
6 Kontrol 1.2.1.a: 48
7 Kontrol 1.2.1.b: 50
8 Kontrol 1.2.1.c: 53
9 Kontrol 1.2.2.a: 56
10 Kontrol 1.2.2.b 58
11 Kontrol 1.2.3.a: 61
12 Kontrol 1.2.4.a: 65
13 Kontrol 1.3.1.a: 70
14 Kontrol 1.3.1.b: 73
15 Kontrol 1.3.2.a: 77
16 Kontrol 1.3.3.a: 81
17 Kontrol 1.3.3.b: 84
18 Kontrol 1.3.4.a: 88
19 Kontrol 1.3.5.a: 92
20 Kontrol 1.3.5.b: 95
21 Kontrol 1.4.1.a: 100
22 Kontrol 1.4.2.a: 104
23 Kontrol 1.4.2.b: 107
24 Kontrol 1.4.3.a: 111
25 Kontrol 1.4.4.a: 114
26 Kontrol 1.4.4.b: 116
27 Kontrol 1.4.4.c: 118
28 Kontrol 1.4.4.d: 120
29 Kontrol 1.4.4.e: 122

30 Kontrol 1.4.4.f: 124
31 Kontrol 1.4.4.g: 126
32 Kontrol 1.4.5.a: 129
33 Kontrol 1.4.5.b: 132
34 Kontrol 1.4.6.a: 135
35 Kontrol 1.4.6.b: 137
36 Kontrol 1.4.7.a: 140
37 Kontrol 1.4.7.b: 142
38 Kontrol 1.4.7.c: 144
39 Kontrol 1.4.8.a: 147
40 Kontrol 1.5.1.a: 151
41 Kontrol 1.5.1.b: 153
42 Kontrol 1.5.2.a: 157
43 Kontrol 1.5.2.b: 159
44 Kontrol 1.5.3.a: 162
45 Kontrol 1.5.3.b: 165
46 Kontrol 1.5.4.a: 168
47 Kontrol 1.5.4.b: 170
48 Kontrol 1.5.4.c: 172
49 Kontrol 1.5.5.a: 175
50 Kontrol 1.5.5.b: 177
51 Kontrol 1.5.5.c: 179
52 Kontrol 2.1.1.a: 184
53 Kontrol 2.1.2.a: 187
54 Kontrol 2.1.2.b: 189
55 Kontrol 2.1.3.a: 192
56 Kontrol 2.1.3.b: 194
57 Kontrol 2.1.4.a: 197
58 Kontrol 2.2.1.a: 201
59 Kontrol 2.2.1.b: 203
60 Kontrol 2.2.1.c: 205
61 Kontrol 2.2.2.a: 208
62 Kontrol 2.2.2.b: 210
63 Kontrol 2.2.3.a: 213

64 Kontrol 2.2.3.b: 215
65 Kontrol 2.2.4.a: 218
66 Kontrol 2.2.5.a: 221
67 Kontrol 2.3.1.a: 225
68 Kontrol 2.3.1.b: 228
69 Kontrol 2.3.2.a: 232
70 Kontrol 2.3.2.b: 235
71 Kontrol 2.3.3.a: 238
72 Kontrol 2.3.3.b: 241
73 Kontrol 2.3.4.a: 245
74 Kontrol 2.3.4.b: 248
75 Kontrol 2.3.5.a: 251
76 Kontrol 2.3.5.b: 253
77 Kontrol 2.3.5.c: 255
78 Kontrol 2.3.5.d: 257
79 Kontrol 2.3.5.e: 259
80 Kontrol 2.3.6.a: 262
81 Kontrol 2.3.7.a: 265
82 Kontrol 2.4.1.a: 269
83 Kontrol 2.4.1.b: 273
84 Kontrol 2.4.1.c: 277
85 Kontrol 2.4.2.a: 282
86 Kontrol 2.4.3.a: 287
87 Kontrol 2.4.4.a: 292
88 Kontrol 2.5.1.a: 298
89 Kontrol 2.5.1.b: 301
90 Kontrol 2.5.2.a: 304
91 Kontrol 2.5.2.b: 307
92 Kontrol 2.5.3.a: 310
93 Kontrol 2.5.3.b: 313
94 Kontrol 2.5.4.a: 317
95 Kontrol 2.5.5.a: 321
96 Kontrol 2.5.5.b: 323
97 Kontrol 2.5.5.c: 326

98 Kontrol 2.5.5.d: 329
99 Kontrol 2.5.6.a: 332
100 Kontrol 2.5.7.a: 335
101 Kontrol 2.6.1.a: 339
102 Kontrol 2.6.1.b: 342
103 Kontrol 2.6.1.c: 344
104 Kontrol 2.6.1.d: 346
105 Kontrol 2.6.1.e: 348
106 Kontrol 2.6.1.f: 350
107 Kontrol 2.6.1.g: 352
108 Kontrol 2.6.2.a: 355
109 Kontrol 2.6.2.b: 358
110 Kontrol 2.6.2.c: 361
111 Kontrol 2.6.3.a: 364
112 Kontrol 2.6.3.b: 366
113 Kontrol 2.6.3.c: 369
114 Kontrol 3.1.1.a: 374
115 Kontrol 3.1.1.b: 377
116 Kontrol 3.1.2.a: 381
117 Kontrol 3.1.2.b: 383
118 Kontrol 3.1.3.a: 386
119 Kontrol 3.1.4.a: 389
120 Kontrol 3.1.4.b: 391
121 Kontrol 3.2.1.a: 395
122 Kontrol 3.2.2.a: 399
123 Kontrol 3.2.2.b: 402
124 Kontrol 3.2.3.a: 406
125 Kontrol 3.2.4.a: 411
126 Kontrol 3.3.1.a: 416
127 Kontrol 3.3.1.b: 419
128 Kontrol 3.3.1.c: 422
129 Kontrol 3.3.2.a: 426
130 Kontrol 3.3.3.a: 430
131 Kontrol 3.3.4.a: 434

132 Kontrol 3.3.4.b: 437
133 Kontrol 4.1.1.a: 443
134 Kontrol 4.1.1.b: 446
135 Kontrol 4.1.1.c: 449
136 Kontrol 4.1.1.d: 452
137 Kontrol 4.1.2.a: 456
138 Kontrol 4.1.2.b: 459
139 Kontrol 4.1.2.c: 462
140 Kontrol 4.1.2.d: 465
141 Kontrol 4.1.3.a: 469
142 Kontrol 4.1.4.a: 473
143 Kontrol 4.1.4.b: 475
144 Kontrol 4.1.4.c: 478
145 Kontrol 4.1.4.d: 481
146 Kontrol 4.1.5.a: 484
147 Kontrol 4.2.1.a: 488
148 Kontrol 4.2.1.b: 490
149 Kontrol 4.2.2.a: 493
150 Kontrol 4.2.3.a: 497
151 Kontrol 4.2.4.a: 500
152 Kontrol 4.2.4.b: 502
153 Kontrol 4.3.1.a: 506
154 Kontrol 4.3.1.b: 508
155 Kontrol 4.3.1.c: 510
156 Kontrol 4.3.1.d: 512
157 Kontrol 4.3.2.a: 515
158 Kontrol 4.3.3.a: 518
159 Kontrol 4.3.3.b: 520
160 Kontrol 4.3.4.a: 524
161 Kontrol 4.3.5.a: 528
162 Kontrol 4.3.6.a: 531
163 Kontrol 4.3.6.b: 534
164 Kontrol 4.3.6.c: 537
165 Kontrol 4.3.6.d: 540

166 Kontrol 4.3.6.e: 543
167 Kontrol 4.3.6.f: 546
168 Kontrol 4.3.7.a: 550
169 Kontrol 4.3.7.b: 552
170 Kontrol 4.3.7.c: 555
171 Kontrol 4.3.8.a: 559
172 Kontrol 4.3.9.a: 563
173 Kontrol 4.3.9.b: 566
174 Kontrol 4.3.10.a: 570
175 Kontrol 4.4.1.a: 575
176 Kontrol 4.4.2.a: 579
177 Kontrol 4.4.2.b: 581
178 Kontrol 4.4.3.a: 584
179 Kontrol 4.4.3.b: 586
180 Kontrol 4.4.4.a: 589
181 Kontrol 4.4.4.b: 591

PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi informasi yang semakin pesat memberikan dampak positif bagi berbagai sektor kehidupan. Namun, di sisi lain, hal ini juga memunculkan ancaman terhadap keamanan siber yang semakin kompleks, khususnya terhadap Infrastruktur Informasi Vital (IIV). IIV berperan krusial dalam keberlangsungan sektor-sektor kritis di negara, seperti sektor pemerintahan, ekonomi, dan layanan publik. Oleh karena itu, perlindungan terhadap IIV harus menjadi prioritas utama dalam menjaga ketahanan nasional.

Untuk itu, Badan Siber dan Sandi Negara (BSSN) melalui Peraturan BSSN Nomor 10 Tahun 2023 mengatur tentang penilaian kematangan keamanan siber, yang bertujuan untuk membantu Penyelenggara IIV dalam menilai sejauh mana penerapan kerangka kerja pelindungan IIV telah dilakukan secara efektif. Panduan Pemenuhan Kontrol Kematangan Keamanan Siber ini hadir sebagai acuan bagi pemangku kepentingan (*stakeholders*) untuk memahami kondisi penerapan keamanan siber serta sebagai panduan dalam pengisian Instrumen Penilaian Kematangan Keamanan Siber (IKAS).

Instrumen Penilaian Kematangan Keamanan Siber (IKAS) disusun untuk mengukur sejauh mana Penyelenggara IIV telah menerapkan kerangka kerja pelindungan IIV yang diatur dalam Peraturan BSSN Nomor 8 Tahun 2023. Dalam penerapan kerangka kerja tersebut, Penyelenggara IIV diharapkan dapat mengacu pada berbagai standar keamanan siber yang relevan. Panduan ini juga memberikan contoh pemetaan kontrol-kontrol kerangka kerja pelindungan IIV terhadap beberapa standar umum seperti SNI ISO/IEC 27001:2022, NIST SP 800-53 revisi 5, NIST CSF 1.1, dan NIST CSF 2.0.

B. TUJUAN

Panduan Pemenuhan Kontrol Kematangan Keamanan Siber ini disusun dengan tujuan sebagai berikut:

1) Meningkatkan Pemahaman Stakeholders

Memberikan gambaran yang jelas tentang kondisi penerapan keamanan siber kepada para pemangku kepentingan (*stakeholders*), serta meningkatkan

pemahaman mereka mengenai pentingnya penilaian kematangan dalam pelaksanaan kerangka kerja pelindungan IIV.

2) **Panduan Pengisian IKAS**

Memberikan petunjuk dan panduan yang komprehensif dalam mengisi Instrumen Penilaian Kematangan Keamanan Siber (IKAS) untuk mengukur tingkat kematangan penerapan kerangka kerja pelindungan IIV yang telah dilakukan oleh Penyelenggara IIV.

3) **Menilai Penerapan Kerangka Kerja Pelindungan IIV**

Membantu Penyelenggara IIV dalam menilai sejauh mana penerapan kerangka kerja pelindungan IIV yang diatur dalam Peraturan BSSN Nomor 8 Tahun 2023 telah diterapkan dengan baik dan efektif.

4) **Mengacu pada Standar Keamanan Informasi**

Memastikan bahwa dalam penerapan kerangka kerja pelindungan IIV, Penyelenggara IIV dapat mengacu pada standar keamanan informasi dan standar lainnya yang relevan untuk memperkuat perlindungan terhadap IIV.

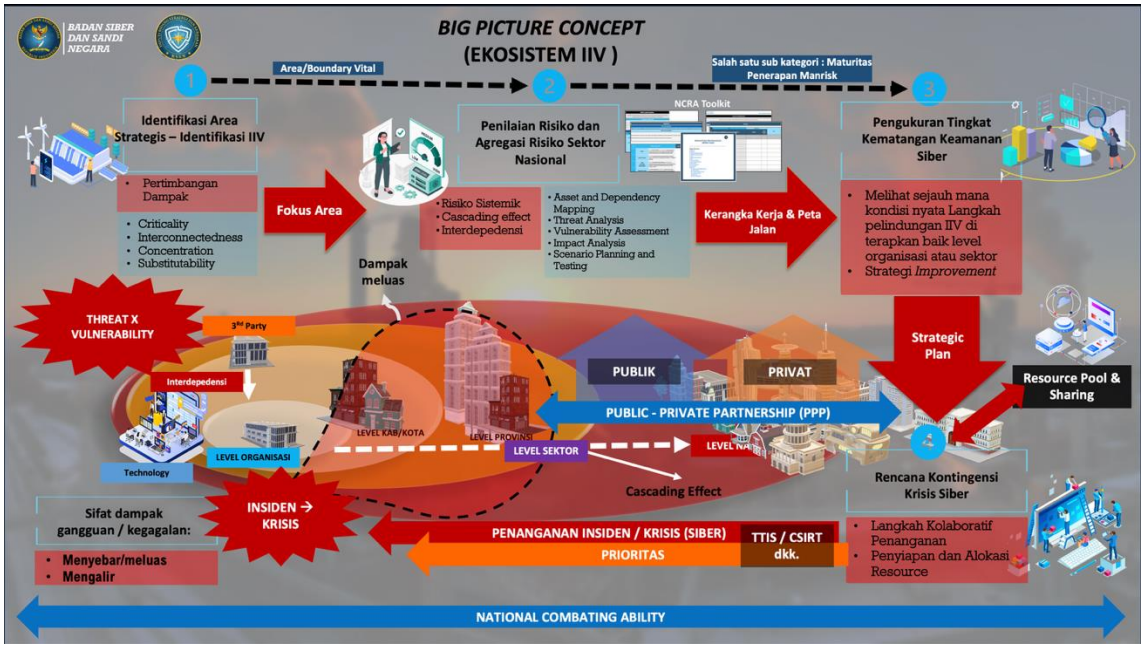
5) **Pemetaan Kontrol terhadap Standar Keamanan Siber**

Menyediakan contoh pemetaan kontrol-kontrol dalam kerangka kerja pelindungan IIV terhadap standar internasional yang umum digunakan, seperti SNI ISO/IEC 27001:2022, NIST SP 800-53 revisi 5, NIST CSF 1.1, dan NIST CSF 2.0, sebagai referensi dalam penerapan kontrol yang efektif dan sesuai.

KEMATANGAN KEAMANAN SIBER

A. KONSEPSI PELINDUNGAN IIV

Peraturan Presiden (Perpres) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) memberikan panduan mengenai apa saja pengamanan yang perlu diterapkan terhadap sistem elektronik yang menyelenggarakan suatu infrastruktur atau layanan yang memiliki potensi dampak serius kepada masyarakat apabila terjadi gangguan terhadapnya. Pada umumnya, sifat dari dampak terhadap layanan strategis itu senantiasa meluas dari level organisasi, sektor, hingga nasional. Sebagai contoh, potensi dampak yang dirasakan ketika terjadi gangguan pada infrastruktur distribusi listrik. Berhentinya layanan distribusi listrik tidak hanya mengakibatkan kerugian pada perusahaan penyedia listrik, namun juga mengakibatkan terganggunya layanan pada sektor lain seperti keuangan, kesehatan, transportasi, hingga administrasi pemerintahan. Bilamana insiden tersebut tidak cepat ditangani, maka berpotensi meluas menjadi sebuah krisis bagi seluruh masyarakat.



Secara umum konsepsi pelindungan terhadap IIV diterapkan dengan mengedepankan aspek manajemen risiko terhadap aset-aset informasi yang bersifat kritikal bagi layanan vital di masyarakat. Pada tahap awal implementasi kebijakan, negara perlu mengidentifikasi infrastruktur informasi mana saja yang memiliki potensi dampak serius bagi masyarakat. Potensi dampak tersebut dapat

dilihat dari seberapa penting sistem tersebut terhadap layanan (vitalitas), seberapa banyak layanan lain yang bergantung terhadap sistem tersebut (interdependensi), adakah sistem lain yang dapat menggantikan ketika terjadi gangguan (substitusi). Oleh karena itu, setiap penyelenggara sistem elektronik yang ada di sektor IIV diminta untuk melakukan identifikasi sistem elektroniknya yang memenuhi kriteria sistem elektronik IIV. Secara keseluruhan proses identifikasi sistem elektronik strategis tersebut telah diatur dalam kebijakan teknis Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital.

Tahap berikutnya adalah penerapan kerangka kerja pelindungan terhadap sistem IIV sesuai dengan hasil manajemen risiko yang ada di masing-masing organisasi penyelenggara IIV. Kerangka kerja yang diterapkan berupa pemenuhan kontrol-kontrol keamanan yang dapat berupa pemenuhan kebijakan keamanan, penerapan teknologi pelindungan, atau peningkatan kapasitas SDM terkait keamanan siber. Dalam rangka memberikan panduan dan target penerapan pelindungan bagi penyelenggara IIV di setiap sektor, maka Kementerian/Lembaga Pembina sektor IIV menyusun Peta Jalan Pelindungan IIV di sektornya yang dapat mengacu kepada Peraturan BSSN Nomor 8 Tahun 2023 tentang pedoman Kerangka Kerja Penerapan Pelindungan IIV, dan Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas SDM Keamanan Siber dan Sandi.

Selanjutnya untuk mengukur pencapaian dan efektivitas dari penerapan kontrol keamanan yang telah dilaksanakan oleh penyelenggara IIV, maka perlu dinilai penerapannya dalam sebuah penilaian tingkat kematangan yang mengacu kepada Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber. Kemudian hasil dari pengukuran tersebut dapat dijadikan sebagai dasar dalam penyusunan rencana strategis oleh penyelenggara IIV untuk menyiapkan dirinya untuk menghadapi setiap ancaman dan insiden siber. Selain itu, dengan hasil tingkat kematangan tersebut, Pemerintah dapat menyusun juga rencana kontingensi nasional untuk menghadapi potensi terjadinya situasi krisis siber yang dapat mengacu kepada Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber.

Untuk mengantisipasi terjadinya krisis siber, maka perlu adanya pihak yang diberikan kewenangan untuk mengelola setiap insiden siber yang terjadi pada

sistem elektronik IIV. Penanganan dan pemulihan insiden siber pada sistem elektronik IIV perlu dilakukan dengan tepat dan cepat. Karena, potensi dampaknya yang dapat meluas dan mengakibatkan terhentinya layanan publik. Oleh karena itu, perlu dibentuk Tim Tanggap Insiden Siber yang bertugas mengelola setiap insiden siber yang terdeteksi pada sektor IIV. Nantinya, eskalasi penanganan dan pemulihan terhadap insiden siber di sektor IIV dapat dilakukan secara bertahap mulai dari Tim Tanggap Insiden Siber Organisasi, Sektoral, hingga Nasional. Secara umum tata kelola pengelolaan insiden siber diatur lebih lanjut dalam Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.

B. INSTRUMEN PENILAIAN KEMATANGAN KEAMANAN SIBER (IKAS)

Penyelenggaraan pelindungan IIV merupakan serangkaian upaya yang dilakukan oleh Penyelenggara IIV untuk mengendalikan keamanan melalui penerapan Kontrol Keamanan pada IIV sesuai dengan Domain pada Kerangka Kerja. Domain pada Kerangka Kerja, meliputi **Identifikasi, Proteksi, Deteksi, dan Penanggulangan dan Pemulihan**.

Target penerapan Kontrol Keamanan merupakan nilai capaian yang bertujuan untuk memberikan gambaran kondisi penerapan keamanan siber pada Penyelenggara IIV terhadap sasaran penyelenggaraan pelindungan IIV dan Domain Kerangka Kerja yang ditentukan berdasarkan hasil pengukuran tingkat kematangan keamanan siber. Pelaksanaan pengukuran Tingkat Kematangan dilakukan dengan menggunakan instrumen pengukuran yaitu IKAS (Instrumen Penilaian Kematangan Keamanan Siber).

Dalam menentukan formulasi Tingkat Kematangan Keamanan Siber, diperlukan pembobotan untuk setiap domain dengan mempertimbangkan berbagai faktor, yaitu ukuran organisasi, kompleksitas infrastruktur, dan profil risiko. Berikut merupakan penjelasan dari pembagian pembobotan yang digunakan di instrumen pengukuran IKAS:



Dasar landasan untuk pembagian pembobotan tersebut dapat disesuaikan dengan mempertimbangkan hal-hal berikut:

- Keseimbangan antara Pencegahan dan Tanggapan: Penting untuk memiliki keseimbangan antara mencegah serangan dan mampu menanggapi ketika serangan terjadi. Proteksi yang kuat mengurangi kemungkinan serangan, sementara deteksi dan respon memastikan bahwa ancaman yang tidak terhindarkan dapat dikelola dengan baik.
- Kebutuhan Organisasi: Organisasi yang berbeda memiliki kebutuhan yang berbeda. Misalnya, organisasi dengan data yang sangat sensitif mungkin memerlukan alokasi yang lebih besar untuk proteksi dan penanggulangan dan pemulihan.
- Regulasi dan Standar Industri: Standar dan regulasi tertentu mungkin mempengaruhi alokasi, seperti yang ditetapkan dalam kerangka kerja seperti NIST *Cybersecurity Framework*, yang menyarankan pendekatan berbasis risiko dan penilaian yang mendalam.

C. TAHAPAN PENGISIAN DAN PELAPORAN IKAS

1. Unduh Form IKAS

   Penyelenggara IIV mengunduh Form IKAS pada laman resmi BSSN: https://www.bssn.go.id/instrumen-penilaian-kematangan-keamanan-siber-ikas/ ;

2. Lengkapi Data Responden

   Penyelenggara IIV mengisi data pada sheet “Responden”. Instrumen ini dianjurkan diisi oleh pejabat yang bertanggung jawab dan berwenang dalam pengelolaan keamanan siber pada seluruh cakupan organisasi.

3. Tentukan Ruang Lingkup dan Target Kematangan

   Penyelenggara IIV menentukan Ruang Lingkup penilaian IKAS untuk menentukan konteks dan Sistem Elektronik yang akan dinilai, serta Target Level Kematangan dan Target Nilai Kematangan yang ingin dicapai organisasi;

4. Isi Indeks Nilai Kematangan

   Penyelenggara IIV mengisi nilai kematangan sesuai kondisi penerapan kontrol di organisasi. Kontrol dinilai dalam rentang indeks 0–5. Pengisian dilakukan per domain, antara lain:

   - Domain Identifikasi (sheet 'I Identifikasi'),
   - Domain Proteksi (sheet 'II Proteksi'),
   - Domain Deteksi (sheet 'III Deteksi'),
   - Domain Penanggulangan dan Pemulihan (sheet 'IV Gulih');

5. Lihat Hasil *Self-Assessment*

   Penyelenggara IIV meninjau hasil pengisian IKAS pada sheet “Kematangan Kamsiber”, yang menampilkan capaian dan gap analisis kematangan;

6. Laporkan Hasil IKAS

   Penyelenggara IIV menyampaikan hasil *self-assessment* kepada Kementerian atau Lembaga Koordinator Sektor untuk dilanjutkan ke tahapan verifikasi IKAS.

TAHAPAN PENGISIAN DAN PELAPORAN INSTRUMEN PENILAIAN KEMATANGAN KEAMANAN SIBER (IKAS)

UNDUH FORM IKAS
01

Form IKAS dapat diunduh pada laman resmi BSSN https://www.bssn.go.id/instrumen-penilaian-kematangan-keamanan-siber-ikas/



LENGKAPI DATA RESPONDEN
02

Penyelenggara IIV mengisi data pada sheet "Responden".



TENTUKAN RUANG LINGKUP DAN TARGET KEMATANGAN
03

Mengisi Ruang Lingkup penilaian IKAS untuk menentukan konteks dan SE yang akan dinilai, serta Target Level kematangan dan Target Nilai Kematangan yang ingin dicapai organisasi.

Nama Sistem Elektronik	:	
Jenis Sistem Elektronik	:	IT
Sektor	:	sektor lain
Alamat	:	
Tahun Pengukuran	:	2025
Target Level Kematangan	:	Level 3
Target Nilai	:	_____ *rentang target nilai/indeks 2,51 – 3,50*
Acuan Manajemen Risiko yang Digunakan	:	
Acuan Keamanan Siber yang Digunakan	:	

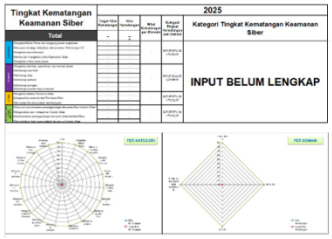
ISI INDEKS NILAI KEMATANGAN
04

Penyelenggara IIV mengisi nilai kematangan sesuai kondisi penerapan kokntrol di organisasi. Kontrol dinilai dalam rentang indeks 0-5. Pengisian dilakukan per domain



LIHAT HASIL SELF ASSESSMENT
05

Penyelenggara IIV meninjau hasil pengisian IKAS pada sheet "Kematangan Kamsiber", yang menampilkan capaian dan gap analisis kematangan.



LAPORKAN HASIL IKAS
06

Penyelenggara IIV menyampaikan hasil self-assessment kepada KL Sektor untuk dilanjutkan ke tahapan verifikasi IKAS.

Pasal 6

(1) Pelaporan hasil pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 2 huruf b disampaikan oleh Penyelengara IIV kepada Kementerian atau Lembaga paling sedikit 1 (satu) kali dalam 1 (satu) tahun sesuai dengan ketentuan yang ditetapkan oleh Kementerian atau Lembaga.

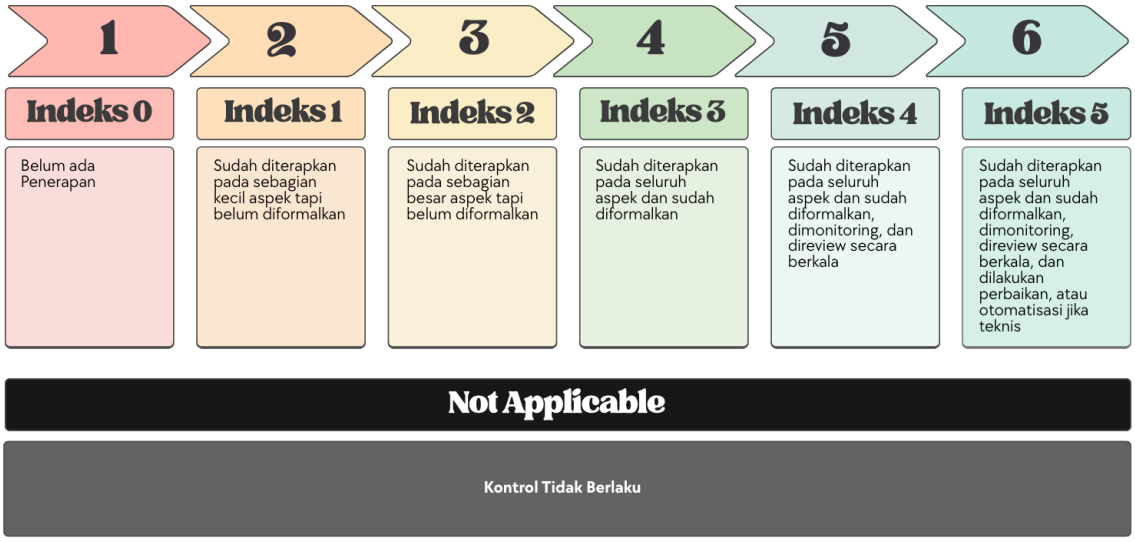
(2) Pelaporan sebagaimana dimaksud pada ayat (1) disampaikan dengan menyertakan:
   a. surat penyampaian hasil pengukuran Tingkat Kematangan;
   b. hasil penilaian mandiri yang telah diotorisasi oleh pejabat yang berwenang mewakili Penyelenggara IIV;
   c. bukti pendukung; dan
   d. informasi narahubung.

(3) Kementerian atau Lembaga wajib menginformasikan pelaporan hasil pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (1) kepada Kepala Badan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(4) Dalam hal Kementerian atau Lembaga sebagai Penyelenggara IIV, pelaporan hasil pengukuran Tingkat Kematangan disampaikan oleh Kementerian atau Lembaga kepada Badan.

D. PENJELASAN INDEKS

Dalam mengisi instrumen pengukuran IKAS, Penyelenggara IIV diminta untuk menentukan tingkat kematangan keamanan siber dengan memilih indeks dari 0 hingga 5 untuk setiap kontrol, sesuai dengan kondisi yang berlaku di organisasi. Untuk mempermudah pemahaman, berikut ini disajikan penjelasan umum mengenai kondisi yang menggambarkan penerapan keamanan siber pada setiap indeks. Penjelasan ini bertujuan agar responden dapat lebih mudah memahami dan menggunakan instrumen pengukuran IKAS secara tepat.



Dalam proses penilaian kematangan menggunakan Instrumen Pengukuran IKAS terdapat Indeks yang disebut ***Not Applicable*** (Tidak Berlaku). Indeks ini digunakan ketika sebuah kontrol kematangan tidak diterapkan dalam konteks tertentu, yang keputusan penerapannya didasarkan pada penilaian risiko yang dilakukan oleh Penyelenggara IIV. Penentuan apakah suatu kontrol termasuk dalam kategori *Not Applicable* atau tidak, sepenuhnya disesuaikan dengan pendekatan pengelolaan risiko masing-masing organisasi atau penyelenggara.

Keputusan untuk mengklasifikasikan suatu kontrol sebagai *Not Applicable* harus berdasarkan hasil identifikasi dan analisis risiko yang jelas dan terdokumentasi, terutama yang berkaitan dengan aset yang dimiliki dan digunakan oleh organisasi. Sebagai contoh, apabila organisasi tidak menggunakan teknologi cloud dan seluruh infrastruktur TI bersifat *on-premise,* maka kontrol-kontrol yang secara khusus ditujukan untuk pengelolaan risiko di lingkungan cloud dapat dikategorikan sebagai *Not Applicable*, karena tidak relevan dengan kondisi operasional organisasi saat ini.

Namun, penting untuk dicatat bahwa tidak semua kontrol dapat dikecualikan hanya karena teknologi tertentu tidak digunakan. Misalnya, meskipun organisasi tidak memanfaatkan layanan *cloud*, tetap terdapat risiko keamanan siber pada infrastruktur *on-premise* yang memerlukan penerapan kontrol seperti firewall, IDS/IPS, dan solusi keamanan lainnya. Dalam hal ini, kontrol terkait tidak bisa dianggap *Not Applicable,* karena tetap relevan terhadap risiko yang dihadapi organisasi.

Dalam penilaian kematangan, kontrol yang dikategorikan sebagai *Not Applicable* tidak dimasukkan ke dalam perhitungan nilai kematangan. Oleh karena itu, klasifikasi ini tidak berdampak negatif terhadap skor penilaian, asalkan dilakukan secara objektif dan berdasarkan justifikasi risiko yang valid.

Asesor atau verifikator memiliki peran penting dalam memastikan bahwa klasifikasi Not Applicable benar-benar didasarkan pada ketidakterkaitan kontrol dengan risiko aktual, bukan sebagai bentuk penghindaran terhadap penerapan kontrol yang semestinya diwajibkan. Asesor atau verifikator harus memastikan bahwa organisasi tidak menggunakan pendekatan risk acceptance sebagai alasan untuk tidak menerapkan kontrol yang relevan, karena pendekatan tersebut tidak dapat digunakan untuk menghindari kewajiban penerapan kontrol yang diperlukan oleh profil risiko organisasi.

Dengan demikian, setiap keputusan untuk menetapkan kontrol sebagai Not Applicable harus disertai dengan justifikasi risiko yang kuat dan terdokumentasi, agar dapat diterima dalam proses asesmen dan tidak menimbulkan bias terhadap hasil penilaian kematangan secara keseluruhan.

E. RUMUS

Rumus yang digunakan pada instrumen pengukuran IKAS, sebagai berikut:

1) Nilai sub-kategori didapatkan dari hasil rata-rata nilai indeks kontrol terkait

$$\overline{k_i} = \frac{\sum_{i=1}^{l} k_i}{l}$$

Keterangan:

$\overline{k_i}$	=Nilai sub-kategori
$\sum_{i=1}^{l} k_i$	=Jumlah seluruh nilai kontrol pada sub-kategori terkait
l	=Jumlah kontrol pada sub-kategori terkait

2) Nilai Kematangan Keamanan Siber per-Kategori didapatkan dari hasil rata-rata nilai sub-kategori pada Kategori terkait

$$\overline{K_i} = \frac{\sum_{i=1}^{m} \overline{k_i}}{m}$$

Keterangan:

$\overline{K_i}$	=Nilai Kematangan Keamanan Siber Kategori
$\sum_{i=1}^{m} \overline{k_i}$	=Jumlah seluruh nilai sub-kategori pada Kategori terkait
m	=Jumlah sub-kategori pada Kategori terkait

3) Nilai Kematangan Keamanan Siber per-Domain didapatkan dari hasil rata-rata nilai Kematangan Keamanan Siber Kategori pada Domain terkait

$$M_I/M_P/M_D/M_R = \frac{\sum_{i=1}^{n} \overline{K_i}}{n}$$

Keterangan:

$M_I/M_P/M_D/M_R$	=Kematangan Keamanan Siber Domain Identifikasi/ Kematangan Keamanan Siber Domain Proteksi/ Kematangan Keamanan Siber Domain Deteksi/ Kematangan Keamanan Siber Domain Penanggulangan dan Pemulihan
$\sum_{i=1}^{n} \overline{K_i}$	=Jumlah Seluruh Nilai Kematangan Keamanan Siber Kategori pada Domain terkait
n	=Jumlah Kategori pada Domain terkait

4) Nilai Kematangan Keamanan Siber Seluruh Domain/Total didapatkan dari penjumlahan Nilai Kematangan Keamanan Siber per-Domain setelah dikalikan dengan bobot per-Domain

$$M_T = (25\% * M_I) + (30\% * M_P) + (25\% * M_D) + (30\% * M_R)$$

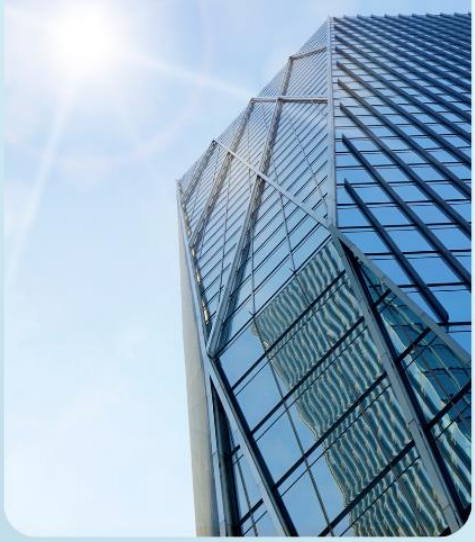
Keterangan:

M_T	=Kematangan Keamanan Siber Seluruh Domain/Total

F. INDIKATOR PADA INSTRUMEN PENGUKURAN IKAS

INDIKATOR EVALUASI PENERAPAN DOMAIN KERANGKA KERJA DAN KATEGORI KEGIATAN							
Kategori Tingkat Kematangan			**Kriteria**				
Level 1 (satu)	Level Awal	Dengan nilai kematangan pada rentang indeks 0 (nol) - 1,50 (satu koma lima nol)	Menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi awal	Penerapan Keamanan Siber belum memiliki prosedur yang terorganisir	Penerapan Keamanan Siber bersifat informal	Keamanan Siber tidak dilakukan secara konsisten dan berkelanjutan	Dokumen manajemen risiko dan dokumen kontrol belum disusun
Level 2 (dua)	Level Berulang	Dengan dengan nilai kematangan pada rentang indeks 1,51 (satu koma lima satu) - 2,50 (dua koma lima nol)	Menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang berulang	Penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir	Penerapan Keamanan Siber bersifat informal	Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan	Dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan
Level 3 (tiga)	Level Terdefinisi	Dengan nilai kematangan pada rentang indeks 2,51 (dua koma lima satu) - 3,50 (tiga koma lima nol)	Menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terdefinisi dengan baik	Penerapan Keamanan Siber telah terorganisir dengan jelas	Penerapan Keamanan Siber bersifat formal	Keamanan Siber dilakukan secara berulang dan konsisten serta direviu secara berkala	Dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan
Level 4 (empat)	Level Terkelola	Dengan nilai kematangan pada rentang indeks 3,51 (tiga koma lima satu) - 4,50 (empat koma lima nol)	Menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terkelola dengan baik	Penerapan Keamanan Siber telah terorganisir dengan baik namun belum dilakukan proses otomatisasi	Penerapan Keamanan Siber bersifat formal	Keamanan Siber dilakukan secara berulang dan implementasi perbaikan dilakukan berkelanjutan	Dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan
Level 5 (lima)	Level Inovatif	Dengan nilai kematangan pada rentang indeks 4,51 (empat koma lima satu) - 5,0 (lima koma nol)	Menggambarkan kondisi penerapan Keamanan Siber telah diimplementasikan secara optimal	Penerapan Keamanan Siber telah terorganisir dengan baik dan telah dilakukan proses otomatisasi	Penerapan Keamanan Siber bersifat formal	- Keamanan siber dilakukan secara berulang dan konsisten serta telah terintegrasi - keamanan siber menjadi bagian budaya organisasi secara menyeluruh	Dokumen manajemen risiko dan dokumen kontrol sudah ditetapkan





I DOMAIN IDENTIFIKASI

"Domain Identifikasi merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam memahami konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV"

1.1. Mengidentifikasi peran dan tanggung jawab organisasi

Penyelenggara IIV mampu mengidentifikasi dan memahami tujuan pelindungan IIV, peran organisasinya dalam pelindungan IIV, dan sekaligus mampu menginformasikan pemangku kepentingan terkait (meliputi unit kerja lain di organisasinya, instansi/perusahaan grupnya, mitra bisnis dari rantai pasokannya, dan perusahaan outsourcing kontrol sistem TI) mengenai peran, tanggung jawab, dan kebijakan keamanan siber yang berlaku di organisasinya.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi;
b) mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya; dan
c) mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor IIV.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Mengidentifikasi peran dan tanggung jawab organisasi” secara efektif antara lain:

NIST CSF 2.0	**:**	**GV.OC-01, GV.OC-04, GV.OC-05**
NIST CSF 1.1	**:**	**ID.BE-1, ID.BE-2, ID.BE-3, ID.BE-4**
NIST SP 800-53r5	**:**	**CP-2, CP-8, PE-9, PE-11, PM-8, PM-11, RA-9, SA-20, SR-1, SR-2, SR-3**
SNI ISO/IEC 27001:2022	**:**	**5.21, 5.22, 7.4, 7.11, 7.12, 8.6**

1.1.1. Menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV menetapkan pelindungan terhadap IIV sebagai sebuah prioritas bisnis/layanan organisasinya dalam bentuk kebijakan atau komitmen pimpinan, dan mengomunikasikannya dengan pihak-pihak terkait baik internal maupun eksternal organisasi
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya dan kemungkinan penggunaan teknologi tambahan dalam menyusun serta mengomunikasikan prioritas kegiatan pelindungan IIV.
Dampak	**Tinggi ke Sangat Tinggi** – Dengan tidak menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi maka organisasi tidak dapat mencapai tujuan yang telah ditargetkan.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen/divisi untuk memastikan bahwa prioritas yang ditetapkan dipahami dan diimplementasikan secara konsisten di seluruh organisasi.
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01** **NIST CSF 1.1: ID.BE-3** **NIST SP 800-53r5: PM-11** **SNI ISO/IEC 27001:2022: -**

1 Kontrol 1.1.1.a:

Kontrol	Pimpinan organisasi menetapkan keamanan siber sebagai prioritas di organisasi dalam bentuk kebijakan atau komitmen pimpinan yang sesuai dengan kondisi bisnis/layanan dan operasional organisasi.
Deskripsi Kontrol	Keamanan siber yang ditetapkan sebagai prioritas oleh pimpinan organisasi merupakan langkah awal dalam menciptakan budaya keamanan yang kokoh dalam organisasi. Kebijakan atau komitmen pimpinan yang jelas, yang sesuai dengan kebutuhan bisnis, layanan, dan operasional organisasi, memastikan bahwa keamanan siber mendapatkan perhatian yang tepat dalam setiap aspek operasional. Tujuan dari kontrol ini adalah untuk menilai apakah pimpinan organisasi telah mengakui pentingnya keamanan siber dan telah menetapkan kebijakan atau komitmen sebagai prioritas utama untuk mendukung keamanan dalam organisasi secara keseluruhan.
Deskripsi Bukti Dukung	Data dukung yang menunjukkan komitmen pimpinan untuk menetapkan keamanan siber sebagai kegiatan prioritas di organisasinya yang tertuang dalam lingkup dokumen, contohnya: - Dokumen kebijakan keamanan siber organisasi. - Surat keputusan atau pernyataan komitmen pimpinan mengenai keamanan siber. - Rencana strategis yang mencakup prioritas keamanan siber - Notulen rapat pimpinan yang membahas keamanan siber.
Ancaman/Risiko yang dimitigasi	TH056 TH059 TH066 TH057 TH060
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01** **NIST CSF 1.1: ID.BE-3** **NIST SP 800-53r5: PM-11** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.1.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum ada penerapan kebijakan atau komitmen pimpinan terkait keamanan siber	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Kebijakan Keamanan Siber diterapkan pada sebagian kecil aspek, namun belum ditetapkan secara formal	Organisasi sudah menerapkan sebagian kecil aspek keamanan siber, contohnya penggunaan kriptografi atau penggunaan antivirus, dan sebagainya	Draft Kebijakan Keamanan Siber yang telah menggambarkan sebagian kecil aspek keamanan siber yang diterapkan di organisasi tersebut. Kriteria sebagian kecil aspek disesuaikan dengan kebijakan masing-masing organisasi dan/atau Kementerian/Lembaga Sektor.
2	Kebijakan Keamanan Siber diterapkan pada sebagian besar aspek, namun belum ditetapkan secara formal	Organisasi sudah menerapkan sebagian besar aspek keamanan siber, contohnya penggunaan kriptografi, penggunaan antivirus, dan sebagainya	Draft Kebijakan Keamanan Siber yang telah menggambarkan sebagian besar aspek keamanan siber yang diterapkan di organisasi tersebut. Kriteria sebagian besar aspek disesuaikan dengan kebijakan masing-masing organisasi dan/atau Kementerian/Lembaga Sektor.
3	- Kebijakan terkait keamanan siber telah disusun dan ditetapkan - Pimpinan berkomitmen untuk memasukkan keamanan siber sebagai prioritas organisasi.	- Organisasi sudah menerapkan seluruh aspek keamanan siber yang ada di dalam kebijakan keamanan siber yang telah ditetapkan, contohnya penggunaan kriptografi, penggunaan antivirus, dan sebagainya. - Keamanan siber masuk ke dalam program kerja tahunan organisasi, contohnya peningkatan kapasitas SDM kamsiber melalui pelatihan, investasi teknologi keamanan siber **yang memiliki sertifikat keamanan**, dan sebagainya.	- Kebijakan Keamanan Siber yang telah menggambarkan seluruh aspek keamanan siber yang diterapkan di organisasi tersebut. Kriteria aspek disesuaikan dengan kebijakan masing-masing organisasi dan/atau Kementerian/Lembaga Sektor. - Program Kerja yang menggambarkan investasi keamanan siber di organisasinya
4	- Kebijakan terkait keamanan siber telah disusun, ditetapkan, dimonitor, dan dilakukan reviu secara berkala - Pimpinan telah memasukkan keamanan siber sebagai prioritas organisasi.	- Organisasi sudah menerapkan seluruh aspek keamanan siber yang ada di dalam kebijakan keamanan siber yang telah ditetapkan, contohnya penggunaan kriptografi, penggunaan antivirus, dan sebagainya. - Keamanan siber masuk ke dalam program kerja tahunan organisasi, contohnya peningkatan kapasitas SDM keamanan siber melalui pelatihan,	- Kebijakan Keamanan Siber yang telah menggambarkan seluruh aspek keamanan siber yang diterapkan di organisasi tersebut. Kriteria aspek disesuaikan dengan kebijakan masing-masing organisasi dan/atau Kementerian/Lembaga Sektor. - Dokumentasi monitoring dan reviu penerapan kebijakan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		- investasi teknologi keamanan siber **yang memiliki sertifikat keamanan**, dan sebagainya. - Penerapan kebijakan keamanan siber telah dimonitor, dan dilakukan reviu secara berkala.	- Program Kerja yang menggambarkan investasi keamanan siber di organisasinya
5	- Kebijakan terkait keamanan siber telah disusun, ditetapkan, dimonitor, dan dilakukan reviu serta pembaruan secara berkala - Pimpinan memberikan arahan, dukungan pelaksanaan keamanan siber sebagai prioritas organisasi.	- Organisasi sudah menerapkan seluruh aspek keamanan siber yang ada di dalam kebijakan keamanan siber yang telah ditetapkan, contohnya penggunaan kriptografi, penggunaan antivirus, dan sebagainya. - Keamanan siber masuk ke dalam program kerja tahunan organisasi, contohnya peningkatan kapasitas SDM kamsiber melalui pelatihan, investasi teknologi keamanan siber **yang memiliki sertifikat keamanan**, dan sebagainya. - Penerapan kebijakan keamanan siber telah dimonitor, dan dilakukan reviu secara berkala. - Kebijakan Keamanan Siber diperbarui secara berkala dengan memperhatikan manajemen risiko.	- Kebijakan Keamanan Siber yang telah menggambarkan seluruh aspek keamanan siber yang diterapkan di organisasi tersebut. Kriteria aspek disesuaikan dengan kebijakan masing-masing organisasi dan/atau Kementerian/Lembaga Sektor. - Dokumentasi monitoring dan reviu penerapan kebijakan. - Dokumen Kebijakan Keamanan Siber yang telah direvisi. - Program Kerja yang menggambarkan investasi keamanan siber di organisasinya

2 Kontrol 1.1.1.b:

Kontrol	Penyelenggara IIV mengomunikasikan perihal komitmen keamanan siber di organisasinya dengan pihak-pihak yang terkait dengan bisnis/layanan organisasi (termasuk kepada penyedia pihak ketiga).
Deskripsi Kontrol	Komunikasi komitmen keamanan siber yang efektif dengan pihak-pihak terkait, termasuk penyedia pihak ketiga, penting untuk memastikan bahwa seluruh elemen dalam rantai bisnis organisasi memahami dan mendukung kebijakan dan standar keamanan yang telah ditetapkan. Tujuan dari kontrol ini adalah untuk menilai sejauh mana organisasi mengomunikasikan komitmen keamanan siber kepada pihak internal dan eksternal yang berhubungan langsung dengan operasi dan layanan organisasi, guna memastikan adanya kesepahaman dalam penerapan standar dan kebijakan keamanan siber.
Deskripsi Bukti Dukung	Data dukung berupa dokumentasi komunikasi komitmen keamanan siber yang efektif dengan pihak-pihak terkait, termasuk penyedia pihak ketiga, contohnya: - Surat edaran atau pengumuman komitmen keamanan siber kepada pihak terkait. - Kontrak atau perjanjian kerjasama dengan penyedia pihak ketiga yang mencantumkan klausul keamanan siber. - Dokumen pelatihan atau sosialisasi kebijakan keamanan siber untuk pihak terkait. - Notulen atau laporan rapat yang membahas komunikasi tentang komitmen keamanan siber.
Ancaman/Risiko yang dimitigasi	TH013 TH059 TH061 TH067 TH069 TH058 TH060 TH066 TH068
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01** **NIST CSF 1.1: ID.BE-3** **NIST SP 800-53r5: PM-11** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.1.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Komitmen dan kebijakan keamanan siber yang harus dipatuhi pihak terkait belum dikomunikasikan	Belum ada komunikasi terkait Komitmen dan kebijakan keamanan siber yang harus dipatuhi pihak terkait	Tidak ada bukti pendukung
1	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada sebagian kecil aspek, namun belum ditetapkan secara formal	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada sebagian kecil aspek (misal: kebijakan password), namun belum ditetapkan secara formal	Bukti komunikasi informal (email, chat, notulen rapat) yang menunjukkan sebagian kecil aspek kebijakan keamanan siber telah dikomunikasikan
2	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada sebagian besar aspek, namun belum ditetapkan secara formal	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada sebagian besar aspek (misal: kebijakan password, kebijakan akses, kebijakan penggunaan internet), namun belum ditetapkan secara formal	Bukti komunikasi informal (email, chat, notulen rapat) yang menunjukkan sebagian besar aspek kebijakan keamanan siber telah dikomunikasikan
3	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek dan sudah ditetapkan secara formal	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek (misal: kebijakan password, kebijakan akses, kebijakan penggunaan internet, kebijakan penanganan insiden) dan sudah ditetapkan secara formal dalam dokumen tertulis	Dokumen formal kebijakan keamanan siber yang telah dikomunikasikan kepada pihak terkait (surat edaran, pedoman, perjanjian kerjasama)
4	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek dan sudah ditetapkan secara formal, dimonitor, dan dilakukan reviu secara berkala	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek dan sudah ditetapkan secara formal, dimonitor, dan dilakukan reviu secara berkala melalui rapat tinjauan manajemen	Dokumen formal kebijakan keamanan siber, bukti monitoring (log, laporan), bukti reviu (notulen rapat, laporan)
5	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek dan sudah ditetapkan secara formal, dimonitor, dan dilakukan reviu secara berkala, dan dilakukan perbaikan.	Kebijakan keamanan siber yang harus dipatuhi pihak terkait sudah dikomunikasikan pada seluruh aspek dan sudah ditetapkan secara formal, dimonitor, dan dilakukan reviu secara berkala, dan dilakukan perbaikan berdasarkan hasil monitoring dan reviu	Dokumen formal kebijakan keamanan siber, bukti monitoring (log, laporan), bukti reviu (notulen rapat, laporan), bukti perbaikan (laporan perbaikan, bukti implementasi perbaikan)

1.1.2. Mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengidentifikasi ketergantungan antara organisasinya dan pihak terkait lainnya, serta pentingnya fungsi masing-masing pihak dalam menjalankan operasional layanan IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan evaluasi ketergantungan, serta komunikasi dengan pihak terkait, tetapi tidak memerlukan teknologi tambahan yang mahal.
Dampak	**Tinggi** – Memahami ketergantungan dengan pihak terkait membantu organisasi mengidentifikasi risiko dan mengelola hubungan dengan lebih efektif, sehingga meningkatkan keamanan IIV.
Kompleksitas	**Sedang** – Memerlukan analisis mendalam dan komunikasi yang efektif dengan pihak terkait untuk mengidentifikasi dan mengelola ketergantungan tersebut.
Referensi Kontrol	**NIST CSF 2.0: GV.OC-04, GV.OC-05** **NIST CSF 1.1: ID.BE-4** **NIST SP 800-53r5: CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2** **SNI ISO/IEC 27001:2022: 7.4, 7.11, 7.12, 8.6**

3 Kontrol 1.1.2.a:

Kontrol	Penyelenggara IIV mengidentifikasi unit kerja di internal organisasinya, maupun pihak lain di luar organisasinya yang memiliki ketergantungan, baik secara langsung maupun tidak langsung terhadap operasional layanan IIV di organisasinya.
Deskripsi Kontrol	Identifikasi unit kerja internal dan pihak eksternal yang memiliki ketergantungan terhadap operasional layanan IIV merupakan langkah penting dalam manajemen risiko dan keberlanjutan operasional organisasi. Dengan mengetahui pihak-pihak yang bergantung pada layanan IIV, organisasi dapat lebih mudah mengelola ketergantungan ini dan mengantisipasi potensi dampak dari gangguan operasional. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah melakukan identifikasi yang komprehensif mengenai unit kerja dan pihak ketiga yang bergantung pada operasional Layanan IIV, baik secara langsung maupun tidak langsung.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini mencakup dokumentasi yang menunjukkan bahwa penyelenggara IIV telah mengidentifikasi unit kerja internal dan pihak eksternal yang bergantung pada operasional layanan IIV, baik secara langsung maupun tidak langsung. Bukti tersebut dapat berupa daftar lengkap unit kerja dan pihak eksternal yang bergantung, prosedur formal untuk identifikasi ketergantungan, serta laporan evaluasi dan pembaruan berkala atas daftar tersebut. Selain itu, adanya mekanisme pembaruan daftar yang terjadwal dan tindak lanjut manajerial berdasarkan hasil identifikasi juga menjadi bukti bahwa kontrol ini diterapkan secara efektif.
Ancaman/Risiko yang dimitigasi	TH013 TH057 TH059 TH061 TH067 TH069 TH056 TH058 TH060 TH066 TH068 TH070
Referensi Kontrol	**NIST CSF 2.0: GV.OC-04, GV.OC-05** **NIST CSF 1.1: ID.BE-4** **NIST SP 800-53r5: CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2** **SNI ISO/IEC 27001:2022: 7.4, 7.11, 7.12, 8.6**

Kriteria Pemenuhan Kontrol 1.1.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum dilakukan identifikasi unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya - Belum ada prosedur identifikasi ketergantungan	Organisasi belum melakukan upaya apapun untuk mengidentifikasi unit kerja atau pihak yang bergantung pada layanan IIV. Tidak ada prosedur yang ditetapkan untuk mengidentifikasi ketergantungan, sehingga proses identifikasi ini belum pernah dilakukan.	- Tidak ada dokumentasi atau daftar yang menunjukkan identifikasi unit kerja atau pihak lain yang bergantung pada layanan IIV. - Tidak ada prosedur tertulis atau kebijakan yang mengatur mengenai identifikasi ketergantungan terhadap layanan IIV. - Tidak ada laporan atau rekaman aktivitas yang menunjukkan identifikasi ketergantungan pada layanan IIV.
1	Organisasi mengetahui sebagian kecil unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya, namun prosedur identifikasi ketergantungan belum ditetapkan secara formal	Organisasi mulai mengenali beberapa unit kerja atau pihak luar yang bergantung pada layanan IIV. Namun, informasi yang diketahui masih terbatas dan belum ada prosedur yang terdokumentasi secara formal untuk mengidentifikasi ketergantungan tersebut. Proses ini bersifat ad hoc dan belum sistematis.	- Daftar sementara atau tidak lengkap mengenai unit kerja atau pihak yang diketahui bergantung pada layanan IIV (misalnya, dokumen yang hanya mencakup sebagian kecil unit kerja). - Prosedur informal yang mungkin ada (misalnya, catatan rapat atau komunikasi internal) namun belum diterapkan secara formal atau terdokumentasi. - Beberapa laporan atau rekaman yang menunjukkan identifikasi ketergantungan namun tidak terstruktur atau belum ada standar yang jelas.
2	Organisasi mengetahui sebagian besar unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya, namun prosedur identifikasi ketergantungan belum ditetapkan secara formal	Sebagian besar unit kerja dan pihak eksternal yang bergantung pada layanan IIV sudah teridentifikasi, namun belum seluruhnya. Meskipun pemahaman tentang ketergantungan sudah cukup, prosedur formal untuk melaksanakan identifikasi ketergantungan tersebut belum ada atau belum terdokumentasi dengan baik.	- Daftar sebagian besar unit kerja atau pihak yang bergantung pada layanan IIV (hampir lengkap tetapi belum menyeluruh). - Prosedur yang ada untuk identifikasi ketergantungan sudah diketahui namun belum diterapkan secara konsisten dan belum terdokumentasi dengan formal (misalnya, prosedur yang hanya dikenal oleh sebagian pihak saja). - Beberapa bukti yang menunjukkan upaya pengidentifikasian ketergantungan pada layanan IIV, namun belum diatur dalam kebijakan atau prosedur formal yang terstruktur
3	- Identifikasi unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya telah dilakukan secara menyeluruh. - Prosedur identifikasi ketergantungan sudah ditetapkan.	Organisasi telah melakukan identifikasi secara menyeluruh terhadap unit kerja dan pihak yang bergantung pada layanan IIV, baik internal maupun eksternal. Prosedur untuk melakukan identifikasi ketergantungan juga sudah ada, terdokumentasi dengan jelas, dan diterapkan dengan konsisten	- Daftar lengkap unit kerja internal dan pihak eksternal yang bergantung pada layanan IIV di organisasi. - Prosedur identifikasi ketergantungan yang sudah formal dan terdokumentasi (misalnya, dalam SOP atau dokumen kebijakan). - Bukti pelaksanaan identifikasi ketergantungan yang menyeluruh, yang melibatkan semua unit kerja dan pihak eksternal terkait
4	- Identifikasi unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya telah dilakukan	Organisasi telah berhasil melakukan identifikasi dan pemantauan ketergantungan unit kerja serta pihak eksternal secara berkala. Prosedur	- Daftar unit kerja dan pihak eksternal yang bergantung pada layanan IIV yang dimonitor dan dievaluasi secara berkala

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Prosedur identifikasi ketergantungan sudah ditetapkan dan dievaluasi secara berkala - Daftar unit kerja atau pihak lain yang bergantung pada layanan IIV di organisasinya dimonitor dan dievaluasi secara berkala - Belum ada mekanisme/siklus pembaruan daftar unit kerja atau pihak lain yang bergantung pada layanan IIV di organisasinya	identifikasi ketergantungan sudah diterapkan dan dievaluasi secara rutin. Namun, mekanisme untuk memperbarui daftar pihak yang bergantung pada layanan IIV belum ada atau belum terstruktur dengan baik.	(misalnya, laporan evaluasi ketergantungan yang dilakukan dalam jangka waktu tertentu). - Prosedur identifikasi ketergantungan yang sudah ditetapkan dan dievaluasi secara berkala (misalnya, pembaruan SOP yang menunjukkan evaluasi dan perbaikan berkelanjutan). - Bukti adanya pemantauan dan evaluasi daftar ketergantungan secara berkala (misalnya, rapat pemantauan, catatan evaluasi, atau dokumen perbaikan). - Belum ada dokumentasi atau bukti mekanisme pembaruan daftar ketergantungan secara terstruktur
5	- Identifikasi unit kerja maupun pihak lain yang bergantung pada layanan IIV di organisasinya telah dilakukan - Prosedur identifikasi ketergantungan sudah ditetapkan dan dievaluasi serta diperbarui secara berkala - Sudah ada mekanisme/siklus pembaruan daftar unit kerja atau pihak lain yang bergantung pada layanan IIV di organisasinya - Daftar unit kerja atau pihak lain yang bergantung pada layanan IIV di organisasinya dimonitor, dievaluasi, dan diperbarui secara berkala	Organisasi telah melaksanakan identifikasi ketergantungan dengan sangat baik. Semua unit kerja internal dan pihak eksternal yang bergantung pada layanan IIV telah diidentifikasi, dan prosedur yang digunakan untuk identifikasi tersebut diperbarui secara berkala. Ada mekanisme yang jelas dan terjadwal untuk memperbarui daftar ketergantungan secara rutin, serta ada pemantauan dan evaluasi yang dilakukan untuk memastikan daftar tetap relevan.	- Daftar unit kerja dan pihak eksternal yang bergantung pada layanan IIV yang dimonitor, dievaluasi, dan diperbarui secara berkala dengan siklus yang terjadwal (misalnya, pembaruan tahunan atau triwulanan). - Prosedur identifikasi ketergantungan yang diperbarui dan dievaluasi secara berkala, dengan dokumentasi yang jelas mengenai pembaruan dan siklus pembaruan prosedur (misalnya, revisi SOP). - Bukti mekanisme/siklus pembaruan daftar ketergantungan yang terstruktur dan terjadwal, serta bukti monitoring dan evaluasi yang konsisten (misalnya, log pembaruan daftar ketergantungan, notulen rapat evaluasi, atau rekaman pembaruan dalam sistem manajemen).

1.1.3. Mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengidentifikasi perannya dalam mendukung layanan Infrastruktur Vital, serta mengomunikasikan dengan pemangku kepentingan baik internal maupun eksternal.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya untuk analisis peran organisasi dan komunikasi dengan pihak terkait, tetapi tidak selalu memerlukan teknologi tambahan.
Dampak	**Tinggi –** Dengan peran yang jelas, organisasi dapat memastikan bahwa semua pihak terkait memahami kontribusi dan tanggung jawab organisasi dalam melindungi IIV, sehingga meningkatkan kolaborasi dan keamanan.
Kompleksitas	**Sedang –** Memerlukan analisis mendalam dan komunikasi yang efektif untuk mengidentifikasi dan mengomunikasikan peran organisasi dengan jelas.
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01, GV.OC-05** **NIST CSF 1.1: ID.BE-1, ID.BE-2** **NIST SP 800-53r5: SR-1, SR-3, PM-8** **SNI ISO/IEC 27001:2022: 5.21, 5.22**

4 Kontrol 1.1.3.a:

Kontrol	Penyelenggara IIV mengidentifikasi dan menetapkan unit kerja atau fungsi yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan IIV di organisasinya.
Deskripsi Kontrol	Identifikasi dan penetapan unit kerja atau fungsi yang bertanggung jawab dalam menerapkan pelindungan Layanan IIV adalah langkah penting dalam memastikan keamanan layanan IIV. Unit kerja atau fungsi ini harus memiliki pemahaman dan kewenangan untuk melaksanakan kebijakan keamanan, mengidentifikasi potensi ancaman, serta merespons insiden yang mungkin terjadi. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah secara jelas mengidentifikasi dan menetapkan unit kerja atau fungsi yang memiliki tanggung jawab khusus dalam penerapan pelindungan IIV, guna menjamin bahwa keamanan sistem dan data yang terlibat dalam layanan IIV dikelola dengan baik.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa dokumentasi yang menunjukkan identifikasi dan penetapan unit kerja atau fungsi yang bertanggung jawab atas penerapan pelindungan IIV di organisasi. Ini bisa mencakup kebijakan internal, struktur organisasi, atau daftar fungsi yang mengatur dan menangani pelindungan IIV. Selain itu, bukti juga bisa berupa prosedur atau panduan tertulis yang menjelaskan tugas dan tanggung jawab masing-masing unit kerja dalam melaksanakan pelindungan IIV, serta bukti rapat atau keputusan manajemen yang mengonfirmasi pembagian tanggung jawab tersebut.
Ancaman/Risiko yang dimitigasi	TH052 TH054 TH057 TH060 TH053 TH056 TH059
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01, GV.OC-05** **NIST CSF 1.1: ID.BE-1, ID.BE-2** **NIST SP 800-53r5: SR-1, SR-3, PM-8** **SNI ISO/IEC 27001:2022: 5.21, 5.22**

Kriteria Pemenuhan Kontrol 1.1.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum adanya rencana terkait identifikasi unit kerja atau fungsi yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan IIV di organisasinya.	Organisasi belum memulai proses identifikasi unit kerja atau fungsi yang bertanggung jawab terhadap pelindungan IIV. Tidak ada rencana atau kebijakan yang mendukung hal ini.	- Tidak ada dokumentasi atau rencana yang menunjukkan identifikasi unit kerja atau fungsi yang bertanggung jawab dalam penerapan pelindungan IIV. - Tidak ada kebijakan atau pedoman yang mengatur pembagian tugas dan tanggung jawab untuk pelindungan IIV.
1	Sudah terdapat unit kerja yang menerapkan sebagian kecil fungsi pelindungan IIV di organisasinya, namun belum ditetapkan tugas dan tanggung jawab secara formal	Beberapa unit kerja terlibat dalam pelindungan IIV, tetapi hanya sebagian kecil dari fungsi yang tercakup. Tugas dan tanggung jawab tersebut masih tidak terformalisasi.	- Terdapat unit kerja yang diketahui bertanggung jawab atas sebagian kecil fungsi pelindungan IIV (misalnya, beberapa fungsi saja yang terlibat). - Beberapa catatan atau dokumen yang menunjukkan penerapan tugas pelindungan IIV, namun tugas dan tanggung jawab tersebut belum tertulis secara formal (misalnya, ada tugas informal yang diketahui oleh beberapa pihak).
2	Sudah terdapat unit kerja yang menerapkan sebagian besar fungsi pelindungan IIV di organisasinya, namun belum ditetapkan tugas dan tanggung jawab secara formal	Sebagian besar fungsi pelindungan IIV telah diterapkan oleh unit kerja yang teridentifikasi, namun belum ada dokumentasi atau kebijakan resmi yang menetapkan tugas dan tanggung jawab secara formal.	- Terdapat unit kerja yang bertanggung jawab atas sebagian besar fungsi pelindungan IIV (hampir seluruh fungsi terkait pelindungan IIV diidentifikasi). - Beberapa dokumentasi yang menunjukkan unit kerja dan tanggung jawab mereka dalam pelindungan IIV, namun belum ada pengaturan formal yang mengikat terkait tugas dan tanggung jawab ini. - Catatan atau laporan informal mengenai pelaksanaan pelindungan IIV yang dilakukan oleh unit kerja yang sudah diidentifikasi.
3	Seluruh fungsi dalam menerapkan pelindungan IIV telah diidentifikasi dan unit kerja yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan IIV di organisasinya telah ditetapkan.	Semua fungsi terkait pelindungan IIV telah diidentifikasi, dan unit kerja yang bertanggung jawab telah ditetapkan dengan jelas dalam dokumen resmi (misalnya, struktur organisasi atau SOP).	- Daftar lengkap unit kerja yang memiliki tugas dan tanggung jawab dalam penerapan pelindungan IIV diorganisasi (misalnya, dalam struktur organisasi atau dokumen pembagian fungsi). - Prosedur tertulis atau dokumen formal yang mengatur tugas dan tanggung jawab unit kerja terkait pelindungan IIV (misalnya, SOP atau kebijakan internal yang menjelaskan secara rinci fungsi dan peran setiap unit kerja). - Bukti pengidentifikasian dan penetapan unit kerja serta tanggung jawabnya dalam pelindungan IIV dalam bentuk dokumen kebijakan atau struktur organisasi yang jelas.
4	- Seluruh fungsi dalam menerapkan pelindungan IIV telah diidentifikasi dan unit kerja yang memiliki tugas dan	Seluruh fungsi pelindungan IIV telah diidentifikasi dan unit kerja yang terlibat sudah ditetapkan. Evaluasi	- Daftar unit kerja dan fungsi pelindungan IIV yang diidentifikasi dan ditetapkan secara formal (misalnya, laporan evaluasi yang menunjukkan evaluasi terhadap fungsi dan tanggung jawab unit kerja).

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	tanggung jawab dalam menerapkan pelindungan IIV di organisasinya telah ditetapkan. - Dilakukan evaluasi berkala terhadap fungsi, tugas, dan tanggung jawab unit kerja tersebut dalam menerapkan pelindungan IIV agar tetap inline dengan tujuan organisasi	berkala dilakukan untuk memastikan bahwa fungsi dan tugas unit kerja sesuai dengan tujuan organisasi.	- Prosedur atau kebijakan yang menjelaskan tentang evaluasi berkala terhadap tugas dan tanggung jawab unit kerja, dan pemantauan apakah pelindungan IIV berjalan sesuai dengan tujuan organisasi. - Bukti adanya evaluasi berkala terhadap fungsi, tugas, dan tanggung jawab unit kerja dalam pelindungan IIV (misalnya, laporan evaluasi tahunan atau rapat internal).
5	- Seluruh fungsi dalam menerapkan pelindungan IIV telah diidentifikasi dan unit kerja yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan IIV di organisasinya telah ditetapkan. - Dilakukan evaluasi berkala terhadap fungsi, tugas, dan tanggung jawab unit kerja tersebut dalam menerapkan pelindungan IIV agar tetap inline dengan tujuan organisasi. - Dilakukan perbaikan berkelanjutan untuk memastikan proses binis yang dijalankan oleh unit kerja tersebut tetap efektif dan sesuai dengan kebutuhan dan kondisi terkini	Selain evaluasi berkala, organisasi juga melakukan perbaikan berkelanjutan pada proses pelindungan IIV. Perbaikan ini bertujuan untuk memastikan bahwa unit kerja tetap efektif dan relevan dengan kebutuhan serta kondisi terkini.	- Daftar lengkap unit kerja dan fungsi pelindungan IIV yang telah diidentifikasi dengan sistem evaluasi berkala yang jelas (misalnya, laporan pembaruan tugas dan tanggung jawab berdasarkan hasil evaluasi). - Prosedur atau kebijakan yang memperlihatkan adanya perbaikan berkelanjutan dalam fungsi dan tugas unit kerja untuk memastikan efektivitas pelindungan IIV (misalnya, pembaruan SOP yang menunjukkan hasil evaluasi dan perbaikan). - Bukti dokumentasi perbaikan berkelanjutan yang dilakukan untuk memastikan fungsi pelindungan IIV tetap efektif dan sesuai dengan kebutuhan organisasi (misalnya, laporan audit atau dokumentasi tindakan perbaikan yang dilaksanakan setelah evaluasi).

5 Kontrol 1.1.3.b:

Kontrol	Penyelenggara IIV mengidentifikasi peran, aktivitas, proses, dan narahubung dari pemangku kepentingan yang mendukung ekosistem bisnis atau layanan IIV, baik di dalam atau di luar organisasi
Deskripsi Kontrol	Identifikasi peran, aktivitas, proses, dan narahubung dari pemangku kepentingan yang mendukung ekosistem bisnis atau layanan IIV penting untuk memastikan bahwa organisasi dapat berkoordinasi dengan pihak-pihak terkait dengan efektif. Pemangku kepentingan ini, baik di dalam maupun di luar organisasi, memiliki kontribusi terhadap keberlanjutan operasional layanan IIV. Tujuan dari kontrol ini adalah untuk menilai sejauh mana organisasi telah melakukan identifikasi yang jelas terhadap pemangku kepentingan yang mendukung ekosistem layanan IIV, termasuk siapa yang berperan, aktivitas apa yang dilakukan,serta proses dan komunikasi yang terlibat.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa dokumentasi yang menunjukkan pemetaan dan identifikasi peran, aktivitas, proses, serta narahubung dari pemangku kepentingan yang terkait dengan ekosistem bisnis atau layanan IIV. Dokumen ini harus mencakup informasi tentang siapa saja pihak yang terlibat, baik internal (seperti departemen atau unit dalam organisasi) maupun eksternal (seperti vendor, mitra bisnis, atau regulator), serta tanggung jawab masing-masing dalam mendukung operasional dan keberlanjutan layanan IIV. Selain itu, bukti dukung ini juga bisa mencakup diagram alur atau matriks yang menggambarkan hubungan antara pemangku kepentingan dan peran mereka dalam ekosistem tersebut.
Ancaman/Risiko yang dimitigasi	TH013 TH057 TH059 TH061 TH067 TH069 TH056 TH058 TH060 TH066 TH068 TH070
Referensi Kontrol	**NIST CSF 2.0: GV.OC-01, GV.OC-05** **NIST CSF 1.1: ID.BE-1, ID.BE-2** **NIST SP 800-53r5: SR-1, SR-3, PM-8** **SNI ISO/IEC 27001:2022: 5.21, 5.22**

Kriteria Pemenuhan Kontrol 1.1.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Peran, aktivitas, proses, dan narahubung pemangku kepentingan belum diidentifikasi.	Organisasi belum mengetahui atau mendokumentasikan siapa saja pemangku kepentingan yang terlibat dalam ekosistem IIV serta peran, aktivitas, dan proses terkait.	Tidak ada dokumen atau catatan yang mengidentifikasi peran, aktivitas, proses, atau narahubung pemangku kepentingan. Tidak ada bukti yang menunjukkan pemahaman organisasi tentang hal ini.
1	Organisasi mengetahui sebagian kecil peran, aktivitas, proses, dan narahubung pemangku kepentingan namun belum ditetapkan secara formal	Organisasi telah mengenali beberapa pemangku kepentingan dan tanggung jawab mereka, tetapi belum ada dokumentasi atau kebijakan formal yang mendasarinya.	Dokumen atau catatan informal yang menunjukkan bahwa organisasi mengetahui sebagian kecil peran, aktivitas, proses, dan narahubung pemangku kepentingan, tetapi belum ada dokumen resmi atau formal. Bisa berupa daftar atau catatan internal yang belum disosialisasikan secara resmi.
2	Organisasi mengetahui sebagian besar peran, aktivitas, proses, dan narahubung pemangku kepentingan namun belum ditetapkan secara formal	Sebagian besar pemangku kepentingan dan peran mereka sudah diketahui, tetapi belum ada dokumen atau prosedur yang secara resmi mendokumentasikan informasi ini.	Dokumentasi yang mencakup sebagian besar peran, aktivitas, proses, dan narahubung pemangku kepentingan, namun belum ada dokumen formal yang diatur atau ditetapkan, seperti laporan atau analisis yang tidak terdokumentasi secara resmi dalam prosedur atau kebijakan organisasi.
3	Peran, aktivitas, proses, dan narahubung pemangku kepentingan telah diidentifikasi dan ditetapkan dalam sebuah dokumen formal.	Organisasi telah melakukan identifikasi yang lengkap terhadap pemangku kepentingan dan peran mereka, dan hal ini telah dituangkan dalam dokumen resmi seperti SOP, kebijakan, atau dokumen lainnya.	Dokumen formal yang memuat peran, aktivitas, proses, dan narahubung pemangku kepentingan yang telah diidentifikasi dan ditetapkan, misalnya SOP, kebijakan, atau dokumen strategi resmi yang mendokumentasikan seluruh pemangku kepentingan dan peran mereka dalam ekosistem IIV.
4	- Peran, aktivitas, proses, dan narahubung pemangku kepentingan telah diidentifikasi dan ditetapkan dalam sebuah dokumen formal. - Penetapan peran, aktivitas, proses, dan narahubung pemangku kepentingan dimonitor dan dievaluasi secara berkala.	Selain identifikasi yang sudah didokumentasikan secara formal, organisasi juga melakukan monitoring dan evaluasi terhadap pemangku kepentingan secara teratur untuk memastikan peran dan tanggung jawabnya tetap relevan dan up-to-date.	Dokumen formal yang mencakup identifikasi peran, aktivitas, proses, dan narahubung pemangku kepentingan, yang juga menunjukkan adanya monitoring dan evaluasi berkala terhadap peran dan aktivitas tersebut, misalnya laporan evaluasi tahunan atau prosedur reviu yang mencatat hasil monitoring pemangku kepentingan secara rutin
5	- Peran, aktivitas, proses, dan narahubung pemangku kepentingan telah diidentifikasi dan ditetapkan dalam sebuah dokumen formal. - Penetapan peran, aktivitas, proses, dan narahubung pemangku kepentingan dimonitor dan dievaluasi secara berkala. - Dilakukan pembaruan secara berkala terhadap penetapan peran, aktivitas, proses, dan narahubung pemangku kepentingan sebagai timbal balik dari evaluasi yang dilakukan.	Selain evaluasi rutin, organisasi juga melakukan pembaruan atau revisi terhadap identifikasi pemangku kepentingan dan peran mereka berdasarkan hasil evaluasi yang dilakukan, memastikan sistem tetap relevan dengan perkembangan ekosistem IIV.	Dokumen formal yang mencakup identifikasi peran, aktivitas, proses, dan narahubung pemangku kepentingan, serta bukti evaluasi berkala dan pembaruan terhadap peran dan aktivitas tersebut sebagai hasil dari evaluasi, misalnya dokumen revisi dan pembaruan berkala yang mencatat perubahan dan perbaikan dalam penetapan peran pemangku kepentingan.

1.2. Menyusun strategi, kebijakan, dan prosedur Pelindungan IIV

Penyelenggara IIV mampu menyusun strategi, kebijakan, dan prosedur yang jelas untuk pelindungan Infrastuktur Informasi Vital (IIV) untuk memastikan semua aspek keamanan tercakup dan diikuti oleh seluruh organisasi.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan Penyelenggara IIV;
b) mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV;
c) menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan;
d) menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Menyusun strategi, kebijakan, dan prosedur Pelindungan IIV” secara efektif antara lain:

NIST CSF 2.0	**:**	**GV.PO-01, GV.PO-02, GV.OC-02, GV.OC-03, GV.OC-04, GV.RR-02, GV.SC-02, GV.RM-03**
NIST CSF 1.1	**:**	**ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4, ID.BE-5, ID.AM-6**
NIST SP 800-53r5	**:**	**tiap kontrol -1 dari semua keluarga kontrol, PS-7, PS-9, PM-2, PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, PM-29, RA-1, RA-2, RA-3, RA-9, SA-2, SA-8, SA-20, CP-2, CP-11**
SNI ISO/IEC 27001:2022	**:**	**5.1, 5.2, 5.4, 5.29, 5.31, 5.32, 5.33, 7.5, 8.14**

Peraturan BSSN Nomor 7 tahun 2024

Peraturan BSSN Nomor 11 Tahun 2024

1.2.1. Menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan penyelenggara IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengembangkan kebijakan keamanan, menentukan peran dan tanggung jawab untuk keamanan siber di seluruh organisasi dan pihak terkait lainnya, dan klarifikasi metode berbagi informasi yang berlaku di antara para pemangku kepentingan tersebut.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengomunikasikan kebijakan, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan kebijakan yang jelas, organisasi dapat mengurangi risiko keamanan dan memastikan bahwa semua anggota mematuhi praktik keamanan yang terbaik.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen untuk memastikan bahwa kebijakan yang ditetapkan dipahami dan diimplementasikan secara konsisten di seluruh organisasi.
Referensi Kontrol	**NIST CSF 2.0: GV.PO-01, GV.PO-02, GV.OC-02, GV.OC-03, GV.RR-02** **NIST CSF 1.1: ID.GV-1, ID.GV-2, ID.GV-3** **NIST SP 800-53r5: Tiap kontrol -1 dari semua keluarga kontrol, PS-7, PS-9, PM-2, PM-29** **SNI ISO/IEC 27001:2022: 5.1, 5.2, 5.4, 5.31, 5.32, 5.33**

6 Kontrol 1.2.1.a:

Kontrol	Penyelenggara IIV menyusun, menetapkan, dan mengembangkan kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan
Deskripsi Kontrol	Penyelenggara IIV menyusun, menetapkan, dan mengembangkan kebijakan keamanan siber yang sesuai dengan standar yang berlaku di sektor serta peraturan perundang-undangan merupakan langkah penting untuk memastikan bahwa organisasi mematuhi aturan yang berlaku dan dapat mengelola risiko keamanan siber dengan baik. Kebijakan ini harus mencakup aspek-aspek penting dalam melindungi data dan sistem informasi, serta mengatur cara organisasi merespons ancaman dan insiden keamanan. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah memiliki kebijakan keamanan siber yang jelas, yang didasarkan pada standar industri dan regulasi yang relevan, serta dapat dijalankan dengan efektif di seluruh bagian organisasi.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat mencakup dokumen kebijakan yang disusun oleh penyelenggara IIV yang menunjukkan bahwa kebijakan keamanan siber yang diterapkan sudah sesuai dengan standar industri atau peraturan perundang-undangan yang relevan. Dokumen tersebut dapat meliputi: Dokumen kebijakan keamanan siber organisasi, Standar atau pedoman yang diikuti dalam penyusunan kebijakan keamanan siber, Surat keputusan atau dokumen resmi yang menetapkan kebijakan keamanan siber, Laporan atau notulen rapat yang membahas penyusunan atau pembaruan kebijakan keamanan siber, Salinan peraturan perundang-undangan yang menjadi acuan dalam kebijakan keamanan siber.
Ancaman/Risiko yang dimitigasi	TH041 TH052 TH054 TH057 TH060 TH049 TH053 TH056 TH059 TH066
Referensi Kontrol	**NIST CSF 2.0: GV.PO-01, GV.PO-02, GV.OC-02, GV.RR-02** **NIST CSF 1.1: ID.GV-1, ID.GV-2** **NIST SP 800-53r5: Tiap kontrol -1 dari semua keluarga kontrol, PS-7, PS-9, PM-2, PM-29** **SNI ISO/IEC 27001:2022: 5.1, 5.2, 5.4**

Kriteria Pemenuhan Kontrol 1.2.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan.	Organisasi belum memiliki kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan. Kebijakan belum disusun sama sekali.	- Tidak ada dokumen kebijakan yang disusun. - Tidak ada referensi terhadap standar keamanan siber yang berlaku atau peraturan perundang-undangan dalam kebijakan yang ada.
1	Organisasi telah menyusun kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang undangan dan sudah menerapkan pada sebagian kecil aspek, namun kebijakan tersebut belum ditetapkan.	Organisasi telah menyusun kebijakan, namun baru diterapkan pada sebagian kecil aspek. Kebijakan belum ditetapkan secara resmi. Mungkin ada kebijakan yang belum sepenuhnya dijalankan.	- Dokumen kebijakan tentang keamanan siber telah disusun. - Kebijakan baru diterapkan pada sebagian kecil aspek (misalnya, beberapa prosedur atau area operasional tertentu). - Kebijakan belum ditetapkan secara resmi.
2	Organisasi telah menerapkan kebijakan keamanan siber pada sebagian besar aspek sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan namun kebijakan tersebut belum ditetapkan.	Organisasi telah menerapkan kebijakan pada sebagian besar aspek, namun kebijakan belum ditetapkan secara resmi. Penerapannya sudah lebih luas, tetapi masih ada aspek yang belum optimal.	- Kebijakan keamanan siber telah diterapkan pada sebagian besar aspek organisasi. - Ada dokumentasi atau laporan yang menunjukkan penerapan kebijakan pada banyak area, tetapi kebijakan belum ditetapkan secara resmi atau formal.
3	Organisasi tidak hanya telah menerapkan, tetapi juga telah menetapkan kebijakan keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan.	Organisasi telah menerapkan dan menetapkan kebijakan keamanan siber sesuai standar yang berlaku. Kebijakan sudah diterapkan dan diatur, namun mungkin belum ada pembaruan atau pengelolaan yang aktif.	- Kebijakan keamanan siber telah diterapkan dan ditetapkan secara resmi dengan dokumen yang ditandatangani oleh pihak berwenang. - Kebijakan mencantumkan referensi terhadap standar yang berlaku di sektor atau regulasi yang relevan.
4	- Organisasi tidak hanya telah menerapkan dan menetapkan kebijakan keamanan siber, tetapi juga secara aktif mengelola dan meninjau kebijakan ini untuk memastikan bahwa mereka tetap relevan dan efektif. - Dilakukannya proses peninjauan dan pembaruan kebijakan yang terstruktur.	Organisasi menerapkan, menetapkan, dan mengelola kebijakan keamanan siber dengan proses peninjauan yang terstruktur untuk memastikan kebijakan tetap relevan dan efektif. Kebijakan dikelola secara aktif dan ditinjau secara berkala.	- Kebijakan telah diterapkan dan ditetapkan secara resmi. - Proses pengelolaan dan peninjauan kebijakan dilakukan secara berkala (misalnya, adanya laporan audit, tinjauan tahunan kebijakan). - Ada bukti adanya pembaruan kebijakan.
5	- Organisasi telah berhasil menyusun, menetapkan, dan mengembangkan kebijakan keamanan siber yang komprehensif dan efektif yang sepenuhnya sesuai dengan standar dan regulasi yang berlaku. - Kebijakan tersebut dikelola dan ditinjau secara berkala, dan ada mekanisme umpan balik serta perbaikan berkelanjutan untuk memastikan bahwa kebijakan ini tetap relevan dan efektif.	Organisasi telah menyusun, menetapkan, dan mengembangkan kebijakan keamanan siber yang komprehensif dan efektif sesuai standar dan regulasi yang berlaku. Kebijakan dikelola dan ditinjau secara berkala dengan mekanisme umpan balik dan perbaikan berkelanjutan. Kebijakan selalu diperbarui untuk tetap relevan dan efektif.	- Kebijakan telah disusun, ditetapkan, dan dikembangkan dengan komprehensif. - Kebijakan sepenuhnya sesuai dengan standar dan regulasi yang berlaku. - Ada mekanisme umpan balik (misalnya, survei, reviu) dan perbaikan kebijakan berkelanjutan. - Proses pembaruan kebijakan secara terstruktur dan berkala, dengan bukti peninjauan dan perbaikan.

7 Kontrol 1.2.1.b:

Kontrol	Penyelenggara IIV mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal.
Deskripsi Kontrol	Penyelenggara IIV mengomunikasikan kebijakan kepada seluruh personel yang relevan dan mengoordinasikan berbagi informasi mengenai kebijakan dan prosedur dengan pemangku kepentingan eksternal adalah langkah penting dalam memastikan bahwa semua pihak yang terlibat memahami dan mengikuti standar serta pedoman keamanan yang telah ditetapkan. Komunikasi yang efektif membantu memastikan konsistensi dalam implementasi kebijakan di seluruh organisasi dan dengan pihak eksternal yang berhubungan. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah berhasil menyebarluaskan kebijakan dan prosedur dengan cara yang sistematis kepada seluruh personel terkait serta menjalin koordinasi yang baik dengan pihak eksternal dalam hal berbagi informasi kebijakan.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat mencakup dokumen yang menunjukkan bahwa kebijakan keamanan siber telah disosialisasikan kepada seluruh personel yang relevan dalam organisasi, seperti melalui pelatihan, workshop, atau komunikasi internal lainnya. Selain itu, bukti juga dapat berupa salinan komunikasi atau memorandum yang menunjukkan koordinasi dan kesepakatan dengan pemangku kepentingan eksternal mengenai metode berbagi informasi terkait kebijakan dan prosedur yang ada. Laporan atau notulen rapat yang menunjukkan diskusi dan persetujuan terkait prosedur berbagi informasi dengan pihak eksternal juga dapat menjadi bukti dukung yang relevan.
Ancaman/Risiko yang dimitigasi	TH041 TH052 TH054 TH057 TH059 TH061 TH067 TH049 TH053 TH056 TH058 TH060 TH066
Referensi Kontrol	**NIST CSF 2.0: GV.PO-01, GV.PO-02, GV.OC-02, GV.RR-02** **NIST CSF 1.1: ID.GV-1, ID.GV-2** **NIST SP 800-53r5: Tiap kontrol -1 dari semua keluarga kontrol, PS-7, PS-9, PM-2, PM-29** **SNI ISO/IEC 27001:2022: 5.1, 5.2, 5.4**

Kriteria Pemenuhan Kontrol 1.2.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum mengomunikasikan dan mengoordinasikan kebijakan dan prosedur dengan personel dan pemangku kepentingan eksternal, dan belum memiliki mekanisme komunikasi terkait hal tersebut.	Organisasi belum mengomunikasikan dan mengoordinasikan kebijakan dan prosedur dengan personel dan pemangku kepentingan eksternal, serta belum memiliki mekanisme komunikasi yang jelas.	Tidak ada dokumen atau bukti komunikasi terkait kebijakan dan prosedur dengan personel dan pemangku kepentingan eksternal.
1	Organisasi mulai mengomunikasikan dan mengoodinasikan kebijakan dan prosedur kepada sebagian kecil personel dan pemangku kepentingan eksternal, namun mekanisme komunikasi tersebut belum ditetapkan.	Organisasi mulai mengomunikasikan dan mengoordinasikan kebijakan dan prosedur kepada sebagian kecil personel dan pemangku kepentingan eksternal, namun tanpa mekanisme komunikasi yang jelas.	Terdapat bukti awal komunikasi, seperti email atau pertemuan dengan sebagian kecil personel dan pemangku kepentingan eksternal.
2	Organisasi telah mengomunikasikan dan mengoodinasikan kebijakan dan prosedur kepada sebagian besar personel dan pemangku kepentingan eksternal, namun mekanisme komunikasi tersebut belum ditetapkan.	Organisasi telah mengomunikasikan dan mengoordinasikan kebijakan dan prosedur kepada sebagian besar personel dan pemangku kepentingan eksternal, tetapi belum memiliki mekanisme komunikasi yang terstruktur.	Bukti dokumentasi komunikasi seperti notulensi rapat, email, atau sosialisasi kepada sebagian besar personel dan pemangku kepentingan eksternal.
3	Organisasi mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal secara efektif dan efisien.	Organisasi mengomunikasikan kebijakan kepada seluruh personel yang relevan dan telah menyepakati metode berbagi informasi mengenai kebijakan dan prosedur dengan pemangku kepentingan eksternal secara efektif.	Dokumen resmi komunikasi kebijakan, kebijakan tertulis yang telah dibagikan, serta kesepakatan dengan pemangku kepentingan eksternal.
4	- Organisasi mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal secara efektif dan efisien. - Mekanisme komunikasi, koordinasi kebijakan dan prosedur dengan	Organisasi secara aktif mengelola komunikasi dan koordinasi kebijakan dengan personel serta pemangku kepentingan eksternal, termasuk peninjauan efektivitas komunikasi secara berkala.	Mekanisme komunikasi dan koordinasi yang terdokumentasi, laporan efektivitas komunikasi, dan evaluasi berkala terhadap kebijakan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	personel dan pemangku kepentingan eksternal yang telah disusun, dikelola dan ditinjau efektivitasnya secara berkala.		
5	- Organisasi mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal secara efektif dan efisien. - Mekanisme komunikasi, koordinasi kebijakan dan prosedur dengan personel dan pemangku kepentingan eksternal yang telah disusun, dikelola dan ditinjau efektivitasnya secara berkala dan ada mekanisme umpan balik serta perbaikan berkelanjutan untuk memastikan bahwa kebijakan ini tetap relevan dan efektif.	Organisasi telah menerapkan mekanisme komunikasi dan koordinasi yang komprehensif serta memiliki sistem umpan balik dan perbaikan berkelanjutan untuk memastikan efektivitas kebijakan.	Bukti umpan balik dari personel dan pemangku kepentingan eksternal, hasil evaluasi dan revisi kebijakan, serta dokumentasi mekanisme komunikasi yang terus diperbarui.

8 Kontrol 1.2.1.c:

Kontrol	Penyelenggara IIV meninjau dan merevisi kebijakannya secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya.
Deskripsi Kontrol	Penyelenggara IIV meninjau dan merevisi kebijakan secara berkelanjutan sesuai dengan perubahan dalam peraturan perundang-undangan yang relevan, serta standar dan pedoman industri yang berlaku, adalah langkah penting untuk memastikan kebijakan tetap up-to-date dan sesuai dengan perkembangan hukum dan regulasi terbaru. Proses ini juga membantu organisasi untuk menyesuaikan diri dengan perubahan di sektor industri yang mungkin mempengaruhi cara organisasi melindungi sistem dan data. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi secara proaktif melakukan peninjauan dan pembaruan kebijakan keamanan siber secara rutin, memastikan bahwa kebijakan tetap relevan dan efektif dalam memenuhi kebutuhan regulasi dan industri.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini mencakup dokumentasi yang menunjukkan bahwa penyelenggara IIV secara rutin meninjau dan merevisi kebijakannya. Bukti tersebut dapat berupa laporan tinjauan kebijakan yang mencatat perubahan yang dilakukan, notulensi rapat terkait evaluasi kebijakan, serta bukti pembaruan dokumen kebijakan yang disesuaikan dengan perubahan peraturan perundang-undangan, standar, atau pedoman industri. Selain itu, bukti komunikasi kepada personel terkait perubahan kebijakan, seperti surat edaran, pelatihan internal, atau pemberitahuan resmi, juga dapat digunakan untuk memastikan bahwa kebijakan yang diperbarui telah disosialisasikan dengan baik.
Ancaman/Risiko yang dimitigasi	TH041 TH056 TH059 TH066 TH049 TH057 TH060
Referensi Kontrol	**NIST CSF 2.0: GV.OC-03** **NIST CSF 1.1: ID.GV-3** **NIST SP 800-53r5: Tiap kontrol -1 dari semua keluarga control** **SNI ISO/IEC 27001:2022: 5.31, 5.32, 5.33**

Kriteria Pemenuhan Kontrol 1.2.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Penyelenggara belum memiliki rencana untuk meninjau dan merevisi kebijakannya secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya	Tidak ada rencana untuk meninjau dan merevisi kebijakan secara berkelanjutan sesuai regulasi dan standar industri yang berlaku.	Tidak terdapat dokumen rencana atau bukti peninjauan kebijakan.
1	Peninjauan dan revisi mulai dilakukan terhadap penerapan kebijakan pada sebagian kecil aspek secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya, namun mekanisme tersebut belum ditetapkan.	Peninjauan dan revisi mulai dilakukan pada sebagian kecil aspek kebijakan, tetapi belum memiliki mekanisme yang ditetapkan.	Bukti awal berupa notulensi, laporan, atau dokumen revisi sebagian kebijakan.
2	Peninjauan dan revisi terhadap penerapan kebijakan pada sebagian besar aspek secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya, telah dilaksanakan namun mekanisme tersebut belum ditetapkan.	Peninjauan dan revisi sudah mencakup sebagian besar aspek kebijakan, tetapi mekanisme tetap belum ditetapkan.	Dokumen revisi kebijakan yang lebih luas, namun belum ada sistem atau prosedur yang terdokumentasi.
3	Peninjauan dan revisi kebijakan yang telah diterapkan pada seluruh aspek secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya, telah dilaksanakan secara menyeluruh dan telah ditetapkan mekanismenya.	Peninjauan dan revisi telah dilakukan pada seluruh aspek kebijakan dengan mekanisme yang telah ditetapkan.	Dokumen resmi mekanisme peninjauan, laporan implementasi, serta hasil evaluasi berkala.
4	Peninjauan dan revisi kebijakan yang telah diterapkan pada seluruh aspek secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya, telah dilaksanakan secara menyeluruh dan secara aktif mengelola dan meninjau efektivitasnya.	Peninjauan dan revisi dilakukan secara menyeluruh, dengan mekanisme yang ditetapkan dan pemantauan aktif terhadap efektivitas kebijakan.	Terdapat laporan hasil evaluasi kebijakan, bukti implementasi perbaikan, serta sistem pemantauan berkelanjutan.
5	Peninjauan dan revisi kebijakan yang telah diterapkan pada seluruh aspek secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya, telah dilaksanakan secara menyeluruh dan secara aktif mengelola dan meninjau efektivitasnya serta terdapat mekanisme perbaikan berkelanjutan untuk memastikan bahwa kebijakan ini tetap relevan dan efektif.	Peninjauan dan revisi dilakukan secara menyeluruh dengan pemantauan aktif serta mekanisme perbaikan berkelanjutan agar kebijakan tetap efektif dan relevan.	Bukti pelaksanaan mekanisme perbaikan berkelanjutan, dokumentasi pembaruan kebijakan berdasarkan hasil evaluasi, serta keterlibatan pihak terkait dalam evaluasi dan perbaikan.

1.2.2. Mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengembangkan strategi penerapan dan peningkatan pelindungan terhadap IIV yang berbasis risiko dan dikomunikasikan kepada seluruh personil serta pihak-pihak yang terkait.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk mengembangkan strategi, dan berpotensi membutuhkan teknologi tambahan untuk otomatisasi yang telah memiliki sertifikat keamanan.
Dampak	**Tinggi** – Strategi yang baik dapat membantu organisasi dalam meningkatkan postur keamanan dan mengurangi risiko kebocoran atau penyalahgunaan informasi identitas.
Kompleksitas	**Sedang** – Memerlukan analisis dan perencanaan yang komprehensif untuk mengembangkan strategi yang efektif dan menyeluruh.
Referensi Kontrol	**NIST CSF 2.0: GV.RM-03** **NIST CSF 1.1: ID.GV-4** **NIST SP 800-53r5: PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2** **SNI ISO/IEC 27001:2022: -** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

9 Kontrol 1.2.2.a:

Kontrol	Penyelenggara IIV senantiasa mengembangkan strategi dalam melindungi aset informasi dengan mempertimbangkan manajemen risiko yang berlaku di organisasi.
Deskripsi Kontrol	Penyelenggara IIV mengembangkan strategi untuk melindungi aset informasi dengan mempertimbangkan manajemen risiko yang berlaku di organisasi merupakan langkah penting untuk memastikan bahwa perlindungan terhadap informasi dan sistem berjalan seiring dengan upaya mitigasi risiko. Strategi ini harus didasarkan pada identifikasi dan evaluasi risiko yang ada serta kemampuan organisasi untuk mengelola risiko tersebut dengan cara yang efektif. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah mengembangkan strategi yang tepat dalam melindungi aset informasi, serta memastikan bahwa strategi tersebut sejalan dengan praktik manajemen risiko yang berlaku dalam organisasi.
Deskripsi Bukti Dukung	Bukti dukung untuk pernyataan tersebut dapat berupa dokumen kebijakan keamanan informasi, hasil analisis manajemen risiko, serta implementasi kontrol keamanan yang diterapkan di organisasi. Misalnya, adanya prosedur penilaian risiko yang terdokumentasi menunjukkan bahwa penyelenggara IIV secara aktif mengidentifikasi, menilai, dan mengelola risiko terhadap aset informasi. Selain itu, penggunaan teknologi keamanan yang memiliki sertifikat keamanan seperti enkripsi, firewall, serta sistem deteksi dan pencegahan intrusi menjadi bukti nyata dalam melindungi data. Audit keamanan berkala dan pelatihan kesadaran keamanan bagi karyawan juga mencerminkan komitmen organisasi dalam menjaga keamanan informasi secara berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH023 TH025 TH053 TH056 TH059 TH065 TH077 TH024 TH052 TH054 TH057 TH060 TH070
Referensi Kontrol	**NIST CSF 2.0: GV.RM-03** **NIST CSF 1.1: ID.GV-4** **NIST SP 800-53r5: PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2** **SNI ISO/IEC 27001:2022: -** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 1.2.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki strategi perlindungan aset informasi dan belum memiliki dokumen manajemen risiko organisasi	Tidak ada strategi perlindungan aset informasi dan dokumen manajemen risiko dalam organisasi.	Tidak ditemukan dokumen terkait strategi perlindungan aset informasi atau manajemen risiko.
1	Prosedur pelindungan aset informasi, manajemen risiko organisasi dan Strategi pelindungan aset informasi sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Strategi dan prosedur perlindungan aset informasi, serta manajemen risiko mulai diterapkan pada sebagian kecil aspek tetapi belum diformalkan.	Terdapat bukti awal penerapan strategi dan prosedur dalam beberapa bagian organisasi, namun belum ada dokumen resmi atau kebijakan yang diformalkan.
2	Prosedur pelindungan aset informasi, manajemen risiko organisasi dan Strategi pelindungan aset informasi sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Strategi dan prosedur perlindungan aset informasi, serta manajemen risiko diterapkan pada sebagian besar aspek, tetapi masih belum diformalkan.	Terdapat dokumen yang menunjukkan penerapan strategi dan prosedur pada berbagai bagian organisasi, namun masih belum menjadi kebijakan resmi.
3	Prosedur pelindungan aset informasi, manajemen risiko organisasi dan Strategi pelindungan aset informasi sudah diterapkan pada seluruh aspek dan sudah diformalkan	Strategi dan prosedur perlindungan aset informasi, serta manajemen risiko telah diterapkan pada seluruh aspek dan telah diformalkan.	Tersedia kebijakan formal dan prosedur resmi terkait perlindungan aset informasi dan manajemen risiko yang telah diterapkan di seluruh aspek organisasi.
4	Prosedur pelindungan aset informasi, manajemen risiko organisasi dan Strategi pelindungan aset informasi sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring dan reviu secara berkala	Strategi dan prosedur perlindungan aset informasi, serta manajemen risiko telah diterapkan secara formal pada seluruh aspek dan dilakukan monitoring serta reviu berkala.	Tersedia dokumen kebijakan resmi, serta laporan monitoring dan reviu berkala terkait efektivitas strategi perlindungan aset informasi dan manajemen risiko.
5	Prosedur pelindungan aset informasi, manajemen risiko organisasi dan Strategi pelindungan aset informasi sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring dan reviu secara berkala, dilakukan perbaikan berkelanjutan dan terintegrasi dalam sistem yang terotomatisasi.	Strategi dan prosedur perlindungan aset informasi, serta manajemen risiko telah diterapkan secara formal, dilakukan monitoring dan reviu berkala, serta ada perbaikan berkelanjutan yang terintegrasi dalam sistem otomatis.	Bukti kebijakan resmi, laporan monitoring berkala, dokumentasi reviu, serta adanya mekanisme perbaikan yang berkelanjutan dengan sistem yang otomatis.

10 Kontrol 1.2.2.b

Kontrol	Penyelenggara IIV harus menetapkan sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan.
Deskripsi Kontrol	Penyelenggara IIV menetapkan sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan adalah langkah krusial untuk memastikan bahwa implementasi keamanan siber dilakukan secara terstruktur dan terukur di seluruh organisasi. Sasaran atau target ini harus spesifik, terukur, dan disesuaikan dengan kebutuhan dan risiko yang dihadapi oleh organisasi di setiap fungsi atau tingkatannya. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menetapkan sasaran atau target yang jelas dalam penerapan keamanan siber, yang meliputi setiap fungsi dan tingkat organisasi yang relevan, guna memastikan pencapaian tujuan keamanan yang efektif.
Deskripsi Bukti Dukung	Bukti dukung yang diperlukan untuk memastikan bahwa penyelenggara IIV telah menetapkan sasaran atau target penerapan keamanan siber meliputi dokumen kebijakan, strategi, atau pedoman resmi yang menguraikan sasaran keamanan siber pada berbagai fungsi dan tingkatan organisasi. Selain itu, dokumen perencanaan yang mencakup tujuan spesifik, indikator kinerja, serta roadmap implementasi keamanan siber dapat menjadi bukti pendukung. Laporan hasil evaluasi, notulen rapat strategis, serta bukti implementasi program keamanan siber di berbagai unit organisasi juga dapat digunakan untuk menunjukkan bahwa sasaran telah ditetapkan dan dijalankan secara efektif.
Ancaman/Risiko yang dimitigasi	TH052 TH054 TH057 TH060 TH070 TH053 TH056 TH059 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: GV.RM-03** **NIST CSF 1.1: ID.GV-4** **NIST SP 800-53r5: PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.2.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan.	Tidak ada sasaran atau target keamanan siber yang diterapkan dalam organisasi.	Tidak terdapat dokumen kebijakan atau bukti penerapan keamanan siber dalam organisasi.
1	Sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan telah dijalankan pada sebagian kecil aspek namun belum ditetapkan.	Sasaran atau target keamanan siber diterapkan dalam lingkup yang terbatas dan belum menjadi kebijakan resmi.	Terdapat inisiatif atau dokumen awal terkait keamanan siber, tetapi belum terstruktur atau ditetapkan secara formal.
2	Sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan telah dijalankan pada sebagian besar aspek namun belum ditetapkan.	Sebagian besar aspek dalam organisasi telah menerapkan keamanan siber, tetapi belum ada penetapan formal.	Dokumen atau prosedur keamanan siber mulai diterapkan di beberapa bagian organisasi, tetapi belum ada kepatuhan menyeluruh.
3	Sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan telah ditetapkan dan dijalankan secara menyeluruh.	Sasaran dan target keamanan siber telah ditetapkan dan diterapkan di seluruh organisasi.	Terdapat dokumen kebijakan resmi, prosedur, dan bukti penerapan di seluruh bagian organisasi.
4	Sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan telah ditetapkan dan dijalankan secara menyeluruh, dilakukan monitoring dan direviu secara berkala.	Sasaran atau target penerapan keamanan siber telah ditetapkan dan dijalankan secara menyeluruh, serta dilakukan monitoring dan reviu berkala untuk memastikan pencapaiannya.	Terdapat dokumen resmi mengenai sasaran atau target keamanan siber, bukti monitoring capaian sasaran, serta laporan hasil reviu berkala.
5	Sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan telah dtetapkan dan dijalankan secara menyeluruh, dilakukan monitoring dan direviu secara berkala serta dievaluasi dan dilakukan perbaikan berkelanjutan.	Sasaran atau target penerapan keamanan siber telah ditetapkan dan dijalankan secara menyeluruh, serta dilakukan monitoring, reviu berkala, evaluasi, dan perbaikan berkelanjutan untuk memastikan efektivitasnya.	Terdapat dokumen evaluasi sasaran keamanan siber, laporan perbaikan berdasarkan hasil evaluasi, serta bukti penerapan strategi peningkatan berkelanjutan.

1.2.3. Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan

Kriteria	Detail
Deskripsi	Penyelenggara IIV menetapkan persyaratan-persyaratan dasar yang harus dipenuhi agar operasional layanan IIV selalu tersedia dalam segala kondisi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan pengembangan persyaratan operasional, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan persyaratan yang jelas, organisasi dapat memastikan bahwa operasional IIV tetap berjalan lancar dan aman dalam berbagai kondisi.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif dan perencanaan untuk menetapkan persyaratan yang tepat.
Referensi Kontrol	**NIST CSF 2.0: GV.OC-04** **NIST CSF 1.1: ID.BE-5** **NIST SP 800-53r5: CP-2, CP-11, RA-9, SA-8, SA-20** **SNI ISO/IEC 27001:2022: 5.29, 7.5, 8.14**

11 Kontrol 1.2.3.a:

Kontrol	Penyelenggara IIV menyusun kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber.
Deskripsi Kontrol	Penyelenggara IIV menyusun kebijakan standar operasional prosedur (SOP) untuk setiap layanan yang mendukung IIV, baik dalam kondisi normal, saat terjadi insiden siber, maupun pasca insiden siber. Ini merupakan langkah penting untuk memastikan bahwa organisasi memiliki panduan yang jelas untuk setiap tahap siklus operasional. SOP ini membantu dalam menjaga konsistensi layanan dan memastikan bahwa respons terhadap insiden siber dan pemulihan pasca insiden dilakukan secara efektif dan terkoordinasi. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menyusun SOP yang memadai dan mencakup semua skenario yang relevan, dengan memastikan prosedur yang diterapkan sesuai dengan keadaan operasional dan peraturan yang berlaku.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa dokumen kebijakan, standar operasional prosedur (SOP), dan pedoman teknis yang disusun oleh penyelenggara IIV terkait pengelolaan layanan dalam berbagai kondisi, termasuk operasi normal, respons terhadap insiden siber, dan pemulihan pasca-insiden. Dokumen tersebut harus mencakup peran dan tanggung jawab, langkah-langkah mitigasi risiko, serta prosedur eskalasi dan koordinasi dengan pihak terkait. Selain itu, bukti dukung dapat berupa hasil simulasi atau uji coba kebijakan, laporan audit kepatuhan, serta catatan insiden yang menunjukkan implementasi prosedur dalam situasi nyata.
Ancaman/Risiko yang dimitigasi	TH023 TH025 TH053 TH056 TH059 TH065 TH077 TH024 TH052 TH054 TH057 TH060 TH070
Referensi Kontrol	**NIST CSF 2.0: GV.OC-04** **NIST CSF 1.1: ID.BE-5** **NIST SP 800-53r5: CP-2, CP-11, RA-9, SA-8, SA-20** **SNI ISO/IEC 27001:2022: 5.29, 7.5, 8.14**

Kriteria Pemenuhan Kontrol 1.2.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber.	Tidak ada kriteria (belum ada pemahaman, kebijakan, maupun komitmen pimpinan organisasi)	Tidak ada bukti pendukung
1	Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber sudah diterapkan pada sebagian besar aspek namun belum ditetapkan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelindungan terhadap layanan IIV dan telah diterapkan pada sebagian aspek. misalnya, pelindungan pada aspek kondisi normal saja, namun belum ada tata laksana atau rencana penanggulangan jika terjadi gangguan atau bahkan insiden siber pada layanan IIV. - Belum ada kebijakan SOP yang ditetapkan oleh organisasi.	- Terdapat bukti implementasi pelindungan terhadap layanan IIV untuk menjaga ketersediaan dan keamanannya pada kondisi normal. - Organisasi belum menyusun draft SOP atau kebijakan terkait pelindungan layanan IIV pada saat normal, terjadi insiden siber, maupun pasca insiden siber
2	Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber sudah diterapkan pada sebagian besar aspek namun belum ditetapkan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelindungan terhadap layanan IIV dan telah diterapkan pada sebagian besar aspek. misalnya, sudah ada implementasi pelindungan pada aspek kondisi normal, serta sudah ada rencana penanggulangan jika terjadi gangguan atau bahkan insiden siber pada layanan IIV. - Belum ada kebijakan SOP yang ditetapkan oleh organisasi.	Organisasi telah menyusun draft SOP spesifik terkait pelindungan layanan IIV pada saat normal, terjadi insiden siber, maupun pasca insiden siber, namun belum ditetapkan.
3	Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber sudah diterapkan pada seluruh aspek dan sudah ditetapkan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelindungan terhadap layanan IIV dan telah diterapkan pada seluruh aspek. misalnya, sudah ada implementasi pelindungan pada aspek kondisi normal, serta sudah ada rencana penanggulangan jika terjadi gangguan atau bahkan insiden siber pada layanan IIV. - Kebijakan SOP tentang pelindungan terhadap layanan IIV pada kondisi normal, gangguan, dan insiden siber yang telah ditetapkan oleh organisasi. - Organisasi telah menyiapkan SDM dengan keahlian spesifik untuk menjaga layanan IIV dari segala kondisi. - Organisasi telah menyiapkan teknologi dan sumber daya lain yang dibutuhkan untuk menjaga layanan IIV dari segala kondisi	- Organisasi telah menetapkan SOP spesifik terkait pelindungan layanan IIV pada saat normal, terjadi insiden siber, maupun pasca insiden siber. - Terdapat SDM, teknologi, maupun sumber daya lain yang disiapkan oleh organisasi untuk menjalankan SOP tersebut

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber sudah diterapkan pada seluruh aspek dan sudah ditetapkan, dilakukan monitoring dan direviu secara berkala.	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana pelindungan terhadap layanan IIV dan telah diterapkan pada seluruh aspek. misalnya, sudah ada implementasi pelindungan pada aspek kondisi normal, serta sudah ada rencana penanggulangan jika terjadi gangguan atau bahkan insiden siber pada layanan IIV. - Kebijakan SOP yang telah ditetapkan oleh organisasi. - Organisasi telah menyiapkan SDM dengan keahlian spesifik untuk menjaga layanan IIV dari segala kondisi, serta melakukan penilaian kinerja dan peningkatan kapasitas SDM secara periodik sesuai kebutuhan keamanan IIV. - Organisasi telah menyiapkan teknologi dan sumber daya lain yang dibutuhkan untuk menjaga layanan IIV dari segala kondisi, serta melakukan monitoring dan evaluasi secara periodik sesuai kebutuhan keamanan IIV. - Organisasi telah menjalankan uji simulasi terhadap skenario-skenario insiden siber pada layanan IIV	- Organisasi telah menetapkan SOP spesifik terkait pelindungan layanan IIV pada saat normal, terjadi insiden siber, maupun pasca insiden siber. - Terdapat SDM, teknologi, maupun sumber daya lain yang disiapkan oleh organisasi untuk menjalankan SOP tersebut. - Terdapat dokumen hasil monitoring terhadap implementasi SOP misalnya, hasil evaluasi kinerja dan kompetensi SDM dalam konteks pelindungan layanan IIV, simulasi insiden siber, laporan audit kepatuhan, atau catatan penanganan insiden yang menunjukkan implementasi prosedur dalam situasi nyata
5	Kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber sudah diterapkan pada seluruh aspek dan sudah ditetapkan, dilakukan monitoring dan direviu secara berkala serta dievaluasi dan dilakukan perbaikan berkelanjutan.	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana pelindungan terhadap layanan IIV dan telah diterapkan pada seluruh aspek. misalnya, sudah ada implementasi pelindungan pada aspek kondisi normal, serta sudah ada rencana penanggulangan jika terjadi gangguan atau bahkan insiden siber pada layanan IIV. - Kebijakan SOP yang telah ditetapkan oleh organisasi. - Organisasi telah menyiapkan SDM dengan keahlian spesifik untuk menjaga layanan IIV dari segala kondisi, serta melakukan penilaian kinerja dan peningkatan kapasitas SDM secara periodik sesuai kebutuhan keamanan IIV. - Organisasi telah menyiapkan teknologi dan sumber daya lain yang dibutuhkan untuk menjaga layanan IIV dari segala kondisi, serta melakukan monitoring dan evaluasi secara periodik sesuai kebutuhan keamanan IIV. - Organisasi telah menjalankan uji simulasi terhadap skenario-skenario insiden siber pada layanan IIV - Organisasi telah melakukan evaluasi terhadap implementasi kebijakan secara periodik, dan membuat rencana peningkatan postur keamanan secara berkelanjutan.	- Organisasi telah menetapkan SOP spesifik terkait pelindungan layanan IIV pada saat normal, terjadi insiden siber, maupun pasca insiden siber. - Terdapat SDM, teknologi, maupun sumber daya lain yang disiapkan oleh organisasi untuk menjalankan SOP tersebut. - Terdapat dokumen hasil monitoring terhadap implementasi SOP misalnya, hasil evaluasi kinerja dan kompetensi SDM dalam konteks pelindungan layanan IIV, hasil simulasi insiden siber, atau catatan penanganan insiden yang menunjukkan implementasi prosedur dalam situasi nyata - Komitmen pimpinan organisasi dalam rencana peningkatan keamanan berkelanjutan yang merupakan hasil evaluasi yang telah dilakukan oleh organisasi.

1.2.4. Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga

Kriteria	Detail
Deskripsi	Penyelenggara IIV menentukan dan menetapkan kebijakan terkait peran dan tanggung jawab seluruh personel dalam rangka menggunakan dan mengelola aset informasi, termasuk juga pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra), dan pihak lainnya yang berhubungan dengan organisasi
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengomunikasikan kebijakan penggunaan aset informasi, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan kebijakan yang jelas, organisasi dapat mengurangi risiko penyalahgunaan aset informasi dan memastikan bahwa semua pengguna mematuhi standar keamanan yang ditetapkan.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen untuk memastikan bahwa kebijakan yang ditetapkan dipahami dan diimplementasikan secara konsisten oleh pegawai dan pihak ketiga.
Referensi Kontrol	**NIST CSF 2.0: GV.RR-02, GV.SC-02** **NIST CSF 1.1: ID.AM-6** **NIST SP 800-53r5: CP-2, PS-7, PM-2, PM-29** **SNI ISO/IEC 27001:2022: 5.2**

12 Kontrol 1.2.4.a:

Kontrol	Penyelenggara IIV menyusun kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi, dsb.
Deskripsi Kontrol	Menyusun kebijakan standar operasional prosedur (SOP) yang diperlukan untuk menjaga keamanan dan ketersediaan setiap aset informasi yang mendukung layanan IIV. Misalnya, kebijakan mengenai setiap peranti yang digunakan di luar premis organisasi yang menyimpan atau memproses informasi (misalnya peranti seluler), termasuk peranti yang dimiliki oleh organisasi dan peranti yang dimiliki secara pribadi dan digunakan atas nama organisasi [bawa peranti Anda sendiri (Bring Your Own Device-BYOD)] memerlukan proteksi. Penggunaan peranti ini sebaiknya diotorisasi oleh manajemen. Kebijakan mengenai prosedur yang harus diimplementasikan untuk memanajemeni instalasi perangkat lunak dengan aman pada sistem operasional. Kebijakan mengenai Personel dan pengguna pihak eksternal yang menggunakan atau memiliki akses ke informasi dan aset terkait lainnya milik organisasi sebaiknya diberi tahu tentang persyaratan keamanan informasi untuk memproteksi dan menangani informasi dan aset terkait lainnya milik organisasi Mereka sebaiknya bertanggung jawab atas penggunaan segala fasilitas pemrosesan informasi.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa dokumen kebijakan resmi yang disusun oleh penyelenggara IIV untuk memastikan ketersediaan aset informasi, seperti kebijakan Bring Your Own Device (BYOD), kebijakan instalasi perangkat lunak, dan kebijakan klasifikasi informasi. Dokumen tersebut harus mencakup aturan, batasan, serta mekanisme pengawasan dan penegakan kebijakan guna mencegah gangguan terhadap ketersediaan informasi. Selain itu, bukti dukung juga dapat berupa sosialisasi kebijakan kepada pegawai, laoran kepatuhan, hasil audit kebijakan, serta rekaman penerapan aturan, seperti daftar perangkat yang diizinkan, catatan persetujuan instalasi perangkat lunak, atau laporan pelanggaran kebijakan.
Ancaman/Risiko yang dimitigasi	TH035 TH043 TH046 TH049 TH053 TH056 TH077 TH041 TH044 TH047 TH052 TH054 TH057
Referensi Kontrol	**NIST CSF 2.0: GV.RR-02, GV.SC-02** **NIST CSF 1.1: ID.AM-6** **NIST SP 800-53r5: CP-2, PS-7, PM-2, PM-29** **SNI ISO/IEC 27001:2022: 5.2**

Kriteria Pemenuhan Kontrol 1.2.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menyusun kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi, dsb	Tidak ada kebijakan formal maupun informal yang mengatur keamanan dan ketersediaan aset informasi, termasuk penggunaan perangkat pribadi, instalasi perangkat lunak, atau klasifikasi informasi.	Tidak ditemukan adanya dokumen pendukung
1	Kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi sudah diterapkan pada sebagian kecil aspek, namun belum ditetapkan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penggunaan aset informasi bagi pegawai dan pihak ketiga, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian unit kerja saja, namun belum menyeluruh kepada seluruh pegawai dan juga pihak ketiga. - penerapan hanya dilakukan pada sebagian aspek keamanan dan ketersediaan aset informasi. - Pimpinan organisai sudah menunjukan komitmen dalam pemenuhan kriteria - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal	Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan kebijakan sebagian aspek keamanan dan ketersediaan aset informasi.
2	Kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi sudah diterapkan pada sebagian besar aspek, namun belum ditetapkan.	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penggunaan aset informasi bagi pegawai dan pihak ketiga, dan telah diterapkan pada sebagian besar aspek. Misalnya, penerapan sudah dilakukan pada seluruh unit kerja saja, namun belum mengatur kepada pihak ketiga. - penerapan hanya dilakukan pada sebagian aspek keamanan dan ketersediaan aset informasi. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria. - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	Draf kebijakan atau pedoman internal yang mencakup sebagian besar aspek keamanan dan ketersediaan aset informasi.
3	Kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penggunaan aset informasi bagi pegawai dan pihak ketiga dan telah diterapkan pada seluruh aspek.	Dokumen kebijakan resmi (mis. kebijakan BYOD, instalasi perangkat lunak, klasifikasi informasi) yang telah disahkan manajemen.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	sudah diterapkan pada seluruh aspek dan sudah ditetapkan.	- Seluruh aspek keamanan dan ketersediaan aset informasi telah memiliki kebijakan formal dan diimplementasikan secara konsisten di seluruh unit kerja.	
4	Kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi sudah diterapkan pada seluruh aspek dan sudah ditetapkan, dilakukan monitoring dan direviu secara berkala.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penggunaan aset informasi bagi pegawai dan pihak ketiga dan telah diterapkan pada seluruh aspek. - Seluruh aspek keamanan dan ketersediaan aset informasi telah memiliki kebijakan formal dan diimplementasikan secara konsisten di seluruh unit kerja.. - Kebijakan formal telah diterapkan secara menyeluruh, dimonitor kepatuhannya, dan dilakukan reviu secara berkala.	Laporan monitoring kepatuhan dan berita acara reviu kebijakan secara berkala.
5	Kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (bring your own devices), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi sudah diterapkan pada seluruh aspek dan sudah ditetapkan, dilakukan monitoring dan direviu secara berkala serta dievaluasi dan dilakukan perbaikan berkelanjutan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penggunaan aset informasi bagi pegawai dan pihak ketiga dan telah diterapkan pada seluruh aspek. - Seluruh aspek keamanan dan ketersediaan aset informasi telah memiliki kebijakan formal dan diimplementasikan secara konsisten di seluruh unit kerja. - Kebijakan formal telah diterapkan secara menyeluruh, dimonitor dan direviu secara berkala, serta dilakukan evaluasi dan perbaikan berkelanjutan berdasarkan hasil monitoring dan reviu.	Laporan hasil evaluasi, daftar tindakan perbaikan, serta bukti implementasi perbaikan terhadap kebijakan keamanan dan ketersediaan aset informasi.

1.3. Mengelola aset informasi

Penyelenggara IIV mengidentifikasi dan mengelola aset informasi yang ada di organisasinya meliputi namum tidak terbatas pada data, personel, perangkat, sistem, dan infrastruktur yang memungkinkan penyelenggara IIV mencapai tujuan bisnis/ layanan sesuai dengan tujuan dan strategi risiko penyelenggara IIV.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) mengelola daftar inventaris aset informasi;
b) memetakan jalur komunikasi dan alur data pada organisasi;
c) menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi;
d) menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya; dan
e) mengendalikan aset informasi milik organisasi.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Mengelola aset informasi” secara efektif antara lain:

NIST CSF 2.0	**:**	**ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, PR.PS-03**
NIST CSF 1.1	**:**	**ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, PR.DS-3**
NIST SP 800-53r5	**:**	**CM-8, PM-5, AC-4, AC-20, CA-3, CA-9, PL-8, SA-9, SA-17, SA-20, CP-2, RA-2, RA-9, SC-6, MP-6 PE-16, PE-20**
SNI ISO/IEC 27001:2022	**:**	**5.9, 5.12, 5.14, 7.9, 7.10, 7.14, 8.8**

1.3.1. Mengelola daftar inventaris aset informasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengelola daftar inventaris aset informasi yang berisi seluruh aset informasi utama seperti perangkat lunak, perangkat keras, dan layanan TIK yang akan dilindungi
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan memelihara daftar inventaris, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan daftar inventaris yang akurat, organisasi dapat mengelola aset informasi dengan lebih efektif dan mengurangi risiko kehilangan atau kerusakan aset
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengelola dan memperbarui daftar inventaris secara berkala
Referensi Kontrol	**NIST CSF 2.0: ID.AM-01, ID.AM-02** **NIST CSF 1.1: ID.AM-1, ID.AM-2** **NIST SP 800-53r5: CM-8, PM-5** **SNI ISO/IEC 27001:2022: 5.9**

13 Kontrol 1.3.1.a:

Kontrol	Dokumentasikan dan kelola dengan tepat daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb).
Deskripsi Kontrol	Mendokumentasikan dan mengelola daftar inventaris aset informasi, seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, adalah langkah penting untuk memastikan bahwa setiap aset yang memiliki nilai dan penting bagi operasi organisasi dapat dikelola dengan baik. Daftar inventaris ini harus mencakup informasi manajerial yang relevan, seperti nama aset, versi perangkat lunak, alamat jaringan, nama penanggung jawab, informasi lisensi, dan detail lainnya yang diperlukan untuk memfasilitasi pengelolaan dan perlindungan aset. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah secara sistematis mendokumentasikan dan mengelola aset informasi yang perlu dilindungi, serta apakah informasi manajemen yang diperlukan tersedia dan dikelola dengan tepat.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa daftar inventaris aset informasi organisasi yang berisikan hasil identifikasi organisasi terhadap informasi dan aset terkait operasional bisnis organisasi dan penyelenggaraan layanan IIV. Dokumentasi sebaiknya dipelihara pada inventori khusus atau yang sudah ada dengan tepat. Inventori informasi dan aset terkait lainnya sebaiknya akurat, mutakhir, konsisten, dan selaras dengan data inventori lainnya. Beberapa opsi untuk memastikan keakuratan inventori informasi dan aset terkait lainnya meliputi: - melakukan reviu reguler dari informasi terindentifikasi dan aset terkait lainnya terhadap inventori aset; - secara otomatis memberlakukan pemutakhiran inventaris dalam proses pemasangan, perubahan, atau pemindahan aset.
Ancaman/Risiko yang dimitigasi	TH022 TH025 TH032 TH034 TH036 TH044 TH047 TH052 TH054 TH077 TH023 TH031 TH033 TH035 TH043 TH046 TH048 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-01, ID.AM-02** **NIST CSF 1.1: ID.AM-1, ID.AM-2** **NIST SP 800-53r5: CM-8, PM-5** **SNI ISO/IEC 27001:2022: 5.9**

Kriteria Pemenuhan Kontrol 1.3.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menyusun daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb), belum mendokumentasikan dan mengelolanya.	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Organisasi telah melakukan dokumentasi dan pengelolaan pada sebagian kecil daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb) namun belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pengelolaan daftar inventaris aset informasi, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal.	Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan kebijakan pada sebagian aspek pengelolaan daftar inventaris aset informasi.
2	Organisasi telah melakukan dokumentasi dan pengelolaan pada sebagian besar daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb) namun belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pengelolaan daftar inventaris aset informasi, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	Draf kebijakan atau pedoman internal yang mencakup sebagian besar aspek keamanan dan ketersediaan aset informasi.
3	Organisasi telah melakukan dokumentasi dan pengelolaan pada seluruh daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pengelolaan daftar inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan	- terdapat kebijakan yang mengatur tata laksana inventarisasi aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb) dan sudah diformalkan	layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, telah terdokumentasi secara formal.	- terdapat bukti implementasi berupa daftar inventarisasi aset informasi pada semua aspek.
4	Organisasi telah melakukan dokumentasi dan pengelolaan pada seluruh daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb) dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pengelolaan daftar inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, telah terdokumentasi secara formal. - terdapat mekanisme pengawasan dan peninjauan yang dilakukan secara berkala	- terdapat kebijakan yang mengatur tata laksana inventarisasi aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa daftar inventarisasi aset informasi pada semua aspek. - terdapat penggunaan teknologi pencatatan aset informasi misalnya, software inventory tools untuk membantu mendokumentasi dan memonitor inventori aset secara otomatis. - terdapat bukti telah dilakukan peninjauan terhadap pencatatan aset informasi.
5	Organisasi telah melakukan dokumentasi dan pengelolaan pada seluruh daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb) dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala serta dievaluasi dan dilakukan perbaikan berkelanjutan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pengelolaan daftar inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, telah terdokumentasi secara formal. - terdapat mekanisme pengawasan dan peninjauan yang dilakukan secara berkala	- terdapat kebijakan yang mengatur tata laksana inventarisasi aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa daftar inventarisasi aset informasi pada semua aspek. - terdapat penggunaan teknologi pencatatan aset informasi misalnya, software inventory tools untuk membantu mendokumentasi dan memonitor inventori aset secara otomatis. - terdapat bukti telah dilakukan peninjauan terhadap pencatatan aset informasi. - terdapat bukti yang menunjukan telah dilakukan peninjauan terhadap tata laksana pencatatan invetaris aset informasi untuk perbaikan berkelanjutan

14 Kontrol 1.3.1.b:

Kontrol	Penyelenggara IIV memastikan pemberian label pada perangkat aset informasi oleh pihak yang berwenang di organisasi
Deskripsi Kontrol	Memastikan pemberian label pada perangkat aset informasi oleh pihak yang berwenang di organisasi adalah langkah penting untuk pengelolaan dan pelacakan aset informasi. Pemberian label yang tepat membantu dalam identifikasi dan pemantauan aset, serta memastikan bahwa setiap perangkat yang digunakan dalam organisasi tercatat dan dilindungi dengan benar sesuai dengan kebijakan keamanan yang berlaku. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menetapkan prosedur yang jelas mengenai pemberian label pada perangkat aset informasi, serta memastikan bahwa perangkat diberi label dengan benar oleh pihak yang berwenang untuk memudahkan pengelolaan dan pengawasan.
Deskripsi Bukti Dukung	Kontrol ini mengharuskan organisasi memberi label pada informasi sesuai dengan skema klasifikasi yang telah ditentukan, sehingga memungkinkan pelacakan dan pengelolaan aset yang efektif. Bukti dukung untuk kontrol ini dapat berupa daftar aset dan prosedur pelabelan informasi yang mencakup informasi dan aset terkait lainnya dalam semua format. Pelabelan harus mencerminkan skema klasifikasi informasi yang ditetapkan organisasi. Prosedur harus memberikan panduan tentang di mana dan bagaimana label dilampirkan dengan mempertimbangkan bagaimana informasi diakses atau aset ditangani tergantung pada jenis media penyimpanan.
Ancaman/Risiko yang dimitigasi	TH031 TH033 TH035 TH044 TH047 TH071 TH032 TH034 TH043 TH046 TH052 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.AM-01, ID.AM-02** **NIST CSF 1.1: ID.AM-1, ID.AM-2** **NIST SP 800-53r5: CM-8, PM-5** **SNI ISO/IEC 27001:2022: 5.9**

Kriteria Pemenuhan Kontrol 1.3.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan belum memastikan pemberian label pada perangkat aset informasi oleh pihak yang berwenang di organisasi	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Organisasi telah menerapkan prosedur pemberian label pada sebagian kecil aspek perangkat aset informasi oleh pihak yang berwenang di organisasi dan belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelabelan pada inventaris aset informasi, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal.	- Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan kebijakan pada sebagian aspek pengelolaan daftar inventaris aset informasi. - terdapat bukti implementasi pelabelan pada sebagian aset informasi
2	Organisasi telah menerapkan prosedur pemberian label pada sebagian besar aspek perangkat aset informasi oleh pihak yang berwenang di organisasi namun belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelabelan daftar inventaris aset informasi, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	- Draf kebijakan atau pedoman internal yang mencakup sebagian besar aspek keamanan dan ketersediaan aset informasi. - terdapat bukti implementasi pelabelan pada sebagian aset informasi
3	Organisasi telah menerapkan prosedur pemberian label pada seluruh aspek perangkat aset informasi oleh pihak yang berwenang di organisasi dan sudah diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelabelan inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, telah terdokumentasi secara formal.	- terdapat kebijakan yang mengatur tata laksana pelabelan aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa daftar pelabelan inventarisasi aset informasi pada semua aspek aset informasi sesuai klasifikasi informasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	Organisasi telah menerapkan prosedur pemberian label pada seluruh aspek perangkat aset informasi oleh pihak yang berwenang di organisasi dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelabelan inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan telah terdokumentasi secara formal. - terdapat mekanisme pengawasan dan peninjauan yang dilakukan secara berkala	- terdapat kebijakan yang mengatur tata laksana pelabelan aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa daftar pelabelan aset informasi pada semua aspek aset informasi sesuai klasifikasi informasi. - terdapat bukti telah dilakukan peninjauan terhadap pelabelan aset informasi.
5	Organisasi telah menerapkan prosedur pemberian label pada seluruh aspek perangkat aset informasi oleh pihak yang berwenang di organisasi dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala, serta dievaluasi dan dilakukan perbaikan berkelanjutan.	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana pelabelan inventaris aset informasi, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan telah terdokumentasi secara formal. - terdapat mekanisme pengawasan dan peninjauan yang dilakukan secara berkala - telah dilakukan kegiatan evaluasi terhadap mekanisme pelabelan informasi pada organisasi.	- terdapat kebijakan yang mengatur tata laksana pelabelan aset informasi organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa daftar pelabelan aset informasi pada semua aspek aset informasi sesuai klasifikasi informasi. - terdapat bukti telah dilakukan peninjauan terhadap pelabelan aset informasi. - terdapat bukti telah dilakukan kegiatan evaluasi untuk perbaikan berkelanjutan terhadap mekanisme pelabelan informasi.

1.3.2. Memetakan jalur komunikasi dan alur data pada organisasi

Kriteria	Detail
Deskripsi	Penyelengara IIV menyusun dan mengelola jalur komunikasi jaringan (network architecture) dan alur data (data flow) yang diterapkan pada organisasi untuk mendukung layanan IIV. Dokumentasi alur data mencakup alur data penyedia layanan dan harus didasarkan pada proses manajemen data perusahaan. Tinjau dan perbarui dokumentasi setiap tahun, atau ketika terjadi perubahan signifikan yang dapat mempengaruhi layanan organisasi. Tetapkan dan kelola diagram arsitektur dan/atau dokumentasi sistem jaringan lainnya. Tinjau dan perbarui dokumentasi setiap tahun, atau ketika terjadi perubahan signifikan yang dapat mempengaruhi layanan organisasi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan pemetaan jalur komunikasi dan alur data, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Memetakan jalur komunikasi dan alur data membantu organisasi mengidentifikasi risiko dan mengelola keamanan informasi dengan lebih baik.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif dan pemetaan yang mendetail untuk mengidentifikasi semua jalur komunikasi dan alur data
Referensi Kontrol	**NIST CSF 2.0: ID.AM-03, ID.AM-07** **NIST CSF 1.1: ID.AM-3** **NIST SP 800-53r5: AC-4, CA-3, CA-9, PL-8, SA-17** **SNI ISO/IEC 27001:2022: 5.14**

15 Kontrol 1.3.2.a:

Kontrol	Penyelenggara IIV menyusun dokumentasi dan mengelola diagram jalur komunikasi jaringan dan aliran data dengan tepat dalam organisasi.
Deskripsi Kontrol	Menyusun dokumentasi dan mengelola diagram jalur komunikasi jaringan serta aliran data dengan tepat dalam organisasi adalah langkah penting untuk memahami dan mengelola infrastruktur jaringan secara efektif. Diagram ini menunjukkan bagaimana data mengalir antar sistem, aplikasi, dan perangkat di dalam jaringan organisasi, serta bagaimana informasi dikendalikan dan diamankan. Hal ini penting untuk mendeteksi potensi kerentanannya, memastikan kontrol akses yang tepat, dan mendukung kebijakan keamanan jaringan. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menyusun dokumentasi yang akurat dan mengelola diagram jalur komunikasi serta aliran data dalam jaringan organisasi, sehingga memudahkan pemantauan, audit, dan pengamanan jaringan.
Deskripsi Bukti Dukung	Kontrol ini mengharuskan organisasi mengumpulkan Informasi Jaringan dan Data yang digunakan pada layanan IIV, meliputi: Struktur Jaringan dan Alur Data. Kemudian organisasi membuat Diagram Jaringan yang terhubung terhadap layanan IIV yang meliputi paling sedikit: Diagram Topologi Fisik dan Diagram Topologi Logis. Organisasi juga diharuskan memiliki diagram alir data (data flow diagram) yang meliputi paling sedikit: Diagram Alur Kerja (Workflow Diagram) dan Diagram Data Flow (DFD).
Ancaman/Risiko yang dimitigasi	TH025 TH030 TH039 TH043 TH052 TH054 TH077 TH029 TH035 TH040 TH044 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-03, ID.AM-07** **NIST CSF 1.1: ID.AM-3** **NIST SP 800-53r5: AC-4, CA-3, CA-9, PL-8, SA-17** **SNI ISO/IEC 27001:2022: 5.14**

Kriteria Pemenuhan Kontrol 1.3.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum dapat menunjukan dokumentasi diagram jalur komunikasi jaringan (network architecture) dan aliran data (document data flow) yang berhubungan dengan layanan IIV. - Organisasi belum dapat menunjukan bahwa jalur komunikasi jaringan dan aliran data yang berhubungan dengan layanan IIV telah dikelola sesuai dengan persyaratan keamanan.	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Organisasi telah menyusun dokumentasi diagram jalur komunikasi jaringan dan aliran data dalam bentuk rancangan, atau dokumen diagram jalur komunikasi jaringan dan aliran data, namun baru diterapkan pada sebagian kecil aspek dan belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria. - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal.	- Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan penyusunan kebijakan atau prosedur teknis tentang dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat bukti implementasi berupa rancangan diagram jalur komunikasi jaringan dan aliran data pada sebagian aset informasi.
2	Organisasi telah menyusun dokumentasi diagram jalur komunikasi jaringan dan aliran data dalam bentuk rancangan, atau dokumen diagram jalur komunikasi jaringan dan aliran data, namun baru diterapkan pada sebagian besar aspek dan belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian aset informasi dan belum menyeluruh kepada seluruh aset informasi yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	- Draf kebijakan atau pedoman internal tentang mekanisme penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat bukti implementasi berupa rancangan diagram jalur komunikasi jaringan dan aliran data pada sebagian aset informasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
3	Organisasi telah menyusun dokumentasi diagram jalur komunikasi jaringan dan aliran data dalam bentuk rancangan, atau dokumen diagram jalur komunikasi jaringan dan aliran data, sudah diterapkan pada seluruh aspek dan sudah diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh jaringan dan data yang terhubung dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, sudah terdokumentasi secara formal.	- terdapat kebijakan yang mengatur tentang mekanisme penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa diagram jalur komunikasi jaringan dan aliran data pada sebagian aset informasi.
4	Organisasi telah menyusun dokumentasi diagram jalur komunikasi jaringan dan aliran data dalam bentuk rancangan, atau dokumen diagram jalur komunikasi jaringan dan aliran data, sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh jaringan dan data yang terhubung dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, sudah terdokumentasi secara formal. - telah dilakukan monitoring dan reviu terhadap diagram aliran jaringan dan data secara berkala.	- terdapat kebijakan yang mengatur tentang mekanisme penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa diagram jalur komunikasi jaringan dan aliran data pada seluruh layanan IIV. - terdapat bukti hasil monitoring dan reviu terhadap diagram aliran jaringan dan data secara berkala
5	Organisasi telah menyusun dokumentasi diagram jalur komunikasi jaringan dan aliran data dalam bentuk rancangan, atau dokumen diagram jalur komunikasi jaringan dan aliran data, sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan secara berkelanjutan	- Organisasi sudah memiliki pemahaman yang cukup mengenai diagram jalur komunikasi jaringan dan aliran data, dan telah diterapkan pada seluruh aspek. Misalnya, penerapan sudah dilakukan pada seluruh aset informasi yang berhubungan dengan layanan IIV (perangkat keras, perangkat lunak, dan saran pendukung lainnya). - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan telah terdokumentasi secara formal. - terdapat mekanisme pengawasan dan peninjauan yang dilakukan secara berkala - telah dilakukan kegiatan evaluasi terhadap mekanisme penyusunan diagram jalur komunikasi jaringan dan aliran data pada organisasi.	- terdapat kebijakan atau pedoman teknis yang mengatur penyusunan diagram jalur komunikasi jaringan dan aliran data organisasi. - terdapat pedoman dan SOP yang mendukung tata laksana tersebut - terdapat bukti implementasi berupa diagram jalur komunikasi jaringan dan aliran data pada seluruh layanan IIV. - terdapat bukti hasil monitoring dan reviu terhadap diagram aliran jaringan dan data secara berkala - terdapat bukti telah dilakukan kegiatan evaluasi untuk perbaikan berkelanjutan terhadap mekanisme penyusunan diagram jalur komunikasi jaringan dan aliran data organisasi.

1.3.3. Menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengidentifikasi dan mendokumentasikan sistem informasi eksternal yang digunakan oleh organisasi, dan juga sistem elektronik eksternal yang terhubung dan menggunakan data yang dikelola oleh organisasi. Tujuannya adalah agar organisasi secara aktif mengelola (inventaris, melacak, dan mengoreksi) semua perangkat lunak (sistem operasi dan aplikasi) milik eksternal yang terhubung pada organisasi sehingga hanya perangkat lunak yang sah saja yang dapat menerima layanan. Organisasi memverifikasi dukungan perangkat lunak tersebut secara berkala.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan memelihara katalog, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan katalog yang lengkap, organisasi dapat mengelola interaksi dengan sistem eksternal dan mengurangi risiko kebocoran atau penyalahgunaan data.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengelola dan memperbarui katalog secara berkala.
Referensi Kontrol	**NIST CSF 2.0: ID.AM-04** **NIST CSF 1.1: ID.AM-4** **NIST SP 800-53r5: AC-20, PM-5, SA-9** **SNI ISO/IEC 27001:2022: 7.9**

16 Kontrol 1.3.3.a:

Kontrol	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang menggunakan data atau layanan IIV
Deskripsi Kontrol	Organisasi menetapkan dan mengelola inventaris sistem elektronik milik penyedia layanan yang terhubung ke IIV. Inventaris ini harus mencantumkan semua penyedia layanan yang diketahui, termasuk klasifikasinya, beserta kontak perusahaan untuk setiap penyedia layanan. Tinjau dan perbarui inventaris setiap tahun, atau ketika terjadi perubahan signifikan di perusahaan yang dapat mempengaruhi layanan IIV. Klasifikasikan penyedia layanan. dengan mempertimbangkan hal-hal seperti sensitivitas data, volume data, persyaratan ketersediaan, peraturan yang berlaku, risiko inheren, dan risiko yang dimitigasi. Perbarui dan tinjau klasifikasi setiap tahun, atau ketika terjadi perubahan signifikan perusahaan yang dapat mempengaruhi layanan IIV ini.
Deskripsi Bukti Dukung	Kontrol ini mengharuskan organisasi untuk memiliki daftar sistem informasi eksternal yang menggunakan layanan IIV yang meliputi paling sedikit informasi mengenai fungsi sistem informasi eksternal tersebut, port yang digunakan, layanan lain yang diperlukan untuk menggunakan sistem eksternal tersebut, layanan lain yang menggunakan sistem eksternal tersebut, dll. Organisasi harus memastikan sistem eksternal yang menggunakan layanan IIV telah memenuhi semua persyaratan keamanan, pemantauan, dan pelaporan organisasi sebelum digunakan. organisasi juga melakukan penilaian tahunan terhadap semua sistem eksternal untuk memastikan mereka tetap sesuai dengan standar organisasi dan catat hasilnya.
Ancaman/Risiko yang dimitigasi	TH013 TH029 TH035 TH040 TH049 TH054 TH059 TH061 TH067 TH077 TH025 TH030 TH039 TH041 TH053 TH058 TH060 TH066 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-04** **NIST CSF 1.1: ID.AM-4** **NIST SP 800-53r5: AC-20, PM-5, SA-9** **SNI ISO/IEC 27001:2022: 7.9**

Kriteria Pemenuhan Kontrol 1.3.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Organisasi telah melaksanakan dokumentasi dan pengelolaan terhadap sebagian kecil aspek dari daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV namun belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV, namun belum mengimplementasikannya. - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal.	- Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan penyusunan kebijakan atau prosedur teknis tentang dokumentasi diagram jalur komunikasi jaringan dan aliran data. - belum terdapat bukti implementasi berupa rancangan diagram jalur komunikasi jaringan dan aliran data pada sebagian aset informasi.
2	Organisasi telah melaksanakan dokumentasi dan pengelolaan terhadap sebagian besar daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV namun belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya dilakukan pada sebagian sistem elektronik eksternal dan belum menyeluruh kepada seluruh sistem elektronik eksternal yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	- Draf kebijakan atau pedoman internal tentang mekanisme penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang terhubung ke layanan IIV namun belum pernah direviu dan diformalkan oleh manajemen organisasi.
3	Organisasi telah melaksanakan dokumentasi dan pengelolaan terhadap seluruh daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV dan sudah diformalkan	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV, dan telah diterapkan pada seluruh aspek. Penerapan telah ilakukan pada seluruh sistem elektronik eksternal yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang terhubung ke layanan IIV dan diformalkan oleh manajemen organisasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		terdokumentasi secara formal dan disetujui oleh manajemen.	
4	Organisasi telah melaksanakan dokumentasi dan pengelolaan terhadap seluruh daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV, dan telah diterapkan pada seluruh aspek. Penerapan telah dilakukan pada seluruh sistem elektronik eksternal yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah terdokumentasi secara formal dan disetujui oleh manajemen.	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang terhubung ke layanan IIV dan diformalkan oleh manajemen organisasi. - terdapat bukti bahwa daftar sistem elektronik eksternal yang terhubung ke layanan IIV telah dilakukan peninjauan secara berkala oleh pihak manajemen.
5	Organisasi telah melaksanakan dokumentasi dan pengelolaan terhadap seluruh daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala, dievaluasi dan dilakukan perbaikan secara berkelanjutan	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV, dan telah diterapkan pada seluruh aspek. Penerapan telah dilakukan pada seluruh sistem elektronik eksternal yang berhubungan dengan layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah terdokumentasi secara formal dan disetujui oleh manajemen.	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang menggunakan data atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang terhubung ke layanan IIV dan diformalkan oleh manajemen organisasi. - terdapat bukti bahwa daftar sistem elektronik eksternal yang terhubung ke layanan IIV telah dilakukan peninjauan secara berkala oleh pihak manajemen. - terdapat bukti bahwa mekanisme penyusunan daftar sistem elektronik eksternal yang terhubung ke layanan IIV telah dilakukan evaluasi untuk perbaikan berkelanjutan.

17 Kontrol 1.3.3.b:

Kontrol	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang digunakan oleh penyelenggara IIV.
Deskripsi Kontrol	Mendokumentasikan dan mengelola daftar sistem informasi eksternal yang digunakan oleh Penyelenggara IIV adalah langkah penting untuk memastikan bahwa seluruh sistem eksternal yang berinteraksi dengan operasional Layanan IIV tercatat dan dikelola dengan baik. Sistem eksternal ini bisa mencakup aplikasi pihak ketiga, platform cloud, atau layanan yang memberikan dukungan terhadap infrastruktur dan layanan IIV. Pengelolaan yang tepat akan membantu dalam memantau risiko yang terkait dengan penggunaan sistem eksternal, memastikan bahwa data dan layanan IIV dilindungi dengan baik, serta mendukung kepatuhan terhadap regulasi yang berlaku. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menyusun dan mengelola daftar yang akurat mengenai sistem eksternal yang digunakan dalam operasional Layanan IIV dan apakah kontrol terhadap sistem-sistem tersebut telah diterapkan dengan tepat.
Deskripsi Bukti Dukung	Kontrol ini mengharuskan organisasi untuk memiliki daftar sistem informasi eksternal yang digunakan oleh organisasi yang meliputi paling sedikit informasi mengenai fungsi sistem informasi eksternal tersebut, port yang digunakan, dan layanan lain yang diperlukan untuk menggunakan sistem eksternal tersebut. Organisasi harus memastikan sistem eksternal yang digunakan oleh organisasi IIV telah memenuhi semua persyaratan keamanan, pemantauan, dan pelaporan organisasi sebelum digunakan. organisasi juga melakukan penilaian tahunan terhadap semua sistem eksternal untuk memastikan mereka tetap sesuai dengan standar organisasi dan catat hasilnya.
Ancaman/Risiko yang dimitigasi	TH013 TH029 TH035 TH040 TH049 TH054 TH059 TH061 TH067 TH071 TH025 TH030 TH039 TH041 TH053 TH058 TH060 TH066 TH070 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.AM-04** **NIST CSF 1.1: ID.AM-4** **NIST SP 800-53r5: AC-20, PM-5, SA-9** **SNI ISO/IEC 27001:2022: 7.9**

Kriteria Pemenuhan Kontrol 1.3.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki daftar sistem informasi eksternal apa saja yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV	Tidak ada kriteria (belum ada kebijakan maupun komitmen pimpinan)	Tidak ada bukti pendukung
1	Organisasi telah melaksanakan dokumentasi dan pengelolaan yang tepat terhadap sebagian kecil aspek dari daftar sistem informasi eksternal yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV, tapi belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV, namun belum mengimplementasikannya. - Belum terdapat kebijakan yang bersifat ad-hoc dan belum terdokumentasi secara formal.	- Catatan rapat atau notulen internal yang menunjukkan adanya pembahasan penyusunan kebijakan atau prosedur teknis tentang dokumentasi diagram jalur komunikasi jaringan dan aliran data. - belum terdapat bukti implementasi berupa rancangan diagram jalur komunikasi jaringan dan aliran data pada sebagian aset informasi.
2	Organisasi telah melaksanakan dokumentasi dan pengelolaan yang tepat terhadap sebagian besar aspek dari daftar sistem informasi eksternal yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV, tapi belum diformalkan	- Organisasi sudah memiliki pemahaman yang cukup mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi da/atau layanan IIV, dan telah diterapkan pada sebagian aspek. Misalnya, penerapan hanya mencantumkan daftar pada sebagian sistem elektronik eksternal dan belum menyeluruh kepada seluruh sistem elektronik eksternal yang digunakan oleh organisasi da/atau layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, namun belum terdokumentasi secara formal. misalnya, masih dalam berupa draft kebijakan.	- Draf kebijakan atau pedoman internal tentang mekanisme penyusunan dokumentasi diagram jalur komunikasi jaringan dan aliran data. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang terhubung ke layanan IIV namun belum pernah direviu dan diformalkan oleh manajemen organisasi.
3	Organisasi telah melaksanakan dokumentasi dan pengelolaan yang tepat terhadap seluruh aspek dari daftar sistem informasi eksternal yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV, dan sudah diformalkan	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV, dan telah diterapkan pada seluruh aspek. yaitu, penerapan telah dilakukan pada seluruh sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang digunakan organisasi dan/atau layanan IIV dan diformalkan oleh manajemen organisasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		- Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah terdokumentasi secara formal dan disetujui oleh manajemen.	
4	Organisasi telah melaksanakan dokumentasi dan pengelolaan yang tepat terhadap seluruh aspek dari daftar sistem informasi eksternal yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV, dan sudah diformalkan, sudah dilakukan monitoring dan direviu secara berkala	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV, dan telah diterapkan pada seluruh aspek. Penerapan telah dilakukan pada seluruh sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah terdokumentasi secara formal dan disetujui oleh manajemen.	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV dan diformalkan oleh manajemen organisasi. - terdapat bukti bahwa daftar sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV telah dilakukan peninjauan secara berkala oleh pihak manajemen.
5	Organisasi telah melaksanakan dokumentasi dan pengelolaan yang tepat terhadap seluruh aspek dari daftar sistem informasi eksternal yang digunakan untuk mendukung penyelenggara IIV dalam menjalankan layanan IIV, dan sudah diformalkan, sudah dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan secara berkelanjutan dan mekanisme otomatisasi diterapkan	- Organisasi sudah memiliki pemahaman yang baik mengenai tata laksana penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV, dan telah diterapkan pada seluruh aspek. Penerapan telah dilakukan pada seluruh sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - Pimpinan organisasi sudah menunjukan komitmen dalam pemenuhan kriteria - Terdapat kebijakan atau pedoman teknis yang bersifat ad-hoc yang berlaku dalam lingkup tertentu, dan sudah terdokumentasi secara formal dan disetujui oleh manajemen.	- kebijakan atau pedoman teknis internal tentang mekanisme penyusunan daftar sistem informasi stakeholder dan pihak eksternal yang digunakan oleh organisasi dan/atau layanan IIV. - terdapat bukti implementasi berupa daftar sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV dan diformalkan oleh manajemen organisasi. - terdapat bukti bahwa daftar sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV telah dilakukan peninjauan secara berkala oleh pihak manajemen. - terdapat bukti bahwa mekanisme penyusunan daftar sistem elektronik eksternal yang digunakan oleh organisasi dan/atau layanan IIV telah dilakukan evaluasi untuk perbaikan berkelanjutan.

1.3.4. Menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya

Kriteria	Detail
Deskripsi	Penyelenggara IIV mendokumentasikan daftar aset informasi yang prioritas dalam perlindungan berdasarkan klasifikasi informasi, nilai bisnis dan tingkat dampak kerusakannya bagi layanan IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan evaluasi aset informasi, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan prioritas yang jelas, organisasi dapat mengelola sumber daya dan risiko dengan lebih efektif, serta melindungi aset yang paling kritis.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif dan perencanaan untuk menyusun prioritas yang sesuai
Referensi Kontrol	**NIST CSF 2.0: ID.AM-05** **NIST CSF 1.1: ID.AM-5** **NIST SP 800-53r5: CP-2, RA-2, RA-9, SA-20, SC-6** **SNI ISO/IEC 27001:2022: 5.12**

18 Kontrol 1.3.4.a:

Kontrol	Mengklasifikasikan dan memprioritaskan aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis
Deskripsi Kontrol	Mengklasifikasikan dan memprioritaskan aset informasi merupakan langkah awal yang penting bagi penyelenggara infrastruktur informasi vital (IIV). Kontrol ini bertujuan untuk memastikan bahwa organisasi secara sistematis mengidentifikasi, mengklasifikasikan, dan memprioritaskan aset informasi, termasuk perangkat keras, perangkat lunak, data, dan layanan TIK, berdasarkan fungsi, tingkat kekritisan, dan nilai bisnisnya. Dengan pendekatan ini, organisasi dapat mengelola risiko keamanan secara efektif, memastikan perlindungan aset yang paling vital, serta mendukung keberlanjutan operasional dan kepatuhan terhadap regulasi keamanan siber. Selain itu, klasifikasi yang jelas memungkinkan organisasi menerapkan kebijakan perlindungan yang sesuai dengan tingkat risiko masing-masing aset.
Deskripsi Bukti Dukung	Agar kontrol terkait klasifikasi dan prioritisasi aset informasi dapat dianggap telah terpenuhi, organisasi perlu menyediakan berbagai bukti dokumentasi dan mekanisme teknis yang mendukung: - Kebijakan dan Prosedur Formal/Resmi, contohnya dokumen kebijakan manajemen aset informasi, prosedur klasifikasi dan prioritisasi aset, dan dokumen pengelolaan risiko aset informasi - Inventaris dan Daftar Aset Informasi, contohnya dokumen inventaris aset informasi, matriks klasifikasi aset, dan dokumen evaluasi dan penilaian risiko aset - Bukti Implementasi dan Monitoring, contohnya laporan audit keamanan aset, log dan rekaman pemantauan aset, laporan evaluasi dan reviu berkala, dan dokumentasi perbaikan berkelanjutan - Mekanisme Otomatisasi dan Teknologi Pendukung, contohnya sistem manajemen aset informasi, sistem keamanan dan monitoring otomatis, dan enkripsi dan pengendalian aset berbasis klasifikasi
Ancaman/Risiko yang dimitigasi	TH022 TH024 TH031 TH033 TH041 TH044 TH049 TH053 TH056 TH060 TH070 TH077 TH023 TH025 TH032 TH035 TH043 TH048 TH052 TH054 TH057 TH065 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-05** **NIST CSF 1.1: ID.AM-5** **NIST SP 800-53r5: CP-2, RA-2, RA-9, SA-20, SC-6** **SNI ISO/IEC 27001:2022: 5.12**

Kriteria Pemenuhan Kontrol 1.3.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki daftar aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya	Organisasi belum melakukan identifikasi aset informasi sehingga tidak memiliki dasar untuk melakukan klasifikasi dan prioritisasi. Risiko keamanan aset tidak terkelola dengan baik, yang dapat menyebabkan gangguan operasional atau kebocoran informasi.	- Tidak ada dokumen atau daftar aset informasi. - Tidak ada kebijakan atau prosedur terkait klasifikasi aset. - Tidak ada sistem atau alat bantu pencatatan aset informasi.
1	Organisasi telah melaksanakan klasifikasi dan menyusun prioritas terhadap sebagian kecil aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis, tapi belum diformalkan	Upaya awal telah dilakukan dengan mengidentifikasi dan mengklasifikasikan sebagian kecil aset informasi. Namun, karena belum diformalkan, tidak ada standar atau panduan yang dapat dijadikan acuan untuk implementasi yang lebih luas dalam organisasi.	- Daftar aset informasi awal tetapi belum mencakup semua aset organisasi. - Catatan klasifikasi aset sebagian kecil dari sistem atau layanan utama. - Tidak ada kebijakan atau prosedur tertulis yang mengatur klasifikasi aset. - Tidak ada bukti formal penerapan klasifikasi dan prioritisasi aset.
2	Organisasi telah melaksanakan klasifikasi dan menyusun prioritas terhadap sebagian besar aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis, tapi belum diformalkan	Organisasi telah melakukan klasifikasi terhadap sebagian besar aset informasi, tetapi tanpa dokumentasi resmi atau kebijakan yang mengatur secara formal. Hal ini dapat menyebabkan ketidakkonsistenan dalam penerapan klasifikasi dan prioritisasi aset.	- Daftar aset informasi yang lebih lengkap tetapi belum sepenuhnya mencakup semua aset. - Hasil klasifikasi dan prioritisasi terhadap sebagian besar aset, namun belum terdokumentasi secara formal. - Tidak ada kebijakan atau prosedur formal yang mengatur penerapan klasifikasi. - Belum ada mekanisme pemantauan atau peninjauan aset.
3	Organisasi telah melaksanakan klasifikasi dan menyusun prioritas terhadap seluruh aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis, dan sudah diformalkan	Semua aset informasi telah diidentifikasi, diklasifikasikan, dan diprioritaskan secara menyeluruh. Selain itu, klasifikasi ini telah terdokumentasi dalam kebijakan formal organisasi, memastikan kepatuhan dan konsistensi dalam penerapannya.	- Daftar aset informasi yang mencakup seluruh aset organisasi. - Kebijakan dan prosedur klasifikasi aset telah terdokumentasi secara formal. - Matriks klasifikasi aset berdasarkan fungsi, kekritisan, dan nilai bisnis. - Dokumentasi formal tentang pemetaan aset dan kepemilikan aset.
4	Organisasi telah melaksanakan klasifikasi dan menyusun prioritas terhadap seluruh aset informasi seperti, perangkat keras, perangkat	Klasifikasi dan prioritisasi aset informasi telah diimplementasikan secara menyeluruh dan terdokumentasi secara formal. Organisasi	- Semua bukti pada Indeks 3. - Log atau laporan hasil pemantauan terhadap aset informasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis, dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala	juga telah melakukan pemantauan serta peninjauan berkala untuk memastikan klasifikasi tetap relevan dan efektif terhadap perubahan lingkungan atau ancaman.	- Laporan reviu berkala terhadap klasifikasi aset. - Bukti pelaksanaan audit internal atau eksternal terkait manajemen aset.
5	Organisasi telah melaksanakan klasifikasi dan menyusun prioritas terhadap seluruh aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis, dan sudah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta mekanisme otomatisasi diterapkan	Organisasi telah mencapai tingkat kematangan tertinggi dalam pengelolaan aset informasi. Selain memiliki sistem pemantauan dan reviu berkala, evaluasi serta perbaikan berkelanjutan dilakukan untuk menyesuaikan dengan perubahan risiko. Mekanisme otomatisasi diterapkan untuk meningkatkan efisiensi dan efektivitas manajemen aset informasi.	- Semua bukti pada Indeks 4. - Bukti hasil evaluasi dan tindakan perbaikan yang telah diterapkan. - Dokumen kebijakan perbaikan berkelanjutan terkait klasifikasi aset. - Penggunaan alat bantu otomatisasi dalam pemantauan dan manajemen aset (misalnya, sistem IT Asset Management atau Security Information and Event Management).

1.3.5. Mengendalikan aset informasi milik organisasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV mendokumentasikan dan memastikan setiap aset informasi dapat ditelusur kondisinya, catatan pengadaan, catatan pemakaian, serta catatan pembaharuan aset informasi, dan pelaporannya kepada manajemen.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem kontrol dan pemantauan aset informasi, tetapi tidak selalu membutuhkan teknologi tambahan yang mahal.
Dampak	**Tinggi** – Dengan kontrol yang efektif, organisasi dapat mengurangi risiko penyalahgunaan atau kehilangan aset informasi, serta memastikan kepatuhan terhadap kebijakan keamanan.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengendalikan dan memantau aset informasi secara efektif.
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.DS-3** **NIST SP 800-53r5: CM-8, MP-6, PE-16, PE-20** **SNI ISO/IEC 27001:2022: 7.10, 7.14, 8.8**

19 Kontrol 1.3.5.a:

Kontrol	Menentukan metode untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa seluruh aset informasi, termasuk perangkat keras, perangkat lunak, data, dan layanan TIK, memiliki ketertelusuran yang jelas sejak pengadaan hingga penggunaannya dalam organisasi. Dengan adanya metode yang terstruktur, organisasi dapat mencatat informasi penting seperti tanggal produksi atau pengadaan, kondisi aset, riwayat pemakaian, serta pelaporan kepada unit kerja terkait. Ketertelusuran aset ini penting untuk mendukung pengelolaan aset yang lebih efektif, meningkatkan keamanan, mencegah kehilangan atau penyalahgunaan aset, serta memastikan kepatuhan terhadap regulasi dan kebijakan keamanan siber.
Deskripsi Bukti Dukung	Agar kontrol terkait metode untuk memastikan ketertelusuran aset informasi dapat dianggap telah terpenuhi, organisasi perlu menyediakan beberapa bukti pendukung berikut: - Dokumen inventaris aset informasi, termasuk data produksi/pengadaan, kondisi terkini, dan lokasi penyimpanan. - Catatan riwayat pemakaian aset, yang mencakup informasi pengguna, waktu penggunaan, dan perubahan status aset. - Sistem manajemen aset otomatis yang mencatat dan memantau status serta pergerakan aset secara berkala. - Laporan audit atau inspeksi aset untuk memastikan kepatuhan terhadap kebijakan dan mengidentifikasi potensi risiko terkait aset. - Dokumentasi prosedur pelaporan kepada unit kerja terkait, yang mengatur alur pelaporan perubahan status, kehilangan, atau penghapusan aset.
Ancaman/Risiko yang dimitigasi	TH022 TH025 TH032 TH034 TH043 TH046 TH048 TH053 TH071 TH023 TH031 TH033 TH035 TH044 TH047 TH052 TH054 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.DS-3** **NIST SP 800-53r5: CM-8, MP-6, PE-16, PE-20** **SNI ISO/IEC 27001:2022: 7.10, 7.14, 8.8**

Kriteria Pemenuhan Kontrol 1.3.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki metode penelusuran aset informasi	Tidak ada kebijakan, prosedur, atau sistem yang diterapkan untuk memastikan ketertelusuran aset informasi. Data aset tidak terdokumentasi, sehingga berisiko tinggi terhadap kehilangan, penyalahgunaan, atau kegagalan pelacakan aset.	- Tidak ada dokumen atau sistem yang mencatat aset informasi. - Tidak terdapat kebijakan atau prosedur terkait ketertelusuran aset. - Tidak ada catatan mengenai pengadaan, kondisi, pemakaian, atau pelaporan aset.
1	Organisasi telah menerapkan metode pada sebagian kecil aspek untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait, tapi belum diformalkan	Beberapa aset informasi telah memiliki pencatatan terbatas, tetapi belum mencakup seluruh jenis aset atau aspek penting lainnya. Tidak ada kebijakan atau prosedur formal yang mengatur ketertelusuran aset, sehingga pencatatan dilakukan secara ad-hoc tanpa standar yang jelas.	- Terdapat pencatatan aset yang masih terbatas pada beberapa kategori aset. - Tidak ada standar pencatatan yang seragam. - Bukti berupa catatan manual atau daftar aset tidak resmi.
2	Organisasi telah menerapkan metode pada sebagian besar aspek untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait, dan belum diformalkan	Pencatatan telah dilakukan untuk sebagian besar aset informasi dengan aspek ketertelusuran yang lebih lengkap, tetapi belum ada standarisasi dan dokumentasi formal. Beberapa aset mungkin masih belum memiliki rekaman penggunaan atau pelaporan yang terdokumentasi dengan baik.	- Terdapat daftar aset yang lebih lengkap tetapi belum terdokumentasi secara formal. - Catatan mencakup sebagian besar aset tetapi masih memiliki kekurangan dalam aspek tertentu seperti pemakaian atau pelaporan. - Tidak ada mekanisme evaluasi atau verifikasi pencatatan.
3	Organisasi telah menerapkan metode pada seluruh aspek untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait, dan telah diformalkan	Seluruh aset informasi memiliki pencatatan yang mencakup aspek-aspek penting seperti tanggal pengadaan, kondisi, riwayat pemakaian, dan pelaporan. Kebijakan dan prosedur formal telah ditetapkan, memastikan standar yang seragam dalam pencatatan aset.	- Dokumen kebijakan dan prosedur pengelolaan aset telah tersedia dan disahkan. - Catatan aset mencakup semua aspek (pengadaan, kondisi, pemakaian, pelaporan). - Ada sistem terstruktur, baik manual maupun digital, untuk pencatatan aset.
4	Organisasi telah menerapkan metode pada seluruh aspek untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Penerapan metode ketertelusuran sudah menjadi bagian dari proses operasional organisasi, dengan monitoring dan reviu berkala untuk memastikan keakuratan data. Ada mekanisme audit yang memungkinkan identifikasi kelemahan atau ketidaksesuaian dalam pencatatan aset.	- Terdapat mekanisme monitoring berkala terhadap aset, dibuktikan dengan laporan audit atau inspeksi. - Sistem pencatatan aset sudah diperiksa secara rutin untuk memastikan akurasi data. - Laporan pemakaian dan kondisi aset tersedia untuk unit kerja terkait.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi telah menerapkan metode pada seluruh aspek untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilaksanakan evaluasi dan perbaikan berkelanjutan serta diterapkan mekanisme otomatisasi	Organisasi telah menerapkan sistem yang sepenuhnya terdokumentasi dan terotomatisasi untuk memastikan ketertelusuran aset. Monitoring, evaluasi, dan perbaikan dilakukan secara berkelanjutan dengan dukungan alat bantu otomatisasi, seperti sistem manajemen aset berbasis teknologi yang memungkinkan pemantauan real-time dan pelaporan yang lebih akurat.	- Sistem pencatatan aset telah menggunakan mekanisme otomatisasi berbasis teknologi (misalnya, sistem manajemen aset atau database terintegrasi). - Hasil evaluasi dan perbaikan terdokumentasi dan dilakukan secara berkala. - Ada laporan audit berkala yang menunjukkan peningkatan efektivitas sistem pencatatan aset. - Notifikasi otomatis untuk pemeliharaan atau pelaporan aset diterapkan.

20 Kontrol 1.3.5.b:

Kontrol	Secara aktif memeriksa keterbaharuan dan memperbaharui dari setiap versi perangkat lunak dan perangkat keras yang digunakan oleh organisasi.
Deskripsi Kontrol	Pemeriksaan keterbaharuan dan pembaruan perangkat lunak serta perangkat keras merupakan langkah penting dalam menjaga keamanan siber suatu organisasi. Perangkat lunak dan perangkat keras yang usang atau tidak diperbarui dapat menjadi celah bagi serangan siber, eksploitasi, dan kerentanan keamanan. Oleh karena itu, organisasi harus memiliki mekanisme yang aktif untuk memantau versi terbaru perangkat lunak dan perangkat keras yang digunakan serta memastikan bahwa pembaruan keamanan dan fitur diterapkan secara tepat waktu.
Deskripsi Bukti Dukung	Untuk memastikan kontrol ini terpenuhi, organisasi perlu menyediakan bukti pendukung yang dapat menunjukkan bahwa pemeriksaan dan pembaruan dilakukan secara aktif dan terdokumentasi. Berikut adalah beberapa bukti dukung yang dapat digunakan: - Daftar Inventaris Perangkat Lunak dan Perangkat Keras - Laporan Pemantauan dan Pemberitahuan Pembaruan - Dokumentasi Jadwal Pembaruan - Log Aktivitas Pembaruan - Hasil Evaluasi Dampak Pembaruan - Mekanisme Otomatisasi Pembaruan - Dokumen Kebijakan dan Prosedur Pembaruan
Ancaman/Risiko yang dimitigasi	TH021 TH023 TH025 TH039 TH046 TH048 TH053 TH065 TH071 TH022 TH024 TH036 TH040 TH047 TH052 TH054 TH070 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.DS-3** **NIST SP 800-53r5: CM-8, MP-6, PE-16, PE-20** **SNI ISO/IEC 27001:2022: 7.10, 7.14, 8.8**

Kriteria Pemenuhan Kontrol 1.3.5.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum pernah memeriksa versi perangkat lunak dan perangkat keras, serta keterbaharuan dari perangkat lunak dan perangkat keras tersebut.	Organisasi belum memiliki mekanisme untuk memeriksa versi dan keterbaharuan perangkat lunak serta perangkat keras yang digunakan. Tidak ada dokumentasi atau kebijakan terkait pemantauan versi perangkat.	- Tidak ada dokumentasi terkait pemeriksaan versi perangkat lunak dan perangkat keras. - Tidak terdapat kebijakan atau prosedur terkait pemantauan keterbaharuan sistem. - Tidak ada bukti bahwa organisasi melakukan pembaruan perangkat.
1	Organisasi telah memeriksa versi pada sebagian kecil perangkat lunak dan perangkat keras, serta keterbaharuannya dari sebagian kecil perangkat-perangkat tersebut yang digunakan oleh organisasi, namun belum diformalkan	Organisasi telah melakukan pemeriksaan pada sebagian kecil perangkat lunak dan perangkat keras, tetapi belum ada proses formal yang terdokumentasi. Pemantauan masih bersifat sporadis dan tidak terjadwal.	- Laporan atau catatan manual terkait pemeriksaan versi pada sebagian kecil perangkat. - Bukti bahwa beberapa perangkat telah diperiksa, tetapi tidak ada mekanisme formal yang terdokumentasi. - Tidak ada kebijakan formal terkait pembaruan sistem.
2	Organisasi telah memeriksa versi pada sebagian besar perangkat lunak dan perangkat keras, serta keterbaharuannya dari sebagian besar perangkat-perangkat tersebut yang digunakan oleh organisasi, namun belum diformalkan	Organisasi telah melakukan pemeriksaan versi dan keterbaharuan pada sebagian besar perangkat lunak dan perangkat keras, namun belum diformalkan. Proses pemantauan dilakukan secara manual dan tidak konsisten di seluruh aset TI.	- Laporan atau catatan pemeriksaan versi pada sebagian besar perangkat. - Dokumentasi awal terkait pemantauan keterbaharuan perangkat. - Bukti adanya pembaruan perangkat lunak atau perangkat keras yang dilakukan secara parsial.
3	Organisasi telah memeriksa versi pada seluruh perangkat lunak dan perangkat keras, serta keterbaharuannya dari seluruh perangkat-perangkat tersebut yang digunakan oleh organisasi, dan telah diformalkan	Organisasi telah melakukan pemeriksaan pada seluruh perangkat lunak dan perangkat keras yang digunakan. Proses ini telah diformalkan melalui kebijakan dan prosedur yang terdokumentasi dengan baik.	- Kebijakan dan prosedur formal terkait pemeriksaan versi dan pembaruan perangkat lunak serta perangkat keras. - Laporan pemeriksaan dan pembaruan perangkat lunak dan perangkat keras secara menyeluruh. - Daftar perangkat yang digunakan organisasi beserta versinya
4	Organisasi telah memeriksa versi pada seluruh perangkat lunak dan perangkat keras, serta keterbaharuannya dari seluruh perangkat-perangkat tersebut yang digunakan oleh organisasi, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Organisasi telah menerapkan pemeriksaan versi dan keterbaharuan untuk seluruh perangkat lunak dan perangkat keras, serta telah melakukan monitoring dan reviu secara berkala untuk memastikan keamanan dan kepatuhan.	- Bukti pelaksanaan pemeriksaan versi yang dilakukan secara berkala. - Dokumentasi proses monitoring keterbaharuan perangkat lunak dan perangkat keras. - Laporan hasil reviu berkala terkait versi perangkat dan rekomendasi pembaruan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi telah memeriksa versi pada seluruh perangkat lunak dan perangkat keras, serta keterbaharuannya dari seluruh perangkat-perangkat tersebut yang digunakan oleh organisasi, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta menerapkan mekanisme otomatisasi	Organisasi telah memastikan pemeriksaan dilakukan pada seluruh perangkat lunak dan perangkat keras, diformalkan, serta dilakukan monitoring dan reviu secara berkala. Selain itu, evaluasi dan perbaikan terus-menerus dilakukan, serta telah diterapkan mekanisme otomatisasi untuk pemantauan dan pembaruan.	- Mekanisme otomatisasi untuk pemeriksaan dan pembaruan versi perangkat lunak serta perangkat keras (misalnya, sistem manajemen aset TI, patch management system). - Laporan hasil evaluasi dan perbaikan berkelanjutan terkait pembaruan sistem. - Dokumentasi kebijakan pembaruan dan pemantauan versi perangkat yang diterapkan dengan sistem otomatis.

1.4. Menilai dan mengelola risiko Keamanan Siber

Penyelenggara IIV memahami risiko keamanan siber terhadap pengoperasian layanan IIV, meliputi potensi risiko terhadap ketersediaan layanan, citra atau reputasi, keberlangsungan aset penyelenggara IIV, dan keselamatan individu. Serta menentukan prioritas, rintangan, toleransi risiko, dan pertimbangan lainnya yang perlu ditetapkan untuk mendukung keputusan risiko organisasi.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi;
b) mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal;
c) mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut;
d) menganalisis nilai risiko terhadap IIV;
e) mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko;
f) menentukan dan mengomunikasikan toleransi risiko organisasi;
g) mengelola hasil penerapan manajemen risiko yang telah ditetapkan; dan
h) melakukan reviu terhadap hasil penerapan manajemen risiko.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Menilai dan mengelola risiko Keamanan Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-01, GV.RM-02, GV.RM-04, GV.RM-06, GV.RR-03**
NIST CSF 1.1	**:**	**ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-1, ID.RM-2, ID.RM-3**
NIST SP 800-53r5	**:**	**CA-2, CA-5, CA-7, CA-8, CP-2, PM-4, PM-8, PM-9, PM-11, PM-12, PM-15, PM-16, PM-28, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, SA-5, SA-11, SI-2, SI-4, SI-5**
SNI ISO/IEC 27001:2022	**:**	**5.7, 8.8, 8.16**

1.4.1. Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi.

Kriteria	Detail
Deskripsi	Penyelenggara IIV mampu mengidentifikasi kerentanan pada seluruh aset informasi yang ada di organisasi, serta mendokumentasikan daftar kerentanan yang teridentifikasi tersebut berdasarkan aset informasi terkait.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk melakukan penilaian kerentanan, tetapi tidak selalu membutuhkan teknologi tambahan yang mahal.
Dampak	**Tinggi** – Dengan mengetahui kerentanan, organisasi dapat mengambil langkah-langkah untuk mengatasi kelemahan tersebut dan mengurangi risiko serangan.
Kompleksitas	**Sedang** – Memerlukan alat dan prosedur yang tepat untuk mengidentifikasi dan mendokumentasikan kerentanan secara efektif
Referensi Kontrol	**NIST CSF 2.0: ID.RA-01** **NIST CSF 1.1: ID.RA-1** **NIST SP 800-53r5: CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5** **SNI ISO/IEC 27001:2022: 8.8**

21 Kontrol 1.4.1.a:

Kontrol	Identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui penetration testing dan vulnerability assessment, serta dokumentasikan daftar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa organisasi memiliki pemahaman yang komprehensif tentang potensi kerentanan yang ada dalam aset informasi mereka. Identifikasi kerentanan dilakukan melalui metode seperti penetration testing dan vulnerability assessment, yang bertujuan untuk mengungkap kelemahan dalam sistem, jaringan, dan aplikasi yang dapat dieksploitasi oleh pihak tidak berwenang. Hasil dari identifikasi ini kemudian harus terdokumentasi dengan baik dalam daftar kerentanan yang mencantumkan aset terkait, sehingga organisasi dapat merencanakan tindakan mitigasi dan perbaikan yang sesuai.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - Dokumentasi Hasil Penilaian Kerentanan: Laporan hasil vulnerability assessment, Laporan hasil penetration testing - Daftar Aset dan Kerentanannya - Kebijakan dan Prosedur Manajemen Kerentanan - Rencana Tindakan Perbaikan (Remediation Plan) - Laporan Monitoring dan Reviu Berkala
Ancaman/Risiko yang dimitigasi	TH021 TH023 TH025 TH029 TH035 TH037 TH039 TH043 TH046 TH048 TH053 TH065 TH077 TH022 TH024 TH027 TH030 TH036 TH038 TH040 TH044 TH047 TH052 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.RA-01** **NIST CSF 1.1: ID.RA-1** **NIST SP 800-53r5: CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melaksanakan identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui penetration testing dan vulnerability assessment, serta belum memiliki daftar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait.	Organisasi belum memiliki langkah apa pun untuk mengidentifikasi kerentanan pada aset informasi. Tidak ada bukti pendukung yang menunjukkan adanya upaya dalam asesmen atau mitigasi kerentanan.	- Tidak ada dokumentasi terkait asesmen kerentanan. - Tidak ada laporan penetration testing atau vulnerability assessment. - Tidak ada daftar aset dan daftar kerentanan terkait.
1	Organisasi telah melaksanakan identifikasi kerentanan terhadap sebagian kecil aset informasi di organisasi, dan melaksanakan dokumentasi terhadap sebagian kecil kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait, tapi belum diformalkan	Organisasi mulai melakukan identifikasi kerentanan secara terbatas namun belum memiliki prosedur atau kebijakan formal. Langkah awal telah diambil, tetapi belum menyeluruh.	- Laporan awal identifikasi kerentanan terhadap sebagian kecil aset. - Daftar aset dengan sebagian kecil kerentanannya. - Tidak ada kebijakan atau prosedur formal terkait identifikasi kerentanan.
2	Organisasi telah melaksanakan identifikasi kerentanan terhadap sebagian besar aset informasi di organisasi, dan melaksanakan dokumentasi terhadap sebagian besar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait, namun belum diformalkan	Organisasi telah memiliki cakupan asesmen yang lebih luas, namun masih belum sepenuhnya formal. Masih diperlukan penguatan kebijakan dan dokumentasi agar lebih terstruktur.	- Laporan asesmen kerentanan terhadap sebagian besar aset. - Daftar aset dengan sebagian besar kerentanannya. - Tidak ada kebijakan formal yang mengatur asesmen kerentanan secara menyeluruh.
3	Organisasi telah melaksanakan identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui penetration testing dan vulnerability assessment, dan melaksanakan dokumentasi terhadap seluruh daftar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait, dan telah diformalkan	Organisasi telah memenuhi standar dasar dengan cakupan asesmen penuh terhadap seluruh aset informasi serta dokumentasi yang telah diformalkan.	- Laporan penetration testing dan vulnerability assessment terhadap seluruh aset. - Daftar aset dengan seluruh kerentanannya. - Kebijakan dan prosedur formal terkait asesmen kerentanan.
4	Organisasi telah melaksanakan identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui penetration testing dan vulnerability assessment, dan melaksanakan dokumentasi terhadap seluruh daftar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Organisasi telah mencapai tingkat pemenuhan yang lebih tinggi dengan monitoring dan reviu berkala untuk memastikan keamanan sistem secara terus-menerus.	- Laporan penetration testing dan vulnerability assessment yang dilakukan secara berkala. - Daftar aset dengan daftar kerentanannya yang diperbarui secara berkala. - Kebijakan dan prosedur formal yang mencakup mekanisme monitoring dan reviu periodik.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi telah melaksanakan identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui penetration testing dan vulnerability assessment, dan melaksanakan dokumentasi terhadap seluruh daftar kerentanan yang teridentifikasi tersebut bersama dengan daftar aset terkait, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta menerapkan mekanisme otomatisasi	Organisasi telah mencapai tingkat pemenuhan tertinggi dengan penerapan evaluasi berkelanjutan serta otomatisasi dalam pemantauan dan mitigasi kerentanan. Sistem keamanan berjalan secara efisien dan adaptif.	- Laporan asesmen kerentanan yang mencerminkan evaluasi berkelanjutan dan perbaikan sistematis. - Daftar aset dan kerentanan yang diperbarui otomatis melalui mekanisme pemantauan berbasis alat keamanan siber. - Implementasi sistem manajemen kerentanan berbasis otomatisasi. - Kebijakan dan prosedur yang mencakup evaluasi dan pembaruan berkelanjutan.

1.4.2. Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal

Kriteria	Detail
Deskripsi	Penyelenggara IIV mampu mengumpulkan dan menganalisis informasi-informasi kerentanan dan ancaman keamanan siber, baik yang bersumber dari internal maupun eksternal (misalnya melalui pengujian internal, informasi dari pihak berwajib, peneliti keamanan, dll), yang berpotensi mengganggu layanan IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis informasi dan sumber daya untuk mengumpulkan serta mendokumentasikan informasi dari berbagai sumber.
Dampak	**Tinggi** – Dengan informasi yang lengkap, organisasi dapat lebih siap dalam menghadapi ancaman dan mengurangi risiko serangan.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur untuk mengumpulkan, menganalisis, dan mendokumentasikan informasi terkait ancaman dan kerentanan.
Referensi Kontrol	**NIST CSF 2.0: ID.RA-02, ID.RA-03** **NIST CSF 1.1: ID.RA-2, ID.RA-3** **NIST SP 800-53r5: PM-12, PM-15, PM-16, RA-3, RA-10, SI-5** **SNI ISO/IEC 27001:2022: 5.7, 8.16**

22 Kontrol 1.4.2.a:

Kontrol	Penyelenggara IIV mengumpulkan informasi termasuk kerentanan dan ancaman dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.)
Deskripsi Kontrol	Penyelenggara Infrastruktur Informasi Vital (IIV) harus secara aktif mengumpulkan informasi terkait kerentanan dan ancaman dari berbagai sumber internal maupun eksternal. Informasi ini dapat diperoleh melalui berbagai metode, seperti pengujian keamanan internal (penetration testing, vulnerability assessment), laporan dari pihak berwajib, hasil penelitian keamanan, serta intelijen ancaman dari komunitas keamanan siber. Tujuan utama dari kontrol ini adalah untuk memastikan bahwa organisasi memiliki pemahaman yang komprehensif mengenai ancaman dan kerentanan yang dapat berdampak pada aset informasi mereka, sehingga dapat mengambil langkah mitigasi yang tepat sebelum terjadi insiden keamanan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumentasi Hasil Penilaian Kerentanan: Laporan hasil vulnerability assessment, Laporan hasil penetration testing, Rekapitulasi audit keamanan internal - Dokumentasi Sumber Informasi Ancaman dan Kerentanan: Laporan atau notifikasi dari lembaga keamanan siber (CERT, BSSN, dll.), Publikasi laporan CVE, Dokumentasi hasil analisis insiden keamanan sebelumnya - Daftar Aset dan Kerentanannya - Kebijakan dan Prosedur Pengelolaan Informasi Ancaman - Dokumentasi Monitoring dan Reviu Keamanan
Ancaman/Risiko yang dimitigasi	TH021 TH023 TH027 TH030 TH036 TH038 TH040 TH046 TH049 TH054 TH071 TH022 TH025 TH029 TH035 TH037 TH039 TH041 TH047 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-02, ID.RA-03** **NIST CSF 1.1: ID.RA-2, ID.RA-3** **NIST SP 800-53r5: PM-12, PM-15, PM-16, RA-3, RA-10, SI-5** **SNI ISO/IEC 27001:2022: 5.7, 8.16**

Kriteria Pemenuhan Kontrol 1.4.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk mengumpulkan informasi tentang kerentanan dan ancaman dari sumber internal dan eksternal. Tidak ada upaya yang dilakukan untuk merencanakan atau mengimplementasikan aktivitas tersebut.	Organisasi belum memiliki langkah apa pun untuk mengumpulkan informasi terkait kerentanan dan ancaman. Tidak ada bukti pendukung yang menunjukkan adanya upaya dalam pengumpulan informasi keamanan.	- Tidak ada dokumentasi atau laporan terkait pengumpulan informasi ancaman dan kerentanan. - Tidak ada mekanisme pengumpulan informasi dari sumber internal maupun eksternal.
1	Organisasi telah melaksanakan pengumpulan informasi termasuk kerentanan dan ancaman pada sebagian kecil aspek dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.), namun belum diformalkan	Organisasi mulai mengumpulkan informasi kerentanan dan ancaman secara terbatas, namun belum memiliki prosedur atau kebijakan formal. Langkah awal telah diambil, tetapi belum menyeluruh.	- Laporan awal pengumpulan informasi ancaman dan kerentanan terhadap sebagian kecil aspek. - Data awal dari hasil pengujian internal atau sumber eksternal yang belum terstruktur. - Tidak ada kebijakan atau prosedur formal terkait pengumpulan informasi ancaman.
2	Organisasi telah melaksanakan pengumpulan informasi termasuk kerentanan dan ancaman pada sebagian besar aspek dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.), namun belum diformalkan	Organisasi telah memiliki cakupan pengumpulan informasi yang lebih luas, namun masih belum sepenuhnya formal. Masih diperlukan penguatan kebijakan dan dokumentasi agar lebih terstruktur.	- Laporan pengumpulan informasi terhadap sebagian besar aspek. - Data hasil pengujian internal atau sumber eksternal dengan cakupan yang lebih luas. - Tidak ada kebijakan formal yang mengatur pengumpulan informasi secara menyeluruh.
3	Organisasi secara aktif telah melaksanakan pengumpulan informasi tentang kerentanan dan ancaman pada seluruh aspek dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.). Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai sumber informasi yang relevan dan telah diformalkan	Organisasi telah memenuhi standar dasar dengan cakupan pengumpulan informasi penuh terhadap seluruh aspek serta dokumentasi yang telah diformalkan.	- Laporan pengumpulan informasi ancaman dan kerentanan terhadap seluruh aspek. - Data hasil pengujian internal dan eksternal yang telah terdokumentasi secara formal. - Kebijakan dan prosedur formal terkait pengumpulan informasi ancaman.
4	Organisasi secara aktif telah melaksanakan pengumpulan informasi tentang kerentanan dan ancaman pada seluruh aspek dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.). Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai sumber informasi yang relevan dan telah	Organisasi telah mencapai tingkat pemenuhan yang lebih tinggi dengan monitoring dan reviu berkala untuk memastikan keamanan sistem secara terus-menerus.	- Laporan pengumpulan informasi yang diperbarui secara berkala. - Data hasil pengujian internal dan eksternal yang dikaji ulang secara periodik. - Kebijakan dan prosedur formal yang mencakup mekanisme monitoring dan reviu periodik.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	diformalkan, dilakukan monitoring dan direviu secara berkala		
5	Organisasi secara aktif telah melaksanakan pengumpulan informasi tentang kerentanan dan ancaman pada seluruh aspek dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.). Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai sumber informasi yang relevan dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta penerapan mekanisme otomatisasi	Organisasi telah mencapai tingkat pemenuhan tertinggi dengan penerapan evaluasi berkelanjutan serta otomatisasi dalam pemantauan dan mitigasi ancaman. Sistem keamanan berjalan secara efisien dan adaptif terhadap ancaman baru.	- Laporan pengumpulan informasi ancaman yang mencerminkan evaluasi berkelanjutan dan perbaikan sistematis. - Data hasil pengujian internal dan eksternal yang diperbarui secara otomatis melalui mekanisme pemantauan berbasis alat keamanan siber. - Implementasi sistem manajemen ancaman berbasis otomatisasi. - Kebijakan dan prosedur yang mencakup evaluasi dan pembaruan berkelanjutan.

23 Kontrol 1.4.2.b:

Kontrol	Menganalisis informasi tersebut apakah termasuk kedalam konteks risiko terhadap aset informasi, dan mendokumentasikannya.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa organisasi tidak hanya mengumpulkan informasi tentang kerentanan dan ancaman yang telah diperoleh atau dimiliki, tetapi juga melakukan analisis terhadap informasi tersebut dalam konteks risiko terhadap aset informasi. Proses analisis ini membantu organisasi memahami sejauh mana kerentanan dan ancaman dapat berdampak pada aset informasi yang dimiliki serta menentukan tindakan mitigasi yang tepat. Dalam implementasinya, organisasi harus mengevaluasi setiap informasi yang dikumpulkan untuk menilai relevansi, tingkat risiko, serta dampaknya terhadap operasional dan keamanan sistem. Dokumentasi hasil analisis ini sangat penting untuk mendukung pengambilan keputusan terkait pengelolaan risiko keamanan informasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen Hasil Analisis Risiko - Risk Register (Pencatatan Risiko) - Laporan Risk Assessment - Threat Intelligence Report - Dokumentasi Keputusan Manajemen Risiko - Incident and Risk Correlation Report
Ancaman/Risiko yang dimitigasi	TH021 TH023 TH025 TH029 TH035 TH039 TH041 TH052 TH054 TH070 TH077 TH022 TH024 TH027 TH030 TH036 TH040 TH049 TH053 TH065 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.RA-02, ID.RA-03** **NIST CSF 1.1: ID.RA-2, ID.RA-3** **NIST SP 800-53r5: PM-12, PM-15, PM-16, RA-3, RA-10, SI-5** **SNI ISO/IEC 27001:2022: 5.7, 8.16**

Kriteria Pemenuhan Kontrol 1.4.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melaksanakan analisis informasi kerentanan dan ancaman dalam konteks risiko terhadap aset informasi dan belum mendokumentasikannya	Organisasi belum memiliki langkah apa pun untuk menganalisis informasi risiko terhadap aset informasi. Tidak ada bukti pendukung yang menunjukkan adanya upaya dalam evaluasi atau mitigasi risiko.	- Tidak ada dokumentasi terkait analisis risiko aset informasi. - Tidak ada laporan atau catatan terkait evaluasi ancaman dan kerentanan.
1	Organisasi telah melaksanakan analisis informasi pada sebagian kecil aspek kerentanan dan ancaman dalam konteks risiko terhadap aset informasi, namun belum didokumentasikan dan diformalkan	Organisasi mulai melakukan analisis risiko secara terbatas namun belum memiliki prosedur atau kebijakan formal. Langkah awal telah diambil, tetapi belum menyeluruh.	- Laporan awal analisis risiko terhadap sebagian kecil aset informasi. - Daftar risiko awal berdasarkan sebagian kecil aset yang dianalisis. - Tidak ada kebijakan atau prosedur formal terkait analisis risiko
2	Organisasi telah melaksanakan analisis informasi dan dokumentasi pada sebagian besar aspek kerentanan dan ancaman dalam konteks risiko terhadap aset informasi, namun belum diformalkan	Organisasi telah memiliki cakupan analisis yang lebih luas, namun masih belum sepenuhnya formal. Masih diperlukan penguatan kebijakan dan dokumentasi agar lebih terstruktur.	- Laporan analisis risiko terhadap sebagian besar aset informasi. - Daftar risiko dengan cakupan yang lebih luas. - Tidak ada kebijakan formal yang mengatur analisis risiko secara menyeluruh.
3	Organisasi secara aktif melakukan analisis informasi kerentanan dan ancaman dalam konteks risiko terhadap aset informasi mereka. Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai aspek risiko yang relevan. Hasil analisis didokumentasikan dengan baik dan sudah diformalkan	Organisasi telah memenuhi standar dasar dengan cakupan analisis risiko penuh terhadap seluruh aset informasi serta dokumentasi yang telah diformalkan.	- Laporan analisis risiko dengan cakupan penuh terhadap seluruh aset informasi. - Dokumentasi formal hasil analisis risiko. - Kebijakan dan prosedur formal terkait analisis risiko.
4	Organisasi secara aktif melakukan analisis informasi kerentanan dan ancaman dalam konteks risiko terhadap aset informasi mereka. Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai aspek risiko yang relevan. Hasil analisis didokumentasikan dengan baik dan sudah diformalkan, dilakukan monitoring dan direviu secara periodik untuk memastikan keakuratan dan keterkinian informasi.	Organisasi telah mencapai tingkat pemenuhan yang lebih tinggi dengan monitoring dan reviu berkala untuk memastikan keakuratan informasi risiko.	- Laporan analisis risiko yang diperbarui secara berkala. - Daftar risiko dengan catatan perubahan dan pembaruan. - Kebijakan dan prosedur formal yang mencakup mekanisme monitoring dan reviu periodik.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi secara aktif melakukan analisis informasi kerentanan dan ancaman dalam konteks risiko terhadap aset informasi mereka. Proses ini telah dijalankan secara menyeluruh dan mencakup berbagai aspek risiko yang relevan. Hasil analisis didokumentasikan dengan baik dan sudah diformalkan, dilakukan monitoring dan direviu secara periodik untuk memastikan keakuratan dan keterkinian informasi, dilakukan evaluasi dan perbaikan berkelanjutan, serta penerapan mekanisme otomatisasi	Organisasi telah mencapai tingkat pemenuhan tertinggi dengan penerapan evaluasi berkelanjutan serta otomatisasi dalam pemantauan dan mitigasi risiko. Sistem keamanan berjalan secara efisien dan adaptif terhadap ancaman baru.	- Laporan analisis risiko yang mencerminkan evaluasi berkelanjutan dan perbaikan sistematis. - Daftar risiko yang diperbarui otomatis melalui mekanisme pemantauan berbasis alat keamanan siber. - Implementasi sistem manajemen risiko berbasis otomatisasi. - Kebijakan dan prosedur yang mencakup evaluasi dan pembaruan berkelanjutan.

1.4.3. Mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut

Kriteria	Detail
Deskripsi	Penyelenggara IIV memeriksa adanya risiko keamanan pada setiap fungsi penting organisasi yang berpotensi mengakibatkan bahaya keselamatan, kerugian, dan keamanan negara.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis risiko dan sumber daya untuk mengevaluasi dampak serta kemungkinan terjadinya.
Dampak	**Tinggi** – Dengan mengetahui potensi dampak, organisasi dapat merencanakan tindakan mitigasi yang efektif untuk mengurangi risiko
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif untuk mengidentifikasi potensi dampak dan mengevaluasi kemungkinan terjadinya
Referensi Kontrol	**NIST CSF 2.0: ID.RA-04** **NIST CSF 1.1: ID.RA-4** **NIST SP 800-53r5: CP-2, PM-9, PM-11, RA-2, RA-3, RA-9** **SNI ISO/IEC 27001:2022: -**

24 Kontrol 1.4.3.a:

Kontrol	Penyelenggara IIV perlu memeriksa pada setiap fungsi penting organisasi apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara.
Deskripsi Kontrol	Penyelenggara Infrastruktur Informasi Vital (IIV) perlu melakukan pemeriksaan terhadap setiap fungsi penting dalam organisasi untuk mengidentifikasi apakah ada risiko keamanan yang diketahui dapat memberikan dampak yang signifikan. Risiko tersebut mencakup kategori berikut: 1) Membahayakan Keselamatan: Risiko yang dapat mengancam keselamatan individu, baik pegawai, pengguna layanan, maupun masyarakat luas. 2) Menimbulkan Kerugian: Risiko yang dapat menyebabkan dampak finansial, operasional, atau reputasi terhadap organisasi maupun pihak terkait. 3) Mengancam Keamanan Negara: Risiko yang dapat berdampak pada stabilitas nasional, termasuk serangan siber yang dapat mengganggu infrastruktur kritis seperti sistem komunikasi pemerintah atau jaringan pertahanan. Kontrol ini bertujuan untuk memastikan bahwa organisasi memahami dan dapat mengelola risiko yang memiliki dampak luas, terutama yang dapat mengancam keberlanjutan operasional dan keamanan nasional. Hasil pemeriksaan ini harus terdokumentasi dengan baik sehingga dapat digunakan sebagai dasar dalam penyusunan kebijakan mitigasi dan pengambilan keputusan strategis.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan Analisis Risiko Keamanan - Dokumen Asesmen Risiko Terhadap Fungsi Penting - Kebijakan dan Prosedur Manajemen Risiko Keamanan - Bukti Pelaksanaan Audit Keamanan dan Reviu Berkala - Hasil Simulasi atau Uji Coba Keamanan (Security Testing & Tabletop Exercise)
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH012 TH065 TH073 TH075 TH077 TH008 TH010 TH026 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: ID.RA-04** **NIST CSF 1.1: ID.RA-4** **NIST SP 800-53r5: CP-2, PM-9, PM-11, RA-2, RA-3, RA-9** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk melakukan pemeriksaan potensi dampak keamanan terhadap setiap fungsi penting yang perlu diketahui.	Organisasi belum melakukan upaya untuk menilai potensi risiko keamanan terhadap fungsi pentingnya. Tidak ada proses yang terdokumentasi atau kebijakan yang diterapkan	- Tidak ada dokumentasi atau laporan terkait pemeriksaan risiko keamanan pada fungsi penting organisasi. - Tidak ada kebijakan atau prosedur yang mengatur identifikasi dan evaluasi risiko keamanan.
1	Organisasi telah melakukan pemeriksaan potensi dampak keamanan terhadap sebagian kecil fungsi penting organisasi yang perlu diketahui, seperti risiko keamanan, namun belum diformalkan	Organisasi mulai melakukan identifikasi risiko, tetapi masih dalam cakupan yang terbatas dan belum memiliki prosedur yang terstruktur serta terdokumentasi dengan baik.	- Laporan awal identifikasi risiko keamanan terhadap sebagian kecil fungsi penting organisasi. - Tidak ada kebijakan atau prosedur formal terkait proses pemeriksaan risiko keamanan. - Tidak ada mekanisme dokumentasi yang baku.
2	Organisasi telah melakukan pemeriksaan potensi dampak keamanan terhadap sebagian besar fungsi penting organisasi yang perlu diketahui, seperti risiko keamanan, namun belum diformalkan	Organisasi telah memperluas cakupan pemeriksaan risiko keamanan, namun belum sepenuhnya diformalkan dalam kebijakan dan prosedur yang jelas.	- Laporan hasil asesmen risiko terhadap sebagian besar fungsi penting organisasi. - Daftar aset dan analisis dampaknya terhadap sebagian besar fungsi penting. - Tidak ada kebijakan formal terkait analisis risiko keamanan yang menyeluruh.
3	Organisasi telah melakukan pemeriksaan potensi dampak keamanan terhadap seluruh fungsi penting organisasi, apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara, dan telah diformalkan	Organisasi telah memenuhi standar dasar dengan melakukan pemeriksaan risiko keamanan terhadap seluruh fungsi penting dan mendokumentasikannya dalam kebijakan dan prosedur yang resmi.	- Laporan asesmen risiko keamanan yang mencakup seluruh fungsi penting organisasi. - Kebijakan dan prosedur formal terkait pemeriksaan risiko keamanan. - Dokumentasi hasil identifikasi risiko yang telah diformalkan.
4	Organisasi telah melakukan pemeriksaan potensi dampak keamanan terhadap seluruh fungsi penting organisasi, apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara, dan telah diformalkan, dilakukan monitoring pelaksanaannya dan direviiew secara berkala	Organisasi telah meningkatkan kedewasaan manajemen risiko dengan melakukan pemantauan dan peninjauan rutin terhadap risiko keamanan pada fungsi pentingnya.	- Laporan asesmen risiko keamanan yang diperbarui secara berkala. - Kebijakan dan prosedur yang mencakup mekanisme monitoring dan reviu periodik. - Bukti pelaksanaan monitoring dan reviu risiko keamanan secara berkala.
5	Organisasi telah melakukan pemeriksaan potensi dampak keamanan terhadap seluruh fungsi penting organisasi, apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara, dan telah diformalkan, dilakukan monitoring pelaksanaannya dan direviu secara berkala, serta penerapan mekanisme otomatisasi	Organisasi telah mencapai tingkat pemenuhan tertinggi dengan menerapkan otomatisasi dalam pemantauan dan mitigasi risiko keamanan, sehingga dapat merespons ancaman secara lebih efektif dan adaptif.	- Implementasi sistem manajemen risiko berbasis otomatisasi. - Laporan asesmen risiko yang mencerminkan evaluasi berkelanjutan dan pembaruan otomatis. - Kebijakan dan prosedur yang mencakup evaluasi dan mitigasi risiko secara otomatis.

1.4.4. Menganalisis nilai risiko terhadap IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mampu menganalisis risiko keamanan siber dan prioritas mitigasinya dengan mempertimbangkan setiap ancaman, kerentanan, kemungkinan (likelihood), dan dampaknya.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis risiko dan sumber daya untuk mengevaluasi nilai risiko.
Dampak	**Tinggi** – Dengan analisis yang tepat, organisasi dapat memahami risiko yang dihadapi dan mengambil langkah-langkah untuk mengelolanya
Kompleksitas	**Sedang** – Memerlukan metodologi yang terstruktur untuk menganalisis dan mengevaluasi nilai risiko
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

25 Kontrol 1.4.4.a:

Kontrol	Pertimbangkan ancaman, kerentanan, kemungkinan, dan dampak saat menganalisis risiko
Deskripsi Kontrol	Menganalisis risiko dengan mempertimbangkan ancaman, kerentanan,kemungkinan, dan dampak adalah pendekatan yang komprehensif dalam manajemen risiko. Kerentanan menggambarkan kelemahan dalam sistem yang dapat dimanfaatkan oleh ancaman, sedangkan ancaman mengacu pada potensi bahaya yang dapat mengeksploitasi kerentanan tersebut. Kemungkinan mengacu pada sejauh mana ancaman tersebut dapat terjadi, sementara dampak menggambarkan potensi kerugian atau kerusakan yang ditimbulkan jika ancaman tersebut terjadi. Dengan mempertimbangkan faktor-faktor ini, organisasi dapat menentukan tingkat risiko yang lebih akurat dan merencanakan langkah-langkah mitigasi yang sesuai. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menggunakan pendekatan yang holistik dalam menganalisis risiko dengan menggabungkan keempat faktor ini dan apakah analisis tersebut terdokumentasi dengan baik.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan analisis risiko: mencakup penilaian ancaman, kerentanan, kemungkinan, dan dampak terhadap aset informasi organisasi - Matriks risiko: hubungan antara ancaman, kerentanannya, kemungkinan terjadinya, dan dampaknya terhadap organisasi. - Dokumentasi yang menjelaskan bagaimana kemungkinan dan dampak diukur dalam konteks risiko yang ada. - Catatan atau log pengambilan keputusan prioritas mitigasi risiko - Rencana mitigasi risiko
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH013 TH023 TH025 TH027 TH035 TH040 TH049 TH053 TH056 TH059 TH065 TH071 TH073 TH075 TH077 TH008 TH010 TH012 TH015 TH024 TH026 TH029 TH039 TH041 TH052 TH054 TH057 TH060 TH070 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak saat menganalisis risiko.	Tidak ada dokumentasi atau bukti bahwa organisasi melakukan analisis risiko.	Tidak ditemukan dokumen kebijakan, laporan analisis risiko, atau bukti diskusi terkait manajemen risiko.
1	Organisasi telah melaksanakan analisis nilai risiko pada sebagian kecil aspek IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak, namun belum diformalkan	Organisasi telah melakukan analisis risiko secara terbatas tetapi belum terdokumentasi secara resmi.	Draft laporan atau catatan internal mengenai analisis risiko, namun belum ada format yang distandarisasi.
2	Organisasi telah melaksanakan analisis nilai risiko pada sebagian besar aspek IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak, namun belum diformalkan	Organisasi telah melakukan analisis risiko pada sebagian besar komponen IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak, tetapi belum terdokumentasi secara resmi.	Dokumen analisis risiko yang mencakup sebagian besar aspek IIV, namun belum memiliki standar atau prosedur baku.
3	Organisasi telah melaksanakan analisis nilai risiko pada seluruh aspek IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak. dan telah diformalkan	Organisasi telah melaksanakan analisis risiko pada seluruh komponen IIV, terdokumentasi secara resmi, dan memiliki metodologi yang jelas.	Dokumen formal analisis risiko, SOP manajemen risiko, laporan hasil evaluasi risiko.
4	Organisasi telah melaksanakan analisis nilai risiko pada seluruh aspek IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak. dan telah diformalkan, dilakukan monitoring dan di reviu secara berkala untuk memastikan bahwa proses ini tetap relevan dan efisien seiring waktu.	Organisasi telah mengadopsi proses analisis risiko yang terdokumentasi secara resmi, dilakukan monitoring dan direviu secara berkala.	Laporan periodik evaluasi risiko, bukti monitoring terhadap risiko yang telah diidentifikasi.
5	Organisasi telah melaksanakan analisis nilai risiko pada seluruh aspek IIV dengan mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak. dan telah diformalkan, dilakukan monitoring dan di reviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta penerapan mekanisme otomatisasi	Organisasi telah menerapkan evaluasi risiko secara terus-menerus, dengan otomatisasi dan pembaruan berkala terhadap metodologi yang digunakan.	Adanya bukti perbaikan berkelanjutan dan penerapan mekanisme otomatisasi, hasil evaluasi risiko yang diperbarui secara berkala, laporan audit risiko.

26 Kontrol 1.4.4.b:

Kontrol	Penyelenggara IIV menentukan level risiko dan prioritas mitigasinya
Deskripsi Kontrol	Menentukan level risiko dan prioritas mitigasinya adalah langkah penting dalam pengelolaan risiko untuk memastikan bahwa sumber daya organisasi dialokasikan secara efektif dan efisien. Level risiko biasanya ditentukan berdasarkan hasil analisis yang mencakup ancaman,kerentanan, kemungkinan terjadinya, dan dampak. Setelah level risiko ditentukan, organisasi perlu menetapkan prioritas mitigasi, yang berarti memilih langkah-langkah yang paling kritis dan mendesak untuk menangani risiko dengan dampak terbesar atau kemungkinan terjadinya tertinggi. Prioritas ini membantu organisasi dalam merencanakan langkah-langkah mitigasi yang tepat, serta memastikan bahwa risiko yang paling merusak atau mengancam terlebih dahulu ditangani. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah menentukan dengan tepat level risiko yang ada dan telah memprioritaskan mitigasi risiko tersebut secara efektif.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan analisis risiko: mencakup penilaian level risiko untuk setiap ancaman dan kerentanannya - Matriks risiko: klasifikasi risiko berdasarkan levelnya (misalnya,rendah, sedang, tinggi, sangat tinggi). - Rencana mitigasi risiko: mencantumkan prioritas tindakan yang harus diambil berdasarkan level risiko yang telah ditentukan - Prosedur atau kebijakan prioritas mitigasi risiko - Catatan atau log pengambilan keputusan prioritas mitigasi risiko
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH025 TH027 TH041 TH053 TH057 TH060 TH071 TH073 TH075 TH077 TH008 TH010 TH012 TH024 TH026 TH035 TH052 TH056 TH059 TH065 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki level risiko dan prioritas mitigasinya.	Organisasi belum memiliki dokumen atau kebijakan terkait level risiko dan prioritas mitigasi.	Tidak tersedia proses, kebijakan, atau dokumen penetapan level risiko dan prioritas.
1	Organisasi telah menerapkan level risiko dan prioritas mitigasinya pada sebagian kecil aspek, tetapi belum diformalkan	Organisasi telah mulai menetapkan level risiko dan prioritas mitigasi tetapi hanya pada sebagian kecil aset.	Catatan internal terkait pengelompokan risiko dan prioritas mitigasi, namun belum ada kebijakan formal.
2	Organisasi telah menerapkan level risiko dan prioritas mitigasinya pada sebagian besar aspek, tetapi belum diformalkan	Organisasi telah menentukan level risiko dan prioritas mitigasi pada sebagian besar aspek, namun belum terdokumentasi secara formal.	Draft dokumen evaluasi risiko yang mencakup sebagian besar aspek.
3	Organisasi telah menerapkan level risiko dan prioritas mitigasinya pada seluruh aspek, dan telah diformalkan. Risiko dievaluasi dengan memperhitungkan dampak potensial dan kemungkinan terjadinya.	Organisasi telah menetapkan level risiko dan prioritas mitigasi secara menyeluruh dan terdokumentasi dengan baik.	Dokumen kebijakan manajemen risiko, SOP mitigasi risiko, laporan penilaian risiko.
4	Organisasi telah menentukan level risiko dan prioritas mitigasinya pada seluruh aspek, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Organisasi melakukan monitoring berkala terhadap level risiko dan mitigasinya serta melakukan reviu reguler.	Bukti monitoring berkala, hasil evaluasi risiko yang diperbarui secara berkala.
5	Organisasi telah menentukan level risiko dan prioritas mitigasinya pada seluruh aspek, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta penerapan mekanisme otomatisasi	Organisasi menerapkan evaluasi dan perbaikan berkelanjutan serta mekanisme otomatisasi dalam pengelolaan risiko.	Penggunaan alat otomatisasi mitigasi risiko, laporan pembaruan kebijakan berdasarkan hasil evaluasi berkala.

27 Kontrol 1.4.4.c:

Kontrol	Penyelenggara IIV memiliki kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk setiap aset informasi vital.
Deskripsi Kontrol	Menentukan kriteria yang jelas dan konsisten untuk tingkat risiko siber dan toleransi risiko pada setiap aset informasi vital sangat penting dalam pengelolaan risiko. Kriteria ini membantu organisasi dalam mengevaluasi dan mengklasifikasikan risiko yang dapat memengaruhi aset informasi yang paling kritis. Tingkat risiko siber dapat dihitung berdasarkan kemungkinan ancaman dan kerentanannya, serta dampak yang dapat ditimbulkan terhadap operasional organisasi. Toleransi risiko menunjukkan sejauh mana organisasi bersedia menerima risiko yang tidak dapat sepenuhnya dihilangkan atau dikurangi. Kriteria ini memastikan bahwa keputusan yang diambil dalam mengelola risiko konsisten dan berdasarkan pada kebijakan yang telah ditetapkan. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki dan menerapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber serta toleransi risiko terhadap aset informasi vital.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen kriteria penentuan tingkat risiko toleransi risiko - Matriks penilaian risiko yang menunjukkan klasifikasi dan toleransi risiko untuk setiap aset informasi. - Prosedur atau pedoman penentuan dan evaluasi toleransi risiko - Laporan atau catatan evaluasi risiko - Catatan keputusan terhadap aset informasi berdasarkan toleransi risiko yang telah ditetapkan
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH008 TH010 TH012 TH023 TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk menetapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk setiap aset informasi vital.	Tidak ada dokumen yang mendefinisikan tingkat risiko siber atau toleransi risiko.	Tidak ditemukan dokumen atau kebijakan yang mengatur tingkat risiko siber.
1	Organisasi telah menerapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk sebagian kecil aset informasi vital, dan belum diformalkan	Organisasi mulai menentukan kriteria risiko siber untuk sebagian kecil aset informasi vital tetapi belum formal.	Catatan internal atau draft dokumen yang menunjukkan upaya identifikasi risiko untuk sebagian kecil aset, namun tanpa formalisasi.
2	Organisasi telah menerapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk sebagian besar aset informasi vital, dan belum diformalkan	Organisasi menerapkan kriteria risiko siber yang lebih luas tetapi belum terdokumentasi secara formal.	Dokumen analisis risiko yang mencakup sebagian besar aset informasi vital, namun tanpa formalisasi.
3	Organisasi telah menetapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk seluruh aset informasi vital, dan telah diformalkan	Organisasi memiliki kriteria risiko siber yang terdokumentasi dengan baik dan digunakan untuk seluruh aset informasi vital.	Kebijakan formal terkait risiko siber, SOP pengelolaan risiko siber.
4	Organisasi telah menetapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk seluruh aset informasi vital, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Organisasi melakukan monitoring dan reviu berkala terhadap tingkat risiko siber dan toleransi risiko.	Laporan evaluasi risiko siber, hasil reviu kebijakan risiko.
5	Organisasi telah menetapkan kriteria yang jelas dan konsisten untuk menentukan tingkat risiko siber dan toleransi risiko untuk seluruh aset informasi vital, dan telah diformalkan, dilakukan monitoring dan direviu secara berkelanjutan, dilakukan evaluasi dan perbaikan berkelanjutan serta penerapan mekanisme otomatisasi	Organisasi menerapkan evaluasi berkelanjutan dan otomatisasi dalam menetapkan serta menyesuaikan tingkat risiko siber.	Log otomatisasi monitoring, laporan evaluasi berkala, bukti perbaikan berkelanjutan.

28 Kontrol 1.4.4.d:

Kontrol	Penyelenggara IIV melakukan penilaian risiko siber secara berkala dan menyeluruh, dengan melibatkan semua pemangku kepentingan yang relevan.
Deskripsi Kontrol	Penyelenggara IIV perlu melakukan penilaian risiko siber secara berkala dan menyeluruh untuk mengidentifikasi potensi risiko yang dapat memengaruhi aset informasi dan operasional organisasi. Penilaian ini harus melibatkan semua pemangku kepentingan yang relevan, baik internal maupun eksternal, guna mendapatkan pandangan yang komprehensif dan memastikan bahwa semua aspek risiko, termasuk ancaman baru dan kerentanannya, dipertimbangkan. Penilaian berkala juga membantu organisasi untuk mengevaluasi efektivitas dari langkah-langkah mitigasi yang sudah diterapkan, serta untuk menyesuaikan strategi mitigasi sesuai dengan perubahan lingkungan dan kondisi operasional. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi secara konsisten melakukan penilaian risiko siber secara menyeluruh dengan melibatkan pihak-pihak yang relevan untuk mendapatkan hasil yang komprehensif dan akurat.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen laporan penilaian risiko siber secara berkala dan menyeluruh - Daftar keterlibatan pihak internal dan eksternal yang terlibat dalam proses penilaian risiko - Protokol atau prosedur yang menggambarkan frekuensi dan cakupan penilaian risiko yang dilakukan oleh organisasi. - Catatan rapat atau diskusi dengan pemangku kepentingan yang relevan terkait dengan penilaian risiko. - Rencana tindak lanjut atau mitigasi yang dihasilkan dari penilaian risiko dan diterapkan oleh organisasi.
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076 TH008 TH010 TH012 TH023 TH025 TH027 TH036 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk melakukan penilaian risiko siber secara berkala dan menyeluruh.	Tidak ada kebijakan atau prosedur formal terkait penilaian risiko siber.	Tidak terdapat laporan atau catatan mengenai evaluasi risiko siber.
1	Organisasi telah melakukan penilaian risiko siber namun belum secara rutin dan hanya sebagian kecil aspek saja serta belum diformalkan	Ada upaya awal untuk mengidentifikasi risiko pada beberapa sistem, tetapi belum terdokumentasi secara resmi.	Draft laporan penilaian risiko pada sebagian kecil aspek yang belum diformalkan atau diresmikan.
2	Organisasi telah melakukan penilaian risiko siber pada sebagian besar aspek tapi belum diformalkan dan belum secara rutin berkala, cakupannya masih terbatas dan mungkin belum melibatkan semua pemangku kepentingan yang relevan.	Terdapat penilaian risiko pada sebagian besar aspek, tetapi belum memiliki prosedur yang konsisten dan belum mencakup seluruh bagian organisasi.	Laporan evaluasi risiko siber yang belum diformalkan.
3	Organisasi telah melakukan penilaian risiko siber pada seluruh aspek secara rutin berkala,dan telah diformalkan, cakupannya telah melibatkan semua pemangku kepentingan yang relevan.	Ada kebijakan dan prosedur tertulis untuk penilaian risiko siber serta penerapan secara rutin dengan pelibatan pemangku kepentingan.	Dokumen kebijakan, SOP manajemen risiko, dan laporan rutin terstruktur.
4	Organisasi telah melakukan penilaian risiko siber pada seluruh aspek secara rutin berkala,dan telah diformalkan, cakupannya telah melibatkan semua pemangku kepentingan yang relevan, dilakukan monitoring dan direviu secara berkala	Monitoring penilaian risiko siber berkala dengan hasil reviu dan perbaikan, semua aspek dilibatkan secara formal.	Catatan hasil monitoring, laporan tinjauan manajemen terkait evaluasi risiko.
5	Organisasi telah melakukan penilaian risiko siber pada seluruh aspek secara rutin berkala,dan telah diformalkan, cakupannya telah melibatkan semua pemangku kepentingan yang relevan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta memastikan bahwa organisasi tetap adaptif terhadap perubahan lingkungan dan ancaman keamanan dan menerapkan mekanisme otomatisasi	Organisasi Sistem monitoring penilaian risiko siber otomatis dan adaptif dengan evaluasi berkelanjutan.	Bukti penerapan otomatisasi, laporan evaluasi berkelanjutan.

29 Kontrol 1.4.4.e:

Kontrol	Penyelenggara IIV menentukan tingkat risiko terkait keamanan siber yang dapat diterima
Deskripsi Kontrol	Menentukan tingkat risiko keamanan siber yang dapat diterima adalah langkah penting dalam manajemen risiko. Tingkat risiko yang dapat diterima (risk appetite) menunjukkan sejauh mana organisasi bersedia menerima dampak dari risiko tanpa memerlukan mitigasi lebih lanjut. Penentuan ini bergantung pada konteks operasional, kebijakan, nilai aset informasi, dan tujuan strategis organisasi. Dengan menetapkan tingkat risiko yang dapat diterima, organisasi dapat mengalokasikan sumber daya secara efisien untuk mengatasi risiko yang berada di atas ambang toleransi, sekaligus memastikan bahwa fokus mitigasi tetap relevan dengan prioritas bisnis. Tujuan dari kontrol ini adalah untuk mengevaluasi apakah organisasi telah menetapkan tingkat risiko keamanan siber yang dapat diterima secara jelas dan konsisten, serta apakah tingkat risiko tersebut mendukung pengambilan keputusan strategis dalam manajemen risiko.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen kebijakan atau pedoman tentang tingkat risiko yang dapat diterima oleh organisasi. - Matriks atau tabel toleransi risiko yang menunjukkan kategori risiko yang dapat diterima. - Notulen rapat atau keputusan manajemen terkait penetapan tingkat risiko yang dapat diterima. - Dokumentasi proses evaluasi risiko yang menunjukkan bagaimana tingkat risiko yang dapat diterima diterapkan dalam penilaian risiko organisasi. - Catatan evaluasi berkala terkait relevansi tingkat risiko yang dapat diterima dengan konteks operasional organisasi. - Dokumen eskalasi risiko: Panduan prosedur eskalasi jika risiko melebihi toleransi organisasi
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077 TH008 TH010 TH012 TH023 TH025 TH027 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.e Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk menentukan tingkat risiko terkait keamanan siber yang dapat diterima.	Tidak ada pedoman atau standar terkait toleransi risiko keamanan siber.	Tidak ada dokumen formal yang mendefinisikan tingkat risiko yang dapat diterima.
1	Organisasi telah merencanakan untuk menentukan tingkat risiko terkait keamanan siber yang dapat diterima pada sebagian kecil aspek, tetapi langkah-langkah konkret belum diambil. Kesadaran akan pentingnya kegiatan ini ada, tetapi belum ada tindakan yang diambil untuk melaksanakannya secara aktif.	Ada inisiatif informal (misalnya diskusi awal, draft, atau rencana kerja) namun belum dilaksanakan.	Draft awal dokumen risiko, notulensi rencana kerja yang belum diimplementasikan, roadmap rencana pengelolaan risiko.
2	Organisasi telah memulai proses untuk menentukan tingkat risiko terkait keamanan siber yang dapat diterima, pada sebagian besar aspek meskipun masih dalam tahap awal atau sebagian besar aspek. Beberapa aspek mungkin telah dipertimbangkan, tetapi cakupannya masih terbatas.	Beberapa aspek sudah memiliki parameter toleransi risiko, tetapi masih dalam tahap pengembangan.	Laporan awal atau draft kebijakan mengenai tingkat risiko yang dapat diterima.
3	Organisasi telah menentukan tingkat risiko terkait keamanan siber yang dapat diterima pada seluruh aspek. Proses ini telah dijalankan secara menyeluruh dan mencakup semua aspek yang relevan. Organisasi telah menetapkan kriteria yang jelas dan terukur untuk menentukan tingkat risiko yang dapat diterima.	Tingkat toleransi risiko mencakup seluruh aspek telah ditetapkan pada dokumen formal.	Dokumen kebijakan risk appetite and tolerance, SOP resmi identifikasi dan evaluasi risiko, dan laporan kepatuhan.
4	Organisasi telah menentukan tingkat risiko terkait keamanan siber yang dapat diterima pada seluruh aspek. Proses ini telah dijalankan secara menyeluruh dan mencakup semua aspek yang relevan. Organisasi telah menetapkan kriteria yang jelas dan terukur untuk menentukan tingkat risiko yang dapat diterima, dilakukan monitoring dan direviu secara berkala untuk memastikan bahwa proses ini tetap relevan dan efisien seiring waktu.	Tingkat toleransi risiko siber telah ditetapkan pada seluruh aspek dan selalu diperbarui dan dipantau secara berkelanjutan.	Catatan hasil monitoring dan tinjauan berkala.
5	Organisasi telah menentukan tingkat risiko terkait keamanan siber yang dapat diterima pada seluruh aspek. Proses ini telah dijalankan secara menyeluruh dan mencakup semua aspek yang relevan. Organisasi telah menetapkan kriteria yang jelas dan terukur untuk menentukan tingkat risiko yang dapat diterima, dilakukan monitoring dan direviu secara berkala untuk memastikan bahwa proses ini tetap relevan dan efisien seiring waktu, dilakukan evaluasi dan perbaikan berkelanjutan.	Organisasi terus menyempurnakan kebijakan yang berkaitan dengan tingkat risiko yang dapat diterima berdasarkan masukan dari audit, insiden, dan perubahan regulasi.	Laporan evaluasi risiko rutin, bukti revisi kebijakan risiko berkala, dokumentasi corrective action plan.

30 Kontrol 1.4.4.f:

Kontrol	Penyelenggara IIV memiliki proses untuk menganalisis dan mengevaluasi data dan informasi yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang
Deskripsi Kontrol	Proses analisis dan evaluasi data serta informasi yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, merupakan elemen penting dalam manajemen risiko. Analisis ini bertujuan untuk memahami karakteristik risiko secara mendalam, mengidentifikasi akar penyebab dari risiko, mengevaluasi dampaknya terhadap aset informasi dan operasi organisasi, serta mengidentifikasi peluang untuk memperkuat keamanan siber. Proses ini membantu organisasi dalam menyusun strategi mitigasi yang efektif dan mengambil keputusan berdasarkan informasi yang valid dan relevan. Evaluasi yang komprehensif juga memungkinkan organisasi untuk memahami prioritas risiko dan dampaknya terhadap tujuan strategis. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki dan menjalankan proses yang sistematis untuk menganalisis dan mengevaluasi data terkait risiko siber.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen prosedur analisis risiko yang berisi panduan langkah-langkah untuk mengidentifikasi, mengevaluasi, dan menilai risiko siber secara sistematis - Laporan analisis risiko siber yang mencakup penyebab, dampak,dan peluang terkait dengan risiko siber - Matriks risiko atau dokumen yang menggambarkan hasil evaluasi risiko berdasarkan analisis data. - Notulen rapat atau diskusi yang mendokumentasikan proses evaluasi risiko dan pengambilan keputusan yang terkait. - Catatan hasil threat intelligence yang berisi informasi terbaru tentang ancaman siber
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076 TH008 TH010 TH012 TH023 TH025 TH027 TH036 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.f Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki rencana atau proses untuk menganalisis dan mengevaluasi data dan informasi terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang.	Tidak ada dokumentasi atau bukti analisis risiko yang dilakukan.	Tidak ada laporan analisis risiko, data terkait insiden, atau evaluasi risiko yang terdokumentasi.
1	Organisasi telah menjalankan proses untuk menganalisis dan mengevaluasi data dan informasi pada sebagian kecil aspek yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, tapi belum diformalkan	Organisasi telah melakukan analisis risiko siber pada sebagian kecil aspek, namun masih terbatas dan belum terdokumentasi secara formal. Proses ini dilakukan secara ad-hoc tanpa kebijakan atau prosedur yang jelas.	Catatan manual, ataupun notulensi rapat internal terkait analisis risiko yang belum lengkap
2	Organisasi telah menjalankan proses untuk menganalisis dan mengevaluasi data dan informasi pada sebagian besar aspek yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, tapi belum diformalkan. Beberapa aspek mungkin telah dipertimbangkan, tetapi cakupannya masih terbatas.	Organisasi telah menjalankan proses analisis pada sebagian besar aspek risiko siber, namun belum dituangkan pada dokumentasi atau kebijakan formal.	Terdapat template dokumen analisis risiko siber ataupun laporan risiko tanpa SOP resmi.
3	Organisasi telah menjalankan proses untuk menganalisis dan mengevaluasi data dan informasi pada seluruh aspek yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, dan telah diformalkan. Organisasi telah memiliki metode yang terstruktur untuk melakukan analisis risiko.	Proses analisis risiko siber yang mencakup seluruh aspek, termasuk penyebab, dampak, dan peluang dilaksanakan dengan metode terstruktur serta telah terdokumentasi dalam kebijakan atau prosedur resmi.	Dokumen SOP analisis risiko siber.
4	Organisasi telah memiliki proses untuk menganalisis dan mengevaluasi data dan informasi pada seluruh aspek yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, dan telah diformalkan. Organisasi telah memiliki metode yang terstruktur untuk melakukan analisis risiko, dilakukan monitoring dan direviu secara berkala	Proses analisis risiko siber yang mencakup seluruh aspek, termasuk penyebab, dampak, dan peluang dilaksanakan dengan metode terstruktur serta telah terdokumentasi dalam kebijakan atau prosedur resmi. Monitoring dilakukan berkala untuk mengidentifikasi perubahan risiko serta terdapat mekanisme reviu rutin.	Laporan monitoring dan reviu risiko secara berkala.
5	Organisasi telah memiliki proses untuk menganalisis dan mengevaluasi data dan informasi pada seluruh aspek yang terkait dengan risiko siber, termasuk penyebab, dampak, dan peluang, dan telah diformalkan. Organisasi telah memiliki metode yang terstruktur untuk melakukan analisis risiko, dilakukan monitoring dan direviu secara berkala. Berdasarkan hasil reviu dan umpan balik, ada tindakan yang diambil untuk memperbaiki proses ini secara terus-menerus, memastikan bahwa Organisasi tetap adaptif terhadap perubahan lingkungan dan ancaman keamanan.	Proses analisis risiko siber menggunakan metode terstruktur mencakup seluruh aspek, termasuk penyebab, dampak, dan peluang, serta telah diformalkan dalam kebijakan atau prosedur yang terdokumentasi. Selain itu, dilakukan monitoring dan reviu berkala untuk mengidentifikasi perubahan dalam risiko serta efektivitas strategi mitigasi. Proses perbaikan berkelanjutan diterapkan berdasarkan hasil reviu dan umpan balik, dengan tindakan korektif yang jelas.	Hasil audit, bukti implementasi rekomendasi reviu, dokumen pembelajaran dari insiden, roadmap peningkatan manajemen risiko.

31 Kontrol 1.4.4.g:

Kontrol	Penyelenggara IIV memiliki kebijakan dan prosedur yang efektif untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan
Deskripsi Kontrol	Memiliki kebijakan dan prosedur yang efektif untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber adalah bagian penting dari manajemen risiko organisasi. Kebijakan ini memastikan bahwa risiko siber ditangani sesuai dengan tingkat risiko dan toleransi risiko yang telah ditetapkan. Strategi pengurangan melibatkan langkah-langkah mitigasi untuk menurunkan risiko ke tingkat yang dapat diterima, sementara penghindaran berfokus pada mengeliminasi risiko tertentu dengan cara tertentu, seperti menghentikan aktivitas yang berisiko tinggi. Transfer risiko dilakukan dengan cara berbagi risiko, misalnya melalui asuransi atau kontrak dengan pihak ketiga. Penerimaan risiko dilakukan untuk risiko yang berada di bawah ambang toleransi, dengan kesadaran bahwa risiko tersebut tidak memerlukan tindakan lebih lanjut. Tujuan dari kontrol ini adalah untuk mengevaluasi apakah organisasi memiliki kebijakan dan prosedur yang dirancang dengan baik dan diterapkan secara konsisten untuk mengelola risiko siber sesuai dengan tingkat toleransi yang telah ditentukan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen kebijakan manajemen risiko yang menguraikan strategi mitigasi, penghindaran, transfer, dan penerimaan risiko. - Prosedur standar operasional untuk pengelolaan risiko siber. - Matriks risiko yang menunjukkan hubungan antara tingkat risiko dan tindakan mitigasi atau strategi lainnya. - Dokumen kontrak pihak ketiga mengenai risiko siber yang menunjukkan mekanisme transfer risiko melalui pihak ketiga seperti asuransi - Laporan hasil tindak lanjut risiko yang berisi catatan hasil pelaksanaan mitigasi, penghindaran, transfer, atau penerimaan risiko. - Dokumentasi keputusan manajemen untuk menerima risiko tertentu beserta justifikasinya
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076 TH008 TH010 TH012 TH023 TH025 TH027 TH036 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-05** **NIST CSF 1.1: ID.RA-5** **NIST SP 800-53r5: CA-2, CA-7, PM-16, PM-28, RA-2, RA-3** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 1.4.4.g Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki kebijakan dan prosedur yang efektif untuk mengelola risiko siber. Tidak ada upaya yang dilakukan untuk merencanakan atau mengimplementasikan aktivitas tersebut.	Tidak ada dokumen kebijakan atau prosedur manajemen risiko.	Tidak ditemukan kebijakan atau pedoman tertulis terkait manajemen risiko siber.
1	Organisasi telah menerapkan kebijakan dan prosedur untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber pada sebagian kecil aspek, sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan. tetapi belum ada penetapan secara formal	Ada kebijakan/prosedur untuk mitigasi risiko pada sebagian kecil aspek, belum diformalkan. Kebijakan tersebut bersifat ad hoc dengan implementasi yang tidak konsisten dan tidak terdokumentasi.	Dokumen draft atau pedoman tidak resmi terkait mitigasi risiko siber.
2	Organisasi telah menerapkan kebijakan dan prosedur untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber pada sebagian besar aspek, sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan. tetapi belum ada penetapan secara formal	Kebijakan yang memuat tindak lanjut risiko telah mencakup lebih banyak aspek, tetapi masih belum ditetapkan secara formal.	Dokumen kebijakan dan prosedur yang memuat mitigasi risiko masih dalam tahap pengembangan.
3	Organisasi telah menerapkan kebijakan dan prosedur untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber pada seluruh aspek, sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan. dan telah ada penetapan secara formal	Seluruh aspek telah memiliki kebijakan dan prosedur mitigasi risiko yang ditetapkan secara formal. Kebijakan dan prosedur tersebut digunakan secara konsisten.	Dokumen kebijakan disetujui, dan ada SOP terkait manajemen risiko.
4	Organisasi telah menerapkan kebijakan dan prosedur untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber pada seluruh aspek, sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan. dan telah ada penetapan secara formal, dilakukan monitoring pelaksanaan kebijakan ini dan direviu secara berkala	Kebijakan dan prosedur yang memuat tindak lanjut risiko telah diformalkan dan digunakan secara konsisten. Serta pelaksanaannya dipantau dan direviu secara berkala.	Jadwal dan dokumentasi monitoring pelaksanaan kebijakan, laporan hasil reviu kebijakan.
5	Organisasi telah menerapkan kebijakan dan prosedur untuk mengurangi, menghindari, mentransfer, atau menerima risiko siber pada seluruh aspek, sesuai dengan tingkat risiko dan toleransi risiko yang ditetapkan. dan telah ada penetapan secara formal, dilakukan monitoring pelaksanaan kebijakan ini dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta penerapan mekanisme otomatisasi	Kebijakan dan prosedur yang memuat tindak lanjut risiko telah diformalkan dan digunakan secara konsisten. Pemantauan pelaksanaan, evaluasi, dan perbaikan terhadap kebijakan dilakukan secara rutin untuk memastikan efektivitasnya. Serta terdapat proses otomatisasi dalam implementasinya.	Dokumentasi otomatisasi monitoring kebijakan mitigasi risiko, laporan evaluasi kebijakan secara berkala, bukti integrasi umpan balik terhadap perbaikan proses.

1.4.5. Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko

Kriteria	Detail
Deskripsi	Penyelenggara IIV memeriksa adanya risiko keamanan pada setiap fungsi penting organisasi yang berpotensi mengakibatkan bahaya keselamatan, kerugian, dan keamanan negara.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan sumber daya untuk mengidentifikasi serta menyusun prioritas mitigasi.
Dampak	**Tinggi** – Dengan prioritas yang jelas, organisasi dapat mengelola risiko dengan lebih efektif dan mengurangi kemungkinan terjadinya insiden
Kompleksitas	**Sedang** – Memerlukan analisis dan perencanaan yang komprehensif untuk menyusun prioritas mitigasi
Referensi Kontrol	**NIST CSF 2.0: ID.RA-06** **NIST CSF 1.1: ID.RA-6** **NIST SP 800-53r5: CA-5, PM-4, PM-9, PM-28, RA-7** **SNI ISO/IEC 27001:2022: -**

32 Kontrol 1.4.5.a:

Kontrol	Berdasarkan hasil penilaian risiko, tentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan dokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan.
Deskripsi Kontrol	Berdasarkan hasil penilaian risiko, organisasi perlu menentukan rincian tindakan pencegahan risiko keamanan secara jelas, termasuk langkah-langkah spesifik untuk memitigasi kemungkinan risiko keamanan siber. Dokumentasi yang terorganisir memungkinkan semua pihak yang relevan memahami ruang lingkup, prioritas, dan tanggung jawab dalam pelaksanaan tindakan mitigasi. Proses ini penting untuk memastikan bahwa tindakan yang diambil sesuai dengan hasil analisis risiko dan berfokus pada area dengan dampak paling signifikan. Tujuan dari kontrol ini adalah untuk mengevaluasi apakah organisasi telah mendokumentasikan rencana mitigasi risiko secara sistematis dan memprioritaskan tindakan berdasarkan tingkat risiko dan dampak terhadap aset informasi dan operasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan Penilaian Risiko yang berisi identifikasi ancaman, kerentanan, kemungkinan kejadian, dan dampak terhadap organisasi. - Dokumen Rencana Mitigasi Risiko yang memuat daftar tindakan pencegahan dan mitigasi yang spesifik untuk setiap risiko yang teridentifikasi. - Matriks Risiko yang menampilkan tingkat risiko berdasarkan kombinasi antara kemungkinan kejadian dan dampaknya. - Laporan kemajuan pelaksanaan tindakan mitigasi. - Catatan Rapat Manajemen Risiko - Bukti adanya diskusi dan keputusan strategis terkait mitigasi risiko oleh tim manajemen organisasi.
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076 TH008 TH010 TH012 TH023 TH025 TH027 TH036 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-06** **NIST CSF 1.1: ID.RA-6** **SNI ISO/IEC 27001:2022: -** **NIST SP 800-53r5: CA-5, PM-4, PM-9, PM-28, RA-7**

Kriteria Pemenuhan Kontrol 1.4.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan belum mendokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko.	Organisasi tidak memiliki dokumen penilaian risiko atau rencana mitigasi risiko yang terdokumentasi. Tidak ada dokumentasi mengenai langkah-langkah pencegahan risiko keamanan. Tidak ada bukti bahwa organisasi telah melakukan identifikasi risiko dan menentukan langkah mitigasi.	Tidak tersedia dokumen yang dapat diperiksa mengenai tindakan pencegahan risiko.
1	Organisasi telah menentukan dengan jelas rincian tindakan pada sebagian kecil aspek untuk mencegah kemungkinan risiko keamanan, dan mendokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko, namun belum diformalkan	Organisasi memiliki dokumentasi tindakan mitigasi, tetapi hanya mencakup sebagian kecil aspek. Tidak ada proses formal dalam penyusunan dokumen mitigasi risiko. Tidak ada standar atau prosedur yang jelas dalam pendokumentasian risiko dan mitigasi.	Draft dokumen penilaian risiko yang belum diformalkan. Catatan internal mengenai risiko keamanan tertentu yang telah diidentifikasi. Laporan insidental terkait risiko yang ditemukan.
2	Organisasi telah menentukan dengan jelas rincian tindakan pada sebagian besar aspek untuk mencegah kemungkinan risiko keamanan, dan mendokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko, namun belum diformalkan	Organisasi telah memiliki dokumen mitigasi risiko yang mencakup sebagian besar aspek. Proses identifikasi dan mitigasi risiko telah dilakukan, tetapi belum diformalkan. Masih terdapat beberapa aspek risiko yang belum didokumentasikan dengan baik.	Dokumen penilaian risiko yang belum memiliki persetujuan formal. Rencana mitigasi risiko yang masih dalam tahap penyusunan atau reviu. Terdapat notulensi rapat yang menunjukkan pembahasan mengenai risiko dan mitigasi.
3	Organisasi telah menentukan dengan jelas rincian tindakan pada seluruh aspek untuk mencegah kemungkinan risiko keamanan, dan mendokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko, dan telah diformalkan	Organisasi telah memiliki dokumen mitigasi risiko yang mencakup seluruh aspek. Dokumen tersebut telah diformalkan dan mendapat persetujuan dari manajemen. Rencana mitigasi sudah diterapkan, tetapi belum ada evaluasi berkala.	Dokumen penilaian risiko yang telah disahkan, kebijakan keamanan informasi yang mencantumkan mitigasi risiko, laporan hasil implementasi mitigasi risiko.
4	Organisasi telah menentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan dokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko dan telah dilakukan secara menyeluruh terhadap setiap aset informasi baik yang mendukung secara langsung fungsi vital, maupun tidak langsung selama masih	Organisasi telah melakukan mitigasi risiko secara menyeluruh terhadap setiap aset informasi. Rencana mitigasi telah diformalkan dan diimplementasikan secara efektif. Dilakukan monitoring dan reviu secara berkala untuk mengetahui efektivitas mitigasi.	Dokumen yang memuat catatan hasil monitoring dan pengkajian ulang berkala rincian tindak pencegahan kemungkinan risiko.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	dikelola oleh Organisasi dan telah diformalkan, dilakukan monitoring dan direviu secara berkala		
5	Organisasi telah menentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan dokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan berdasarkan hasil penilaian risiko dan telah dilakukan secara menyeluruh terhadap setiap aset informasi baik yang mendukung secara langsung fungsi vital, maupun tidak langsung selama masih dikelola oleh Organisasi dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, serta selalu melakukan perbaikan bekelanjutan	Organisasi telah melakukan mitigasi risiko secara menyeluruh terhadap setiap aset informasi. Rencana mitigasi telah diformalkan dan diimplementasikan secara efektif. Dilakukan monitoring dan reviu secara berkala untuk mengetahui efektivitas mitigasi. Perbaikan dilakukan terhadap mitigasi risiko berdasarkan hasil evaluasi secara berkelanjutan.	Dokumen yang memuat catatan hasil monitoring dan pengkajian ulang berkala rincian tindak pencegahan kemungkinan risiko. Serta memuat histori perbaikan rutin proses mitigasi risiko berdasarkan hasil evaluasi.

33 Kontrol 1.4.5.b:

Kontrol	Evaluasi hasil penerapan respon risiko secara berkelanjutan.
Deskripsi Kontrol	Evaluasi hasil penerapan respon risiko secara berkelanjutan bertujuan untuk memastikan bahwa langkah-langkah mitigasi, penghindaran, transfer, atau penerimaan risiko yang telah diambil efektif dalam mengelola risiko siber. Evaluasi berkelanjutan memungkinkan organisasi untuk mengidentifikasi kelemahan atau celah dalam penerapan respon risiko dan mengambil tindakan perbaikan jika diperlukan. Selain itu, evaluasi ini membantu organisasi untuk menyesuaikan strategi mitigasi berdasarkan perubahan kondisi internal maupun eksternal, termasuk munculnya ancaman baru atau perubahan dalam tingkat risiko. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki mekanisme pemantauan dan evaluasi berkelanjutan terhadap respon risiko yang diterapkan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan evaluasi hasil penerapan respon risiko yang berisi hasil analisis efektivitas kontrol keamanan yang telah diterapkan. - Dokumen hasil audit internal atau eksternal yang menilai kepatuhan organisasi terhadap kebijakan respon risiko yang telah ditetapkan. - Hasil audit internal atau eksternal terhadap penerapan respon risiko. - Dokumen reviu dan monitoring risiko yang memuat hasil monitoring berkelanjutan atas risiko yang diidentifikasi sebelumnya. - Catatan insiden keamanan yang menunjukkan risiko yang berhasil dikelola atau tidak dikelola dengan baik. - Dokumen perbaikan atau penyesuaian strategi mitigasi berdasarkan hasil evaluasi. - Notulen rapat manajemen risiko terkait evaluasi hasil penerapan respon risiko.
Ancaman/Risiko yang dimitigasi	TH023 TH025 TH035 TH040 TH053 TH056 TH059 TH065 TH070 TH072 TH074 TH076 TH024 TH027 TH039 TH052 TH054 TH057 TH060 TH067 TH071 TH073 TH075 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.RA-06** **NIST CSF 1.1: ID.RA-6** **SNI ISO/IEC 27001:2022: -** **NIST SP 800-53r5: CA-5, PM-4, PM-9, PM-28, RA-7**

Kriteria Pemenuhan Kontrol 1.4.5.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan evaluasi terhadap hasil penerapan respon risiko secara berkelanjutan.	Organisasi tidak memiliki dokumen yang mendefinisikan rincian respon penerapan risiko. Tidak ada bukti bahwa organisasi telah melakukan evaluasi penerapan respon risiko.	Tidak ada proses, dokumen, atau laporan terkait evaluasi hasil respon risiko.
1	Organisasi telah melakukan evaluasi pada sebagian kecil aspek terhadap hasil penerapan respon risiko secara berkelanjutan, namun masih belum melakukan tindakan kongkrit, dan belum diformalkan	Ada bukti parsial evaluasi pada aspek-aspek tertentu terhadap hasil penerapan respon risiko tanpa tindakan lanjutan atau dokumen formal.	Adanya laporan atau catatan evaluasi sebagian kecil aspek pada hasil penerapan respon risiko, belum ada kebijakan formal.
2	Organisasi telah melakukan evaluasi pada sebagian besar aspek terhadap hasil penerapan respon risiko secara berkelanjutan, dan belum diformalkan	Evaluasi mencakup sebagian besar aspek pada hasil penerapan respon risiko, tetapi tidak didukung oleh kebijakan atau prosedur formal	Laporan evaluasi hasil penerapan respon risiko sebagian besar aspek, draft kebijakan atau SOP yang belum diformalkan
3	Organisasi telah melakukan evaluasi pada seluruh aspek terhadap hasil penerapan respon risiko secara berkelanjutan, dan telah diformalkan	Evaluasi hasil penerapan respon risiko sudah mencakup semua aspek, didokumentasikan secara formal dan mendapat persetujuan manajemen.	Dokumen formal evaluasi hasil penerapan respon risiko lengkap dan dokumentasi prosedurnya
4	Organisasi telah melakukan evaluasi pada seluruh aspek terhadap hasil penerapan respon risiko secara berkelanjutan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Adanya kebijakan formal, proses monitoring dan reviu berkala, serta laporan hasil evaluasi hasil penerapan respon risiko	Dokumen kebijakan, laporan monitoring dan reviu rutin, bukti pelaksanaan pertemuan evaluasi.
5	Organisasi telah melakukan evaluasi pada seluruh aspek terhadap hasil penerapan respon risiko secara berkelanjutan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan dan menerapkan mekanisme otomatisasi	Sistem evaluasi hasil penerapan respon risiko berbasis otomatisasi, laporan perbaikan, dan bukti proses evaluasi berkelanjutan.	Dokumentasi sistem otomatisasi evaluasi hasil penerapan respon risiko, log monitoring otomatis, laporan perbaikan terus-menerus.

1.4.6. Menentukan dan mengomunikasikan toleransi risiko organisasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian/analisis risiko, sumber daya, dan dampaknya terhadap layanan publik.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan sumber daya untuk menentukan serta mengomunikasikan toleransi risiko.
Dampak	**Tinggi** – Dengan toleransi risiko yang jelas, organisasi dapat mengambil keputusan yang lebih baik dan mengelola risiko dengan lebih efektif
Kompleksitas	**Sedang** – Memerlukan koordinasi dan komunikasi yang efektif untuk menentukan dan mengomunikasikan toleransi risiko
Referensi Kontrol	**NIST CSF 2.0: GV.RM-02, GV.RM-04** **NIST CSF 1.1: ID.RM-2, ID.RM-3** **NIST SP 800-53r5: PM-8, PM-9, PM-11, RA-9** **SNI ISO/IEC 27001:2022: -**

34 Kontrol 1.4.6.a:

Kontrol	Menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku.
Deskripsi Kontrol	Organisasi perlu menentukan tingkat toleransi risiko berdasarkan hasil penilaian risiko yang telah dilakukan dan kebijakan keamanan yang berlaku. Toleransi risiko ini merupakan batasan yang dapat diterima oleh organisasi terhadap kemungkinan dampak yang terjadi akibat ancaman atau kerentanan pada sistem dan aset informasi. Tingkat toleransi risiko membantu organisasi dalam pengambilan keputusan terkait strategi mitigasi, penerimaan risiko, atau transfer risiko. Toleransi ini harus ditentukan berdasarkan analisis risiko yang dilakukan secara menyeluruh, kapasitas organisasi dalam menghadapi ancaman, dampak terhadap layanan publik dan keberlangsungan operasional. Penerapan toleransi risiko yang efektif harus didokumentasikan, disahkan oleh pimpinan, dimonitor secara berkala, serta dievaluasi untuk memastikan kesesuaiannya dengan perubahan lingkungan risiko.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen kebijakan manajemen risiko yang berisi penetapan tingkat toleransi risiko organisasi dan disahkan oleh pimpinan organisasi - Laporan hasil penilaian risiko yang berisi hasil analisis risiko terhadap sistem dan aset informasi. Menunjukkan dampak dan kemungkinan ancaman. - Matriks risiko yang menampilkan klasifikasi tingkat risiko (rendah, sedang, tinggi). Berisi metode penentuan dan batas toleransi yang diterapkan. - Laporan monitoring dan evaluasi risiko yang merupakan hasil pemantauan tingkat toleransi risiko yang menunjukkan perubahan dalam toleransi risiko berdasarkan insiden sebelumnya.
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH040 TH049 TH053 TH056 TH059 TH065 TH067 TH071 TH073 TH075 TH077 TH008 TH010 TH012 TH023 TH025 TH027 TH039 TH041 TH052 TH054 TH057 TH060 TH066 TH070 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: GV.RM-02, GV.RM-04** **NIST CSF 1.1: ID.RM-2, ID.RM-3** **NIST SP 800-53r5: PM-8, PM-9, PM-11, RA-9** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.6.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku.	Organisasi belum menentukan tingkat toleransi risiko berdasarkan hasil penilaian risiko dan kebijakan yang berlaku.	Tidak ada dokumen atau bukti bahwa toleransi risiko telah ditentukan.
1	Organisasi telah menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku pada sebagian kecil aspek, tetapi belum ada tindakan yang diambil untuk melaksanakannya secara aktif dan belum diformalkan	Organisasi telah menentukan tingkat toleransi risiko tetapi hanya pada sebagian kecil aspek, belum ada tindakan nyata untuk menerapkannya dan belum diformalkan.	Draft dokumen manajemen risiko yang belum mendapat persetujuan, catatan internal terkait toleransi risiko, laporan sementara terkait penilaian risiko.
2	Organisasi telah menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku pada sebagian besar aspek, dan belum diformalkan	Organisasi telah menentukan tingkat toleransi risiko pada sebagian besar aspek, tetapi belum diformalkan.	Dokumen risk assessment yang mencakup sebagian besar aset, kebijakan keamanan yang mengacu pada toleransi risiko namun belum mendapat validasi formal.
3	Organisasi telah menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku secara menyeluruh terhadap aspek yang relevan dan telah disahkan pimpinan dalam bentuk formal	Organisasi telah menentukan tingkat toleransi risiko secara menyeluruh dan telah disahkan dalam bentuk formal.	Dokumen kebijakan manajemen risiko yang telah disetujui pimpinan, laporan risk assessment yang lengkap dan telah diterapkan.
4	Organisasi telah menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku secara menyeluruh terhadap aspek yang relevan dan telah disahkan pimpinan dalam bentuk formal, dilakukan monitoring dan direviu secara berkala	Organisasi telah menentukan tingkat toleransi risiko secara menyeluruh, diformalkan, dimonitor, dan direviu secara berkala.	Laporan monitoring risiko, hasil evaluasi tahunan, laporan kepatuhan terhadap kebijakan manajemen risiko.
5	Organisasi telah menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku secara menyeluruh terhadap aspek yang relevan dan telah disahkan pimpinan dalam bentuk formal, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan serta menerapkan mekanisme otomatisasi	Organisasi telah menentukan tingkat toleransi risiko secara menyeluruh, diformalkan, dimonitor secara berkala, dievaluasi, serta menerapkan mekanisme otomatisasi untuk pemantauan.	Sistem pemantauan risiko otomatis, laporan evaluasi berkala, hasil audit terkait tingkat toleransi risiko.

35 Kontrol 1.4.6.b:

Kontrol	Penyelenggara IIV memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan
Deskripsi Kontrol	Agar manajemen risiko dapat berjalan efektif, organisasi harus memiliki mekanisme komunikasi untuk menyampaikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan. Komunikasi ini penting untuk memastikan pimpinan dan pemangku kepentingan memahami risiko yang dihadapi, tindakan mitigasi dapat direncanakan dan diimplementasikan, koordinasi yang baik antara tim keamanan, manajemen, dan regulator. Mekanisme komunikasi ini dapat berupa laporan resmi, rapat koordinasi, sistem berbasis teknologi, atau kanal komunikasi lainnya yang memastikan informasi terkait risiko dapat diakses oleh pihak yang berkepentingan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen prosedur komunikasi risiko yang berisi mekanisme komunikasi hasil manajemen risiko. Menunjukkan pihak-pihak yang harus menerima informasi risiko. - Laporan hasil analisis risiko yang dikirim ke pihak berwenang yang berisi hasil analisis risiko yang telah dikomunikasikan. Ditujukan kepada pemangku kepentingan atau regulator. - Notulensi rapat koordinasi keamanan informasi yang mencatat hasil diskusi terkait risiko dan mitigasinya. Memuat rekomendasi tindakan kepada pihak terkait.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.RM-02, GV.RM-04** **NIST CSF 1.1: ID.RM-2, ID.RM-3** **NIST SP 800-53r5: PM-8, PM-9, PM-11, RA-9** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.6.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan. Tidak ada upaya yang dilakukan untuk merencanakan atau mengimplementasikan aktivitas tersebut.	Organisasi belum memiliki mekanisme komunikasi hasil manajemen risiko kepada pihak yang berwenang dan relevan.	Tidak ada dokumen komunikasi hasil manajemen risiko, tidak ada catatan rapat terkait risiko.
1	Organisasi telah memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan, dan menerapkannya pada sebagian kecil aspek, dan belum diformalkan	Organisasi memiliki mekanisme komunikasi hasil dan rekomendasi proses manajemen risiko tetapi hanya diterapkan pada sebagian kecil aspek, dan belum diformalkan.	Draft prosedur komunikasi hasil manajemen risiko, laporan internal yang belum terstruktur, catatan komunikasi hasil manajemen risiko yang tidak terdokumentasi secara resmi.
2	Organisasi telah memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan, dan menerapkannya pada sebagian besar aspek, dan belum diformalkan	Organisasi telah memiliki mekanisme komunikasi hasil manajemen risiko dan menerapkannya pada sebagian besar aspek, namun belum diformalkan.	Adanya bukti mekanisme komunikasi hasil manajemen risiko yang aktif namun belum terdokumentasi sebagai kebijakan organisasi.
3	Organisasi telah memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan, dan menerapkannya secara menyeluruh dan mencakup semua aspek yang relevan, dan telah diformalkan	Organisasi telah memiliki mekanisme komunikasi hasil manajemen risiko yang mencakup seluruh aspek dan telah diformalkan.	Dokumen prosedur komunikasi hasil manajemen risiko yang telah disetujui pimpinan, laporan risiko yang terstruktur dan dikirimkan secara berkala.
4	Organisasi telah memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan, dan menerapkannya secara menyeluruh dan mencakup semua aspek yang relevan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Organisasi telah memiliki mekanisme komunikasi hasil manajemen risiko yang mencakup seluruh aspek, diformalkan, dimonitor, dan direviu secara berkala.	Catatan evaluasi komunikasi hasil manajemen risiko risiko, laporan kepatuhan terhadap kebijakan komunikasi, hasil audit komunikasi.
5	Organisasi telah memiliki mekanisme untuk mengomunikasikan hasil dan rekomendasi dari proses manajemen risiko kepada pihak-pihak yang berwenang dan relevan, dan menerapkannya secara menyeluruh dan mencakup semua aspek yang relevan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi untuk memperbaiki mekanisme tersebut secara terus-menerus, memastikan bahwa Organisasi tetap adaptif terhadap perubahan lingkungan dan kebutuhan komunikasi yang mungkin berubah.	Organisasi telah memiliki mekanisme komunikasi hasil manajemen risiko yang mencakup seluruh aspek, diformalkan, dimonitor secara berkala, serta dilakukan evaluasi berkelanjutan dengan penerapan sistem otomatisasi.	Sistem komunikasi hasil penerapan manajemen risiko berbasis digital, laporan otomatis yang dikirim ke pemangku kepentingan, hasil evaluasi berkala terhadap efektivitas komunikasi.

1.4.7. Mengelola hasil penerapan manajemen risiko yang telah ditetapkan

Kriteria	Detail
Deskripsi	Penyelenggara IIV menetapkan kebijakan berupa proses manajemen risiko keamanan siber organisasi, serta mengomunikasikannya kepada pihak yang terkait sesuai dengan ruang lingkup tanggung jawabnya.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan pemantauan dan evaluasi berkelanjutan terhadap hasil penerapan manajemen risiko.
Dampak	**Tinggi** – Dengan pengelolaan yang baik, organisasi dapat memastikan bahwa risiko tetap terkendali dan tindakan mitigasi yang diambil efektif
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengelola dan memantau hasil penerapan manajemen risiko
Referensi Kontrol	**NIST CSF 2.0: GV.RM-01, GV.RM-06, GV.RR-03** **NIST CSF 1.1: ID.RM-1** **NIST SP 800-53r5: PM-9, PM-28** **SNI ISO/IEC 27001:2022: -**

36 Kontrol 1.4.7.a:

Kontrol	Konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan komunikasikan hasilnya kepada pihak yang tepat di dalam organisasi (misalnya pimpinan organisasi).
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa organisasi memiliki proses yang sistematis untuk menilai status implementasi manajemen risiko keamanan siber. Informasi ini harus dikomunikasikan kepada pihak yang berkepentingan, seperti pimpinan organisasi, untuk mendukung pengambilan keputusan strategis. Komunikasi ini dapat dilakukan dalam bentuk laporan berkala, dashboard keamanan, atau rapat koordinasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan manajemen risiko keamanan siber Memuat hasil evaluasi risiko keamanan siber organisasi dan status implementasi kontrol terkait. - Notula rapat manajemen risiko Catatan hasil rapat yang membahas status implementasi dan langkah tindak lanjut yang perlu dilakukan. - Dokumentasi komunikasi internal Email, memo, atau laporan berkala yang dikirimkan kepada pimpinan atau unit terkait.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.RM-01, GV.RM-06, GV.RR-03** **NIST CSF 1.1: ID.RM-1** **NIST SP 800-53r5: PM-9, PM-28** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.7.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi	Tidak ada bukti bahwa organisasi mengonfirmasi status implementasi manajemen risiko dan mengomunikasikan hasilnya.	Tidak ada dokumen atau catatan pendukung.
1	Organisasi sudah melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi, namun baru diterapkan pada sebagian kecil aspek dan belum diformalkan	Ada beberapa bukti awal konfirmasi status implementasi manajemen risiko, tetapi tidak terdokumentasi formal.	Draft laporan konfirmasi status implementasi manajemen risiko, email informal ke pimpinan, atau catatan rapat tidak resmi.
2	Organisasi sudah melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi, diterapkan pada sebagian besar aspek namun belum diformalkan	Konfirmasi status implementasi manajemen risiko dilakukan secara lebih luas, tetapi belum memiliki prosedur terdokumentasi formal.	Draft SOP atau kebijakan komunikasi status implementasi manajemen risiko, catatan meeting internal.
3	Organisasi sudah melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi, diterapkan pada seluruh aspek dan telah diformalkan	Konfirmasi status implementasi manajemen risiko dilakukan di seluruh organisasi dan terdokumentasi dengan baik.	Kebijakan manajemen risiko siber yang disetujui pimpinan, SOP komunikasi status implementasi manajemen risiko siber yang terdokumentasi.
4	Organisasi sudah melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi, diterapkan pada seluruh aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Ada mekanisme reviu berkala untuk memastikan status implementasi manajemen risiko diperbarui, laporan hasil monitoring.	Agenda dan notulen rapat berkala, laporan monitoring status implementasi manajemen risiko, laporan reviu berkala komunikasi konfirmasi status implementasi manajemen risiko.
5	Organisasi sudah melakukan konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan mengomunikasikan hasilnya kepada pihak yang tepat di dalam organisasi, diterapkan pada seluruh aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan diperbaiki secara berkelanjutan	Ada evaluasi berkelanjutan untuk meningkatkan proses konfirmasi status implementasi manajemen risiko.	Laporan evaluasi berkala, action plan perbaikan.

37 Kontrol 1.4.7.b:

Kontrol	Tetapkan serta terapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa organisasi tidak hanya mengevaluasi risiko internal, tetapi juga risiko yang berkaitan dengan pihak ketiga (vendor, mitra, atau subkontraktor). Organisasi perlu menetapkan kebijakan dan prosedur untuk menilai kepatuhan pihak terkait terhadap standar keamanan siber.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Checklist atau kuesioner penilaian pihak ketiga Formulir yang digunakan untuk menilai status kepatuhan vendor atau mitra terhadap kebijakan keamanan siber. - Kontrak atau perjanjian keamanan siber Dokumen yang mencantumkan kewajiban penerapan keamanan siber bagi pihak ketiga. - Laporan audit vendor Hasil audit yang menunjukkan tingkat kepatuhan pihak ketiga. - Notulensi rapat dengan dengan vendor Notulensi pertemuan yang membahas status risiko dan tindakan mitigasi.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.RM-01, GV.RM-06, GV.RR-03** **NIST CSF 1.1: ID.RM-1** **NIST SP 800-53r5: PM-9, PM-28** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.7.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait.	Tidak ada mekanisme penilaian risiko pihak terkait.	Tidak ada dokumen pendukung.
1	Organisasi sudah menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait, namun baru diterapkan pada sebagian kecil aspek dan belum diformalkan	Ada upaya awal menilai pihak terkait, hanya beberapa pihak terkait yang diminta menginformasikan status keamanannya, prosesnya bersifat informal dan belum terdokumentasi.	Email komunikasi dengan vendor.
2	Organisasi sudah menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait, diterapkan pada sebagian besar aspek namun belum diformalkan	Ada proses lebih terstruktur untuk menilai risiko pihak terkait yang mencakup sebagian besar pihak terkait, tetapi belum ada kebijakan formal.	Daftar pihak terkait dengan status keamanan, draft template evaluasi risiko pihak terkait, catatan tanggapan pihak terkait.
3	Organisasi sudah menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait, diterapkan pada seluruh aspek dan telah diformalkan	Proses konfirmasi status penerapan manajemen risiko keamanan pihak terkait telah terdokumentasi dalam kebijakan resmi.	Kebijakan evaluasi vendor, SLA dengan klausul keamanan.
4	Organisasi sudah menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait, diterapkan pada seluruh aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Dilakukan pemantauan dan reviu berkala terhadap proses konfirmasi status penerapan manajemen risiko keamanan pihak terkait.	Jadwal reviu pihak terkait, laporan hasil monitoring, laporan audit berkala pihak terkait.
5	Organisasi sudah menetapkan serta menerapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait, diterapkan pada seluruh aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan diperbaiki secara berkelanjutan	Proses evaluasi dan pemutakhiran kebijakan dan mekanisme konfirmasi status penerapan manajemen risiko keamanan pihak terkait dilakukan secara rutin, diterapkan perbaikan dari hasil temuan dan feedback, dilakukan continuous improvement terdokumentasi.	Rencana perbaikan dan update kebijakan konfirmasi status penerapan manajemen risiko keamanan pihak terkait, versi kebijakan terbaru.

38 Kontrol 1.4.7.c:

Kontrol	Penyelenggara IIV memiliki meknisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa organisasi melakukan audit internal maupun eksternal secara berkala untuk menilai efektivitas manajemen risiko. Hasil audit digunakan untuk perbaikan berkelanjutan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan audit keamanan siber Dokumen hasil audit internal atau eksternal. - Dokumentasi tindakan perbaikan (Corrective action plan) Catatan mengenai rekomendasi audit dan tindak lanjut yang dilakukan. - Kebijakan dan prosedur audit Dokumen yang menjelaskan bagaimana audit dilakukan.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.RM-01, GV.RM-06, GV.RR-03** **NIST CSF 1.1: ID.RM-1** **NIST SP 800-53r5: PM-9, PM-28** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.7.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko atau mengimplementasikan rekomendasi perbaikan. Tidak ada upaya yang dilakukan untuk merencanakan atau mengimplementasikan aktivitas tersebut.	Tidak ada audit proses manajemen risiko.	Tidak tersedia laporan audit atau perencanaan audit manajemen risiko.
1	Organisasi telah memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan, namun baru diterapkan pada sebagian kecil aspek dan belum diformalkan	Terdapat audit awal yang dilakukan hanya terhadap area terbatas, pelaksanaannya bersifat ad-hoc atau informal, dan tidak ada prosedur baku atau kebijakan formal.	Email atau notulen audit informal, rencana audit terbatas, draft laporan audit awal.
2	Organisasi telah memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan, telah diterapkan pada sebagian besar aspek namun belum diformalkan	Audit terhadap sebagian besar aspek dilakukan tetapi belum memiliki kebijakan resmi, rekomendasi perbaikan diimplementasikan namun belum dalam kerangka kebijakan resmi.	Laporan audit internal dan eksternal sebagian, tindak lanjut terbatas tercatat, draft kebijakan atau prosedur audit.
3	Organisasi telah memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan, telah diterapkan pada seluruh besar aspek dan telah diformalkan	Audit telah menjadi bagian dari kebijakan organisasi, terdapat jadwal audit yang terstruktur, dan rekomendasi dilaksanakan serta dilacak.	Kebijakan audit, jadwal audit, laporan audit lengkap, dan dokumentasi implementasi rekomendasi.
4	Organisasi telah memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan, telah diterapkan pada seluruh besar aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala meninjau kembali dan mengevaluasi efektivitasnya. Ada upaya untuk memastikan bahwa audit tersebut tetap relevan dan efisien seiring waktu.	Audit dilakukan berkala dan hasilnya direviu, relevansi audit dievaluasi seiring perubahan bisnis, dan audit menjadi bagian dari program pemantauan berkelanjutan.	Rencana monitoring efektivitas audit, hasil evaluasi berkala, rekomendasi penyesuaian kebijakan audit.
5	Organisasi telah memiliki mekanisme untuk melakukan audit internal dan eksternal terhadap proses manajemen risiko dan mengimplementasikan rekomendasi perbaikan, telah diterapkan pada seluruh besar aspek dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan untuk memastikan bahwa Organisasi terus berkembang dan meningkatkan keefektifan dan efisiensinya.	Audit dan evaluasi dilakukan untuk perbaikan berkelanjutan.	Evaluasi audit berkala, revisi kebijakan audit, continuous improvement report.

1.4.8. Melakukan reviu terhadap hasil penerapan manajemen risiko

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan reviu risiko terhadap profil risiko secara periodik atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah risiko, atau informasi bahwa mitigasi risiko yang sudah terlaksana tidak efektif
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk melakukan reviu secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan reviu yang rutin, organisasi dapat memastikan bahwa proses manajemen risiko tetap relevan dan efektif
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur untuk melakukan reviu secara efektif dan menyeluruh
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

39 Kontrol 1.4.8.a:

Kontrol	Penyelenggara IIV melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko
Deskripsi Kontrol	Kontrol ini memastikan bahwa organisasi melakukan reviu terhadap manajemen risiko secara berkala serta ketika ada informasi baru yang berpotensi mempengaruhi profil risiko. Tujuan dari reviu ini adalah untuk memastikan bahwa strategi mitigasi risiko yang telah diterapkan tetap efektif dan sesuai dengan perkembangan ancaman yang ada.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan reviu manajemen risiko Dokumen yang mencatat hasil reviu risiko, termasuk perubahan dalam profil risiko dan langkah mitigasi yang diperbarui. - Notulensi rapat reviu risiko Catatan pertemuan yang membahas hasil reviu risiko dan langkah tindak lanjut. - Hasil audit keamanan siber Dokumen audit yang menyoroti efektivitas mitigasi risiko dan rekomendasi perbaikan. - Dokumentasi perubahan profil risiko Dokumen atau sistem yang menunjukkan pembaruan terhadap peta risiko organisasi berdasarkan informasi baru. - Surat persetujuan dari pimpinan Dokumen resmi yang menunjukkan bahwa pimpinan telah menyetujui hasil reviu dan tindakan mitigasi yang diusulkan.
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH015 TH024 TH026 TH035 TH040 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075 TH008 TH010 TH012 TH023 TH025 TH027 TH039 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 1.4.8.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko. Tidak ada upaya yang dilakukan untuk merencanakan atau mengimplementasikan aktivitas tersebut.	Tidak ada bukti bahwa organisasi melakukan reviu manajemen risiko atau rencana pelaksanaan reviu manajemen risiko. Tidak ada mekanisme atau kebijakan terkait reviu manajemen risiko.	Tidak ada dokumen atau catatan terkait reviu risiko.
1	Organisasi sudah melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko, tetapi baru diterapkan pada sebagian kecil aspek dan belum diformalkan	Organisasi telah mulai melakukan reviu manajemen risiko secara ad-hoc dan terbatas, tetapi belum memiliki kebijakan atau prosedur yang formal.	Draft laporan reviu, email atau komunikasi informal terkait perubahan risiko.
2	Organisasi sudah melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko, telah diterapkan pada sebagian besar aspek namun belum diformalkan	Reviu telah mencakup sebagian besar aspek, tetapi belum diatur dalam kebijakan atau SOP formal.	Laporan reviu manajemen risiko parsial, template reviu manajemen risiko, catatan rapat internal.
3	Organisasi sudah melakukan reviu secara keseluruhan terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko dan telah diformalkan	Terdapat SOP/prosedur reviu manajemen risiko yang berlaku untuk seluruh aspek dan dijalankan secara rutin berdasarkan kebijakan atau prosedur yang ditetapkan.	Laporan reviu manajemen risiko formal, notulensi rapat pimpinan terkait evaluasi manajemen risiko, kebijakan terkait reviu manajemen risiko.
4	Organisasi sudah melakukan reviu secara keseluruhan dan disahkan oleh pimpinan terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko, dilakukan monitoring dan direviu secara berkala	Reviu manajemen risiko telah menjadi bagian dari kebijakan organisasi, disetujui oleh pimpinan, dan dilakukan pemantauan serta evaluasi berkala terhadap implementasi hasil reviu.	Laporan reviu yang telah ditandatangani pimpinan, dokumen monitoring reviu manajemen risiko
5	Organisasi sudah melakukan reviu secara keseluruhan dan disahkan oleh pimpinan terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan	Reviu risiko dilakukan secara periodik dan berkala dengan perbaikan berkelanjutan berdasarkan hasil evaluasi.	Laporan evaluasi berkelanjutan, dan laporan peningkatan berkelanjutan berdasarkan hasil reviu.

1.5. Mengelola risiko rantai pasok

Penyelenggara IIV mengidentifikasi prioritas, rintangan, toleransi risiko, dan asumsi penyelenggara IIV yang perlu ditetapkan dan digunakan untuk mendukung keputusan risiko yang terkait dengan pengelolaan risiko rantai pasokan. Penyelenggara IIV telah menetapkan dan mengimplementasikan proses untuk mengidentifikasi, menilai dan mengelola risiko rantai pasokan.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok;
b) mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV;
c) memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV;
d) melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya; dan
e) menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Mengelola risiko rantai pasok” secara efektif antara lain:

NIST CSF 2.0	**:**	**GV.SC-01, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, GV.OC-02, GV.RM-05, ID.IM-02, ID.RA-10**
NIST CSF 1.1	**:**	**ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5**
NIST SP 800-53r5	**:**	**PM-9, PM-30, RA-3, SA-4, SA-9, SA-11, SA-15, SR-1, SR-2, SR-3, SR-5, SR-6, AU-6, CA-2, CA-7, PS-7, CP-2, CP-4, IR-3, IR-4, IR-8, IR-9**
SNI ISO/IEC 27001:2022	**:**	**5.19, 5.20, 5.21, 5.22, 5.29**

1.5.1. Mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok

Kriteria	Detail
Deskripsi	Penyelenggara IIV merumuskan langkah-langkah keamanan yang relevan terhadap rantai pasokan bisnis/layanan IIV, dengan mempertimbangkan proses manajemen risiko rantai pasokan yang meliputi jenis akses yang diberikan, alasan kebutuhan akses, metode akses, jangka waktu, dan potensi risiko yang terjadi apabila akses tersebut disalahgunakan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk mengembangkan dan mengimplementasikan proses manajemen risiko rantai pasok.
Dampak	**Tinggi** – Dengan proses yang jelas, organisasi dapat mengidentifikasi dan mengelola risiko rantai pasok secara efektif, sehingga mengurangi kemungkinan terjadinya insiden keamanan yang disebabkan oleh pihak ketiga.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif dan perencanaan untuk mengembangkan proses manajemen risiko rantai pasok yang efektif
Referensi Kontrol	**NIST CSF 2.0: GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10, GV.RM-05** **NIST CSF 1.1: ID.SC-1** **NIST SP 800-53r5: PM-30, SA-9, SR-1, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21, 5.22**

40 Kontrol 1.5.1.a:

Kontrol	Merumuskan standar tindakan keamanan yang relevan dengan rantai pasokan dan menyepakati konten dengan mitra bisnis setelah memperjelas ruang lingkup tanggung jawab masing-masing
Deskripsi Kontrol	Penyelenggara IIV harus merumuskan standar tindakan keamanan yang relevan dengan rantai pasokan untuk memastikan bahwa seluruh pihak yang terlibat dalam proses pasokan, baik internal maupun mitra bisnis eksternal, mematuhi kebijakan dan prosedur keamanan yang sesuai. Standar ini bertujuan untuk melindungi integritas dan kerahasiaan informasi yang mengalir melalui rantai pasokan. Penyepakatan konten dengan mitra bisnis harus dilakukan setelah memperjelas ruang lingkup tanggung jawab masing-masing pihak dalam mengelola dan melindungi aset informasi. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi telah merumuskan tindakan keamanan yang jelas, serta menyepakati dan memastikan tanggung jawab keamanan antara organisasi dan mitra bisnis dalam rantai pasokan.
Deskripsi Bukti Dukung	Bukti Dukung yang diperlukan untuk memastikan penerapan standar keamanan dalam rantai pasok antara lain: - Kebijakan atau prosedur yang mengatur standar keamanan dalam rantai pasokan. - Perjanjian atau kontrak dengan mitra bisnis yang mencantumkan kewajiban keamanan siber dan ruang lingkup tanggung jawab. - Dokumen kesepakatan antara organisasi dan mitra bisnis terkait standar keamanan yang diterapkan. - Notulen rapat yang membahas penyusunan dan penyepakatan standar keamanan dengan mitra bisnis. - Daftar pemangku kepentingan dalam rantai pasokan yang terlibat dalam penerapan standar keamanan. - Laporan peninjauan atau audit terhadap implementasi standar keamanan dalam rantai pasokan.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10, GV.RM-05** **NIST CSF 1.1: ID.SC-1** **NIST SP 800-53r5: PM-30, SA-9, SR-1, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21, 5.22**

Kriteria Pemenuhan Kontrol 1.5.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki standar tindakan keamanan yang relevan terkait rantai pasok	Tidak Ada	Tidak Ada
1	Organisasi telah merumuskan sebagian kecil aspek standar tindakan keamanan yang relevan terkait rantai pasok tapi belum diformalkan dalam bentuk NSPK	Organisasi memiliki draft awal standar keamanan rantai pasok yang masih dalam tahap perumusan.	- Dokumen konsep atau draft kebijakan keamanan rantai pasok. - Notulensi diskusi awal terkait penyusunan kebijakan keamanan rantai pasok.
2	- Organisasi telah merumuskan sebagian kecil aspek standar tindakan keamanan yang relevan terkait rantai pasok tapi belum diformalkan dalam bentuk NSPK. - Hal-hal kesepakatan terkait konten keamanan dengan mitra bisnis mulai diperjelas.	Organisasi memiliki kebijakan keamanan rantai pasok yang masih dalam tahap pengembangan tetapi telah mulai dibahas dengan mitra bisnis.	- Draft kebijakan keamanan rantai pasok yang sedang dibahas dengan mitra bisnis. - Catatan atau dokumen yang menunjukkan adanya diskusi awal dengan mitra bisnis terkait keamanan rantai pasok.
3	- Organisasi telah merumuskan seluruh aspek standar tindakan keamanan yang relevan terkait rantai pasok dan telah diformalkan dalam bentuk NSPK. - Hal-hal terkait kesepakatan pembagian peran dan tanggung jawab masing-masing pihak telah ditentukan.	- Organisasi telah memiliki dokumen NSPK yang mencakup seluruh aspek keamanan rantai pasok dan telah ditetapkan secara formal. - Kesepakatan dengan mitra bisnis terkait pembagian peran dan tanggung jawab keamanan telah didokumentasikan	- Dokumen NSPK yang mencakup seluruh aspek keamanan rantai pasok. - Perjanjian atau kontrak yang mencantumkan pembagian peran dan tanggung jawab keamanan.
4	- Organisasi telah merumuskan seluruh aspek standar tindakan keamanan yang relevan terkait rantai pasok dan telah diformalkan dalam bentuk NSPK. - Hal-hal terkait implementasi keamanan dengan pihak-pihak terkait telah dimonitoring, direviu secara berkala untuk mendapatkan hasil yang efektif	Organisasi telah memiliki sistem monitoring dan reviu berkala terhadap implementasi keamanan rantai pasok.	- Laporan hasil monitoring dan reviu keamanan rantai pasok. - Dokumentasi hasil evaluasi risiko rantai pasok. - Notulensi pertemuan koordinasi dengan mitra bisnis terkait monitoring keamanan rantai pasok.
5	- Organisasi telah merumuskan seluruh aspek standar tindakan keamanan yang relevan terkait rantai pasok dan telah diformalkan dalam bentuk NSPK. - Hal-hal terkait implementasi keamanan dengan pihak-pihak terkait dimonitoring, direviu secara berkala, dan dilakukan perbaikan untuk mendapatkan hasil yang efektif	Organisasi tidak hanya memonitor dan mereviu keamanan rantai pasok secara berkala tetapi juga menerapkan perbaikan berkelanjutan berdasarkan hasil evaluasi.	- Dokumen kebijakan yang telah diperbarui berdasarkan hasil monitoring dan reviu. - Laporan hasil evaluasi dan rekomendasi perbaikan keamanan rantai pasok. - Bukti implementasi tindakan perbaikan keamanan rantai pasok.

41 Kontrol 1.5.1.b:

Kontrol	Hal yang perlu dipertimbangkan dalam proses manajemen risiko rantai pasokan diantaranya adalah penentuan jenis akses yang diberikan, alasan kebutuhan akses, metode akses, jangka waktu, dan potensi risiko yang terjadi apabila akses tersebut disalahgunakan
Deskripsi Kontrol	Dalam proses manajemen risiko rantai pasokan, penting untuk mempertimbangkan beberapa hal terkait akses yang diberikan kepada pihak ketiga, termasuk jenis akses yang diberikan, alasan kebutuhan akses, metode akses yang digunakan, serta jangka waktu akses yang diberikan. Hal ini bertujuan untuk memastikan bahwa akses yang diberikan sesuai dengan kebutuhan operasional dan tidak berisiko menambah kerentanannya. Selain itu, potensi risiko yang dapat terjadi jika akses tersebut disalahgunakan juga harus diperhitungkan, guna mengidentifikasi dan mengurangi dampak yang mungkin timbul. Tujuan dari kontrol ini adalah untuk memastikan bahwa kebijakan dan kontrol akses yang diterapkan dalam rantai pasokan dapat mengelola risiko yang terkait dengan potensi penyalahgunaan akses tersebut.
Deskripsi Bukti Dukung	Bukti Dukung yang diperlukan untuk memastikan penerapan standar keamanan dalam rantai pasok antara lain: - Kebijakan atau prosedur yang mengatur kontrol akses dan manajemen risiko akses di rantai pasokan. - Dokumen atau kontrak yang menjelaskan jenis akses yang diberikan kepada mitra bisnis dan alasan pemberian akses. - Rekaman permintaan akses yang menjelaskan alasan, metode, dan jangka waktu akses. - Daftar kontrol akses yang mencakup siapa yang memiliki akses dan jenis akses yang diberikan. - Penilaian risiko yang terkait dengan pemberian akses kepada pihak ketiga dan potensi risiko penyalahgunaan akses. - Protokol atau prosedur untuk melakukan audit terhadap akses dan penggunaannya. - Dokumentasi evaluasi dan perbaikan terhadap kontrol akses yang ditemukan memiliki kerentanannya.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10, GV.RM-05** **NIST CSF 1.1: ID.SC-1** **NIST SP 800-53r5: PM-30, SA-9, SR-1, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21, 5.22**

Kriteria Pemenuhan Kontrol 1.5.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum merencanakan pengaturan akses kontrol terkait rantai pasok	Tidak Ada	Tidak Ada
1	Organisasi telah menjalankan sebagian kecil metode penentuan akses yang diberikan terhadap rantai pasok. metode penentuan akses yang telah dilakukan meliputi : 1. Penentuan jenis akses yang diberikan; 2. reviu kebutuhan akses; 3. metode akses yang diberikan; 4. jangka waktu yang diberikan; atau 5. identifikasi potensi risiko yang terjadi apabila akses disalahgunakan namun belum diformalkan	Organisasi telah menerapkan satu atau dua metode dari daftar di atas secara parsial.	- Dokumen awal kebijakan akses rantai pasok. - Catatan akses yang telah diberikan kepada beberapa entitas.
2	Organisasi telah menjalankan sebagian besar metode penentuan akses yang diberikan terhadap rantai pasok. Metode penentuan akses yang telah dilakukan meliputi : 1. Penentuan jenis akses yang diberikan; 2. reviu kebutuhan akses; 3. metode akses yang diberikan; 4. jangka waktu yang diberikan; atau 5. identifikasi potensi risiko yang terjadi apabila akses disalahgunakan. namun belum diformalkan	Organisasi telah menerapkan tiga atau lebih metode dari daftar di atas.	- Draft kebijakan akses yang telah dikembangkan. - Bukti implementasi akses dengan monitoring terbatas.
3	Organisasi telah menjalankan keseluruhan metode penentuan akses yang diberikan terhadap rantai pasok dan telah diformalkan dalam bentuk NSPK. Metode penentuan akses yang telah dilakukan meliputi : 1. Penentuan jenis akses yang diberikan; 2. reviu kebutuhan akses; 3. metode akses yang diberikan; 4. jangka waktu yang diberikan; atau 5. identifikasi potensi risiko yang terjadi apabila akses disalahgunakan.	Semua metode telah diterapkan dan terdokumentasi secara resmi.	- Dokumen NSPK yang mengatur akses dalam rantai pasok. - Bukti penerapan kebijakan akses dalam operasi sehari-hari.
4	Organisasi telah menjalankan keseluruhan metode penentuan akses yang diberikan terhadap rantai pasok dan telah diformalkan dalam bentuk NSPK. Metode penentuan akses yang telah dilakukan meliputi : 1. Penentuan jenis akses yang diberikan; 2. reviu kebutuhan akses;	Monitoring dan reviu dilakukan secara periodik.	- Laporan monitoring dan reviu akses. - Evaluasi kebijakan akses secara berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	3. metode akses yang diberikan; 4. jangka waktu yang diberikan; atau 5. identifikasi potensi risiko yang terjadi apabila akses disalahgunakan. Komponen-komponen terkait telah dimonitoring dan direviu secara berkala namun belum ada upaya perbaikan berkelanjutan		
5	Organisasi telah menjalankan keseluruhan metode penentuan akses yang diberikan terhadap rantai pasok dan telah diformalkan dalam bentuk NSPK. Metode penentuan akses yang telah dilakukan meliputi : 1. Penentuan jenis akses yang diberikan; 2. reviu kebutuhan akses; 3. metode akses yang diberikan; 4. jangka waktu yang diberikan; atau 5. identifikasi potensi risiko yang terjadi apabila akses disalahgunakan. Komponen-komponen terkait telah dimonitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan	Evaluasi dan perbaikan berkelanjutan telah menjadi bagian dari kebijakan akses.	- Dokumen NSPK yang telah direvisi secara berkala. - Laporan hasil monitoring dan evaluasi. - Bukti perubahan atau pembaruan kebijakan akses sesuai rekomendasi evaluasi.

1.5.2. Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mampu mengidentifikasi dan mengevaluasi para pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra) yang dapat menopang bisnis/layanan IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan analisis dan sumber daya untuk mengidentifikasi semua pemasok dan mitra pihak ketiga, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan informasi yang lengkap tentang pemasok dan mitra pihak ketiga, organisasi dapat mengelola risiko dan menjaga keamanan aset informasi dengan lebih baik.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif dan pemetaan semua hubungan dengan pihak ketiga
Referensi Kontrol	**NIST CSF 2.0: GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-07, GV.OC-02, ID.RA-10** **NIST CSF 1.1: ID.SC-2, ID.SC-3** **NIST SP 800-53r5: PM-9, RA-3, SA-4, SA-9, SA-15, SR-2, SR-3, SR-5, SR-6** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21, 5.22**

42 Kontrol 1.5.2.a:

Kontrol	Identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan dengan penyelenggara IIV.
Deskripsi Kontrol	Penyelenggara IIV perlu mengidentifikasi peran dan tanggung jawab keamanan siber dari pemangku kepentingan pihak ketiga, seperti pemasok, pelanggan, atau mitra bisnis, serta pihak lainnya yang berhubungan dengan Penyelenggara IIV. Hal ini untuk memastikan bahwa semua pihak yang terlibat memiliki pemahaman yang jelas mengenai tanggung jawab mereka dalam melindungi aset informasi dan memitigasi risiko terkait. Dengan adanya pembagian peran dan tanggung jawab yang jelas, organisasi dapat lebih efektif dalam mengelola risiko keamanan siber di sepanjang rantai pasokan atau hubungan bisnis.Tujuan dari kontrol ini adalah untuk memastikan bahwa pihak ketiga dan mitra bisnis yang terkait memahami peran dan kewajiban mereka dalam hal keamanan siber yang dapat mempengaruhi organisasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa dokumen kebijakan, perjanjian kontrak, atau audit kepatuhan yang menunjukkan bahwa peran dan tanggung jawab keamanan siber telah diidentifikasi dan diterapkan oleh pihak ketiga, misalnya: - Daftar pemangku kepentingan eksternal yang terlibat, seperti pemasok, pelanggan, dan mitra bisnis, beserta peran mereka dalam organisasi. - Perjanjian atau kontrak dengan pihak ketiga yang mencantumkan tanggung jawab keamanan siber dan kewajiban masing-masing pihak. - Protokol atau prosedur untuk memastikan pemangku kepentingan memahami dan mematuhi peran mereka dalam keamanan siber. - Laporan audit atau penilaian yang menunjukkan kepatuhan pemangku kepentingan terhadap kewajiban keamanan siber mereka. - Rencana penanggulangan risiko yang mencakup tanggung jawab yang diberikan kepada pihak ketiga terkait keamanan siber. - Rekaman komunikasi yang menyepakati peran dan tanggung jawab keamanan siber dengan pemangku kepentingan eksternal.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.OC-02, GV.SC-03, GV.SC-04, GV.SC-07, ID.RA-10** **NIST CSF 1.1: ID.SC-2** **NIST SP 800-53r5: PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6** **SNI ISO/IEC 27001:2022: 5.22**

Kriteria Pemenuhan Kontrol 1.5.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menjalankan identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan.	Tidak Ada	Tidak Ada
1	Organisasi telah melaksanakan sebagian kecil aspek identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan, dan belum diformalkan.	Identifikasi dilakukan secara informal tanpa adanya dokumentasi resmi.	Draft awal kebijakan atau komunikasi awal dengan pihak ketiga.
2	Organisasi telah melaksanakan sebagian besar aspek identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan namun belum diformalkan.	Identifikasi mencakup sebagian besar pihak ketiga, namun belum ada standar dokumentasi formal.	Laporan internal terkait identifikasi pihak ketiga.
3	Organisasi telah melaksanakan keseluruhan identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan dan telah diformalkan.	Identifikasi mencakup seluruh pihak ketiga dan terdokumentasi secara resmi.	Dokumen formal peran dan tanggung jawab pihak ketiga.
4	Organisasi telah melaksanakan keseluruhan identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya dan telah diformalkan. Hasil identifikasi dilakukan monitoring dan reviu secara berkala.	Identifikasi dikaji ulang secara berkala untuk memastikan efektivitas.	Laporan monitoring dan reviu berkala.
5	Organisasi telah melaksanakan keseluruhan identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya dan telah diformalkan. Hasil identifikasi dilakukan monitoring dan reviu secara berkala serta perbaikan yang berkelanjutan.	Evaluasi berkala digunakan untuk meningkatkan efektivitas identifikasi.	Dokumen hasil evaluasi dan perbaikan berkala.

43 Kontrol 1.5.2.b:

Kontrol	Merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga.
Deskripsi Kontrol	Penyelenggara IIV perlu merumuskan dan mengelola persyaratan keamanan yang berlaku bagi anggota atau personel pihak ketiga, serta pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga. Hal ini bertujuan untuk memastikan bahwa personel pihak ketiga atau pihak eksternal yang terlibat dalam penyediaan layanan kepada organisasi mematuhi standar keamanan yang telah ditetapkan. Persyaratan ini mencakup kebijakan keamanan informasi, kontrol akses, pelatihan keamanan, serta prosedur yang harus diikuti untuk melindungi aset dan data yang sensitif. Tujuan dari kontrol ini adalah untuk memastikan bahwa pihak ketiga dan personil yang terlibat dalam operasi layanan memiliki kewajiban dan standar yang jelas terkait keamanan siber.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur keamanan siber yang diterapkan kepada anggota atau personel pihak ketiga. - Kontrak atau perjanjian dengan pihak ketiga yang mencantumkan persyaratan keamanan siber yang harus dipatuhi oleh personel mereka. - Protokol kontrol akses yang mengatur hak akses bagi anggota atau personel pihak ketiga dalam sistem atau jaringan organisasi. - Program pelatihan atau sertifikasi keamanan siber untuk personel pihak ketiga. - Audit atau penilaian terhadap implementasi persyaratan keamanan oleh pihak ketiga. - Dokumen yang menjelaskan standar keamanan yang harus dipatuhi oleh pihak ketiga dan pemangku kepentingan lainnya.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-05** **NIST CSF 1.1: ID.SC-3** **NIST SP 800-53r5, SA-4, SA-9, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20,5.21**

Kriteria Pemenuhan Kontrol 1.5.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki program perumusan dan pengelolaan persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga.	Tidak Ada	Tidak Ada
1	Organisasi telah merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga, yang diterapkan pada sebagian kecil aspek namun belum diformalkan	Hanya mencakup beberapa pihak ketiga tanpa dokumentasi formal.	Draft awal kebijakan keamanan.
2	Organisasi telah merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga, yang diterapkan pada sebagian besar aspek namun belum diformalkan	Kebijakan hampir lengkap tetapi belum diimplementasikan sepenuhnya.	Laporan internal terkait persyaratan keamanan.
3	Organisasi telah secara menyeluruh merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga secara efektif. Penyusunan program telah melibatkan pihak-pihak terkait termasuk pihak ketiga yang terlibat dan telah diformalkan.	Persyaratan keamanan diterapkan secara efektif dengan dokumentasi formal.	Dokumen kebijakan keamanan yang berlaku.
4	Organisasi telah menjalankan keseluruhan program perumusan dan pengelolaan persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga secara efektif. Penyusunan program telah melibatkan pihak-pihak terkait termasuk pihak ketiga yang terlibat. Program yang disusun dilakukan monitoring dan reviu secara berkala untuk mengukur tingkat efektifitas kegiatan.	Evaluasi reguler diterapkan untuk menjaga efektivitas.	Laporan hasil monitoring dan evaluasi.
5	Organisasi telah menjalankan keseluruhan program perumusan dan pengelolaan persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga secara efektif. Penyusunan program telah melibatkan pihak-pihak terkait termasuk pihak ketiga yang terlibat. Program yang disusun dilakukan monitoring, reviu dan diperbaiki secara berkala untuk meningkatkan efektifitas kegiatan.	Perbaikan berkelanjutan diterapkan berdasarkan hasil evaluasi.	Dokumen revisi kebijakan dan laporan perbaikan berkala.

1.5.3. Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV memastikan bahwa manajemen, produk atau layanan, dan personel yang disediakan oleh pihak ketiga telah dengan benar mematuhi persyaratan keamanan sesuai dengan standar dan peraturan perundangan yang berlaku.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk mengevaluasi serta menyesuaikan perjanjian kerja sama, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan perjanjian yang sesuai, organisasi dapat memastikan bahwa pemasok dan mitra pihak ketiga mematuhi kebijakan keamanan siber yang ditetapkan, sehingga mengurangi risiko keamanan
Kompleksitas	**Sedang** – Memerlukan evaluasi yang komprehensif dan penyesuaian perjanjian kerja sama untuk memastikan kepatuhan terhadap kebijakan keamanan.
Referensi Kontrol	**NIST CSF 2.0: GV.SC-05** **NIST CSF 1.1: ID.SC-3** **NIST SP 800-53r5: SA-4, SA-9, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21**

44 Kontrol 1.5.3.a:

Kontrol	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah manajemen pihak ketiga telah dengan benar mematuhi persyaratan keamanan, standar, dan peraturan perundangan yang berlaku, dengan mempertimbangkan tujuan kontrak tersebut dan hasil manajemen risiko.
Deskripsi Kontrol	Penyelenggara IIV perlu merumuskan dan mengelola persyaratan keamanan yang berlaku bagi anggota atau personel pihak ketiga, serta pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga. Hal ini bertujuan untuk memastikan bahwa personel pihak ketiga atau pihak eksternal yang terlibat dalam penyediaan layanan kepada organisasi mematuhi standar keamanan yang telah ditetapkan. Persyaratan ini mencakup kebijakan keamanan informasi, kontrol akses, pelatihan keamanan, serta prosedur yang harus diikuti untuk melindungi aset dan data yang sensitif. Tujuan dari kontrol ini adalah untuk memastikan bahwa pihak ketiga dan personil yang terlibat dalam operasi layanan memiliki kewajiban dan standar yang jelas terkait keamanan siber.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Salinan kontrak yang mencantumkan persyaratan keamanan, standar, dan peraturan yang wajib dipatuhi oleh pihak ketiga. - Laporan audit kepatuhan yang menunjukkan bahwa pihak ketiga mematuhi persyaratan keamanan yang relevan. - Penilaian manajemen risiko yang dilakukan terhadap risiko yang mungkin ditimbulkan oleh pihak ketiga. - Dokumentasi terkait pembahasan dan evaluasi kepatuhan pihak ketiga terhadap regulasi dan standar yang berlaku dalam konteks kontrak. - Sertifikat atau bukti bahwa pihak ketiga memenuhi standar keamanan yang relevan (misalnya ISO/IEC27001 atau standar keamanan lainnya). - Daftar temuan dari evaluasi risiko yang menunjukkan tindakan mitigasi yang harus diambil oleh pihak ketiga untuk mematuhi persyaratan keamanan.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-05** **NIST CSF 1.1: ID.SC-3** **NIST SP 800-53r5: SA-4, SA-9, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21**

Kriteria Pemenuhan Kontrol 1.5.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan kegiatan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak.	Tidak Ada	Tidak Ada
1	Organisasi telah melakukan kegiatan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak, yang diterapkan pada sebagian kecil aspek namun belum diformalkan	Pemeriksaan hanya dilakukan pada sebagian kecil aspek, misalnya hanya mencakup pemenuhan standar dasar keamanan atau sebagian kecil dari ruang lingkup kontrak.	- Draft kontrak yang mencantumkan sebagian kecil aspek keamanan. - Bukti komunikasi awal mengenai persyaratan keamanan dengan pihak ketiga. - Laporan internal terkait verifikasi keamanan yang masih terbatas pada aspek tertentu.
2	Organisasi telah melakukan kegiatan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak. yang diterapkan pada sebagian besar aspek namun belum diformalkan	Pemeriksaan dilakukan terhadap sebagian besar aspek kontrak tetapi belum sepenuhnya menyeluruh atau terdokumentasi secara formal.	- Draft kontrak yang mencantumkan sebagian besar aspek keamanan. - Hasil evaluasi internal yang mencakup sebagian besar aspek kontrak. - Notulen rapat terkait pembahasan persyaratan keamanan dengan pihak ketiga.
3	Organisasi telah melakukan keseluruhan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak secara menyeluruh dengan mempertimbangkan dari tujuan penandatanganan kontrak serta hasil manajemen risiko. Pelaksanaan telah diformalkan.	Pemeriksaan sudah mencakup seluruh aspek keamanan yang diperlukan dan sudah terdokumentasi secara formal.	- Dokumen kontrak yang sudah mencakup seluruh aspek keamanan. - Laporan hasil evaluasi manajemen risiko pihak ketiga. - Dokumentasi hasil audit internal sebelum penandatanganan kontrak.
4	Organisasi telah mewajibkan menjalankan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak secara menyeluruh dengan mempertimbangkan dari tujuan penandatanganan kontrak serta hasil manajemen risiko. Komponen-komponen yang menjadi perhatian dalam kontrak	Selain pemeriksaan awal, organisasi juga melakukan pemantauan secara berkala terhadap kepatuhan pihak ketiga terhadap perjanjian keamanan siber.	- Dokumen kebijakan yang mengatur pemantauan rutin terhadap kepatuhan pihak ketiga. - Laporan monitoring dan reviu keamanan siber terkait pihak ketiga. - Kontrak dengan klausul pemantauan berkala terkait keamanan siber.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	dilakukan monitoring, reviu secara berkala namun belum dilakukan perbaikan berkelanjutan		
5	Organisasi telah mewajibkan menjalankan pemeriksaan kepatuhan manajemen pihak ketiga terhadap persyaratan keamanan, standar, dan peraturan perundangan yang berlaku saat penandatangan kontrak secara menyeluruh dengan mempertimbangkan dari tujuan penandatanganan kontrak serta hasil manajemen risiko. Komponen-komponen yang menjadi perhatian dalam kontrak dilakukan monitoring, reviu secara berkala, dan telah dilakukan perbaikan berkelanjutan	Organisasi tidak hanya melakukan pemantauan tetapi juga menerapkan perbaikan berkelanjutan untuk meningkatkan kepatuhan dan mitigasi risiko yang lebih baik.	- Laporan pemantauan yang menunjukkan perbaikan yang dilakukan oleh pihak ketiga. - Kontrak yang mencakup klausul pembaruan dan peningkatan keamanan secara berkala. - Dokumentasi hasil audit serta rencana perbaikan yang diterapkan berdasarkan evaluasi.

45 Kontrol 1.5.3.b:

Kontrol	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah produk dan layanan yang disediakan oleh pihak ketiga sesuai dengan persyaratan keamanan yang ada di organisasi.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa produk dan layanan yang disediakan oleh pihak ketiga memenuhi persyaratan keamanan yang ditetapkan oleh organisasi. Hal ini penting untuk memastikan bahwa produk atau layanan yang diberikan tidak menambah risiko terhadap keamanan siber organisasi. Pemeriksaan ini dilakukan sebelum penandatanganan kontrak untuk memverifikasi kesesuaian produk dan layanan pihak ketiga dengan standar dan kebijakan keamanan organisasi, serta memastikan bahwa potensi ancaman atau kerentanannya dapat diminimalkan. Tujuan dari kontrol ini adalah untuk memastikan bahwa Penyelenggara IIV hanya bekerja dengan pihak ketiga yang dapat menyediakan solusi atau layanan yang aman dan sesuai dengan kebijakan keamanan yang berlaku.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Spesifikasi teknis produk dan layanan yang diberikan oleh pihak ketiga, yang mencakup kontrol keamanan yang diterapkan. - Penilaian risiko yang menunjukkan potensi ancaman atau kerentanannya terhadap organisasi. - Hasil audit keamanan yang menunjukkan kesesuaian produk atau layanan dengan kebijakan keamanan organisasi. - Kontrak atau perjanjian yang memuat klausul yang mengharuskan pihak ketiga untuk memenuhi standar keamanan yang berlaku di organisasi. - Bukti pengujian keamanan yang dilakukan pada produk atau layanan pihak ketiga (misalnya, hasil penetration testing atau vulnerability assessment). - Sertifikasi atau laporan kepatuhan dari pihak ketiga yang menunjukkan pemenuhan terhadap standar atau regulasi yang relevan, seperti ISO/IEC 27001 atau standar industri lainnya.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-05** **NIST CSF 1.1: ID.SC-3** **NIST SP 800-53r5: SA-4, SA-9, SR-2, SR-3, SR-5** **SNI ISO/IEC 27001:2022: 5.19, 5.20, 5.21**

Kriteria Pemenuhan Kontrol 1.5.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan kegiatan pemeriksaan terhadap produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi.	Tidak Ada	Tidak Ada
1	Organisasi telah melaksanakan kegiatan pemeriksaan terhadap produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi, yang diterapkan pada sebagian kecil aspek namun belum diformalkan	Hanya sebagian kecil produk dan layanan yang diperiksa tanpa prosedur yang terdokumentasi secara resmi.	- Catatan atau laporan informal terkait evaluasi sebagian kecil produk atau layanan. - Bukti komunikasi awal terkait persyaratan keamanan produk.
2	Organisasi telah melaksanakan pemeriksaan terhadap produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi namun pelaksanaanya pada sebagian besar aspek dan masih belum menyeluruh, serta belum diformalkan	Sebagian besar aspek produk dan layanan sudah diperiksa, namun belum ada dokumen kebijakan yang mengaturnya.	- Laporan internal terkait pemeriksaan sebagian besar aspek produk dan layanan. - Dokumen hasil evaluasi teknis keamanan.
3	Organisasi telah melaksanakan pemeriksaan terhadap produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi, diterapkan pada seluruh aspek dan telah diformalkan	Pemeriksaan dilakukan pada seluruh aspek produk dan layanan dengan dokumen kebijakan yang jelas.	- Laporan hasil audit produk dan layanan pihak ketiga. - Klausul keamanan dalam kontrak.
4	Organisasi telah mewajibkan terhadap pemeriksaan produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi secara menyeluruh dan telah diformalkan. Komponen-komponen yang menjadi perhatian dalam kontrak dilakukan reviu secara berkala namun belum dilakukan perbaikan berkelanjutan	Pemeriksaan telah diformalkan, dilakukan reviu berkala, tetapi belum dilakukan perbaikan berkelanjutan.	- Dokumentasi evaluasi berkala. - Bukti implementasi perbaikan berkelanjutan dalam kebijakan organisasi.
5	Organisasi telah mewajibkan terhadap pemeriksaan produk dan layanan yang disediakan oleh pihak ketiga telah sesuai dengan persyaratan keamanan yang ada di organisasi secara menyeluruh dan telah diformalkan. Komponen-komponen yang menjadi perhatian dalam kontrak dilakukan reviu secara berkala dan dilakukan perbaikan secara berkelanjutan	Pemeriksaan telah diformalkan, dilakukan reviu berkala, dan perbaikan berkelanjutan.	- Dokumentasi evaluasi berkala. - Bukti implementasi perbaikan berkelanjutan dalam kebijakan organisasi

1.5.4. Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan penilaian secara berkala melalui audit, hasil pengujian, atau pemeriksaan lain dari pihak terkait seperti mitra bisnis untuk memastikan mereka memenuhi kewajiban kontraktual mereka.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan audit dan pemeriksaan secara periodik, termasuk waktu, tenaga kerja, dan alat evaluasi.
Dampak	**Tinggi** – Dengan pemeriksaan yang rutin, organisasi dapat mengidentifikasi dan mengatasi potensi masalah keamanan yang terkait dengan pemasok dan mitra pihak ketiga.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk melakukan pemeriksaan secara periodik dan menyeluruh.
Referensi Kontrol	**NIST CSF 2.0: GV.SC-07, ID.RA-10** **NIST CSF 1.1: ID.SC-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, PS-7, SA-9, SA-11** **SNI ISO/IEC 27001:2022: 5.22**

46 Kontrol 1.5.4.a:

Kontrol	Melakukan penilaian secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka.
Deskripsi Kontrol	Penyelenggara IIV harus melakukan penilaian secara berkala terhadap pihak ketiga untuk memastikan bahwa mereka mematuhi kewajiban kontraktual yang telah disepakati. Penilaian ini bisa dilakukan melalui audit, pengujian keamanan, atau pemeriksaan yang dilakukan oleh pihak terkait yang berwenang. Tujuan dari proses ini adalah untuk memastikan bahwa pihak ketiga tetap memenuhi persyaratan yang ditetapkan dalam kontrak, termasuk standar keamanan yang berlaku, serta mengidentifikasi dan menangani potensi risiko yang mungkin muncul selama masa berlakunya kontrak. Dengan demikian, organisasi dapat memastikan bahwa hubungan dengan pihak ketiga tetap aman dan sesuai dengan kesepakatan yang telah dibuat.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan audit internal atau eksternal yang menunjukkan kepatuhan pihak ketiga terhadap kewajiban kontraktual yang telah disepakati. - Hasil pengujian keamanan yang dilakukan pada produk atau layanan pihak ketiga, misalnya hasil penetration testing atau vulnerability assessment. - Catatan evaluasi dan pemeriksaan berkala yang dilakukan oleh tim pengelola risiko atau keamanan di organisasi. - Surat laporan dari pihak ketiga yang menunjukkan hasil verifikasi atau audit yang telah dilakukan untuk memastikan kepatuhan. - Daftar temuan audit yang menunjukkan ketidaksesuaian dan tindakan yang telah diambil untuk memperbaiki kekurangan tersebut. - Kontrak yang mencantumkan persyaratan audit atau pemeriksaan yang wajib dilakukan terhadap pihak ketiga.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-07, ID.RA-10** **NIST CSF 1.1: ID.SC-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, PS-7, SA-9, SA-11** **SNI ISO/IEC 27001:2022: 5.22**

Kriteria Pemenuhan Kontrol 1.5.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan penilaian	Tidak Ada	Tidak Ada
1	Organisasi telah melakukan penilaian yang diterapkan pada sebagian kecil aspek untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka, namun belum diformalkan	Penilaian dilakukan pada sebagian kecil aspek, tetapi belum diformalkan.	Catatan informal atau laporan insidental terkait evaluasi pemasok.
2	Organisasi telah melakukan penilaian yang diterapkan pada sebagian besar aspek untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka, namun belum diformalkan	Penilaian diterapkan pada sebagian besar aspek, namun belum diformalkan.	Laporan hasil pengujian keamanan tanpa prosedur yang terdokumentasi.
3	Organisasi telah melakukan Penilaian yang diterapkan pada seluruh aspek secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka dan telah diformalkan	Penilaian dilakukan pada seluruh aspek secara berkala dan telah diformalkan.	- Laporan audit berkala yang terdokumentasi. - Hasil pengujian keamanan dengan prosedur standar.
4	Organisasi telah melakukan Penilaian yang diterapkan pada seluruh aspek secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka dan telah diformalkan, dimonitoring dan direviu secara berkala.	Penilaian dilakukan secara berkala, diformalkan, dimonitoring, dan direviu.	- Daftar temuan audit dan tindakan perbaikan yang terdokumentasi. - Evaluasi terhadap hasil audit sebelumnya.
5	Organisasi telah melakukan Penilaian yang diterapkan pada seluruh aspek secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka dan telah diformalkan, dimonitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan	Penilaian dilakukan secara berkala, diformalkan, dimonitoring, direviu, serta ada evaluasi dan perbaikan berkelanjutan.	- Laporan perbaikan berdasarkan evaluasi audit sebelumnya. - Hasil evaluasi efektivitas tindakan korektif.

47 Kontrol 1.5.4.b:

Kontrol	Merumuskan dan menerapkan prosedur untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan.
Deskripsi Kontrol	Penyelenggara IIV harus merumuskan dan menerapkan prosedur yang jelas untuk menangani ketidakpatuhan terhadap persyaratan kontrak yang ditemukan selama penilaian atau audit. Prosedur ini bertujuan untuk memastikan bahwa setiap pelanggaran atau ketidaksesuaian dapat segera diidentifikasi, dievaluasi, dan diperbaiki. Prosedur ini harus mencakup langkah-langkah seperti pemberitahuan resmi kepada pihak ketiga, tindakan perbaikan yang diperlukan, serta penetapan jangka waktu untuk perbaikan. Selain itu, perlu ada mekanisme untuk menentukan apakah ketidakpatuhan tersebut dapat menimbulkan risiko signifikan terhadap keamanan atau integritas layanan yang diberikan oleh pihak ketiga. Tujuan dari prosedur ini adalah untuk menjaga agar kewajiban kontraktual yang berkaitan dengan keamanan tetap dipatuhi dan risiko yang ditimbulkan oleh ketidakpatuhan dapat diminimalkan.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen prosedur atau pedoman yang menjelaskan langkah-langkah yang diambil untuk menangani ketidakpatuhan terhadap persyaratan kontrak. - Laporan atau notifikasi yang menginformasikan pihak ketiga mengenai temuan ketidakpatuhan terhadap persyaratan kontrak. - Dokumen perjanjian atau kontrak yang mencantumkan sanksi atau konsekuensi terhadap ketidakpatuhan, seperti denda atau pemutusan kontrak. - Catatan tentang tindakan korektif yang telah diterapkan untuk menangani ketidakpatuhan, termasuk bukti perbaikan. - Laporan evaluasi ulang setelah tindakan perbaikan untuk memastikan bahwa ketidakpatuhan telah diperbaiki. - Surat atau laporan dari pihak ketiga yang menyatakan bahwa ketidakpatuhan telah diperbaiki dan langkah-langkah pencegahan telah diterapkan.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-07, ID.RA-10** **NIST CSF 1.1: ID.SC-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, PS-7, SA-9, SA-11** **SNI ISO/IEC 27001:2022: 5.22**

Kriteria Pemenuhan Kontrol 1.5.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Prosedur belum dirumuskan	Tidak Ada	Tidak Ada
1	Organisasi telah merumuskan dan menerapkan prosedur pada sebagian kecil aspek untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan, namun belum diformalkan	Prosedur diterapkan pada sebagian kecil aspek, tetapi belum diformalkan.	Catatan insidental terkait penanganan ketidakpatuhan.
2	Organisasi telah merumuskan dan menerapkan prosedur pada sebagian besar aspek untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan, namun belum diformalkan	Prosedur diterapkan pada sebagian besar aspek, namun belum diformalkan.	Laporan ketidakpatuhan tanpa mekanisme tindak lanjut yang jelas.
3	Organisasi telah merumuskan dan menerapkan prosedur pada seluruh aspek untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan, dan telah diformalkan	Prosedur diterapkan pada seluruh aspek dan telah diformalkan.	- Dokumen prosedur penanganan ketidakpatuhan. - Kontrak yang mencantumkan sanksi ketidakpatuhan.
4	Organisasi telah merumuskan dan menerapkan prosedur pada seluruh aspek untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Prosedur diterapkan pada seluruh aspek, diformalkan, dimonitoring, dan direviu.	- Laporan tindakan korektif dan evaluasi efektivitasnya. - Laporan pemantauan kepatuhan terhadap prosedur.
5	Organisasi telah merumuskan dan menerapkan prosedur pada seluruh aspek untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dilakukan evaluasi dan perbaikan berkelanjutan	Prosedur diterapkan pada seluruh aspek, diformalkan, dimonitoring, direviu, serta ada evaluasi dan perbaikan berkelanjutan.	- Analisis perbaikan berkelanjutan berdasarkan data historis ketidakpatuhan. - Evaluasi efektivitas sistem kepatuhan secara keseluruhan.

48 Kontrol 1.5.4.c:

Kontrol	Mengumpulkan dan menyimpan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa data yang mengonfirmasi pemenuhan kewajiban kontraktual dengan pihak atau individu lain disimpan dengan aman dan dikelola dengan tepat. Data ini harus mencakup bukti-bukti yang menunjukkan bahwa kewajiban yang ditetapkan dalam kontrak telah dipenuhi, seperti laporan audit, bukti pengiriman produk atau layanan, serta komunikasi atau persetujuan antara pihak terkait. Penyimpanan data ini harus dilakukan dengan mengutamakan aspek keamanan, termasuk pengamanan fisik dan elektronik, serta mematuhi kebijakan retensi data yang relevan. Tujuan dari prosedur ini adalah untuk memudahkan akses dan pengungkapan data tersebut jika diperlukan untuk keperluan penegakan hukum, serta menjaga integritas dan keaslian data yang relevan dengan kewajiban kontraktual.
Deskripsi Bukti Dukung	Laporan audit atau pengujian yang menunjukkan pemenuhan kewajiban kontraktual. - Dokumen kontrak atau perjanjian yang mencatat kewajiban dan pemenuhan tersebut. - Bukti pengiriman barang atau layanan, termasuk tanda terima atau laporan pengiriman. - Surat atau komunikasi yang menunjukkan persetujuan atau konfirmasi dari pihak terkait. - Prosedur atau pedoman terkait dengan penyimpanan data kontraktual, termasuk kebijakan retensi dan pengamanan data. - Log sistem yang menunjukkan akses yang sah dan pemeliharaan data kontraktual. - Laporan yang menunjukkan langkah-langkah pengamanan dan perlindungan data yang diterapkan untuk menjaga kerahasiaan dan integritas data.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH066 TH074 TH076 TH041 TH052 TH054 TH060 TH071 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-07, ID.RA-10** **NIST CSF 1.1: ID.SC-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, PS-7, SA-9, SA-11** **SNI ISO/IEC 27001:2022: 5.22**

Kriteria Pemenuhan Kontrol 1.5.4.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Pengumpulan dan penyimpanan data belum dilakukan	Tidak Ada	Tidak Ada
1	Organisasi telah melakukan Pengumpulan dan penyimpanan sebagian kecil data dengan aman, namun belum ada prosedur formal	Pengumpulan dan penyimpanan data dilakukan pada sebagian kecil aspek, tetapi belum diformalkan.	Dokumen informal atau komunikasi email terkait pemenuhan kewajiban.
2	Organisasi telah mengumpulkan dan menyimpan sebagian besar data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum, namun belum diformalkan	Pengumpulan dan penyimpanan data dilakukan pada sebagian besar aspek, tetapi belum diformalkan.	Laporan pemenuhan kewajiban tanpa sistem penyimpanan yang jelas.
3	Organisasi telah mengumpulkan dan menyimpan keseluruhan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum, dan telah diformalkan	Pengumpulan dan penyimpanan data dilakukan pada seluruh aspek dan telah diformalkan.	- Dokumen kontrak atau perjanjian yang terdokumentasi. - Bukti pengiriman barang atau layanan.
4	Organisasi telah mengumpulkan dan menyimpan keseluruhan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Pengumpulan dan penyimpanan data dilakukan secara berkala, diformalkan, dimonitoring, dan direviu.	- Log sistem terkait akses dan pemeliharaan data. - Laporan kepatuhan terhadap kebijakan penyimpanan data.
5	Organisasi telah mengumpulkan dan menyimpan keseluruhan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, serta dilakukan evaluasi dan perbaikan berkelanjutan	Pengumpulan dan penyimpanan data dilakukan secara berkala, diformalkan, dimonitoring, direviu, serta ada evaluasi dan perbaikan berkelanjutan.	- Evaluasi efektivitas sistem penyimpanan data. - Kebijakan penyimpanan yang diperbarui berdasarkan hasil monitoring dan reviu.

1.5.5. Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut

Kriteria	Detail
Deskripsi	Penyelenggara IIV perlu menyiapkan dan menguji prosedur untuk respons insiden dengan pihak ketiga (termasuk mitra kerja dan pemasok) yang terlibat dalam penyelenggaraan IIV, untuk memastikan tindakan respons insiden dilaksanakan dalam rantai pasokan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun rencana penanggulangan dan pemulihan, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan rencana yang jelas, organisasi dapat merespons dan pulih dari insiden keamanan dengan cepat, sehingga mengurangi dampak negatif pada operasional dan reputasi organisasi.
Kompleksitas	**Sedang** – Memerlukan koordinasi dengan pihak ketiga dan perencanaan yang komprehensif untuk menyusun rencana penanggulangan dan pemulihan yang efektif.
Referensi Kontrol	**NIST CSF 2.0: GV.SC-08, ID.IM-02** **NIST CSF 1.1: ID.SC-5** **NIST SP 800-53r5: CP-2, CP-4, IR-3, IR-4, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.29**

49 Kontrol 1.5.5.a:

Kontrol	Menyiapkan dan menguji prosedur respons insiden dengan pihak terkait yang terlibat dalam aktivitas respons insiden untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan.
Deskripsi Kontrol	Penyelenggara IIV harus menyiapkan prosedur respons insiden yang jelas dan terstruktur, yang mencakup seluruh pihak terkait dalam rantai pasokan yang terlibat dalam menangani insiden keamanan. Prosedur ini harus mengidentifikasi langkah-langkah yang perlu diambil oleh masing-masing pihak, memastikan bahwa semua pihak mengetahui peran dan tanggung jawabnya dalam respons insiden, serta menguji kesiapan dan efektivitas prosedur tersebut secara berkala. Tujuan dari prosedur ini adalah untuk memastikan bahwa respons terhadap insiden keamanan dapat dilaksanakan dengan cepat, tepat, dan terkoordinasi dengan baik antara organisasi dan pihak ketiga yang terlibat dalam rantai pasokan. Pengujian rutin juga bertujuan untuk memastikan bahwa prosedur tersebut efektif dan dapat diterapkan dengan baik saat terjadi insiden.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Prosedur respons insiden yang mencakup peran dan tanggung jawab pihak ketiga dalam rantai pasokan. - Laporan hasil uji prosedur respons insiden yang melibatkan pihak ketiga. - Dokumen yang mencatat hasil uji coba simulasi insiden dan identifikasi kekurangan dalam respons. - Laporan evaluasi terhadap pengujian prosedur respons insiden dan rekomendasi perbaikan. - Dokumentasi komunikasi dengan pihak ketiga yang terlibat dalam respons insiden. - Rencana pemulihan dan dokumentasi yang terkait dengan dampak insiden terhadap rantai pasokan.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-08, ID.IM-02** **NIST CSF 1.1: ID.SC-5** **NIST SP 800-53r5: CP-2, CP-4, IR-3, IR-4, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.29**

Kriteria Pemenuhan Kontrol 1.5.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Prosedur respons insiden belum dirumuskan	Tidak Ada	Tidak Ada
1	Organisasi telah menerapkan Prosedur respons insiden pada sebagian kecil aspek yang melibatkan pihak terkait untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan, namun belum diformalkan	Diterapkan pada sebagian kecil aspek, belum diformalkan.	Prosedur sementara atau rancangan prosedur awal, tetapi belum diuji.
2	Organisasi telah menerapkan Prosedur respons insiden pada sebagian besar aspek yang melibatkan pihak terkait untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan, namun belum diformalkan	Diterapkan pada sebagian besar aspek, belum diformalkan.	Prosedur telah diuji sebagian, tetapi belum ada dokumentasi formal.
3	Organisasi telah menerapkan Prosedur respons insiden pada seluruh aspek yang melibatkan pihak terkait untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan, dan telah diformalkan	Diterapkan pada seluruh aspek, telah diformalkan.	Dokumen formal prosedur respons insiden yang mencakup seluruh aspek.
4	Organisasi telah menyiapkan dan menguji pada seluruh aspek prosedur respons insiden dengan pihak terkait yang terlibat dalam aktivitas respons insiden untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala	Diterapkan, diformalkan, dimonitoring, dan direviu secara berkala.	Laporan reviu berkala terhadap prosedur respons insiden.
5	Organisasi telah menyiapkan dan menguji pada seluruh aspek prosedur respons insiden dengan pihak terkait yang terlibat dalam aktivitas respons insiden untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan, dan telah diformalkan, dilakukan monitoring dan direviu secara berkala, dievaluasi dan dilakukan perbaikan berkelanjutan	Diterapkan, diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan berkelanjutan.	Dokumentasi evaluasi dan perbaikan prosedur respons insiden secara berkala.

50 Kontrol 1.5.5.b:

Kontrol	Menyusun prosedur keamanan yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak)
Deskripsi Kontrol	Penyelenggara IIV harus menyusun prosedur yang jelas mengenai langkah-langkah keamanan yang harus diambil saat kontrak dengan pihak ketiga berakhir. Prosedur ini meliputi pemutusan hak akses terhadap sistem dan data organisasi, serta pengelolaan aset yang diberikan kepada pihak ketiga selama masa kontrak. Tujuan dari prosedur ini adalah untuk mencegah akses yang tidak sah dan memastikan bahwa informasi yang dimiliki oleh pihak ketiga dikendalikan dengan baik setelah kontrak berakhir. Prosedur ini juga harus mencakup mekanisme untuk mengembalikan data, menghancurkan informasi yang tidak diperlukan, serta memastikan bahwa tidak ada kebocoran data atau risiko lainnya setelah hubungan kontraktual selesai.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Prosedur pemutusan akses yang mengidentifikasi langkah-langkah yang diambil saat kontrak dengan pihak ketiga berakhir. - Laporan audit terhadap hak akses yang dimiliki pihak ketiga selama masa kontrak. - Surat pemberitahuan atau dokumentasi terkait pemutusan akses dan pengembalian aset. - Dokumentasi pengembalian data atau penghancuran informasi yang tidak diperlukan setelah kontrak berakhir. - Protokol terkait proses penutupan hubungan kontraktual dan pemeriksaan akses yang masih aktif.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH071 TH041 TH052 TH054 TH066 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-08, ID.IM-02** **NIST CSF 1.1: ID.SC-5** **NIST SP 800-53r5: CP-2, CP-4, IR-3, IR-4, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.29**

Kriteria Pemenuhan Kontrol 1.5.5.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Prosedur respons insiden belum dirumuskan	Tidak Ada	Tidak Ada
1	Organisasi telah menerapkan Prosedur keamanan pada sebagian kecil aspek yang akan dijalankan ketika kontrak dengan pihak ketiga selesai, namun belum diformalkan	Diterapkan pada sebagian kecil aspek, belum diformalkan.	Rancangan prosedur pemutusan akses, tetapi belum ada implementasi luas.
2	Organisasi telah menerapkan Prosedur keamanan pada sebagian besar aspek yang akan dijalankan ketika kontrak dengan pihak ketiga selesai, namun belum diformalkan	Diterapkan pada sebagian besar aspek, belum diformalkan.	Sebagian besar hak akses sudah dikelola, tetapi belum ada dokumentasi formal.
3	Organisasi telah menerapkan prosedur keamanan pada seluruh aspek yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak), dan telah diformalkan	Diterapkan pada seluruh aspek, telah diformalkan.	Dokumen prosedur formal yang mencakup seluruh proses pemutusan akses.
4	Organisasi telah menerapkan prosedur keamanan pada seluruh aspek yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak), dan telah diformalkan, telah dimonitoring dan direviu tetapi belum perbaikan berkelanjutan	Diterapkan, diformalkan, dimonitoring, dan direviu tetapi belum ada perbaikan berkelanjutan.	Laporan monitoring dan reviu rutin terkait pemutusan akses.
5	Organisasi telah menerapkan prosedur keamanan pada seluruh aspek yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak), dan telah diformalkan, telah dimonitoring dan direviu dan telah diperbaiki berkelanjutan	Diterapkan, diformalkan, dimonitoring, direviu, dan dilakukan perbaikan berkelanjutan.	Dokumentasi evaluasi dan perbaikan prosedur pemutusan akses secara berkala.

51 Kontrol 1.5.5.c:

Kontrol	Senantiasa meningkatkan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok.
Deskripsi Kontrol	Penyelenggara IIV perlu secara aktif meningkatkan standar langkah-langkah keamanan yang diterapkan kepada mitra rantai pasok. Langkah ini bertujuan untuk mengantisipasi ancaman baru, memastikan kesesuaian dengan perkembangan teknologi, regulasi, dan praktik terbaik industri. Peningkatan ini juga mencakup peninjauan reguler terhadap perjanjian keamanan, audit keamanan, serta penguatan kolaborasi dengan mitra rantai pasok untuk menjaga keselarasan antara standar keamanan organisasi dengan mitra. Dengan standar yang ditingkatkan, organisasi dapat meminimalkan risiko yang berasal dari rantai pasok dan memastikan keberlanjutan layanan yang aman.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau dokumen standar keamanan terbaru yang berlaku untuk rantai pasok. - Laporan audit keamanan mitra rantai pasok. - Rekaman hasil pelatihan atau workshop tentang peningkatan standar keamanan untuk mitra. - Protokol komunikasi dan kolaborasi untuk menyelaraskan langkah-langkah keamanan dengan mitra. - Dokumentasi pembaruan perjanjian atau kontrak keamanan dengan mitra rantai pasok.
Ancaman/Risiko yang dimitigasi	TH025 TH027 TH041 TH052 TH054 TH057 TH060 TH067 TH072 TH074 TH076 TH026 TH035 TH049 TH053 TH056 TH059 TH066 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.SC-08, ID.IM-02** **NIST CSF 1.1: ID.SC-5** **NIST SP 800-53r5: CP-2, CP-4, IR-3, IR-4, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.29**

Kriteria Pemenuhan Kontrol 1.5.5.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Peningkatan standar belum dilakukan	Tidak Ada	Tidak Ada
1	Peningkatan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok telah diterapkan pada sebagian kecil aspek dan belum disahkan	Diterapkan pada sebagian kecil aspek, belum disahkan.	Rancangan standar keamanan baru tetapi belum diimplementasikan.
2	Peningkatan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok telah diterapkan pada sebagian besar aspek namun belum disahkan	Diterapkan pada sebagian besar aspek, belum disahkan.	Sebagian besar kebijakan telah diperbarui tetapi belum ada pengesahan formal.
3	Peningkatan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok telah diterapkan keseluruhan dan telah disahkan	Diterapkan secara keseluruhan dan telah disahkan.	Dokumen resmi standar keamanan yang telah diberlakukan.
4	Peningkatan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok telah dimonitoring dan direviu tetapi belum perbaikan berkelanjutan	Diterapkan, dimonitoring, dan direviu tetapi belum ada perbaikan berkelanjutan.	Laporan monitoring dan reviu rutin terhadap standar keamanan.
5	Peningkatan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok sudah diperbaiki berkelanjutan	Diterapkan, dimonitoring, direviu, dan dilakukan perbaikan berkelanjutan.	Dokumentasi evaluasi dan peningkatan standar keamanan secara berkala.





II DOMAIN PROTEKSI

"Domain Proteksi merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam mencegah, membatasi, atau menahan dampak dari Insiden Siber"

2.1. Mengelola identitas, autentikasi, dan kendali akses

Penyelenggara Infrastruktur Informasi Vital (IIV) harus mengelola identitas, autentikasi, dan kendali akses secara ketat untuk melindungi sistem dan data dari akses tidak sah serta ancaman siber. Manajemen identitas mencakup pengelolaan siklus hidup identitas pengguna, perangkat, dan layanan menggunakan Identity and Access Management (IAM), termasuk pembuatan, pemeliharaan, serta penghapusan akun secara otomatis. Autentikasi diperkuat dengan Multi-Factor Authentication (MFA) untuk mencegah penyalahgunaan kredensial, serta implementasi autentikasi berbasis risiko guna mendeteksi anomali akses. Kendali akses diterapkan melalui model Role-Based Access Control (RBAC) atau Attribute-Based Access Control (ABAC) untuk memastikan pengguna hanya memiliki hak akses yang diperlukan, sesuai dengan prinsip least privilege dan Just-in-Time (JIT) access.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) mengelola identitas dan kredensial yang menggunakan layanan IIV;
b) mengelola akses jarak jauh terhadap layanan IIV;
c) mengelola izin akses dan otorisasi layanan IIV; dan
d) memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Mengelola identitas, autentikasi, dan kendali akses” secara efektif antara lain:

NIST CSF 2.0	**:**	**PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01**
NIST CSF 1.1	**:**	**PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7**
NIST SP 800-53r5	**:**	**IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, AC-1, AC-2, AC-3, AC-5, AC-6, AC-7, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15**
SNI ISO/IEC 27001:2022	**:**	**5.14, 5.15, 5.16, 5.17, 5.18, 5.34, 6.7, 6.8, 8.2, 8.3, 8.5, 8.18, 8.20**

Peraturan BSSN Nomor 7 tahun 2024

Peraturan BSSN Nomor 11 Tahun 2024

2.1.1. Mengelola identitas dan kredensial yang menggunakan layanan IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengelola identitas dan kredensial yang menggunakan layanan Infrastruktur Informasi Vital (IIV) bertujuan untuk memastikan bahwa hanya entitas yang sah yang dapat mengakses sistem, sehingga mencegah penyalahgunaan atau akses tidak sah. Identitas pengguna, perangkat, dan layanan harus dikelola menggunakan Identity and Access Management (IAM), yang mencakup proses pembuatan, pemeliharaan, serta penghapusan akun sesuai siklus hidupnya. Kredensial seperti kata sandi, token, atau sertifikat digital harus dilindungi dengan Multi-Factor Authentication (MFA) serta mekanisme autentikasi berbasis risiko guna mengurangi ancaman seperti phishing atau credential stuffing. Selain itu, kebijakan least privilege access harus diterapkan melalui model Role-Based Access Control (RBAC) atau Attribute-Based Access Control (ABAC) agar pengguna hanya memiliki akses sesuai dengan perannya.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi autentikasi dan sistem manajemen identitas yang memiliki sertifikat keamanan, tetapi tidak selalu membutuhkan sumber daya yang besar.
Dampak	**Tinggi** – Mengurangi risiko akses tidak sah dan pelanggaran data. Kontrol ini memastikan bahwa akses ke sistem dan data hanya diberikan kepada individu yang tepat dengan otorisasi yang sesuai.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem dan prosedur yang tepat, serta pelatihan karyawan untuk memahami dan menggunakan sistem manajemen identitas.
Referensi Kontrol	**NIST CSF 2.0: PR.AA-01, PR.AA-05** **NIST CSF 1.1: PR.AC-1** **NIST SP 800-53r5: IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12** **SNI ISO/IEC 27001:2022: 5.16, 5.17, 5.18, 8.5** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

52 Kontrol 2.1.1.a:

Kontrol	Menetapkan dan menerapkan prosedur untuk menerbitkan, mengelola, memeriksa, membatalkan, dan memantau informasi tentang identitias dan kredensial terhadap aset informasi dan personel yang menggunakan IIV.
Deskripsi Kontrol	Penyelenggara IIV perlu menetapkan dan menerapkanprosedur yang mengatur penerbitan, pengelolaan, pemeriksaan, pembatalan, dan pemantauan informasi terkait identitas dan kredensial aset informasi serta personel yang menggunakan Layanan IIV. Prosedur ini bertujuan untuk memastikan bahwa hanya individu atau perangkat yang terotorisasi yang dapat mengakses aset informasi dan sistem. Hal ini juga mendukung kontrol akses yang ketat dan perlindungan terhadap penyalahgunaan atau akses tidak sah. Selain itu, proses ini memperkuat auditabilitas dan ketertelusuran dalam penggunaan Layanan IIV.
Deskripsi Bukti Dukung	Dokumen dan catatan yang menunjukkan kepatuhan terhadap kebijakan dan prosedur yang berlaku. Prosedur ini harus mencakup mekanisme untuk mengidentifikasi dan memverifikasi personel yang berhak mengakses aset informasi, serta pemberian, pengelolaan, dan pembaruan kredensial akses secara berkala. Salah satu elemen penting yang dapat diperiksa adalah prosedur terkait pembuatan, pengelolaan, dan penghapusan akun pengguna. Selain itu, catatan terkait audit dan pemantauan akses pengguna yang memverifikasi apakah akses hanya diberikan kepada individu yang berwenang dan sesuai dengan peran mereka juga sangat penting untuk ditinjau. Contoh dokumen yang dapat diperiksa oleh verifikator untuk menilai kematangan keamanan siber dalam hal ini antara lain adalah kebijakan Identity and Access Management (IAM), kebijakan User Account Management, dan prosedur Access Control. Verifikator juga dapat memeriksa log audit yang mencatat aktivitas akses pengguna, termasuk waktu dan jenis akses yang dilakukan. Selain itu, catatan pembatalan atau perubahan akses pengguna, seperti saat seorang karyawan keluar atau peran mereka berubah, perlu diperiksa untuk memastikan bahwa akses yang tidak lagi diperlukan telah dibatalkan dengan tepat. Dokumen lain yang relevan adalah laporan pemeriksaan rutin yang memastikan kredensial yang telah diterbitkan tetap valid dan aman, serta bukti penerapan autentikasi multi-faktor (MFA) atau kontrol lainnya untuk memastikan bahwa kredensial yang diberikan hanya digunakan oleh individu yang sah.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH071 TH041 TH052 TH054 TH066 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.AA-01, PR.AA-05** **NIST CSF 1.1: PR.AC-1** **NIST SP 800-53r5: IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12** **SNI ISO/IEC 27001:2022: 5.16, 5.17, 5.18, 8.5** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.1.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pengelolaan aset informasi dan personel yang menggunakan IIV	Tidak ditemukan kebijakan atau prosedur pengelolaan aset informasi dan personel yang menggunakan IIV dalam bentuk apapun.	Tidak ditemukan dokumen kebijakan, SOP, atau catatan terkait praktik pengelolaan akses dan aset informasi.
1	Prosedur pengelolaan aset informasi dan personel yang menggunakan IIV sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Terdapat bukti bahwa beberapa aspek pengelolaan aset informasi dan personel yang menggunakan IIV mulai diterapkan, namun belum terdokumentasi secara resmi.	- Bukti penerapan praktik informal (misalnya, daftar akses manual, pencatatan akses, kebijakan lisan). - Tidak ada kebijakan atau prosedur resmi yang terdokumentasi.
2	Prosedur pengelolaan aset informasi dan personel yang menggunakan IIV sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek pengelolaan aset informasi dan personel yang menggunakan IIV telah diterapkan, namun prosedur belum terdokumentasi sebagai kebijakan formal.	- Bukti penerapan prosedur pada berbagai aspek pengelolaan. - Draft kebijakan atau prosedur yang belum disahkan.
3	Prosedur pengelolaan aset informasi dan personel yang menggunakan IIV sudah diformalkan dan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur formal yang telah disahkan dan diterapkan di semua aspek yang relevan.	- Dokumen kebijakan dan prosedur yang sudah disahkan. - Catatan penerapan prosedur di semua aspek, seperti daftar kontrol akses dan laporan perubahan akses.
4	- Prosedur pengelolaan aset informasi dan personel yang menggunakan IIV sudah diformalkan dan diterapkan pada seluruh aspek. - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala.	Kebijakan dan prosedur telah diterapkan sepenuhnya, dengan adanya pemantauan dan audit rutin untuk menilai kepatuhan dan efektivitasnya.	- Laporan audit dan pemantauan akses. - Bukti adanya tinjauan berkala terhadap prosedur dan kepatuhan pengguna.
5	- Prosedur pengelolaan aset informasi dan personel yang menggunakan IIV sudah diformalkan dan diterapkan pada seluruh aspek. - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan.	Prosedur dan kebijakan tidak hanya diterapkan dan diawasi, tetapi juga ditingkatkan secara berkelanjutan berdasarkan evaluasi berkala dan perubahan risiko.	- Hasil evaluasi dan rekomendasi perbaikan prosedur. - Bukti implementasi perbaikan dari hasil evaluasi dan audit sebelumnya. - Catatan pengelolaan risiko terkait aset informasi dan personel.

2.1.2. Mengelola akses jarak jauh terhadap layanan IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengelola akses jarak jauh terhadap layanan IIV dengan mengontrol, memantau, dan melindungi akses ke sistem kritikal. Aspek utama yang dinilai mencakup kebijakan dan prosedur, penerapan autentikasi *Multi-Factor Authentication* (MFA), keamanan koneksi melalui enkripsi dan VPN atau ZTNA, serta pemantauan aktivitas dengan logging dan deteksi anomali.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan teknologi yang memiliki sertifikat keamanan untuk mengamankan akses jarak jauh, seperti VPN atau sistem autentikasi multifaktor, tetapi tidak selalu membutuhkan sumber daya yang besar.
Dampak	**Tinggi** – Mengurangi risiko akses tidak sah dan serangan melalui akses jarak jauh. Kontrol ini memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem dari jarak jauh dengan cara yang aman.
Kompleksitas	**Sedang** – Memerlukan pengaturan teknologi yang tepat dan pelatihan karyawan untuk memahami serta menggunakan akses jarak jauh dengan aman.
Referensi Kontrol	**NIST CSF 2.0: PR.AA-03, PR.AA-05, PR.IR-01** **NIST CSF 1.1: PR.AC-3** **NIST SP 800-53r5: AC-1, AC-17, AC-19, AC-20, SC-15** **SNI ISO/IEC 27001:2022: 5.14, 6.7, 8.20** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

53 Kontrol 2.1.2.a:

Kontrol	Penyelenggara IIV menyusun prosedur tentang mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan, termasuk pemberian koneksi terhadap pengguna, perangkat IoT, dan/atau server.
Deskripsi Kontrol	Penyelenggara IIV perlu menyusun prosedur yang mengatur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan. Prosedur ini mencakup pemberian koneksi untuk pengguna, perangkat IoT, dan/atau server. Tujuannya adalah memastikan hanya pengguna, perangkat, atau entitas yang teridentifikasi dan terotorisasi yang dapat mengakses layanan atau aset informasi, guna mengurangi risiko akses tidak sah, pelanggaran data, atau ancaman keamanan lainnya. Langkah ini juga mendukung pengelolaan akses yang efektif, auditabilitas, serta pemenuhan peraturan keamanan siber yang berlaku.
Deskripsi Bukti Dukung	Dalam menilai kematangan keamanan siber penyelenggara Infrastruktur Informasi Vital (IIV) terkait mekanisme identifikasi pengguna, pemberian akses, dan otorisasi layanan, diperlukan bukti yang menunjukkan bahwa prosedur tersebut telah disusun, diterapkan, dan dimonitor secara berkala. Salah satu data dukung utama adalah dokumen kebijakan dan prosedur yang mengatur mekanisme identifikasi pengguna layanan, baik bagi pengguna internal maupun eksternal. Prosedur ini harus mencakup bagaimana pengguna diverifikasi sebelum diberikan akses, bagaimana akses diberikan berdasarkan prinsip least privilege, serta mekanisme pencatatan dan audit akses yang dilakukan. Selain itu, dokumen yang menunjukkan penggunaan teknologi autentikasi, seperti Multi-Factor Authentication (MFA) atau integrasi dengan Identity and Access Management (IAM), menjadi indikator penting dalam menilai tingkat kematangan kontrol keamanan.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH071 TH041 TH052 TH054 TH066 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.AA-03, PR.AA-05, PR.IR-01** **NIST CSF 1.1: PR.AC-3** **NIST SP 800-53r5: AC-1, AC-17, AC-19, AC-20, SC-15** **SNI ISO/IEC 27001:2022: 5.14, 6.7, 8.20** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.1.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan	Tidak ditemukan kebijakan, prosedur, atau dokumen terkait mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi.	Tidak ditemukan dokumen kebijakan, SOP, atau catatan terkait praktik identifikasi dan akses pengguna.
1	Prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Terdapat bukti bahwa beberapa aspek mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi mulai diterapkan, namun belum terdokumentasi secara resmi.	- Bukti penerapan praktik informal (misalnya, daftar akses manual, pencatatan akses, kebijakan lisan). - Tidak ada kebijakan atau prosedur resmi yang terdokumentasi.
2	Prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi telah diterapkan, namun prosedur belum terdokumentasi sebagai kebijakan formal.	- Bukti penerapan prosedur pada berbagai aspek pengelolaan. - Draft kebijakan atau prosedur yang belum disahkan.
3	Prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan sudah diformalkan dan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur formal yang telah disahkan dan diterapkan di semua aspek yang relevan.	- Dokumen kebijakan dan prosedur yang sudah disahkan. - Catatan penerapan prosedur di semua aspek, seperti daftar kontrol akses dan laporan perubahan akses.
4	- Prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan sudah diformalkan dan diterapkan pada seluruh aspek. - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala.	Kebijakan dan prosedur telah diterapkan sepenuhnya, dengan adanya pemantauan dan audit rutin untuk menilai kepatuhan dan efektivitasnya.	- Laporan audit dan pemantauan akses. - Bukti adanya tinjauan berkala terhadap prosedur dan kepatuhan pengguna.
5	- Prosedur mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan sudah diformalkan dan diterapkan pada seluruh aspek. - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan.	Prosedur dan kebijakan tidak hanya diterapkan dan diawasi, tetapi juga ditingkatkan secara berkelanjutan berdasarkan evaluasi berkala dan perubahan risiko.	- Hasil evaluasi dan rekomendasi perbaikan prosedur. - Bukti implementasi perbaikan dari hasil evaluasi dan audit sebelumnya.

54 Kontrol 2.1.2.b:

Kontrol	Tersedianya dan diterapkannya prosedur pencegahan terhadap upaya memasuki perangkat atau jaringan secara tidak sah, dengan menerapkan langkah-langkah seperti menerapkan fungsi untuk penguncian setelah sejumlah upaya masuk yang gagal dan memberikan interval waktu hingga keamanannya dipastikan.
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan tersedianya dan diterapkannya prosedur pencegahan terhadap upaya akses tidak sah ke perangkat atau jaringan. Prosedur ini mencakup langkah-langkah seperti penguncian otomatis setelah sejumlah percobaan masuk yang gagal dan pemberian interval waktu sebelum akses dapat dicoba kembali. Tujuannya adalah melindungi perangkat dan jaringan dari risiko brute-force attack atau upaya masuk tidak sah lainnya, memastikan integritas serta keamanan sistem, dan meminimalkan potensi ancaman terhadap data atau layanan vital organisasi.
Deskripsi Bukti Dukung	Data dukung yang dapat menjadi penunjang dalam memeriksa penyelenggara IT (Information Technology) terkait ketersediaan dan penerapan prosedur pencegahan terhadap upaya memasuki perangkat atau jaringan secara tidak sah meliputi beberapa aspek. Pertama, dokumen kebijakan keamanan informasi yang menjelaskan langkah-langkah pencegahan seperti penerapan fungsi penguncian setelah sejumlah upaya masuk yang gagal dan interval waktu yang ditetapkan hingga keamanan dipastikan. Dokumen ini harus mencakup prosedur teknis dan operasional yang jelas, termasuk konfigurasi sistem, log aktivitas, dan mekanisme pemulihan akses. Kedua, laporan audit keamanan siber yang menunjukkan hasil penilaian terhadap efektivitas langkah-langkah keamanan yang diterapkan. Laporan ini dapat mencakup hasil penetration testing, vulnerability assessment, dan simulasi serangan siber. Selain itu, dokumen pelatihan dan kesadaran keamanan bagi karyawan juga penting untuk memastikan bahwa semua pihak memahami dan menerapkan prosedur keamanan dengan benar.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH071 TH041 TH052 TH054 TH066 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.AA-03, PR.AA-05, PR.IR-01** **NIST CSF 1.1: PR.AC-3** **NIST SP 800-53r5: AC-1, AC-17, AC-19, AC-20, SC-15** **SNI ISO/IEC 27001:2022: 5.14, 6.7, 8.20** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.1.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan	Tidak ditemukan kebijakan, prosedur, atau mekanisme perlindungan terhadap upaya serangan melalui perangkat atau jaringan.	Tidak ditemukan dokumen kebijakan atau SOP yang mengatur pencegahan serangan.
1	Prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Terdapat bukti bahwa beberapa aspek pencegahan serangan mulai diterapkan, tetapi belum terdokumentasi secara resmi.	- Bukti konfigurasi keamanan seperti log sistem yang menunjukkan upaya pencegahan manual. - Tidak ada kebijakan atau prosedur formal.
2	Prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek pencegahan serangan telah diterapkan, tetapi belum terdokumentasi sebagai kebijakan formal.	- Bukti penerapan firewall, IDS/IPS, dan sistem otentikasi. - Draft kebijakan atau prosedur yang belum disahkan.
3	Prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan sudah diformalkan dan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur formal yang telah disahkan dan diterapkan di semua aspek yang relevan.	- Dokumen kebijakan dan prosedur yang sudah disahkan. - Bukti penerapan prosedur di semua sistem jaringan dan perangkat.
4	- Prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Kebijakan dan prosedur telah diterapkan sepenuhnya, dengan adanya pemantauan dan audit rutin.	- Laporan audit keamanan jaringan. - Bukti pemantauan terhadap serangan yang dicegah.
5	- Prosedur pencegahan terhadap upaya serangan melalui perangkat atau jaringan sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan	Prosedur dan kebijakan tidak hanya diterapkan dan diawasi, tetapi juga ditingkatkan secara berkelanjutan berdasarkan evaluasi berkala.	- Hasil evaluasi dan rekomendasi perbaikan prosedur. - Bukti implementasi perbaikan dari hasil audit sebelumnya.

2.1.3. Mengelola izin akses dan otorisasi layanan IIV

Kriteria	Detail
Deskripsi	Penyelenggara IIV Mengelola izin akses dan otorisasi layanan Infrastruktur Informasi Vital (IIV) untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan beroperasi pada sistem atau layanan yang memiliki peran penting dalam IIV. Dalam konteks ini, penyelenggara IIV bertanggung jawab untuk mengelola pihak atau entitas yang memiliki akses ke layanan, sejauh mana akses tersebut diberikan, dan bagaimana akses tersebut dapat dikendalikan serta diawasi. Pengelolaan izin akses dan otorisasi layanan IIV oleh penyelenggara sangat penting untuk melindungi sistem kritikal dari ancaman keamanan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem manajemen izin dan otorisasi, tetapi tidak selalu membutuhkan teknologi tambahan yang mahal.
Dampak	**Tinggi** – Mengurangi risiko akses tidak sah dan pelanggaran kebijakan akses. Kontrol ini memastikan bahwa setiap pengguna hanya memiliki akses ke data dan sistem yang relevan dengan peran mereka.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang tepat untuk mengelola dan memperbarui izin akses dan otorisasi secara berkala.
Referensi Kontrol	**NIST CSF 2.0: PR.AA-05** **NIST CSF 1.1: PR.AC-4** **NIST SP 800-53r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24** **SNI ISO/IEC 27001:2022: 5.15, 6.8, 8.2, 8.3, 8.18**

55 Kontrol 2.1.3.a:

Kontrol	Menyusun dan menerapkan prosedur untuk memisahkan hak akses sesuai tugas dan area tanggung jawab (misalnya, pisahkan fungsi untuk pengguna dari fungsi untuk administrator sistem)
Deskripsi Kontrol	Penyelenggara IIV perlu menyusun dan menerapkan prosedur untuk memastikan hak akses diberikan sesuai dengan tugas dan area tanggung jawab setiap individu dalam organisasi. Pemisahan ini, seperti memisahkan fungsi pengguna dari administrator sistem, bertujuan untuk mengurangi risiko penyalahgunaan akses, mencegah konflik kepentingan, dan meningkatkan keamanan sistem dengan prinsip least privilege (akses seminimal mungkin sesuai kebutuhan). Langkah ini juga mendukung auditabilitas, memastikan bahwa hanya pihak yang berwenang dapat mengakses fungsi atau data tertentu.
Deskripsi Bukti Dukung	Data dukung yang dapat menjadi penunjang dalam memeriksa penyelenggara IIV terkait penyusunan dan penerapan prosedur untuk memisahkan hak akses sesuai tugas dan area tanggung jawab meliputi beberapa aspek kunci. Pertama, dokumen kebijakan keamanan informasi yang menjelaskan prinsip pemisahan tugas (segregation of duties) dan pembatasan hak akses berdasarkan role-based access control (RBAC). Kebijakan ini harus mencakup definisi peran (roles), tanggung jawab, dan batasan akses untuk setiap pengguna, termasuk pemisahan antara pengguna biasa dan administrator sistem. Kedua, dokumen teknis seperti matriks hak akses (access control matrix) yang mendetailkan siapa yang memiliki akses ke sistem, data, atau fungsi tertentu, serta konfigurasi sistem yang menunjukkan penerapan pembatasan akses. Selain itu, laporan audit internal atau eksternal yang memverifikasi kepatuhan terhadap kebijakan pemisahan tugas juga menjadi bukti penting.
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH053 TH059 TH071 TH041 TH052 TH054 TH066 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.AA-05** **NIST CSF 1.1: PR.AC-4** **NIST SP 800-53r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24** **SNI ISO/IEC 27001:2022: 5.15, 6.8, 8.2, 8.3, 8.18**

Kriteria Pemenuhan Kontrol 2.1.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pemisahan hak akses	Tidak ditemukan kebijakan, prosedur, atau mekanisme formal maupun informal terkait pemisahan hak akses.	Tidak ada dokumen kebijakan, SOP, atau catatan akses pengguna berdasarkan peran.
1	Prosedur pemisahan hak akses sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Terdapat bukti penerapan pemisahan hak akses dalam beberapa aspek, tetapi belum terdokumentasi sebagai kebijakan resmi.	- Bukti penerapan pemisahan akses dalam beberapa bagian sistem. - Tidak ada dokumen resmi, hanya pencatatan manual atau kebijakan lisan.
2	Prosedur pemisahan hak akses sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek pemisahan hak akses sudah diterapkan, tetapi prosedur belum diformalkan sebagai kebijakan yang terdokumentasi.	- Bukti penerapan pemisahan hak akses dalam sebagian besar sistem. - Draft kebijakan yang belum disahkan. - Konfigurasi awal RBAC tanpa dokumentasi formal.
3	Prosedur pemisahan hak akses sudah diformalkan dan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur resmi terkait pemisahan hak akses, yang telah diterapkan di seluruh organisasi.	- Dokumen kebijakan dan prosedur yang telah disahkan. - Catatan daftar kontrol akses. - Laporan penerapan pemisahan hak akses.
4	- Prosedur pemisahan hak akses sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Kebijakan dan prosedur telah diterapkan sepenuhnya dengan adanya pemantauan dan audit rutin.	- Laporan audit kepatuhan terhadap pemisahan hak akses. - Bukti adanya tinjauan berkala terhadap hak akses pengguna. - Bukti pencabutan akses dari pengguna yang tidak lagi berwenang.
5	- Prosedur pemisahan hak akses sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutanserta dilakukan perbaikan secara berkelanjutan	- Prosedur dan kebijakan tidak hanya diterapkan dan diawasi, tetapi juga ditingkatkan secara berkelanjutan berdasarkan evaluasi berkala dan perubahan risiko.	- Hasil evaluasi dan rekomendasi perbaikan prosedur pemisahan hak akses. - Bukti implementasi perbaikan dari hasil evaluasi dan audit sebelumnya. - Penerapan prinsip zero trust atau konsep just-in-time access.

56 Kontrol 2.1.3.b:

Kontrol	Tersedianya prosedur pembatasan komunikasi oleh perangkat dan server kepada pengguna sesuai dengan tingkat risikonya.
Deskripsi Kontrol	Penyelenggara IIV perlu memiliki prosedur untuk membatasi komunikasi perangkat dan server kepada pengguna berdasarkan tingkat risiko yang telah diidentifikasi. Prosedur ini bertujuan untuk mengelola potensi ancaman dengan menerapkan pembatasan akses hanya pada komunikasi yang diperlukan, sehingga mengurangi eksposur aset informasi terhadap risiko keamanan. Hal ini dapat mencakup pembatasan port, protokol, atau layanan tertentu yang tidak relevan untuk pengguna tertentu. Prosedur ini juga mendukung pengamanan data sensitif dan memastikan perlindungan sistem dari akses atau komunikasi yang tidak sah.
Deskripsi Bukti Dukung	Data dukung yang dapat menjadi penunjang dalam memeriksa penyelenggara IT terkait ketersediaan prosedur pembatasan komunikasi oleh perangkat dan server kepada pengguna sesuai dengan tingkat risikonya meliputi beberapa aspek penting. Pertama, dokumen kebijakan keamanan informasi yang menjelaskan prinsip pembatasan komunikasi berdasarkan tingkat risiko, termasuk aturan firewall, kebijakan segmentasi jaringan, dan kontrol akses jaringan. Kebijakan ini harus mencakup penjelasan tentang bagaimana komunikasi antara perangkat, server, dan pengguna dibatasi berdasarkan klasifikasi risiko, seperti pembatasan akses ke sistem kritis atau data sensitif. Kedua, dokumen teknis seperti konfigurasi firewall, aturan jaringan (network rules), dan log aktivitas jaringan yang menunjukkan penerapan pembatasan komunikasi. Selain itu, laporan audit keamanan yang memverifikasi kepatuhan terhadap kebijakan pembatasan komunikasi juga menjadi bukti penting.
Ancaman/Risiko yang dimitigasi	TH010 TH017 TH030 TH054 TH016 TH023 TH035 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.AA-05** **NIST CSF 1.1: PR.AC-4** **NIST SP 800-53r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24** **SNI ISO/IEC 27001:2022: 5.15, 6.8, 8.2, 8.3, 8.18**

Kriteria Pemenuhan Kontrol 2.1.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pembatasan komunikasi perangkat dan server	Tidak ditemukan kebijakan, prosedur, atau mekanisme pembatasan komunikasi.	Tidak ada dokumen kebijakan, SOP, atau catatan pembatasan komunikasi berdasarkan tingkat risiko.
1	Prosedur pembatasan komunikasi perangkat dan server sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Terdapat bukti penerapan pembatasan komunikasi dalam beberapa aspek, tetapi belum terdokumentasi sebagai kebijakan resmi.	- Bukti penerapan firewall atau segmentasi jaringan dalam beberapa bagian sistem. - Tidak ada dokumen resmi, hanya pencatatan manual atau kebijakan lisan.
2	Prosedur pembatasan komunikasi perangkat dan server sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek pembatasan komunikasi sudah diterapkan, tetapi prosedur belum diformalkan sebagai kebijakan yang terdokumentasi.	- Bukti penerapan segmentasi jaringan dalam sebagian besar sistem. - Draft kebijakan yang belum disahkan. - Konfigurasi awal kontrol komunikasi tanpa dokumentasi formal.
3	Prosedur pembatasan komunikasi perangkat dan server sudah diformalkan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur resmi terkait pembatasan komunikasi, yang telah diterapkan di seluruh organisasi.	- Dokumen kebijakan dan prosedur yang telah disahkan. - Catatan daftar komunikasi yang diizinkan. - Laporan penerapan firewall, segmentasi jaringan, dan whitelisting.
4	- Prosedur pembatasan komunikasi perangkat dan server sudah diformalkan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Kebijakan dan prosedur telah diterapkan sepenuhnya dengan adanya pemantauan dan audit rutin.	- Laporan audit kepatuhan terhadap kebijakan pembatasan komunikasi. - Bukti adanya tinjauan berkala terhadap aturan komunikasi perangkat dan server. - Bukti pencabutan akses komunikasi dari perangkat atau pengguna yang tidak lagi berwenang.
5	- Prosedur pembatasan komunikasi perangkat dan server sudah diformalkan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan	Prosedur dan kebijakan tidak hanya diterapkan dan diawasi, tetapi juga ditingkatkan secara berkelanjutan berdasarkan evaluasi berkala dan perubahan risiko.	- Hasil evaluasi dan rekomendasi perbaikan prosedur pembatasan komunikasi. - Bukti implementasi perbaikan dari hasil evaluasi dan audit sebelumnya.

2.1.4. Memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya

Kriteria	Detail
Deskripsi	Penyelenggara IIV menerapkan sistem autentikasi yang tepat untuk pengguna, perangkat, dan aset informasi sesuai dengan tingkat risikonya adalah langkah penting dalam menjaga keamanan Infrastruktur Informasi Vital (IIV). Penyelenggara IIV harus memastikan bahwa tingkat autentikasi yang diterapkan sesuai dengan sensitivitas data atau layanan yang diakses, serta potensi ancaman yang ada. Hal ini bertujuan untuk melindungi sistem kritikal dari akses yang tidak sah dan serangan siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan teknologi autentikasi dan sumber daya untuk mengimplementasikan serta memelihara sistem tersebut.
Dampak	**Tinggi** – Mengurangi risiko akses tidak sah dan meningkatkan keamanan akses. Dengan autentikasi yang sesuai tingkat risiko, organisasi dapat memastikan bahwa akses ke data dan sistem dilakukan dengan cara yang aman.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem autentikasi yang tepat dan pelatihan karyawan untuk memahami serta menggunakan sistem tersebut dengan benar.
Referensi Kontrol	**NIST CSF 2.0: PR.AA-03** **NIST CSF 1.1: PR.AC-7** **NIST SP 800-53r5: AC-7, AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11** **SNI ISO/IEC 27001:2022: 5.16, 5.17, 5.34, 8.5**

57 Kontrol 2.1.4.a:

Kontrol	Perangkat, pengguna, dan aset informasi lainnya menggunakan sistem otentikasi tertentu (misalnya, *multi-factor authentication*) sesuai dengan tingkat risiko nya terhadap sistem.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa perangkat, pengguna, dan aset informasi lainnya menggunakan sistem otentikasi tertentu yang sesuai dengan tingkat risiko yang terkait dengan akses terhadap sistem. Sistem otentikasi yang digunakan, seperti autentikasi multi-faktor (MFA), bertujuan untuk meningkatkan keamanan akses terhadap aset informasi dengan menambahkan lapisan perlindungan. Langkah ini penting untuk mencegah akses tidak sah, mengurangi risiko pelanggaran keamanan, dan melindungi data sensitif, terutama pada sistem atau layanan dengan tingkat kritikalitas yang tinggi.
Deskripsi Bukti Dukung	Data dukung yang dapat menjadi penunjang dalam memeriksa penggunaan sistem otentikasi tertentu (seperti multi-factor authentication/MFA) untuk perangkat, pengguna, dan aset informasi lainnya sesuai dengan tingkat risikonya meliputi beberapa aspek kunci. Pertama, kebijakan keamanan informasi yang menjelaskan persyaratan otentikasi berdasarkan tingkat risiko, termasuk kapan dan di mana MFA harus diterapkan. Kebijakan ini harus mencakup klasifikasi aset informasi, penilaian risiko, dan pedoman penerapan otentikasi yang sesuai. Kedua, dokumen teknis seperti konfigurasi sistem otentikasi, daftar pengguna yang telah diaktifkan MFA, dan log aktivitas otentikasi yang menunjukkan penggunaan MFA. Selain itu, laporan audit keamanan yang memverifikasi kepatuhan terhadap kebijakan otentikasi dan efektivitas penerapannya juga menjadi bukti penting.
Ancaman/Risiko yang dimitigasi	TH030 TH041 TH052 TH054 TH066 TH075 TH035 TH049 TH053 TH059 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.AA-03** **NIST CSF 1.1: PR.AC-7** **NIST SP 800-53r5: AC-7, AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11** **SNI ISO/IEC 27001:2022: 5.16, 5.17, 5.34, 8.5**

Kriteria Pemenuhan Kontrol 2.1.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya	Tidak ditemukan kebijakan, prosedur, atau mekanisme otentikasi untuk pengguna, perangkat, dan aset informasi.	Tidak ada sistem otentikasi, catatan autentikasi, atau kebijakan keamanan terkait autentikasi.
1	Sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Terdapat bukti penerapan otentikasi dasar di beberapa aspek, tetapi belum ada kebijakan atau prosedur resmi yang terdokumentasi.	- Log autentikasi pengguna yang menunjukkan penerapan autentikasi pada sebagian kecil sistem. - Konfigurasi dasar autentikasi dalam beberapa perangkat atau aplikasi.
2	Sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Sebagian besar aspek telah menerapkan autentikasi, tetapi belum ada kebijakan atau prosedur resmi.	- Log autentikasi yang menunjukkan cakupan lebih luas. - Konfigurasi keamanan akun pengguna dan perangkat. - Draft kebijakan autentikasi yang belum disahkan.
3	Sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya sudah diformalkan dan diterapkan pada seluruh aspek	Tersedianya kebijakan dan prosedur autentikasi resmi yang telah diterapkan di seluruh organisasi.	- Dokumen kebijakan autentikasi yang telah disahkan. - Log penerapan autentikasi pada seluruh sistem. - Bukti penggunaan MFA pada akses sistem kritikal.
4	- Sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya sudah diformalkan dan diterapkan pada seluruh aspek - Sistem tersebut dimonitor pelaksanaanya dan direviu secara berkala	Kebijakan dan prosedur telah diterapkan secara menyeluruh dengan adanya pemantauan dan audit rutin.	- Laporan audit kepatuhan autentikasi. - Bukti tinjauan ulang kebijakan autentikasi berdasarkan perubahan risiko.
5	- Sistem otentikasi untuk perangkat, pengguna, dan aset informasi lainnya sudah diformalkan dan diterapkan pada seluruh aspek, serta dilakukan otomatisasi - Sistem tersebut dimonitor pelaksanaanya dan direviu secara berkala	Sistem autentikasi tidak hanya diterapkan dan diawasi tetapi juga terus diperbaiki dengan otomatisasi dan penerapan teknologi autentikasi adaptif.	- Laporan evaluasi dan pengembangan sistem autentikasi berbasis risiko. - Bukti implementasi perbaikan autentikasi berdasarkan hasil audit dan monitoring sebelumnya. - Bukti penerapan sistem autentikasi adaptif atau berbasis zero trust.

2.2. Melindungi aset fisik

Melindungi aset fisik dalam mendukung layanan IIV merupakan upaya strategis yang mencakup serangkaian prosedur operasional guna memastikan keamanan dan keandalan aset informasi. Prosedur ini dirancang untuk mencegah akses fisik yang tidak sah serta melindungi aset dari kerusakan atau gangguan operasional. Setiap proses perbaikan dan pemeliharaan aset informasi dilakukan secara berkala, dicatat, dan dikendalikan sesuai dengan prosedur yang telah ditetapkan, sehingga memastikan akuntabilitas dan transparansi dalam pengelolaannya. Selain itu, pemeliharaan jarak jauh terhadap aset informasi hanya diperbolehkan apabila telah mendapatkan persetujuan dari penanggung jawab layanan IIV dan seluruh aktivitas tersebut wajib terdokumentasi dengan baik. Lingkungan fisik tempat aset informasi berada juga dipantau secara rutin untuk mendeteksi potensi ancaman seperti suhu ekstrem, kelembaban tinggi, atau adanya upaya akses ilegal. Keseluruhan kegiatan ini dilakukan untuk memastikan bahwa prosedur keamanan fisik tidak hanya tersedia secara administratif, tetapi juga benar-benar diterapkan secara konsisten guna menjaga keberlangsungan dan keandalan layanan IIV.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV;
b) memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur;
c) memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur;
d) memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman; dan
e) memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melindungi aset fisik” secara efektif antara lain:

NIST CSF 2.0	**:**	**ID.AM-08, PR.PS-02, PR.PS-03, PR.AA-06, PR.IR-02, ID.IM-03, DE.CM-02**
NIST CSF 1.1	**:**	**PR.MA-1, PR.MA-2, PR.AC-2, PR.IP-5, PR.IP-7, DE.CM-2**
NIST SP 800-53r5	**:**	**PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, PE-20, MA-1, MA-2, MA-3, MA-4, MA-5, MA-6, CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6**
SNI ISO/IEC 27001:2022	**:**	**5.19, 5.22, 7.1, 7.2, 7.3, 7.4, 7.5, 7.10, 7.11, 7.12, 7.13**

2.2.1. Menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV

Kriteria	Detail
Deskripsi	Penyelenggaran IIV mampu menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengimplementasikan prosedur, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan prosedur yang jelas, organisasi dapat melindungi aset fisik dari ancaman dan akses tidak sah, sehingga mengurangi risiko kerusakan atau kehilangan aset penting
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengelola dan melindungi aset fisik secara efektif
Referensi Kontrol	**NIST CSF 2.0: PR.IR-02, PR.AA-06** **NIST CSF 1.1: PR.IP-5, PR.AC-2** **NIST SP 800-53r5: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9** **SNI ISO/IEC 27001:2022: 7.1, 7.2, 7.3, 7.4, 7.5, 7.11, 7.12**

58 Kontrol 2.2.1.a:

Kontrol	Menetapkan dan menerapkan prosedur keamanan fisik terhadap akses kontrol yang sesuai seperti mengunci dan membatasi akses ke area tempat perangkat dan server dipasang, menggunakan kontrol masuk dan keluar, otentikasi biometrik, memasang kamera pengintai, dan/atau memeriksa barang bawaan.
Deskripsi Kontrol	Penyelenggara IIV harus menetapkan dan menerapkan prosedur keamanan fisik terhadap akses kontrol untuk melindungi perangkat, server, dan aset informasi lainnya. Prosedur ini mencakup tindakan seperti mengunci dan membatasi akses ke area tempat perangkat dan server dipasang, menggunakan kontrol akses masuk dan keluar (misalnya, kartu akses atau otentikasi biometrik), memasang kamera pengintai untuk pemantauan, serta memeriksa barang bawaan personel atau tamu. Langkah ini bertujuan untuk mencegah akses fisik tidak sah, melindungi aset dari gangguan fisik, pencurian, atau kerusakan, dan memastikan keamanan keseluruhan dari infrastruktur organisasi.
Deskripsi Bukti Dukung	Untuk mendukung kontrol ini, organisasi perlu menyediakan bukti penerapan prosedur keamanan fisik seperti adanya dokumentasi prosedur akses fisik (SOP), log akses masuk dan keluar, rekaman CCTV, catatan penggunaan sistem otentikasi (misalnya kartu identitas, biometrik), serta bukti pembatasan fisik area kritikal seperti ruangan server. Bukti tambahan berupa hasil audit internal, laporan monitoring berkala, dan catatan reviu serta tindak lanjut atas kelemahan yang ditemukan akan menguatkan posisi indeks yang lebih tinggi. Tingkat kematangan keamanan akan bergantung pada sejauh mana prosedur ini diterapkan, didokumentasikan, dimonitor, dan terus ditingkatkan.
Ancaman/Risiko yang dimitigasi	TH001 TH003 TH025 TH030 TH052 TH054 TH066 TH075 TH002 TH004 TH026 TH035 TH053 TH059 TH071 TH076
Referensi Kontrol	**NIST CSF 2.0: PR.IR-02, PR.AA-06** **NIST CSF 1.1: PR.IP-5, PR.AC-2** **NIST SP 800-53r5: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9** **SNI ISO/IEC 27001:2022: 7.1, 7.2, 7.3, 7.4, 7.5, 7.11, 7.12**

Kriteria Pemenuhan Kontrol 2.2.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur keamanan fisik terhadap akses kontrol	Tidak ada sistem otentikasi dan pengamanan fisik terhadap perangkat, pengguna, dan aset informasi. Area kritikal terbuka dan tidak terpantau.	Tidak tersedia dokumen prosedur atau catatan implementasi. Akses area penting terbuka tanpa kontrol, tidak ada kamera pengintai atau sistem identifikasi.
1	Prosedur keamanan fisik terhadap akses kontrol sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Pengamanan fisik mulai diterapkan, namun hanya sebagian kecil (misalnya hanya di ruang server), dan belum ada SOP atau dokumentasi formal.	Foto atau deskripsi adanya akses terbatas di sebagian area (misal ruang server), catatan manual pengunjung terbatas, belum ada SOP resmi.
2	Prosedur keamanan fisik terhadap akses kontrol sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Pengamanan fisik telah diterapkan secara luas, mencakup sebagian besar area penting, tetapi belum diiringi dengan prosedur formal tertulis.	Dokumentasi adanya sistem akses kontrol di beberapa area penting, daftar kontrol pengunjung, sebagian log penggunaan otentikasi, tetapi belum terdokumentasi formal.
3	Prosedur keamanan fisik terhadap akses kontrol sudah diformalkan dan diterapkan pada seluruh aspek	Pengamanan fisik telah mencakup seluruh area penting dan prosedur sudah terdokumentasi dalam bentuk SOP atau kebijakan resmi.	SOP keamanan fisik dan akses kontrol tersedia, diterapkan di semua area kritikal, disertai log akses, rekaman CCTV, dan penggunaan kartu identitas atau biometrik.
4	- Prosedur pelindungan aset fisik sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Seluruh aspek pengamanan fisik telah diformalkan dan diterapkan. Selain itu, pelaksanaan prosedur dimonitor dan hasilnya direviu secara berkala.	SOP dan kebijakan sudah diformalkan, dokumentasi penerapan di semua area tersedia, log monitoring rutin, hasil reviu keamanan secara periodik disimpan.
5	- Prosedur pelindungan aset fisik sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan	Selain semua di Indeks 4, organisasi secara aktif melakukan perbaikan berkelanjutan atas hasil monitoring dan reviu untuk meningkatkan efektivitas pengamanan fisik.	Terdapat SOP, log monitoring, hasil reviu berkala, dan catatan tindakan perbaikan atau peningkatan keamanan sebagai tindak lanjut reviu, misal upgrade sistem kontrol akses atau pemasangan tambahan sensor/kamera.

59 Kontrol 2.2.1.b:

Kontrol	Tersedianya dan diterapkannya prosedur pelindungan fisik seperti menyiapkan catu daya cadangan, fasilitas proteksi kebakaran, dan perlindungan dari resapan air yang mengikuti kebijakan dan standar yang berlaku.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan tersedianya dan diterapkannya prosedur perlindungan fisik untuk infrastruktur penting. Langkah-langkah ini mencakup menyiapkan catu daya cadangan (seperti UPS atau generator), fasilitas proteksi kebakaran (seperti alat pemadam kebakaran, detektor asap, atau sistem pemadaman otomatis), dan perlindungan terhadap resapan air (seperti sistem drainase, sensor kebocoran air, atau pemasangan peralatan di area yang terlindungi). Prosedur tersebut harus disusun sesuai kebijakan dan standar yang berlaku guna meminimalkan risiko kerusakan fisik terhadap aset informasi.
Deskripsi Bukti Dukung	Bukti dukung terhadap kontrol pelindungan fisik mencakup dokumen kebijakan dan prosedur formal terkait pelindungan fisik aset seperti SOP mitigasi bencana, rencana penanganan kebakaran, dan sistem backup daya. Bukti fisik berupa dokumentasi atau foto pemasangan UPS atau genset, alat pemadam kebakaran (APAR), smoke detector, serta sistem drainase atau peringatan dini terhadap kebocoran air dapat disertakan. Log inspeksi rutin, sertifikat layak fungsi dari pihak ketiga, serta hasil audit dan perbaikan menunjukkan bahwa prosedur tidak hanya tersedia dan diterapkan, tetapi juga dimonitor dan ditingkatkan secara berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH001 TH003 TH007 TH009 TH023 TH076 TH002 TH004 TH008 TH015 TH026
Referensi Kontrol	**NIST CSF 2.0: PR.IR-02, PR.AA-06** **NIST CSF 1.1: PR.IP-5, PR.AC-2** **NIST SP 800-53r5: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9** **SNI ISO/IEC 27001:2022: 7.1, 7.2, 7.3, 7.4, 7.5, 7.11, 7.12**

Kriteria Pemenuhan Kontrol 2.2.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pelindungan aset fisik	Tidak ada prosedur atau fasilitas pelindungan fisik terhadap aset penting (tidak ada UPS, APAR, atau perlindungan air).	Tidak terdapat SOP, prosedur atau fasilitas fisik seperti UPS, APAR, atau sistem anti-resapan air.
1	Prosedur pelindungan aset fisik sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Beberapa fasilitas pelindungan sudah tersedia (misalnya hanya APAR), tapi tanpa prosedur tertulis dan tidak mencakup seluruh aspek.	Foto atau bukti sebagian kecil perlindungan fisik (misal 1 APAR), namun belum ada SOP atau dokumentasi tertulis. Tidak ada pelatihan atau pengecekan rutin.
2	Prosedur keamanan fisik terhadap akses kontrol sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar aspek pelindungan fisik telah diterapkan (misal UPS dan APAR), namun belum memiliki SOP atau kebijakan formal.	Bukti penerapan perlindungan pada sebagian besar area (misal tersedia UPS dan APAR di hampir semua ruang), namun belum ada dokumen prosedur atau kebijakan formal.
3	Prosedur pelindungan aset fisik sudah diformalkan dan diterapkan pada seluruh aspek	Terdapat SOP atau kebijakan resmi pelindungan fisik dan sudah diterapkan secara menyeluruh pada seluruh aspek.	SOP pelindungan fisik tersedia dan mencakup semua aspek (catu daya, proteksi kebakaran, dan anti-resapan air), disertai bukti implementasi seperti log pengecekan peralatan.
4	- Prosedur pelindungan aset fisik sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Prosedur formal telah diterapkan secara penuh dan disertai monitoring serta evaluasi berkala terhadap implementasinya.	Terdapat SOP lengkap, dokumentasi implementasi, log pemeliharaan rutin, laporan monitoring dan reviu berkala (misal inspeksi APAR bulanan atau uji genset).
5	- Prosedur pelindungan aset fisik sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan	Selain diterapkan dan dimonitor, hasil evaluasi digunakan untuk perbaikan dan peningkatan berkelanjutan terhadap sistem pelindungan fisik.	Selain seluruh bukti pada indeks 4, terdapat catatan perbaikan atau peningkatan sistem (misalnya upgrade sistem UPS, penambahan sensor air, pelatihan rutin tim tanggap darurat).

60 Kontrol 2.2.1.c:

Kontrol	Tersedianya prosedur dan sarana pengamanan terhadap perangkat komputer yang digunakan untuk pengolahan data IIV.
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa prosedur dan sarana pengamanan yang memadai tersedia untuk melindungi perangkat komputer yang digunakan dalam pengolahan data IIV. Pengamanan ini mencakup langkah-langkah fisik dan teknis untuk melindungi perangkat keras dan perangkat lunak yang digunakan dalam pengolahan data, termasuk pengamanan terhadap ancaman fisik seperti pencurian atau kerusakan, serta ancaman siber seperti malware dan akses yang tidak sah. Prosedur pengamanan ini bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data yang diolah oleh perangkat komputer yang digunakan. Pengamanan ini juga harus mematuhi standar yang berlaku di sektor dan peraturan perundangundangan yang relevan.
Deskripsi Bukti Dukung	Bukti dukung terhadap tersedianya prosedur dan sarana pengamanan perangkat komputer untuk pengolahan data IIV mencakup dokumen resmi seperti kebijakan atau SOP yang mengatur perlindungan perangkat, serta bukti penerapannya secara teknis. Bukti teknis mencakup penggunaan antivirus, firewall, sistem enkripsi, pembatasan akses pengguna, serta log pemantauan sistem. Selain itu, terdapat dokumentasi audit internal, laporan monitoring keamanan berkala, dan bukti perbaikan atau peningkatan keamanan perangkat. Untuk mencapai indeks tertinggi, organisasi juga harus menunjukkan adanya proses reviu berkala dan perbaikan berkelanjutan berdasarkan hasil evaluasi tersebut.
Ancaman/Risiko yang dimitigasi	TH023 TH030 TH032 TH052 TH054 TH071 TH025 TH031 TH035 TH053 TH059 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.IR-02, PR.AA-06** **NIST CSF 1.1: PR.IP-5, PR.AC-2** **NIST SP 800-53r5: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9** **SNI ISO/IEC 27001:2022: 7.1, 7.2, 7.3, 7.4, 7.5, 7.11, 7.12**

Kriteria Pemenuhan Kontrol 2.2.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur dan sarana pengamanan terhadap perangkat komputer untuk pengolahan data IIV	Belum ada prosedur maupun sarana pengamanan yang diterapkan untuk perangkat komputer pengolah data IIV.	Tidak terdapat SOP, kebijakan, atau sarana pengamanan perangkat (tidak ada antivirus, firewall, atau sistem autentikasi).
1	Prosedur pengamanan terhadap perangkat komputer untuk pengolahan data IIV sudah diterapkan pada sebagian kecil aspek beserta sarana pengamanannya namun belum diformalkan	Pengamanan diterapkan hanya pada sebagian kecil perangkat, seperti penggunaan antivirus dasar, namun belum memiliki prosedur formal.	Antivirus atau pengamanan lain diterapkan hanya di sebagian kecil perangkat. Belum ada dokumentasi kebijakan atau prosedur resmi.
2	Prosedur pengamanan terhadap perangkat komputer untuk pengolahan data IIV sudah diterapkan pada sebagian besar aspek beserta sarana pengamanannya namun belum diformalkan	Sebagian besar perangkat telah dilengkapi sarana pengamanan seperti firewall dan pembatasan akses, tetapi prosedur pengamanan belum didokumentasikan secara formal.	Sebagian besar perangkat menggunakan sarana pengamanan (misalnya firewall, pembatasan akses), namun belum tersedia prosedur tertulis.
3	Prosedur pengamanan terhadap perangkat komputer untuk pengolahan data IIV sudah diterapkan pada sebagian besar aspek beserta sarana pengamanannya namun belum diformalkan	Prosedur pengamanan telah diformalkan dan diterapkan secara menyeluruh, serta seluruh perangkat pengolah data IIV telah dilengkapi sarana pengamanan.	Terdapat SOP atau kebijakan formal mengenai pengamanan perangkat komputer, seluruh perangkat pengolah data IIV telah menerapkannya dengan sarana pendukung.
4	- Prosedur pengamanan terhadap perangkat komputer untuk pengolahan data IIV sudah diformalkan dan diterapkan pada seluruh aspek beserta sarana pengamanannya - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Prosedur yang telah diformalkan dan diterapkan secara menyeluruh juga dimonitor pelaksanaannya serta direviu secara berkala untuk memastikan efektivitas.	Seluruh aspek telah dilengkapi pengamanan dan prosedur formal, serta terdapat bukti monitoring (log sistem, hasil audit keamanan, laporan kepatuhan) dan reviu berkala.
5	- Prosedur pengamanan terhadap perangkat komputer untuk pengolahan data IIV sudah diformalkan dan diterapkan pada seluruh aspek beserta sarana pengamanannya - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala serta dilakukan perbaikan secara berkelanjutan	Selain seluruh prosedur dan sarana sudah diterapkan, dilakukan monitoring dan reviu berkala, serta terdapat upaya perbaikan berkelanjutan berbasis hasil evaluasi dan perkembangan teknologi.	Termasuk semua bukti pada Indeks 4, ditambah dokumentasi peningkatan atau perbaikan berkelanjutan (misalnya upgrade sistem pengamanan, patch keamanan rutin, pelatihan staf IT).

2.2.2. Memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur

Kriteria	Detail
Deskripsi	Penyelenggaran IIV mampu memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk memastikan bahwa proses perbaikan dan pemeliharaan dilakukan dengan benar dan sesuai prosedur.
Dampak	**Tinggi** – Dengan memastikan bahwa proses perbaikan dan pemeliharaan dilakukan sesuai prosedur, organisasi dapat mengurangi risiko kerusakan dan memastikan bahwa aset informasi tetap berfungsi dengan baik
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan sistem pencatatan yang tepat untuk mengelola proses perbaikan dan pemeliharaan
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.MA-1** **NIST SP 800-53r5: MA-1, MA-2, MA-3, MA-5, MA-6** **SNI ISO/IEC 27001:2022: 7.2, 7.10, 7.13**

61 Kontrol 2.2.2.a:

Kontrol	Tentukan metode untuk melakukan pembaruan keamanan dan sejenisnya pada perangkat dan server. Kemudian, terapkan pembaruan keamanan tersebut dengan teknologi yang benar dan tepat pada waktunya.
Deskripsi Kontrol	Penyelenggara IIV perlu menentukan metode yang efektif untuk melakukan pembaruan keamanan pada perangkat dan server, dengan memperhatikan teknologi yang tepat dan penerapan pada waktunya. Pembaruan keamanan ini mencakup pembaruan perangkat keras dan perangkat lunak yang relevan untuk mengatasi kerentanannya dan mencegah potensi ancaman atau serangan. Metode yang digunakan dapat mencakup penerapan pembaruan otomatis atau manual, serta pemantauan berkelanjutan terhadap pembaruan yang diperlukan. Implementasi pembaruan keamanan harus dilakukan sesuai dengan kebijakan yang ada, serta harus meminimalkan dampak pada operasional organisasi. Tujuannya adalah untuk memastikan perangkat dan server tetap terlindungi dengan baik dari ancaman yang berkembang dan memiliki keamanan yang terkini.
Deskripsi Bukti Dukung	Bukti dukung terhadap kontrol ini mencakup adanya dokumen formal berupa prosedur atau kebijakan pembaruan keamanan (patch management) pada perangkat dan server, yang menjelaskan metode identifikasi, persetujuan, dan penerapan pembaruan. Bukti teknis dapat berupa log pembaruan sistem, laporan hasil penerapan patch, tangkapan layar dashboard pembaruan perangkat/server, dan catatan waktu penerapan. Untuk organisasi yang lebih matang, terdapat mekanisme monitoring otomatis pembaruan, reviu berkala efektivitas patch, serta dokumentasi perubahan atau perbaikan lanjutan berdasarkan hasil evaluasi keamanan.
Ancaman/Risiko yang dimitigasi	TH023 TH052 TH054 TH072 TH074 TH025 TH053 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.MA-1** **NIST SP 800-53r5: MA-1, MA-2, MA-3, MA-5, MA-6** **SNI ISO/IEC 27001:2022: 7.2, 7.10, 7.13**

Kriteria Pemenuhan Kontrol 2.2.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server	Tidak ada prosedur atau metode pembaruan keamanan yang diterapkan pada perangkat maupun server. Sistem berisiko terhadap kerentanan.	Tidak ada kebijakan, SOP, atau catatan pembaruan keamanan. Sistem belum pernah melakukan patch/perbaikan keamanan.
1	Prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Pembaruan dilakukan secara terbatas dan tidak terstruktur pada sebagian kecil perangkat/server. Belum ada dokumentasi prosedur.	Bukti ad-hoc pembaruan di beberapa perangkat (misalnya log pembaruan otomatis pada beberapa komputer), tanpa dokumentasi prosedur atau sistem monitoring.
2	Prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Pembaruan dilakukan secara rutin pada sebagian besar perangkat/server, namun belum memiliki prosedur atau kebijakan tertulis.	Bukti pembaruan berkala di sebagian besar sistem/server (misal log pembaruan, tangkapan layar), namun belum ada SOP atau dokumen formal.
3	Prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server sudah diformalkan dan diterapkan pada seluruh aspek	Terdapat prosedur formal pembaruan keamanan, diterapkan secara menyeluruh pada seluruh perangkat dan server.	SOP atau kebijakan formal pembaruan keamanan tersedia dan diterapkan ke seluruh perangkat/server. Disertai log pembaruan dan dokumentasi proses.
4	- Prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Prosedur sudah diterapkan secara menyeluruh dan disertai monitoring pelaksanaan serta reviu berkala terhadap efektivitas pembaruan.	Terdapat sistem monitoring otomatis pembaruan, hasil evaluasi patch, serta laporan reviu rutin atas efektivitas pembaruan yang telah diterapkan.
5	- Prosedur pembaruan keamanan dan sejenisnya pada perangkat dan server sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala serta dilakukan perbaikan secara berkelanjutan	Selain seluruh prosedur diterapkan, monitoring dan reviu dilakukan secara berkala, serta ada perbaikan/peningkatan berkelanjutan atas proses pembaruan keamanan.	Semua bukti pada Indeks 4, ditambah dokumentasi tindakan perbaikan berkelanjutan (misalnya penggantian tools update, perbaikan SOP, evaluasi vendor, pelatihan staf teknis).

62 Kontrol 2.2.2.b:

Kontrol	Dokumentasikan kegiatan pembaruan keamanan pada perangkat organisasi dan laporkan kepada manajemen secara berkala.
Deskripsi Kontrol	Penyelenggara IIV perlu mendokumentasikan seluruh kegiatan pembaruan keamanan pada perangkat yang digunakan dalam organisasi. Dokumentasi ini bertujuan untuk memastikan bahwa setiap pembaruan dilakukan sesuai dengan kebijakan yang berlaku dan untuk memberikan transparansi mengenai upaya perlindungan terhadap perangkat yang digunakan dalam operasional. Selain itu, hasil dari pembaruan keamanan tersebut perlu dilaporkan secara berkala kepada manajemen agar mereka dapat memantau status keamanan dan efektivitas tindakan yang telah dilakukan. Pelaporan ini membantu manajemen untuk memastikan bahwa langkah-langkah yang diperlukan untuk menjaga keamanan perangkat dan sistem informasi sudah dilakukan sesuai dengan standar yang ditetapkan.
Deskripsi Bukti Dukung	Bukti dukung atas kontrol ini mencakup adanya catatan atau log pembaruan keamanan pada perangkat organisasi yang terdokumentasi dengan rapi, seperti laporan patching, log sistem, jadwal update, dan ringkasan hasil implementasi pembaruan. Laporan tersebut idealnya disusun dalam format yang dapat dipahami manajemen dan disampaikan secara berkala (bulanan, triwulanan, dll.). Pada tingkat yang lebih matang, bukti tambahan berupa sistem pemantauan penerapan pembaruan, hasil audit internal terhadap pelaksanaan update, serta perbaikan berkelanjutan dari hasil evaluasi dokumentasi dan pelaporan juga tersedia.
Ancaman/Risiko yang dimitigasi	TH023 TH052 TH054 TH072 TH074 TH025 TH053 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-03** **NIST CSF 1.1: PR.MA-1** **NIST SP 800-53r5: MA-1, MA-2, MA-3, MA-5, MA-6** **SNI ISO/IEC 27001:2022: 7.2, 7.10, 7.13**

Kriteria Pemenuhan Kontrol 2.2.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Kegiatan pembaruan keamanan pada perangkat organisasi belum didokumentasikan dan dilaporkan kepada manajemen secara berkala	Tidak ada dokumentasi maupun pelaporan kepada manajemen terkait pembaruan keamanan perangkat organisasi.	Tidak tersedia log pembaruan, laporan teknis, maupun komunikasi kepada manajemen.
1	Kegiatan pembaruan keamanan pada perangkat organisasi sebagian kecil sudah didokumentasikan dan dilaporkan kepada manajemen secara berkala secara informal	Hanya sebagian kecil kegiatan pembaruan terdokumentasi dan disampaikan kepada manajemen secara informal (misal melalui obrolan atau email biasa).	Terdapat log atau catatan update sebagian kecil perangkat. Laporan disampaikan melalui media informal (chat/email biasa), tidak terdokumentasi secara sistematis.
2	Kegiatan pembaruan keamanan pada perangkat organisasi sebagian besar sudah didokumentasikan dan dilaporkan kepada manajemen secara berkala secara informal	Sebagian besar kegiatan pembaruan terdokumentasi dan dilaporkan kepada manajemen secara informal, namun belum dalam format standar atau resmi.	Terdapat laporan sebagian besar pembaruan yang dilakukan, namun penyampaian ke manajemen tidak konsisten dan belum menggunakan format atau jalur formal.
3	Kegiatan pembaruan keamanan pada perangkat organisasi sudah didokumentasikan seluruhnya dan dilaporkan kepada manajemen secara berkala secara formal	Semua kegiatan pembaruan terdokumentasi dan dilaporkan secara formal kepada manajemen secara berkala (misal dalam laporan resmi).	Seluruh pembaruan terdokumentasi dalam log sistem atau laporan teknis, dan dilaporkan kepada manajemen secara formal dan berkala (misalnya dalam laporan keamanan TI).
4	- Kegiatan pembaruan keamanan pada perangkat organisasi sudah didokumentasikan seluruhnya dan dilaporkan kepada manajemen secara berkala secara formal - Prosedur dokumentasi dimonitor pelaksanaanya dan direviu secara berkala	Dokumentasi dan pelaporan dilakukan secara menyeluruh dan formal, serta terdapat pemantauan dan reviu berkala atas pelaksanaan dokumentasi.	Selain dokumentasi dan pelaporan formal, terdapat bukti monitoring penerapan update (misal dashboard status pembaruan), serta notulen atau hasil evaluasi rutin.
5	- Kegiatan pembaruan keamanan pada perangkat organisasi sudah didokumentasikan seluruhnya dan dilaporkan kepada manajemen secara berkala secara formal - Prosedur dokumentasi dimonitor pelaksanaanya dan direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan	Selain seluruh kegiatan terdokumentasi dan dilaporkan secara formal serta dimonitor, terdapat evaluasi dan perbaikan berkelanjutan terhadap proses dokumentasi dan pelaporan.	Termasuk semua pada Indeks 4, serta adanya dokumen tindak lanjut dan peningkatan berkelanjutan (contoh: revisi format pelaporan, penyempurnaan proses dokumentasi, pelatihan staf terkait dokumentasi pembaruan).

2.2.3. Memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur

Kriteria	Detail
Deskripsi	Penyelenggaran IIV mampu memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk memastikan bahwa proses pemeliharaan jarak jauh dilakukan sesuai prosedur dan didokumentasikan dengan benar.
Dampak	**Tinggi** – Dengan memastikan bahwa pemeliharaan jarak jauh dilakukan dengan persetujuan dan didokumentasikan, organisasi dapat mengurangi risiko penyalahgunaan dan memastikan bahwa aset informasi tetap aman
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan sistem pencatatan yang tepat untuk mengelola pemeliharaan jarak jauh
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-02** **NIST CSF 1.1: PR.MA-2** **NIST SP 800-53r5: MA-4** **SNI ISO/IEC 27001:2022: 5.19, 5.22, 7.13**

63 Kontrol 2.2.3.a:

Kontrol	Mengidentifikasi perangkat yang memiliki mekanisme pembaruan jarak jauh untuk melakukan pembaruan massal berbagai program perangkat lunak (OS, driver, dan aplikasi) melalui perintah jarak jauh.
Deskripsi Kontrol	Penyelenggara IIV perlu mengidentifikasi perangkat yang mendukung mekanisme pembaruan jarak jauh, yang memungkinkan pembaruan massal untuk berbagai program perangkat lunak seperti sistem operasi (OS), driver, dan aplikasi. Proses ini bertujuan untuk memastikan bahwa semua perangkat yang terhubung ke jaringan dapat diperbarui secara terpusat dan efisien, tanpa perlu pembaruan manual satu per satu. Pengelolaan pembaruan perangkat secara jarak jauh membantu meminimalkan potensi kerentanannya serta memastikan bahwa semua perangkat selalu diperbarui dengan versi terbaru yang mencakup perbaikan keamanan dan peningkatan fungsionalitas. Ini juga dapat menghemat waktu dan sumber daya yang dibutuhkan untuk memperbarui perangkat secara manual.
Deskripsi Bukti Dukung	Bukti Dukung kontrol ini dapat berupa daftar atau inventaris perangkat yang sudah dilengkapi dengan mekanisme pembaruan jarak jauh, baik melalui endpoint management tools, centralized patch management system, maupun platform seperti WSUS, SCCM, atau MDM (Mobile Device Management). Dokumentasi formal identifikasi, hasil pemindaian perangkat secara berkala, laporan audit sistem, serta dashboard monitoring perangkat yang mendukung pembaruan jarak jauh menjadi indikator implementasi. Pada level lanjut, terdapat proses otomatisasi identifikasi dan reviu berkala terhadap perubahan jumlah dan jenis perangkat untuk memastikan efektivitas pembaruan sistem secara remote.
Ancaman/Risiko yang dimitigasi	TH023 TH052 TH054 TH072 TH074 TH025 TH053 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-02** **NIST CSF 1.1: PR.MA-2** **NIST SP 800-53r5: MA-4** **SNI ISO/IEC 27001:2022: 5.19, 5.22, 7.13**

Kriteria Pemenuhan Kontrol 2.2.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum dilakukan identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh	Belum dilakukan identifikasi terhadap perangkat yang memiliki kemampuan pembaruan jarak jauh.	Tidak tersedia inventaris perangkat, tidak ada catatan sistem pembaruan jarak jauh.
1	Identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh sebagian kecil sudah diidentifikasi secara informal	Sebagian kecil perangkat telah diidentifikasi memiliki mekanisme pembaruan jarak jauh, namun hanya secara informal (belum terdokumentasi resmi).	Terdapat catatan manual atau tidak resmi (misalnya daftar pribadi teknisi) mengenai sebagian kecil perangkat dengan fitur update jarak jauh.
2	Identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh sebagian besar sudah diidentifikasi secara informal	Sebagian besar perangkat telah diidentifikasi secara informal, tetapi belum ada dokumentasi atau sistem pendukung yang terstandar.	Sebagian besar perangkat tercatat secara tidak resmi, misal dalam spreadsheet atau catatan teknis, tanpa dokumentasi formal atau kebijakan yang mengaturnya.
3	Identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh sudah diidentifikasi seluruhnya secara formal	Seluruh perangkat yang memiliki fitur pembaruan jarak jauh telah diidentifikasi secara formal dan tercatat dalam dokumentasi resmi.	Terdapat dokumen formal (SOP/inventaris) yang mencakup seluruh perangkat dengan kemampuan pembaruan jarak jauh.
4	- Identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh sudah diidentifikasi seluruhnya secara formal - Proses identifikasi perangkat dimonitor pelaksanaanya dan direviu secara berkala	Identifikasi perangkat dilakukan secara menyeluruh dan formal, serta dimonitor dan direviu secara berkala oleh tim pengelola.	Selain dokumen formal, tersedia bukti monitoring dan reviu berkala terhadap kondisi perangkat (misal log audit, jadwal evaluasi, laporan periodik perangkat aktif).
5	- Identifikasi perangkat yang memiliki mekanisme pembaruan melalui perintah jarak jauh sudah diidentifikasi seluruhnya secara formal, serta dilakukan otomatisasi - Proses identifikasi perangkat dimonitor pelaksanaanya dan direviu secara berkala	Selain seluruh perangkat diidentifikasi secara formal, proses identifikasinya telah otomatis (menggunakan tools scanning) dan direviu serta diperbaiki secara berkala.	Sistem identifikasi perangkat bersifat otomatis (menggunakan tool seperti Lansweeper, SCCM, atau MDM), dengan reviu rutin dan bukti tindak lanjut dari hasil reviu (contoh: update konfigurasi, penghapusan perangkat usang).

64 Kontrol 2.2.3.b:

Kontrol	Melakukan pemeliharaan perangkat dan server yang telah disetujui dari jarak jauh dan mencatat setiap log masuknya, sehingga akses yang tidak sah dapat dicegah.
Deskripsi Kontrol	Penyelenggara IIV perlu melakukan pemeliharaan perangkat dan server yang telah disetujui dari jarak jauh, dengan memastikan bahwa setiap log masuk dicatat untuk mencegah akses yang tidak sah. Proses ini termasuk pemantauan akses jarak jauh untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses perangkat dan server. Log akses yang tercatat harus menyertakan informasi seperti waktu login, identitas pengguna, alamat IP yang digunakan, serta aktivitas yang dilakukan selama sesi akses. Pencatatan log ini berfungsi untuk mendeteksi dan merespons potensi ancaman atau akses yang tidak sah. Selain itu, kebijakan akses jarak jauh harus mengharuskan penggunaan autentikasi yang kuat (misalnya, multi-factor authentication) untuk meningkatkan keamanan.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini dapat berupa dokumentasi formal prosedur pemeliharaan jarak jauh yang telah disetujui oleh otoritas internal, serta bukti teknis pelaksanaan seperti log akses remote, rekaman aktivitas pemeliharaan, dan sistem otentikasi yang digunakan (VPN, 2FA, RDP Gateway). Log masuk pengguna harus tersedia dan menunjukkan siapa yang mengakses, kapan, dari mana, serta tindakan apa yang dilakukan. Sistem pemantauan otomatis serta audit berkala terhadap aktivitas pemeliharaan menjadi indikator penting dalam memastikan pemeliharaan dilakukan secara sah, aman, dan terdokumentasi. Pada level yang lebih tinggi, sistem pemeliharaan dilakukan secara otomatis dan terdokumentasi penuh dalam sistem terintegrasi.
Ancaman/Risiko yang dimitigasi	TH023 TH052 TH054 TH072 TH074 TH025 TH053 TH071 TH073 TH075
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08, PR.PS-02** **NIST CSF 1.1: PR.MA-2** **NIST SP 800-53r5: MA-4** **SNI ISO/IEC 27001:2022: 5.19, 5.22, 7.13**

Kriteria Pemenuhan Kontrol 2.2.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Pemeliharaan perangkat dan server yang disetujui dari jarak jauh belum dilakukan	Tidak ada pemeliharaan jarak jauh yang dilakukan atau tidak tersedia mekanisme yang disetujui.	Tidak ada kegiatan pemeliharaan jarak jauh, tidak tersedia log masuk, atau tidak ada izin formal.
1	Sebagian kecil perangkat dan server yang disetujui dari jarak jauh sudah dilakukan pemeliharaan namun belum diformalkan	Pemeliharaan jarak jauh dilakukan pada sebagian kecil perangkat/server secara ad-hoc tanpa prosedur formal dan tanpa pencatatan log lengkap.	Beberapa aktivitas pemeliharaan jarak jauh dilakukan tanpa prosedur tertulis, log masuk dicatat sebagian, dan tidak ada sistem monitoring.
2	Sebagian besar perangkat dan server yang disetujui dari jarak jauh sudah dilakukan pemeliharaan namun belum diformalkan	Sebagian besar perangkat/server dilakukan pemeliharaan jarak jauh, namun belum ada prosedur formal atau sistem pencatatan log yang menyeluruh.	Pemeliharaan dilakukan pada sebagian besar perangkat dengan log masuk manual atau terpisah, namun prosedur belum diformalkan.
3	Seluruh perangkat dan server yang disetujui dari jarak jauh sudah dilakukan pemeliharaan dan sudah diformalkan	Seluruh perangkat dan server dilakukan pemeliharaan jarak jauh sesuai prosedur yang telah diformalkan, disertai pencatatan log masuk secara konsisten.	Terdapat SOP formal pemeliharaan jarak jauh, seluruh perangkat/server masuk dalam cakupan, dan log masuk dicatat dengan tools yang sah (misal: SIEM, RDP logs, SSH audit trail).
4	- Seluruh perangkat dan server yang disetujui dari jarak jauh sudah dilakukan pemeliharaan dan sudah diformalkan - Prosedur pemeliharaan perangkat dimonitor pelaksanaanya dan direviu secara berkala	Prosedur formal diterapkan pada seluruh perangkat, log masuk dimonitor, dan evaluasi dilakukan secara berkala terhadap efektivitas prosedur.	Selain log masuk terekam dan terdokumentasi, monitoring dan evaluasi berkala dilakukan secara sistematis dan dibuktikan dengan laporan audit/reviu.
5	- Seluruh perangkat dan server yang disetujui dari jarak jauh sudah dilakukan pemeliharaan dan sudah diformalkan, dan dilakukan otomatisasi - Prosedur pemeliharaan perangkat dimonitor pelaksanaanya dan direviu secara berkala	Selain diformalkan dan dimonitor, pemeliharaan dilakukan secara otomatis atau melalui sistem terjadwal, serta hasil monitoring direviu dan ditindaklanjuti secara berkelanjutan.	Sistem pemeliharaan jarak jauh dilakukan secara otomatis (misal melalui patch scheduler, centralized management), log terintegrasi, dan terdapat proses perbaikan berkelanjutan berdasarkan hasil monitoring dan evaluasi.

2.2.4. Memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman

Kriteria	Detail
Deskripsi	Penyelenggaran IIV mampu memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan teknologi pemantauan dan sumber daya untuk melakukan pemantauan secara berkala.
Dampak	**Tinggi** – Dengan pemantauan yang rutin, organisasi dapat mendeteksi dan merespons ancaman dengan cepat, sehingga mengurangi risiko kerusakan atau kehilangan aset.
Kompleksitas	**Sedang** – Memerlukan sistem pemantauan yang tepat dan pelatihan karyawan untuk memahami serta menggunakan teknologi pemantauan dengan efektif.
Referensi Kontrol	**NIST CSF 2.0: DE.CM-02** **NIST CSF 1.1: DE.CM-2** **NIST SP 800-53r5: CA-7, PE-6, PE-20** **SNI ISO/IEC 27001:2022: 7.4**

65 Kontrol 2.2.4.a:

Kontrol	Penyelenggara IIV memastikan lingkungan fisik aset IIV dipantau secara tepat melalui pengaturan, perekaman, dan pemantauan akses fisik terhadap aset IIV. (misalnya cctv, akses kontrol, sensor, dll).
Deskripsi Kontrol	Penyelenggara IIV memastikan bahwa lingkungan fisik yang menyimpan aset IIV dipantau dengan tepat untuk melindungi dari ancaman fisik. Hal ini dilakukan melalui pengaturan akses fisik yang terkontrol dan pemantauan secara terus-menerus. Langkahlangkah ini meliputi penggunaan sistem pengawasan seperti CCTV, kontrol akses pintu menggunakan kartu ID atau biometrik, serta sensor untuk mendeteksi pergerakan atau aktivitas mencurigakan. Pemantauan ini bertujuan untuk mencegah akses yang tidak sah, meminimalisir risiko pencurian atau kerusakan fisik terhadap aset IIV, dan memastikan bahwa hanya personel yang berwenang yang dapat mengakses area yang sensitif. Semua aktivitas yang terkait dengan akses fisik harus direkam dan dapat diaudit untuk keperluan investigasi atau evaluasi keamanan.
Deskripsi Bukti Dukung	Bukti Dukung atas kontrol ini mencakup keberadaan dan penerapan sistem pemantauan fisik seperti kamera CCTV, sistem akses kontrol (misalnya kartu ID, biometrik), sensor gerak, serta pencatatan log akses ke area yang menyimpan aset IIV. Bukti dapat berupa rekaman CCTV, log akses masuk/keluar, laporan pengawasan rutin, serta prosedur formal yang mengatur mekanisme pemantauan lingkungan fisik. Pada tingkat yang lebih tinggi, tersedia laporan hasil evaluasi, audit kepatuhan terhadap kebijakan akses fisik, dan pembaruan sistem monitoring berdasarkan hasil reviu berkala dan perbaikan berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH001 TH003 TH023 TH032 TH053 TH059 TH076 TH002 TH004 TH031 TH035 TH054 TH075
Referensi Kontrol	**NIST CSF 2.0: DE.CM-02** **NIST CSF 1.1: DE.CM-2** **NIST SP 800-53r5: CA-7, PE-6, PE-20** **SNI ISO/IEC 27001:2022: 7.4**

Kriteria Pemenuhan Kontrol 2.2.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pemantauan lingkungan fisik aset IIV	Tidak tersedia prosedur atau sarana pemantauan lingkungan fisik aset IIV. Akses fisik tidak terkontrol atau tidak tercatat.	Tidak ada CCTV, akses kontrol, sensor, atau pencatatan akses fisik; tidak tersedia prosedur pengawasan lingkungan fisik.
1	Prosedur pemantauan lingkungan fisik aset IIV sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Pemantauan lingkungan fisik hanya dilakukan pada sebagian kecil area penting secara informal, belum ada dokumentasi atau standar operasional prosedur (SOP).	Ada sebagian area dengan pemantauan seperti satu CCTV di ruang server utama, namun tanpa dokumentasi atau log akses yang memadai.
2	Prosedur pemantauan lingkungan fisik aset IIV sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Sebagian besar lingkungan fisik aset IIV sudah dipantau (misal sebagian besar ruang server terpasang CCTV), namun belum terdokumentasi secara formal.	CCTV dan akses kontrol digunakan di sebagian besar area penting, tetapi tidak ada SOP atau kebijakan tertulis yang mengatur penggunaannya.
3	Prosedur pemantauan lingkungan fisik aset IIV sudah diformalkan dan diterapkan pada seluruh aspek	Pemantauan fisik aset IIV sudah diterapkan secara menyeluruh, dengan SOP resmi yang mencakup pengaturan akses, pencatatan, dan rekaman aktivitas.	Tersedia SOP atau kebijakan tertulis tentang pemantauan lingkungan fisik; CCTV dan akses kontrol sudah terpasang dan digunakan di seluruh area aset IIV; log akses terdokumentasi.
4	- Prosedur pemantauan lingkungan fisik aset IIV sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Prosedur pemantauan sudah diformalkan dan diterapkan menyeluruh serta dilakukan monitoring pelaksanaan dan evaluasi berkala terhadap efektivitasnya.	Selain SOP dan penerapan menyeluruh, terdapat bukti monitoring dan reviu rutin (misalnya: audit keamanan fisik, laporan tinjauan sistem pemantauan).
5	- Prosedur pemantauan lingkungan fisik aset IIV sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala serta dilakukan perbaikan secara berkelanjutan	Pemantauan lingkungan fisik dilakukan menyeluruh dan berbasis sistem otomatis, disertai reviu dan perbaikan berkelanjutan terhadap kebijakan dan teknologi yang digunakan.	Termasuk semua pada Indeks 4, serta adanya pembaruan sistem monitoring, peningkatan teknologi (misal integrasi sensor ke SIEM), dan dokumentasi perbaikan berkelanjutan berdasarkan hasil evaluasi.

2.2.5. Memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman

Kriteria	Detail
Deskripsi	Penyelenggaran IIV mampu memahami perkembangan ancaman baik internal maupun eksternal melalui tinjauan dan analisis terhadap hasil reviu dari respons insiden keamanan dan hasil pemantauan, pengukuran, dan evaluasi dalam rangka memastikan prosedur dan penerapan pelindungan aset fisik.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk melakukan peninjauan dan peningkatan prosedur secara berkala.
Dampak	**Tinggi** – Dengan peninjauan dan peningkatan yang rutin, organisasi dapat memastikan bahwa prosedur pelindungan tetap efektif dan sesuai dengan perkembangan ancaman terbaru.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan sistem peninjauan yang tepat untuk melakukan peninjauan dan peningkatan secara berkala.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: PR.IP-7** **NIST SP 800-53r5: CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6** **SNI ISO/IEC 27001:2022: -**

66 Kontrol 2.2.5.a:

Kontrol	Penyelenggara IIV senantiasa melakukan peninjauan, analisis, dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu dari respons insiden keamanan dan hasil pemantauan, pengukuran, dan evaluasi ancaman internal dan eksternal.
Deskripsi Kontrol	Penyelenggara IIV secara berkelanjutan meninjau, menganalisis, dan meningkatkan kontrol keamanan yang telah diterapkan. Proses ini dilakukan berdasarkan hasil reviu dari respons terhadap insiden keamanan serta pemantauan, pengukuran, dan evaluasi terhadap ancaman baik dari dalam maupun luar organisasi. Dengan pendekatan ini, kontrol keamanan dapat terus disesuaikan dan diperkuat guna menghadapi potensi risiko yang berkembang, sehingga keamanan informasi tetap terjaga secara optimal.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - Audit Internal (Bukti hasil audit internal (temuan dan tindak lanjut) - Reviu Penerapan prosedur/kebijakan dan kontrol keamanan
Ancaman/Risiko yang dimitigasi	TH023 TH052 TH054 TH071 TH073 TH075 TH025 TH053 TH059 TH072 TH074 TH076
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: PR.IP-7** **NIST SP 800-53r5: CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 2.2.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu	Tidak ada	Tidak ada
1	Prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu sudah diterapkan pada sebagian kecil aspek namun belum diformalkan	Organisasi telah menerapkan prosedur peninjauan, analisis, dan peningkatan kontrol keamanan tetapi hanya pada sebagian kecil aspek, serta belum ada formalitas dalam pendokumentasian atau implementasinya.	Bukti penerapan terbatas dalam bentuk laporan atau notulen yang menunjukkan adanya upaya peninjauan, analisis, atau peningkatan kontrol keamanan, tetapi tidak terdokumentasi dengan baik.
2	Prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu sudah diterapkan pada sebagian besar aspek namun belum diformalkan	Prosedur telah diterapkan pada sebagian besar aspek dalam organisasi, tetapi masih belum diformalkan dalam kebijakan atau prosedur tertulis.	Laporan atau catatan internal yang menunjukkan penerapan prosedur pada sebagian besar aspek, namun tidak ada kebijakan formal yang mengaturnya.
3	Prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu sudah diformalkan dan diterapkan pada seluruh aspek	Prosedur sudah diformalkan dalam kebijakan atau prosedur tertulis dan telah diterapkan pada seluruh aspek organisasi.	- Dokumen kebijakan dan prosedur formal yang mencakup seluruh aspek organisasi. - Bukti implementasi dalam bentuk laporan pelaksanaan prosedur.
4	- Prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala	Prosedur yang diformalkan telah diterapkan secara menyeluruh, dimonitor pelaksanaannya, dan dilakukan reviu secara berkala untuk memastikan efektivitasnya.	- Dokumen kebijakan dan prosedur yang diformalkan serta mencakup seluruh aspek organisasi. - Bukti pemantauan pelaksanaan prosedur melalui laporan audit atau hasil reviu berkala.
5	- Prosedur peninjauan, analisis dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu sudah diformalkan dan diterapkan pada seluruh aspek - Prosedur tersebut dimonitor pelaksanaanya dan direviu secara berkala serta dilakukan perbaikan secara berkelanjutan	Prosedur yang diformalkan telah diterapkan menyeluruh, dimonitor, direviu secara berkala, serta dilakukan perbaikan secara berkelanjutan untuk meningkatkan efektivitas kontrol keamanan.	- Dokumentasi perubahan atau perbaikan yang dilakukan berdasarkan hasil reviu dan evaluasi berkala. - Bukti adanya mekanisme continuous improvement seperti siklus PDCA (Plan-Do-Check-Act) atau inisiatif peningkatan lainnya.

2.3. Melindungi data

Melindungi data dalam layanan IIV merupakan langkah krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelola oleh penyelenggara. Pelindungan ini mencakup data yang disimpan maupun data yang dikirim, dengan menerapkan kontrol keamanan yang ketat untuk mencegah akses tidak sah, kebocoran, atau modifikasi yang tidak diinginkan. Ketersediaan kapasitas ruang penyimpanan yang memadai juga menjadi prioritas agar layanan tetap optimal tanpa mengorbankan keamanan data. Untuk menjamin keandalan sistem, mekanisme pengecekan integritas diterapkan secara berkala guna memverifikasi kondisi perangkat keras, perangkat lunak, dan data itu sendiri. Di samping itu, prosedur pencadangan data dirancang, dipelihara, dan diuji secara rutin agar data tetap tersedia dalam situasi darurat. Sebagai bentuk tanggung jawab akhir terhadap siklus hidup data, penyelenggara juga wajib menyediakan dan menerapkan kebijakan pemusnahan data secara aman, sehingga tidak ada risiko kebocoran setelah data tidak lagi digunakan. Seluruh upaya ini bertujuan memastikan bahwa data pada layanan IIV terlindungi secara menyeluruh dari berbagai potensi ancaman.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) pelindungan terhadap data yang tersimpan pada Penyelenggara IIV;
b) pelindungan terhadap data yang terkirim dari Penyelenggara IIV;
c) memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai;
d) mengimplementasikan pelindungan dari kebocoran data;
e) mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data;
f) memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala; dan
g) menyediakan kebijakan pemusnahan data.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melindungi data” secara efektif antara lain:

NIST CSF 2.0	**:**	**PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11, PR.IR-04, DE.CM-09, ID.RA-09, RC.RP-03, ID.AM-08**
NIST CSF 1.1	**:**	**PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-5, PR.DS-6, PR.DS-8, PR.IP-4, PR.IP-6**
NIST SP 800-53r5	**:**	**MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-5, SC-7, SC-8, SC-11, SC-28, AU-4, AU-13, CP-2, CP-4, CP-6, CP-9, PE-11, PE-19, PS-6, AC-4, AC-5, AC-6, SI-4, SI-7, SI-10, SA-10, SR-12**
SNI ISO/IEC 27001:2022	**:**	**5.3, 5.10, 5.13, 5.14, 5.15, 5.29, 5.33, 6.1, 6.2, 6.5, 7.10, 7.13, 7.14, 8.2, 8.3, 8.4, 8.7, 8.8, 8.13, 8.17, 8.19, 8.20, 8.22, 8.26**

Peraturan BSSN Nomor 7 tahun 2024

Peraturan BSSN Nomor 11 Tahun 2024

2.3.1. Pelindungan terhadap data yang tersimpan pada Penyelenggara IIV

Kriteria	Detail
Deskripsi	Perlindungan terhadap data yang tersimpan pada Penyelenggara IIV merupakan aspek krusial dalam menjaga keamanan dan keandalan sistem nasional. Dalam hal terjadi pertukaran informasi yang bersifat dilindungi dengan organisasi lain, Penyelenggara IIV wajib memastikan bahwa organisasi tersebut terlebih dahulu menyetujui persyaratan keamanan yang ditetapkan untuk menjamin perlindungan informasi selama proses pertukaran maupun penyimpanannya. Selain itu, seluruh informasi yang dikelola oleh Penyelenggara IIV harus dienkripsi menggunakan tingkat kekuatan yang sesuai dengan standar keamanan informasi yang berlaku, guna mencegah akses ilegal, menjaga kerahasiaan, serta menjamin integritas data.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi enkripsi dan kontrol akses yang memiliki sertifikat keamanan, serta pengembangan kebijakan dan prosedur manajemen data.
Dampak	**Tinggi** – Melindungi kerahasiaan, integritas, dan ketersediaan data yang penting bagi operasional dan keamanan organisasi.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem dan prosedur yang tepat untuk melindungi data yang tersimpan, serta pelatihan karyawan tentang pentingnya keamanan data.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01** **NIST CSF 1.1: PR.DS-1** **NIST SP 800-53r5: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28** **SNI ISO/IEC 27001:2022: 8.8** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

67 Kontrol 2.3.1.a:

Kontrol	Jika Penyelenggara IIV bertukar informasi yang perlu dilindungi dengan organisasi lain, maka Penyelenggara IIV perlu meminta organisasi lain tersebut untuk menyetujui persyaratan keamanan untuk perlindungan informasi tersebut.
Deskripsi Kontrol	Setiap pertukaran informasi yang perlu dilindungi antara Penyelenggara IIV dan organisasi lain dilakukan dengan keamanan yang terjamin. Sebelum berbagi informasi, Penyelenggara IIV harus memastikan bahwa organisasi penerima menyetujui dan mematuhi persyaratan keamanan yang ditetapkan untuk melindungi informasi tersebut. Langkah ini bertujuan untuk mencegah kebocoran, penyalahgunaan, atau akses tidak sah terhadap informasi sensitif, serta menjaga kepatuhan terhadap kebijakan dan regulasi keamanan yang berlaku.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - Non-Disclosure Agreement (NDA) atau perjanjian kerja sama yang mencantumkan persyaratan perlindungan informasi - SOP Pertukaran Informasi / Pengendalian Informasi - Permohonan permintaan Informasi dan Persetujuannya - Persyaratan keamanan dan pengiriman informasi untuk peihak penerima informasi - Melakukan verifikasi persyaratan keamanan untuk pihak yang meminta informasi
Ancaman/Risiko yang dimitigasi	TH031 TH053 TH059 TH075 TH035 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01** **NIST CSF 1.1: PR.DS-1** **NIST SP 800-53r5: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 2.3.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum meminta organisasi lain untuk menyetujui persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi belum memiliki kebijakan internal atau prosedur teknis mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain. - Organisasi belum memiliki konsep atau format dokumen persetujuan persyaratan keamanan yang disahkan pimpinan untuk melindungi informasi yang ditukarkan dengan organisasi lain.	Tidak ada	Tidak ada
1	- Organisasi sudah meminta organisasi lain untuk menyetujui sebagian kecil aspek persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi telah memiliki konsep atau rancangan kebijakan internal atau prosedur teknis mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain. - Organisasi telah memiliki konsep atau format dokumen persetujuan persyaratan keamanan yang belum disahkan pimpinan untuk melindungi informasi yang ditukarkan dengan organisasi lain.	Organisasi telah meminta organisasi lain untuk menyetujui sebagian kecil aspek persyaratan keamanan. Konsep kebijakan dan prosedur teknis telah dirancang, tetapi belum diformalkan. Format dokumen persetujuan telah ada, tetapi belum disahkan pimpinan.	- Contoh kasus atau bukti terbatas mengenai permintaan persetujuan persyaratan keamanan dari organisasi lain. - Konsep kebijakan internal atau prosedur teknis yang masih dalam tahap rancangan. - Konsep dokumen persetujuan persyaratan keamanan yang belum disahkan pimpinan.
2	- Organisasi sudah meminta organisasi lain untuk menyetujui sebagian besar aspek persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi telah memiliki konsep atau rancangan kebijakan internal atau prosedur teknis mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain. - Organisasi telah memiliki konsep atau format dokumen persetujuan persyaratan keamanan yang belum disahkan pimpinan untuk melindungi informasi yang ditukarkan dengan organisasi lain.	Organisasi telah meminta organisasi lain untuk menyetujui sebagian besar aspek persyaratan keamanan. Konsep kebijakan dan prosedur teknis telah ada, tetapi belum diformalkan. Format dokumen persetujuan telah disusun, namun belum disahkan pimpinan.	- Bukti komunikasi dengan organisasi lain terkait sebagian besar aspek persyaratan keamanan. - Draf kebijakan dan prosedur teknis yang mencakup pertukaran informasi, meskipun belum diformalkan - Konsep dokumen persetujuan persyaratan keamanan yang masih menunggu pengesahan pimpinan.
3	- Organisasi sudah meminta organisasi lain untuk menyetujui seluruh aspek persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi telah memiliki kebijakan internal atau prosedur teknis yang diformalkan mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain.	Organisasi telah meminta organisasi lain untuk menyetujui seluruh aspek persyaratan keamanan. Kebijakan dan prosedur teknis telah diformalkan serta diterapkan. Format dokumen persetujuan telah disahkan pimpinan dan digunakan dalam praktik.	- Dokumen kebijakan dan prosedur yang telah disahkan dan diberlakukan secara resmi. - Bukti bahwa organisasi lain telah menyetujui seluruh aspek persyaratan keamanan. - Dokumen persetujuan persyaratan keamanan yang telah

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Organisasi telah memiliki format dokumen persetujuan persyaratan keamanan yang disahkan pimpinan untuk melindungi informasi yang ditukarkan dengan organisasi lain.		disahkan pimpinan dan diterapkan dalam praktik.
4	- Organisasi sudah meminta organisasi lain untuk menyetujui seluruh aspek persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi telah memiliki kebijakan internal atau prosedur teknis yang diformalkan, dimonitoring, dan direviu secara berkala mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain. - Organisasi telah memiliki format dokumen persetujuan persyaratan keamanan yang disahkan pimpinan, dimonitoring, dan direviu secara berkala untuk melindungi informasi yang ditukarkan dengan organisasi lain.	Organisasi telah meminta organisasi lain untuk menyetujui seluruh aspek persyaratan keamanan. Kebijakan dan prosedur teknis yang diformalkan telah diterapkan, dimonitor, dan direviu secara berkala. Format dokumen persetujuan yang disahkan pimpinan juga dimonitor dan direviu secara berkala.	- Laporan hasil monitoring dan reviu berkala terhadap kebijakan dan prosedur pertukaran informasi. - Bukti pelaksanaan audit atau evaluasi keamanan informasi terkait pertukaran data dengan organisasi lain.
5	- Organisasi sudah meminta organisasi lain untuk menyetujui seluruh aspek persyaratan keamanan untuk perlindungan informasi yang ditukarkan. - Organisasi telah memiliki kebijakan internal atau prosedur teknis yang diformalkan, dimonitoring, direviu secara berkala dan dilakukan perbaikan mengenai pertukaran informasi yang perlu dilindungi dengan organisasi lain. - Organisasi telah memiliki format dokumen persetujuan persyaratan keamanan yang disahkan pimpinan, dimonitoring, direviu dan dilakukan perbaikan secara berkala untuk melindungi informasi yang ditukarkan dengan organisasi lain.	Organisasi tidak hanya menerapkan, memonitor, dan mereviu kebijakan serta prosedur formal secara berkala, tetapi juga melakukan perbaikan berkelanjutan untuk meningkatkan perlindungan informasi yang ditukarkan.	- Bukti implementasi perbaikan yang dilakukan berdasarkan hasil monitoring dan reviu. - Dokumentasi perubahan kebijakan, prosedur, atau dokumen persetujuan berdasarkan evaluasi dan continuous improvement.

68 Kontrol 2.3.1.b:

Kontrol	Mengenkripsi informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan.
Deskripsi Kontrol	Penyelenggara IIV memastikan bahwa setiap informasi yang perlu dilindungi dienkripsi menggunakan algoritma dan tingkat kekuatan keamanan yang sesuai dengan standar yang berlaku. Enkripsi diterapkan baik pada data yang disimpan (data at rest) maupun data.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: Bukti kesesuaian sesuai dengan standar keamanan yang direkomendasikan oleh BSSN melalui peraturan badan tentang penyelenggaraan algoritma kriptografi indonesia Informasi kritikal sudah di lakukan enkripsi sesuai standar
Ancaman/Risiko yang dimitigasi	TH030 TH032 TH054 TH074 TH031 TH035 TH071 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01** **NIST CSF 1.1: PR.DS-1** **NIST SP 800-53r5: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28** **SNI ISO/IEC 27001:2022: 8.8** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.3.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki kebijakan internal maupun prosedur enkripsi informasi dengan tingkat kekuatan keamanan sesuai dengan standar keamanan; - Organisasi belum menerapkan enkripsi pada informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki konsep kebijakan internal maupun prosedur enkripsi informasi dengan tingkat kekuatan keamanan sesuai dengan standar keamanan - Organisasi sudah menerapkan enkripsi pada sebagian kecil informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan	Organisasi memiliki konsep kebijakan dan prosedur enkripsi, tetapi belum disahkan. Enkripsi baru diterapkan pada sebagian kecil informasi dengan tingkat kekuatan keamanan yang sesuai standar.	- Draft kebijakan atau prosedur enkripsi yang masih dalam tahap konsep. - Bukti penerapan enkripsi pada sebagian kecil informasi (misalnya, hanya pada dokumen tertentu). - Log implementasi enkripsi pada sebagian kecil sistem.
2	- Organisasi sudah memiliki konsep kebijakan internal maupun prosedur enkripsi informasi dengan tingkat kekuatan keamanan sesuai dengan standar keamanan - Organisasi sudah menerapkan enkripsi pada sebagian besar informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan	Organisasi memiliki konsep kebijakan dan prosedur enkripsi, tetapi belum diformalkan. Enkripsi sudah diterapkan pada sebagian besar informasi dengan tingkat kekuatan keamanan yang sesuai standar.	- Draft kebijakan atau prosedur enkripsi yang lebih matang tetapi belum disahkan. - Bukti penerapan enkripsi pada sebagian besar informasi (misalnya, sebagian besar basis data atau file penting). - Log penerapan enkripsi pada berbagai sistem organisasi.
3	- Organisasi sudah memiliki kebijakan internal maupun prosedur enkripsi informasi yang disahkan pimpinan dengan tingkat kekuatan keamanan sesuai dengan standar keamanan - Organisasi sudah menerapkan enkripsi pada seluruh informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan	Organisasi telah memiliki kebijakan dan prosedur enkripsi yang disahkan pimpinan. Enkripsi diterapkan pada seluruh informasi dengan tingkat kekuatan keamanan yang sesuai standar.	- Dokumen kebijakan dan prosedur enkripsi yang telah disahkan pimpinan. - Bukti bahwa seluruh informasi organisasi telah dienkripsi dengan standar keamanan yang sesuai. - Laporan audit atau bukti kepatuhan terhadap kebijakan enkripsi.
4	- Organisasi sudah memiliki kebijakan internal maupun prosedur enkripsi informasi yang disahkan pimpinan, dimonitoring, dan direviu secara berkala	Organisasi telah memiliki kebijakan dan prosedur enkripsi yang disahkan pimpinan, serta dimonitor dan direviu secara berkala. Enkripsi diterapkan pada seluruh	- Laporan monitoring dan reviu penerapan enkripsi secara berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	dengan tingkat kekuatan keamanan sesuai dengan standar keamanan - Organisasi sudah menerapkan enkripsi pada seluruh informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan, dimonitoring penerapannya, dan direviu secara berkala	informasi, dengan pemantauan dan evaluasi berkala.	- Bukti pelaksanaan audit keamanan informasi yang mencakup enkripsi data.
5	- Organisasi sudah memiliki kebijakan internal maupun prosedur enkripsi informasi yang disahkan pimpinan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan sesuai dengan standar keamanan - Organisasi sudah menerapkan enkripsi pada seluruh informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan, dimonitoring penerapannya, direviu secara berkala, dan dilakukan perbaikan secara otomatis	Organisasi telah memiliki kebijakan dan prosedur enkripsi yang disahkan pimpinan, dimonitor, direviu berkala, dan diperbaiki sesuai standar keamanan. Enkripsi diterapkan pada seluruh informasi, dengan pemantauan, evaluasi, dan perbaikan otomatis untuk meningkatkan keamanan.	- Bukti implementasi perbaikan enkripsi berdasarkan hasil monitoring dan reviu. - Dokumentasi perubahan kebijakan dan prosedur enkripsi sebagai bagian dari continuous improvement. - Bukti penggunaan sistem otomatis untuk perbaikan dan peningkatan enkripsi sesuai standar keamanan terbaru.

2.3.2. Pelindungan terhadap data yang terkirim dari Penyelenggara IIV

Kriteria	Detail
Deskripsi	Pelindungan terhadap data yang terkirim dari Penyelenggara IIV menuntut penerapan langkah-langkah keamanan yang cermat untuk menjaga kerahasiaan dan integritas data selama proses transmisi. Penyelenggara IIV wajib memastikan bahwa saluran komunikasi yang digunakan untuk berinteraksi antara perangkat IIV dan server IIV dilindungi dengan enkripsi yang kuat, guna mencegah akses tidak sah selama pengiriman data. Selain itu, Penyelenggara IIV bertanggung jawab untuk memastikan bahwa kunci enkripsi yang digunakan dalam proses tersebut dikontrol dengan aman sepanjang siklus hidupnya, dari penerbitan hingga penghancuran, untuk menjaga keaslian serta keamanan pengoperasian sistem. Dengan cara ini, data yang ditransmisikan, diterima, dan disimpan akan terlindungi secara efektif dari potensi ancaman, menjaga kepercayaan dan ketahanan infrastruktur informasi vital negara.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi enkripsi dan kontrol akses yang memiliki sertifikat keamanan pada data yang dikirim, serta pengembangan kebijakan dan prosedur manajemen data yang dikirim.
Dampak	**Tinggi** – Melindungi data yang dikirim dari risiko intersepsi, perubahan, atau pengungkapan yang tidak sah, sehingga menjaga kerahasiaan dan integritas data.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem dan prosedur yang tepat untuk melindungi data yang dikirim, serta pelatihan karyawan tentang pentingnya keamanan data saat dikirim.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-02** **NIST CSF 1.1: PR.DS-2** **NIST SP 800-53r5: SC-8, SC-11** **SNI ISO/IEC 27001:2022: 5.10, 5.14, 8.20, 8.26** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

69 Kontrol 2.3.2.a:

Kontrol	Penyelenggara IIV memastikan saluran komunikasi menerapkan enkripsi saat berkomunikasi antara perangkat IIV dan server IIV.
Deskripsi Kontrol	Penyelenggaran IIV memastikan bahwa setiap komunikasi antara perangkat IIV dan server IIV dilakukan melalui saluran yang terenkripsi untuk melindungi kerahasiaan dan integritas data yang dikirimkan. Dengan menerapkan enkripsi pada saluran komunikasi, seperti menggunakan protokol keamanan yang sesuai (misalnya TLS atau VPN), risiko penyadapan, manipulasi, atau akses tidak sah terhadap data dapat diminimalkan. Langkah ini bertujuan untuk menjaga keamanan informasi yang ditransmisikan serta memastikan kepatuhan terhadap standar dan regulasi keamanan yang berlaku.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - Topologi Sistem (Termasuk jalur komunikasi dan enkripsinya) - Pemakaian enkripsi untuk jalur atar sistem kritikal
Ancaman/Risiko yang dimitigasi	TH030 TH054 TH074 TH040 TH071 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.DS-02** **NIST CSF 1.1: PR.DS-2** **NIST SP 800-53r5: SC-8, SC-11** **SNI ISO/IEC 27001:2022: 5.10, 5.14, 8.20, 8.26** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.3.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV - Organisasi belum menerapkan enkripsi pada saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki konsep kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV - Organisasi telah menerapkan enkripsi pada sebagian kecil saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV	Organisasi memiliki konsep kebijakan dan prosedur penerapan enkripsi, tetapi belum disahkan. Enkripsi baru diterapkan pada sebagian kecil saluran komunikasi antara perangkat IIV dan server IIV.	- Draft kebijakan atau prosedur enkripsi yang masih dalam tahap konsep. - Bukti penerapan enkripsi pada sebagian kecil saluran komunikasi (misalnya, hanya pada beberapa endpoint). - Log implementasi enkripsi pada sebagian kecil komunikasi antara perangkat IIV dan server IIV.
2	- Organisasi sudah memiliki konsep kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV - Organisasi telah menerapkan enkripsi pada sebagian besar saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV	Organisasi memiliki konsep kebijakan dan prosedur penerapan enkripsi, tetapi belum diformalkan. Enkripsi sudah diterapkan pada sebagian besar saluran komunikasi antara perangkat IIV dan server IIV.	- Draft kebijakan atau prosedur enkripsi yang lebih matang tetapi belum disahkan. - Bukti penerapan enkripsi pada sebagian besar saluran komunikasi antara perangkat IIV dan server IIV. - Log penerapan enkripsi pada berbagai titik komunikasi organisasi.
3	- Organisasi sudah memiliki kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV yang disahkan pimpinan - Organisasi telah menerapkan enkripsi pada seluruh saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV	Organisasi telah memiliki kebijakan dan prosedur penerapan enkripsi yang disahkan pimpinan. Enkripsi diterapkan pada seluruh saluran komunikasi antara perangkat IIV dan server IIV.	- Dokumen kebijakan dan prosedur enkripsi yang telah disahkan pimpinan. - Bukti bahwa seluruh komunikasi antara perangkat IIV dan server IIV telah dienkripsi. - Laporan audit atau bukti kepatuhan terhadap kebijakan enkripsi komunikasi.
4	- Organisasi sudah memiliki kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat	Organisasi telah memiliki kebijakan dan prosedur penerapan enkripsi yang	- Laporan monitoring dan reviu penerapan enkripsi secara berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	berkomunikasi antara perangkat IIV dan server IIV yang disahkan pimpinan, dimonitoring penerapannya, dan direviu secara berkala - Organisasi telah menerapkan enkripsi pada seluruh saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV, dimonitoring penerapannya, dan direviu secara berkala	disahkan pimpinan, serta dimonitor dan direviu secara berkala. Enkripsi diterapkan pada seluruh saluran komunikasi antara perangkat IIV dan server IIV, dengan pemantauan dan evaluasi berkala.	- Bukti pelaksanaan audit keamanan informasi yang mencakup enkripsi komunikasi.
5	- Organisasi sudah memiliki kebijakan internal maupun prosedur penerapan enkripsi saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV yang disahkan pimpinan, dimonitoring penerapannya, direviu secara berkala, dan dilakukan perbaikan. - Organisasi telah menerapkan enkripsi pada seluruh saluran komunikasi saat berkomunikasi antara perangkat IIV dan server IIV, dimonitoring penerapannya, direviu secara berkala dan dilakukan perbaikan	Organisasi telah memiliki kebijakan dan prosedur penerapan enkripsi yang disahkan pimpinan, dimonitor, direviu berkala, dan diperbaiki sesuai standar keamanan. Enkripsi diterapkan pada seluruh saluran komunikasi antara perangkat IIV dan server IIV, dengan pemantauan, evaluasi, dan perbaikan berkelanjutan.	- Bukti implementasi perbaikan enkripsi berdasarkan hasil monitoring dan reviu. - Dokumentasi perubahan kebijakan dan prosedur enkripsi sebagai bagian dari continuous improvement. - Bukti penggunaan sistem otomatis untuk perbaikan dan peningkatan enkripsi sesuai standar keamanan terbaru.

70 Kontrol 2.3.2.b:

Kontrol	Penyelenggara IIV memastikan kunci enkripsi dikontrol dengan aman sepanjang siklus hidup kunci enkripsi tersebut untuk memastikan pengoperasian yang benar dan data yang ditransmisikan, diterima, dan disimpan dengan aman.
Deskripsi Kontrol	Penyelenggara IIV memastikan bahwa kunci enkripsi dikelola dengan aman sepanjang siklus hidupnya, mulai dari pembuatan, distribusi, penyimpanan, penggunaan, hingga penghancuran, untuk mencegah akses tidak sah atau penyalahgunaan. Pengelolaan kunci yang baik mencakup penggunaan mekanisme perlindungan seperti modul keamanan perangkat keras (HSM), rotasi kunci secara berkala, serta kebijakan akses terbatas hanya bagi pihak yang berwenang. Dengan penerapan kontrol ini, proses enkripsi dan dekripsi dapat berjalan dengan benar, sehingga data yang ditransmisikan, diterima, dan disimpan tetap aman serta terjaga kerahasiaannya sesuai standar keamanan yang berlaku.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - SOP Manajemen Kunci - Daftar Kunci Enkripsi dan PIC nya - Log audit dari sistem manajemen kunci - Laporan hasil asesmen keamanan, konfigurasi sistem yang menunjukkan implementasi kontrol akses terhadap kunci enkripsi
Ancaman/Risiko yang dimitigasi	TH030 TH053 TH071 TH075 TH035 TH054 TH074
Referensi Kontrol	**NIST CSF 2.0: PR.DS-02** **NIST CSF 1.1: PR.DS-2** **NIST SP 800-53r5: SC-8, SC-11** **SNI ISO/IEC 27001:2022: 5.10, 5.14, 8.20, 8.26**

Kriteria Pemenuhan Kontrol 2.3.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Tidak ada	Tidak ada
1	Organisasi telah menyusun prosedur dan menerapkan sebagian kecil pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Organisasi telah menyusun prosedur pengamanan kunci enkripsi, tetapi belum disahkan. Penerapan pengamanan hanya mencakup sebagian kecil aspek siklus hidup kunci enkripsi.	- Draft prosedur pengamanan kunci enkripsi yang belum disahkan. - Bukti implementasi awal pada sebagian kecil sistem yang menggunakan enkripsi. - Log atau dokumentasi terbatas mengenai perlindungan kunci enkripsi.
2	Organisasi telah menyusun prosedur dan menerapkan sebagian besar pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Organisasi telah menyusun prosedur pengamanan kunci enkripsi, tetapi belum diformalkan. Penerapan pengamanan sudah mencakup sebagian besar aspek siklus hidup kunci enkripsi	- Draft prosedur yang lebih matang tetapi belum disahkan. - Bukti penerapan pengamanan kunci enkripsi pada sebagian besar sistem atau aplikasi. - Log rotasi atau penyimpanan kunci enkripsi di sebagian besar sistem.
3	Organisasi telah mengesahkan prosedur dan menerapkan secara menyeluruh pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Organisasi telah mengesahkan prosedur pengamanan kunci enkripsi dan menerapkannya secara menyeluruh sepanjang siklus hidup kunci enkripsi, mencakup pembuatan, distribusi, penyimpanan, rotasi, dan penghancuran kunci.	- Dokumen prosedur pengamanan kunci enkripsi yang telah disahkan oleh pimpinan. - Bukti implementasi penuh perlindungan kunci enkripsi dalam seluruh sistem yang menggunakan enkripsi. - Log audit terkait siklus hidup kunci enkripsi (pembuatan, rotasi, penyimpanan, penghancuran).
4	Organisasitelah mengesahkan prosedur, menerapkan secara menyeluruh, memonitoring dan mereviu secara berkala pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Organisasi telah mengesahkan prosedur, menerapkan pengamanan secara menyeluruh, serta melakukan monitoring dan reviu berkala terhadap implementasi pengamanan kunci enkripsi.	- Laporan monitoring dan hasil reviu berkala terhadap pengamanan kunci enkripsi. - Bukti kepatuhan terhadap standar keamanan terkait pengelolaan kunci enkripsi (misalnya, NIST atau ISO 27001).
5	Organisasi telah mengesahkan prosedur, menerapkan secara menyeluruh, memonitoring, mereviu secara berkala dan melakukan perbaikan mengenai pengamanan kunci enkripsi sepanjang siklus hidup kunci enkripsi	Organisasi telah mengesahkan prosedur, menerapkan pengamanan secara menyeluruh, memonitor, mereviu secara berkala, serta melakukan perbaikan dan penyesuaian berkelanjutan terhadap pengamanan kunci enkripsi sesuai standar keamanan terbaru.	- Bukti implementasi perbaikan atau peningkatan pengamanan kunci enkripsi berdasarkan hasil monitoring dan reviu. - Dokumentasi perubahan prosedur pengamanan kunci enkripsi sebagai bagian dari perbaikan berkelanjutan. - Bukti penggunaan sistem otomatis untuk manajemen kunci enkripsi yang lebih aman dan efisien.

2.3.3. Memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai

Kriteria	Detail
Deskripsi	Penyelenggara IIV bertanggung jawab untuk menyediakan sumber daya yang memadai bagi setiap sistem IIV, termasuk ruang penyimpanan, sumber daya komputasi, dan sistem redundan guna memastikan kelangsungan operasional. Selain itu, mereka juga wajib melakukan pemeriksaan kualitas ruang penyimpanan data secara berkala, mendeteksi potensi kegagalan operasional, serta memastikan pembaruan perangkat lunak pada perangkat penyimpanan data agar sistem tetap andal dan aman. Kombinasi dari kedua kontrol ini bertujuan untuk menjaga ketersediaan, integritas, dan performa sistem IIV secara optimal.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam infrastruktur penyimpanan data yang memadai dan pemeliharaan berkala.
Dampak	**Tinggi** – Dengan kapasitas penyimpanan yang memadai, organisasi dapat mengelola dan menyimpan data dengan efisien, serta mengurangi risiko kehilangan data akibat kapasitas yang tidak memadai.
Kompleksitas	**Sedang** – Memerlukan perencanaan yang tepat untuk memastikan kapasitas penyimpanan yang memadai dan pemeliharaan berkala.
Referensi Kontrol	**NIST CSF 2.0: PR.IR-04** **NIST CSF 1.1: PR.DS-4** **NIST SP 800-53r5: AU-4, CP-2, PE-11, SC-5** **SNI ISO/IEC 27001:2022: 8.13**

71 Kontrol 2.3.3.a:

Kontrol	Penyelenggara IIV menyediakan sumber daya yang cukup untuk setiap sistem IIV (misalnya ruang penyimpanan, sumber daya, dan sistem redundan).
Deskripsi Kontrol	Penyelenggara IIV menyediakan sumber daya yang memadai untuk mendukung operasional setiap sistem IIV, termasuk ruang penyimpanan yang cukup, kapasitas komputasi yang memadai, serta sistem redundan untuk memastikan ketersediaan layanan. Dengan penyediaan sumber daya yang optimal, sistem dapat beroperasi secara efisien, menghindari kegagalan akibat keterbatasan kapasitas, serta meningkatkan ketahanan terhadap gangguan atau insiden. Langkah ini juga mendukung keberlanjutan layanan dan kepatuhan terhadap standar keamanan serta kinerja yang telah ditetapkan.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - SOP Manajemen Kapasitas - Form Daftar Monitoring Kapasitas dan Proyeksinya
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH014 TH008 TH010 TH013 TH015
Referensi Kontrol	**NIST CSF 2.0: PR.IR-04** **NIST CSF 1.1: PR.DS-4** **NIST SP 800-53r5: AU-4, CP-2, PE-11, SC-5** **SNI ISO/IEC 27001:2022: 8.13**

Kriteria Pemenuhan Kontrol 2.3.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum merencanakan atau membuat strategi penyediaan sumber daya untuk setiap sistem IIV yang dimiliki. - Organisasi belum menyediakan sumber daya yang cukup untuk setiap sistem IIV.	Tidak ada	Tidak ada
1	- Organisasi telah menyusun strategi penyediaan sumber daya untuk setiap sistem IIV namun belum diformalkan. - Organisasi sudah menyediakan sumber daya yang cukup untuk sebagian kecil aspek pada sistem IIV.	Organisasi telah menyusun strategi penyediaan sumber daya, tetapi belum diformalkan. Penyediaan sumber daya hanya mencakup sebagian kecil kebutuhan sistem IIV.	- Draft strategi penyediaan sumber daya yang belum disahkan. - Bukti penyediaan sumber daya untuk sebagian kecil sistem IIV, seperti dokumentasi peningkatan kapasitas penyimpanan atau penambahan sistem redundan terbatas. - Laporan atau catatan mengenai kendala akibat keterbatasan sumber daya.
2	- Organisasi telah menyusun strategi penyediaan sumber daya untuk setiap sistem IIV namun belum diformalkan. - Organisasi sudah menyediakan sumber daya yang cukup untuk sebagian besar aspek pada sistem IIV.	Organisasi telah menyusun strategi penyediaan sumber daya, tetapi belum diformalkan. Penyediaan sumber daya telah mencakup sebagian besar kebutuhan sistem IIV.	- Draft strategi penyediaan sumber daya yang lebih lengkap tetapi belum diformalkan. - Bukti penyediaan sumber daya yang mencakup sebagian besar sistem IIV, misalnya laporan penggunaan server, storage, atau peningkatan kapasitas infrastruktur. - Dokumentasi pemantauan awal terhadap penggunaan sumber daya.
3	- Organisasi telah menyusun strategi penyediaan sumber daya untuk setiap sistem IIV yang disahkan pimpinan. - Organisasi sudah menyediakan sumber daya yang cukup untuk seluruh aspek pada sistem IIV.	Organisasi telah menyusun strategi penyediaan sumber daya yang disahkan oleh pimpinan. Penyediaan sumber daya telah mencakup seluruh aspek yang dibutuhkan oleh sistem IIV.	- Dokumen strategi penyediaan sumber daya yang telah disahkan oleh pimpinan. - Bukti bahwa seluruh aspek sistem IIV telah mendapatkan sumber daya yang cukup, seperti data kapasitas penyimpanan, sumber daya server, dan mekanisme failover yang diterapkan. - Laporan audit internal terkait pemenuhan kebutuhan sumber daya.
4	- Organisasi telah menyusun strategi penyediaan sumber daya untuk setiap sistem IIV yang disahkan pimpinan, dimonitoring, dan direviu secara berkala.	Organisasi telah menyusun strategi penyediaan sumber daya yang disahkan oleh pimpinan dan dilakukan monitoring serta reviu berkala terhadap	- Laporan monitoring dan hasil reviu berkala terhadap penggunaan sumber daya sistem IIV.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Organisasi sudah menyediakan sumber daya yang cukup untuk seluruh aspek pada sistem IIV, dimonitoring dan direviu penerapannya secara berkala.	penerapannya. Penyediaan sumber daya mencakup seluruh aspek sistem IIV dengan mekanisme pemantauan dan evaluasi yang berjalan.	- Dokumen evaluasi kinerja sistem berdasarkan penyediaan sumber daya. - Bukti kepatuhan terhadap standar atau best practices dalam pengelolaan infrastruktur IT.
5	- Organisasi telah menyusun strategi penyediaan sumber daya untuk setiap sistem IIV yang disahkan pimpinan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan. - Organisasi sudah menyediakan sumber daya yang cukup untuk seluruh aspek pada sistem IIV, dimonitoring, direviu penerapannya secara berkala dan dilakukan perbaikan	Organisasi telah menyusun strategi penyediaan sumber daya yang disahkan oleh pimpinan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan berkelanjutan. Penyediaan sumber daya telah mencakup seluruh aspek sistem IIV, dengan adanya perbaikan yang terus dilakukan berdasarkan hasil monitoring dan evaluasi.	- Bukti adanya perbaikan atau peningkatan strategi penyediaan sumber daya berdasarkan hasil monitoring dan evaluasi. - Dokumentasi perubahan dan optimalisasi infrastruktur, seperti peningkatan kapasitas penyimpanan, implementasi cloud computing, atau sistem redundansi yang lebih canggih. - Bukti implementasi teknologi otomatisasi dalam pengelolaan sumber daya.

72 Kontrol 2.3.3.b:

Kontrol	Penyelenggara IIV memastikan dilakukannya pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.
Deskripsi Kontrol	Penyelenggara IIV memastikan bahwa kualitas ruang penyimpanan data selalu terjaga melalui pemeriksaan berkala, deteksi dini terhadap kegagalan operasional, dan pembaruan perangkat lunak pada perangkat penyimpanan. Dengan pemeriksaan rutin, potensi masalah seperti degradasi penyimpanan atau kapasitas yang hampir penuh dapat diidentifikasi dan ditangani sebelum berdampak pada operasional. Pendeteksian kegagalan operasional memungkinkan tindakan cepat untuk mencegah kehilangan atau kerusakan data, sementara pembaruan perangkat lunak memastikan sistem penyimpanan tetap aman, stabil, dan sesuai dengan standar terkini. Hal ini bertujuan untuk menjaga ketersediaan, integritas, dan keamanan data dalam sistem IIV.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan keamanan siber yang telah di-sahkan oleh pimpinan organisasi dan komitmen pimpinan berupa penetapan keamanan siber sebagai kegiatan prioritas di organisasinya, contohnya: - SOP Manajemen Kapasitas - Form Daftar Monitoring Kapasitas dan Proyeksinya - Log dan notifikasi batasan kapasitas
Ancaman/Risiko yang dimitigasi	TH006 TH009 TH011 TH015 TH007 TH010 TH014
Referensi Kontrol	**NIST CSF 2.0: PR.IR-04** **NIST CSF 1.1: PR.DS-4** **NIST SP 800-53r5: AU-4, CP-2, PE-11, SC-5** **SNI ISO/IEC 27001:2022: 8.13**

Kriteria Pemenuhan Kontrol 2.3.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki dan menerapkan prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.	Tidak ada	Tidak ada
1	Organisasi telah menyusun dan menerapkan sebagian kecil aspek prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data pada sebagian aspek.	Organisasi telah menyusun prosedur pemeriksaan kualitas ruang penyimpanan data, deteksi kegagalan operasional, dan pembaruan perangkat lunak, tetapi baru diterapkan pada sebagian kecil aspek penyimpanan data.	- Draft prosedur pemeriksaan kualitas ruang penyimpanan data yang belum lengkap atau belum diformalkan. - Dokumentasi awal atau catatan insidental terkait pemantauan ruang penyimpanan data. - Bukti penerapan sistem deteksi kegagalan operasional pada sebagian kecil perangkat penyimpanan. - Bukti pembaruan perangkat lunak yang masih terbatas pada sebagian perangkat penyimpanan data.
2	Organisasi telah menyusun dan menerapkan sebagian besar aspek prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.	Organisasi telah menyusun prosedur yang lebih komprehensif dan telah menerapkan sebagian besar aspek pemeriksaan kualitas ruang penyimpanan data, pendeteksi kegagalan operasional, serta pembaruan perangkat lunak untuk perangkat penyimpanan data.	- Prosedur pemeriksaan kualitas ruang penyimpanan data yang lebih komprehensif tetapi belum sepenuhnya diformalkan. - Bukti implementasi sistem deteksi kegagalan operasional yang mencakup sebagian besar perangkat penyimpanan. - Catatan pembaruan perangkat lunak untuk sebagian besar perangkat penyimpanan data. - Laporan awal terkait efektivitas pemantauan kualitas penyimpanan data. -
3	Organisasi telah mengesahkan dan menerapkan seluruh aspek prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.	Organisasi telah mengesahkan prosedur yang mencakup seluruh aspek pemeriksaan kualitas ruang penyimpanan data, pendeteksi kegagalan operasional, dan pembaruan perangkat lunak, serta	- Dokumen prosedur pemeriksaan kualitas ruang penyimpanan data, pendeteksi kegagalan operasional, dan pembaruan perangkat lunak yang telah disahkan oleh pimpinan. - Bukti penerapan sistem monitoring kualitas ruang penyimpanan data secara menyeluruh.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		telah menerapkannya secara menyeluruh.	- Bukti bahwa seluruh perangkat penyimpanan telah memiliki mekanisme pendeteksi kegagalan operasional. - Laporan audit atau asesmen internal terkait implementasi pembaruan perangkat lunak untuk semua perangkat penyimpanan. -
4	Organisasi telah mengesahkan dan menerapkan seluruh aspek prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data, dimonitoring, dan direviu secara berkala.	Organisasi telah mengesahkan dan menerapkan seluruh aspek prosedur pemeriksaan kualitas ruang penyimpanan data, pendeteksi kegagalan operasional, serta pembaruan perangkat lunak, dengan mekanisme monitoring dan reviu yang dilakukan secara berkala.	- Laporan hasil monitoring dan reviu berkala terhadap kualitas ruang penyimpanan data. - Catatan evaluasi efektivitas sistem pendeteksi kegagalan operasional dan pembaruan perangkat lunak. - Bukti kepatuhan terhadap standar keamanan dan keandalan sistem penyimpanan data.
5	Organisasi telah mengesahkan dan menerapkan seluruh aspek prosedur pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data, dimonitoring, direviu secara berkala dan dilakukan perbaikan.	Organisasi telah mengesahkan dan menerapkan seluruh aspek prosedur, serta melakukan monitoring dan reviu berkala dengan tindak lanjut berupa perbaikan berkelanjutan dalam pengelolaan ruang penyimpanan data, deteksi kegagalan operasional, dan pembaruan perangkat lunak.	- Bukti adanya perbaikan atau optimalisasi ruang penyimpanan data berdasarkan hasil reviu berkala. - Dokumentasi perubahan atau peningkatan dalam sistem deteksi kegagalan operasional. - Bukti pembaruan perangkat lunak yang berkelanjutan berdasarkan hasil evaluasi dan perkembangan teknologi. - Catatan perbaikan dan tindakan mitigasi dari hasil audit atau insiden terkait penyimpanan data.

2.3.4. Mengimplementasikan pelindungan dari kebocoran data

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus mengimplementasikan pelindungan dari kebocoran data
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pelindungan kebocoran data (Data Loss Prevention/DLP) dan pengembangan kebijakan serta prosedur pelindungan data.
Dampak	**Tinggi** – Melindungi data sensitif dari risiko kebocoran, sehingga menjaga kerahasiaan dan integritas data yang penting bagi operasional organisasi.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem dan prosedur yang tepat untuk melindungi data dari kebocoran, serta pelatihan karyawan tentang pentingnya pelindungan data.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.DS-02, PR.DS-10** **NIST CSF 1.1: PR.DS-5** **NIST SP 800-53r5: AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4** **SNI ISO/IEC 27001:2022: 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 8.2, 8.3, 8.4, 8.17, 8.22, 8.26**

73 Kontrol 2.3.4.a:

Kontrol	Saat menangani informasi yang akan dilindungi atau pengadaan perangkat yang memiliki fungsi penting bagi organisasi, pilih perangkat dan server yang dilengkapi dengan perangkat anti-tampering.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa perangkat yang digunakan untuk menangani informasi yang perlu dilindungi atau perangkat yang memiliki fungsi penting dilengkapi dengan teknologi anti-tampering. Teknologi anti-tampering dirancang untuk mencegah upaya perusakan atau manipulasi fisik terhadap perangkat yang dapat membahayakan integritas informasi atau data yang disimpan. Tujuan dari pernyataan ini adalah untuk memastikan bahwa perangkat yang digunakan memiliki lapisan perlindungan fisik yang mencegah modifikasi tidak sah, serta menjaga keamanan operasional perangkat yang penting bagi organisasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa daftar perangkat dan server yang dilengkapi dengan fitur anti-tampering, laporan uji coba atau evaluasi perangkat anti-tampering, Kebijakan dan prosedur pemilihan perangkat yang aman dan tahan terhadap manipulasi, dan/atau kontrak pembelian atau pengadaan perangkat dengan spesifikasi keamanan terkait.
Ancaman/Risiko yang dimitigasi	TH004 TH006 TH031 TH035 TH054 TH005 TH013 TH032 TH053 TH075
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.DS-02, PR.DS-10** **NIST CSF 1.1: PR.DS-5** **NIST SP 800-53r5: AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4** **SNI ISO/IEC 27001:2022: 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 8.2, 8.3, 8.4, 8.17, 8.22, 8.26**

Kriteria Pemenuhan Kontrol 2.3.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur pengadaan untuk pemilihan pernagkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi belum menerapkan pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	Tidak ada prosedur tertentu dalam pengadaan perangkat.	Tidak ada dokumen atau bukti
1	- Organisasi sudah menyusun prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi telah menerapkan sebagian kecil pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	- Prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait. - Sebagian kecil prosedur telah diterapkan.	- Dokumen prosedur resmi yang disetujui, seperti kebijakan atau SOP. - Kontrak dengan penyedia layanan.
2	- Organisasi sudah menyusun prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi telah menerapkan sebagian besar pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	- Prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait. - Sebagian besar prosedur telah diterapkan.	- Dokumen prosedur resmi yang disetujui, seperti kebijakan atau SOP. - Kontrak dengan penyedia layanan.
3	- Organisasi sudah mengesahkan prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi telah menerapkan seluruh pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	- Prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait. - Seluruh prosedur telah diterapkan.	- Dokumen prosedur resmi yang disetujui, seperti kebijakan atau SOP. - Kontrak dengan penyedia layanan.
4	- Organisasi sudah mengesahkan prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering, dimonitoring dan direviu secara berkala. - Organisasi telah menerapkan seluruh pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering, dimonitoring dan direviu secara berkala.	- Prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait. - Selain diterapkan, prosedur pengadaan juga dimonitor secara rutin dan di-reviu berkala untuk mengevaluasi efektivitasnya.	- Dokumen prosedur resmi yang disetujui, seperti kebijakan atau SOP. - Kontrak dengan penyedia layanan dan laporan monitoring, catatan reviu, dan dokumen evaluasi yang menunjukkan proses monitoring dan reviu berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	- Organisasi sudah mengesahkan prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering, dimonitoring, direviu secara berkala, dan dilakukan perbaikan. - Organisasi telah menerapkan seluruh pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering, dimonitoring dan direviu secara berkala, dan dilakukan perbaikan.	- Prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait. - Selain diterapkan, prosedur pengadaan juga dimonitor secara rutin, di-reviu berkala untuk mengevaluasi efektivitasnya dan dilakukan perbaikan secara berkelanjutan.	- Dokumen prosedur resmi yang disetujui, seperti kebijakan atau SOP. - Kontrak dengan penyedia layanan dan laporan monitoring, catatan reviu, dan dokumen evaluasi yang menunjukkan proses monitoring, reviu, dan perbaikan berkala.

74 Kontrol 2.3.4.b:

Kontrol	Memastikan bahwa jalur komunikasi yang digunakan untuk mengirim informasi telah dilindungi dengan kontrol keamanan yang tepat.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa jalur komunikasi yang digunakan untuk mengirim informasi telah dilindungi dengan kontrol keamanan yang tepat.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumentasi kebijakan dan prosedur pengamanan jalur komunikasi. - Laporan implementasi enkripsi dan protokol aman (misalnya: penggunaan HTTPS, VPN, atau TLS). - Audit atau pemeriksaan keamanan terkait jalur komunikasi yang digunakan. - Bukti uji keamanan jalur komunikasi, seperti uji penetrasi atau vulnerability scanning.
Ancaman/Risiko yang dimitigasi	TH030 TH040 TH071 TH075 TH035 TH054 TH074
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.DS-02, PR.DS-10** **NIST CSF 1.1: PR.DS-5** **NIST SP 800-53r5: AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4** **SNI ISO/IEC 27001:2022: 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 8.2, 8.3, 8.4, 8.17, 8.22, 8.26**

Kriteria Pemenuhan Kontrol 2.3.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki dan menerapkan prosedur melindungi jalur komunikasi dengan kontrol keamanan yang tepat.	Tidak ada kebijakan, prosedur, atau implementasi pengamanan jalur komunikasi.	Tidak ada dokumen kebijakan atau prosedur, tidak ditemukan bukti implementasi kontrol keamanan komunikasi.
1	- Organisasi telah menyusun dan menerapkan sebagian kecil prosedur melindungi jalur komunikasi dengan kontrol keamanan yang tepat.	Baru sebagian unit atau sistem saja yang menggunakan jalur komunikasi aman.	Draf prosedur awal, konfigurasi terbatas pada beberapa sistem komunikasi, catatan implementasi sebagian VPN/enkripsi.
2	- Organisasi sudah menyusun prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi telah menerapkan sebagian besar pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	Sebagian besar jalur komunikasi telah diamankan, namun belum mencakup semuanya.	Dokumen prosedur mencakup sebagian besar sistem, log penggunaan TLS/VPN di beberapa divisi, pelatihan sebagian personel.
3	- Organisasi telah menyusun dan menerapkan sebagian besar prosedur melindungi jalur komunikasi dengan kontrol keamanan yang tepat.	Semua jalur komunikasi telah dilindungi sesuai prosedur yang telah disahkan.	Prosedur pengamanan telah disahkan manajemen, dokumentasi lengkap, seluruh komunikasi internal dan eksternal diamankan (misalnya dengan TLS, VPN, firewall).
4	- Organisasi telah mengesahkan dan menerapkan seluruh prosedur melindungi jalur komunikasi dengan kontrol keamanan yang tepat, dimonitoring dan direviu secara berkala.	Sistem pengamanan menyeluruh dan ada pemantauan serta evaluasi rutin.	Seluruh bukti pada Indeks 3 ditambah laporan monitoring berkala, hasil audit, log sistem keamanan, catatan reviu berkala, serta rencana perbaikan.
5	- Organisasi telah mengesahkan dan menerapkan seluruh prosedur melindungi jalur komunikasi dengan kontrol keamanan yang tepat, dimonitoring dan direviu secara berkala serta dilakukan perbaikan.	Sistem pengamanan menyeluruh dan ada pemantauan serta evaluasi rutin disertai upaya perbaikan berkelanjutan.	Seluruh bukti pada Indeks 4 ditambah bukti perbaikan

2.3.5. Mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pengecekan integritas dan pengembangan prosedur verifikasi.
Dampak	**Tinggi** – Dengan mekanisme pengecekan integritas yang efektif, organisasi dapat mendeteksi dan mengatasi perubahan tidak sah pada perangkat lunak, perangkat keras, dan data, sehingga menjaga integritas sistem dan data.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem dan prosedur yang tepat untuk pengecekan integritas, serta pelatihan karyawan tentang pentingnya verifikasi integritas.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, DE.CM-09, ID.RA-09** **NIST CSF 1.1: PR.DS-6, PR.DS-8** **NIST SP 800-53r5: SI-7, SI-10, SA-10** **SNI ISO/IEC 27001:2022: 7.13, 8.7, 8.19, 8.26**

75 Kontrol 2.3.5.a:

Kontrol	Melakukan pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan oleh organisasi, untuk mencegah pemasangan perangkat lunak yang tidak sah.
Deskripsi Kontrol	Penyelenggara IIV harus melakukan pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server secara berkala untuk memastikan bahwa hanya perangkat lunak yang sah yang diizinkan untuk berjalan pada sistem organisasi. Pemeriksaan ini bertujuan untuk mendeteksi perangkat lunak yang tidak sah atau modifikasi perangkat lunak yang dapat membahayakan sistem atau data. Hal ini juga penting untuk mencegah ancaman yang mungkin timbul dari perangkat lunak berbahaya, seperti malware atau aplikasi yang tidak terdaftar yang dapat mengeksploitasi celah keamanan. Pemeriksaan integritas perangkat lunak ini harus dilakukan sesuai dengan jadwal yang ditentukan oleh kebijakan keamanan organisasi.
Deskripsi Bukti Dukung	Untuk memastikan tidak terpasangnya perangkat lunak tidak sah di perangkat dan server, organisasi harus melakukan pemeriksaan integritas perangkat lunak secara terjadwal. Bukti dukung dapat berupa kebijakan dan prosedur pemeriksaan integritas yang disahkan, dokumentasi konfigurasi tools seperti antivirus, EDR (Endpoint Detection and Response), atau SIEM yang digunakan untuk memantau software, hasil laporan audit sistem, log hasil pemeriksaan berkala, serta bukti tindak lanjut atau perbaikan terhadap temuan. Reviu berkala dan catatan perubahan konfigurasi juga memperkuat bahwa kontrol dijalankan secara berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH025 TH053 TH071 TH073 TH075 TH052 TH054 TH072 TH074
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, DE.CM-09** **NIST CSF 1.1: PR.DS-6** **NIST SP 800-53r5: SI-7, SI-10** **SNI ISO/IEC 27001:2022: 8.7, 8.19, 8.26**

Kriteria Pemenuhan Kontrol 2.3.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki dan menerapkan prosedur pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan organisasi.	Tidak ada kebijakan/prosedur, belum ada aktivitas pemeriksaan integritas software sama sekali.	Tidak tersedia dokumen kebijakan/prosedur, tidak ditemukan tool atau aktivitas pemeriksaan integritas software.
1	Organisasi telah menyusun dan menerapkan sebagian kecil prosedur pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan organisasi.	Hanya sebagian kecil sistem atau perangkat yang dilakukan pemeriksaan integritas.	Draft prosedur, catatan uji coba pemeriksaan di perangkat tertentu, penggunaan alat dasar (misal antivirus bawaan) di sebagian perangkat.
2	- Organisasi sudah menyusun prosedur pengadaan untuk pemilihan perangkat dan server yang dilengkapi dengan perangkat anti-tampering. - Organisasi telah menerapkan sebagian besar pemilihan pengadaan perangkat dan server dengan perangkat anti-tampering.	Pemeriksaan dilakukan pada sebagian besar sistem, namun belum mencakup keseluruhan perangkat.	Prosedur sebagian besar telah disusun dan dijalankan, laporan hasil pemeriksaan pada sebagian besar server, penggunaan tools EDR/SIEM terbatas.
3	Organisasi telah menyusun dan menerapkan sebagian besar prosedur pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan organisasi.	Semua perangkat dan server telah tercakup dalam prosedur yang telah disahkan dan dijalankan.	Dokumen kebijakan dan prosedur lengkap dan disahkan, daftar perangkat dan server yang diperiksa, hasil pemeriksaan, konfigurasi sistem keamanan.
4	Organisasi telah mengesahkan dan menerapkan seluruh prosedur pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan organisasi, dimonitring dan direviu secara berkala.	Ada log monitoring dan laporan hasil reviu rutin terkait pemeriksaan integritas.	Ditambah laporan monitoring berkala, hasil audit integritas sistem, log hasil pemeriksaan otomatis, catatan evaluasi berkala, dan bukti reviu formal.
5	Organisasi telah mengesahkan dan menerapkan seluruh prosedur pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan organisasi, dimonitring dan direviu secara berkala serta dilakukan perbaikan	Ditemukan evidence perbaikan nyata atas temuan dari proses monitoring dan reviu sebelumnya.	Ditambah bukti tindakan korektif atau mitigasi atas temuan integritas (misal uninstall software ilegal, patching sistem), serta rencana peningkatan sistem keamanan.

76 Kontrol 2.3.5.b:

Kontrol	Melakukan pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan.
Deskripsi Kontrol	Penyelenggara IIV perlu melakukan pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan untuk memastikan bahwa informasi tersebut tidak mengalami perubahan yang tidak sah selama proses pengiriman atau penyimpanan. Pemeriksaan ini bertujuan untuk mencegah terjadinya pengubahan data, kerusakan informasi, atau manipulasi yang dapat merugikan organisasi. Integritas informasi juga harus dijaga selama proses penyimpanan, baik di server maupun dalam salinan cadangan, dengan menggunakan teknik seperti hashing atau tanda tangan digital untuk memverifikasi keaslian dan konsistensi data. Proses ini penting untuk menjaga kepercayaan dalam komunikasi dan pengelolaan data, serta mencegah potensi ancaman yang dapat mengganggu kerahasiaan atau keandalan data.
Deskripsi Bukti Dukung	Untuk memastikan tidak terpasangnya perangkat lunak tidak sah di perangkat dan server, organisasi harus melakukan pemeriksaan integritas perangkat lunak secara terjadwal. Bukti dukung dapat berupa kebijakan dan prosedur pemeriksaan integritas yang disahkan, dokumentasi konfigurasi tools seperti antivirus, EDR (Endpoint Detection and Response), atau SIEM yang digunakan untuk memantau software, hasil laporan audit sistem, log hasil pemeriksaan berkala, serta bukti tindak lanjut atau perbaikan terhadap temuan. Reviu berkala dan catatan perubahan konfigurasi juga memperkuat bahwa kontrol dijalankan secara berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH035 TH071 TH073 TH075 TH040 TH072 TH074
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, DE.CM-09** **NIST CSF 1.1: PR.DS-6** **NIST SP 800-53r5: SI-7, SI-10** **SNI ISO/IEC 27001:2022: 8.7, 8.19, 8.26**

Kriteria Pemenuhan Kontrol 2.3.5.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki mekanisme dan menerapkan pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan.	Tidak ada kebijakan/prosedur, belum ada aktivitas pemeriksaan integritas software sama sekali.	Tidak tersedia dokumen kebijakan/prosedur, tidak ditemukan tool atau aktivitas pemeriksaan integritas software.
1	Organisasi telah menyusun mekanisme dan menerapkan sebagian kecil pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan.	Hanya sebagian kecil sistem atau perangkat yang dilakukan pemeriksaan integritas.	Draft prosedur, catatan uji coba pemeriksaan di perangkat tertentu, penggunaan alat dasar (misal antivirus bawaan) di sebagian perangkat.
2	Organisasi telah menyusun dan menerapkan sebagian besar mekanisme pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan	Pemeriksaan dilakukan pada sebagian besar sistem, namun belum mencakup keseluruhan perangkat.	Prosedur sebagian besar telah disusun dan dijalankan, laporan hasil pemeriksaan pada sebagian besar server, penggunaan tools EDR/SIEM terbatas.
3	Organisasi mengesahkan dan menerapkan secara menyeluruh mekanisme pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan	Semua perangkat dan server telah tercakup dalam prosedur yang telah disahkan dan dijalankan.	Dokumen kebijakan dan prosedur lengkap dan disahkan, daftar perangkat dan server yang diperiksa, hasil pemeriksaan, konfigurasi sistem keamanan.
4	Organisasi telah mengesahkan, menerapkan secara menyeluruh, memonitoring dan mereviu secara berkala mekanisme pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan	Ada log monitoring dan laporan hasil reviu rutin terkait pemeriksaan integritas.	Ditambah laporan monitoring berkala, hasil audit integritas sistem, log hasil pemeriksaan otomatis, catatan evaluasi berkala, dan bukti reviu formal.
5	Organisasi telah mengesahkan, menerapkan secara menyeluruh, memonitoring dan mereviu secara berkala serta melakukan perbaikan mekanisme pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan	Ditemukan evidence perbaikan nyata atas temuan dari proses monitoring dan reviu sebelumnya.	Ditambah bukti tindakan korektif atau mitigasi atas temuan integritas (misal uninstall software ilegal, patching sistem), serta rencana peningkatan sistem keamanan.

77 Kontrol 2.3.5.c:

Kontrol	Memperkenalkan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras.
Deskripsi Kontrol	Penyelenggara IIV perlu memperkenalkan mekanisme pemeriksaan integritas untuk memverifikasi bahwa perangkat keras yang digunakan dalam organisasi tidak dimodifikasi atau dirusak. Pemeriksaan integritas perangkat keras dapat dilakukan melalui penggunaan teknologi seperti checksum, tanda tangan digital, atau sistem pengawasan berbasis perangkat keras (hardware-based monitoring). Tujuan dari kontrol ini adalah untuk memastikan bahwa perangkat keras yang digunakan tetap dalam kondisi asli dan tidak terpengaruh oleh perubahan atau kerusakan yang dapat merusak fungsionalitas atau keamanan sistem.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencakup dokumentasi kebijakan dan prosedur resmi terkait pemeriksaan integritas perangkat keras, catatan sosialisasi kepada stakeholder, laporan pelaksanaan monitoring dan reviu, serta bukti perbaikan berkelanjutan. Bukti juga dapat mencakup hasil audit, notulen rapat pengesahan, pelatihan internal, dan dokumen evaluasi efektivitas mekanisme tersebut. Setiap tingkat indeks membutuhkan bukti yang lebih komprehensif dan menyeluruh untuk menunjukkan tingkat adopsi dan pematangan kontrol.
Ancaman/Risiko yang dimitigasi	TH006 TH023 TH032 TH073 TH013 TH031 TH072 TH075
Referensi Kontrol	**NIST CSF 2.0: DE.CM-09, ID.RA-09** **NIST CSF 1.1: PR.DS-8** **NIST SP 800-53r5: SA-10** **SNI ISO/IEC 27001:2022: 7.13**

Kriteria Pemenuhan Kontrol 2.3.5.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memperkenalkan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras.	Tidak ada mekanisme pemeriksaan integritas perangkat keras yang disusun atau diperkenalkan.	Tidak ada dokumentasi terkait mekanisme pemeriksaan integritas perangkat keras.
1	Organisasi telah menyusun mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras dan memperkenalkan pada sebagian kecil stakeholder.	Mekanisme telah disusun, tetapi baru diperkenalkan ke sebagian kecil stakeholder (contoh: satu unit/divisi).	- Draf mekanisme pemeriksaan integritas perangkat keras - Bukti distribusi/sosialisasi kepada sebagian kecil stakeholder (email, notulen rapat, dll)
2	Organisasi telah menyusun mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras dan memperkenalkan kepada sebagian besar stakeholder	Mekanisme telah disusun dan diperkenalkan ke sebagian besar stakeholder (misalnya lintas beberapa divisi/departemen).	- Dokumen mekanisme lengkap - Daftar stakeholder yang telah menerima sosialisasi - Materi presentasi/sosialisasi yang digunakan
3	Organisasi telah mengesahkan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras dan memperkenalkan kepada seluruh stakeholder	Mekanisme telah mendapatkan pengesahan resmi (misalnya melalui SK/keputusan manajemen) dan diperkenalkan ke seluruh stakeholder organisasi.	- Surat Keputusan atau dokumen pengesahan mekanisme - Daftar kehadiran atau bukti komunikasi internal ke seluruh stakeholder
4	Organisasi telah mengesahkan, memonitoring dan mereviu secara berkala mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras dan memperkenalkan kepada seluruh stakeholder	Mekanisme telah disahkan dan dilengkapi proses monitoring dan reviu berkala untuk menjamin efektivitasnya, serta diperkenalkan secara menyeluruh.	- Laporan monitoring dan hasil reviu berkala - Jadwal rutin evaluasi - Notulen rapat tinjauan berkala
5	Organisasi telah mengesahkan, memonitoring, mereviu secara berkala dan melakukan perbaikan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras dan memperkenalkan kepada seluruh stakeholder	Selain disahkan dan dimonitoring, organisasi juga melakukan perbaikan berkelanjutan berdasarkan hasil reviu, serta disosialisasikan ke semua pihak.	- Dokumen perbaikan/pembaruan mekanisme berbasis hasil reviu - Rencana aksi tindak lanjut - Bukti komunikasi perubahan ke seluruh stakeholder

78 Kontrol 2.3.5.d:

Kontrol	Konfirmasikan bahwa perangkat keras dan perangkat lunak adalah produk asli dan memiliki sertifikat keamanan.
Deskripsi Kontrol	Penyelenggara IIV perlu mengkonfirmasi bahwa perangkat keras dan perangkat lunak yang digunakan adalah produk asli dan dilengkapi dengan sertifikat keamanan yang valid. Verifikasi ini bertujuan untuk memastikan bahwa perangkat keras dan perangkat lunak tidak hanya asli dan tidak dimodifikasi, tetapi juga telah disertifikasi aman oleh badan yang berwenang, sesuai dengan standar industri dan regulasi yang berlaku. Tujuan dari kontrol ini adalah untuk mencegah penggunaan perangkat atau perangkat lunak yang dapat membahayakan keamanan, seperti perangkat palsu atau perangkat lunak yang rentan terhadap serangan.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencakup : 1. Dokumen sertifikat keamanan perangkat atau Surat keterangan Verifikasi dan/ atau Rekognisi 2. Dokumentasi kebijakan dan prosedur resmi terkait pemeriksaan integritas perangkat keras, catatan sosialisasi kepada stakeholder, laporan pelaksanaan monitoring dan reviu, serta bukti perbaikan berkelanjutan. 3. Bukti juga dapat mencakup hasil audit, notulen rapat pengesahan, pelatihan internal, dan dokumen evaluasi efektivitas mekanisme tersebut. Setiap tingkat indeks membutuhkan bukti yang lebih komprehensif dan menyeluruh untuk menunjukkan tingkat adopsi dan kematangan kontrol.
Ancaman/Risiko yang dimitigasi	TH013 TH025 TH053 TH071 TH073 TH023 TH052 TH054 TH072 TH075
Referensi Kontrol	**NIST CSF 2.0: DE.CM-09, ID.RA-09** **NIST CSF 1.1: PR.DS-8** **NIST SP 800-53r5: SA-10** **SNI ISO/IEC 27001:2022: 7.13** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.3.5.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak.	Tidak ada dokumen atau kebijakan yang menjelaskan verifikasi keaslian & keamanan perangkat.	- Tidak ada dokumen prosedur - Tidak ada catatan verifikasi perangkat - Tidak ada sertifikat keamanan.
1	Organisasi telah menyusun prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak kepada sebagian kecil stakeholder.	Terdapat draft prosedur & bukti pelaksanaan pada unit atau proyek terbatas.	- Draft prosedur verifikasi keaslian & keamanan perangkat - Bukti implementasi pada 1–2 unit kerja
2	Organisasi telah menyusun prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak kepada sebagian besar stakeholder	Prosedur mulai dijalankan di banyak unit, meski belum menyeluruh. Bukti implementasi meningkat.	- Prosedur terdokumentasi - Bukti pelaksanaan di sebagian besar unit (misal: 60–70%) - Data hasil verifikasi terbatas
3	Organisasi telah mengesahkan prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak kepada seluruh stakeholder	Prosedur formal tersedia, disahkan oleh manajemen, dan diterapkan di seluruh organisasi.	- Prosedur disahkan oleh manajemen - Bukti pelaksanaan di seluruh unit - Daftar perangkat keras/lunak dengan bukti keaslian dan sertifikat
4	Organisasi telah mengesahkan prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak kepada seluruh stakeholder, monitoring dan direviu secara berkala	Terdapat jadwal monitoring & laporan reviu berkala terkait keaslian & sertifikasi perangkat.	- Semua bukti indeks 3 - Jadwal monitoring berkala - Laporan hasil monitoring dan reviu periodik
5	Organisasi telah mengesahkan prosedur dan mengonfirmasikan keaslian dan kepemilikan sertifikat keamanan pada perangkat keras dan perangkat lunak kepada seluruh stakeholder, dimonitoring, direviu secara berkala dan dilakukan perbaikan	Ditemukan bukti tindakan perbaikan (corrective action) berdasarkan hasil reviu & monitoring.	- Semua bukti indeks 4 - Dokumen tindakan perbaikan dari hasil reviu - Bukti audit internal/eksternal terhadap pelaksanaan kontrol

79 Kontrol 2.3.5.e:

Kontrol	Pelihara, perbarui, dan kelola informasi seperti asal data, dan riwayat pemrosesan data, di seluruh siklus hidup data.
Deskripsi Kontrol	Penyelenggara IIV perlu memelihara, memperbarui, dan mengelola informasi terkait asal data dan riwayat pemrosesan data sepanjang siklus hidup data. Hal ini mencakup pencatatan informasi tentang sumber data, cara data diperoleh, bagaimana data diproses, serta perubahan yang terjadi pada data selama siklus hidupnya. Tujuan dari kontrol ini adalah untuk memastikan bahwa data yang digunakan dalam organisasi dapat dilacak, diperiksa, dan diverifikasi asal-usulnya serta keabsahannya. Ini penting untuk menjaga integritas data, menghindari kebocoran data, dan memenuhi persyaratan kepatuhan hukum dan regulasi
Deskripsi Bukti Dukung	Untuk mendukung kontrol terkait pemeliharaan, pembaruan, dan pengelolaan informasi seperti asal data dan riwayat pemrosesan di seluruh siklus hidup data, organisasi perlu menyediakan bukti berupa kebijakan, prosedur operasional, serta dokumentasi penerapan yang menunjukkan bahwa informasi dikelola secara sistematis dan terdokumentasi. Bukti dukung juga dapat berupa catatan audit, hasil pemantauan berkala, serta hasil evaluasi dan perbaikan berkelanjutan yang mencerminkan kedewasaan proses manajemen data dari perencanaan hingga perbaikan berkelanjutan.
Ancaman/Risiko yang dimitigasi	TH035 TH053 TH071 TH073 TH075 TH052 TH054 TH072 TH074
Referensi Kontrol	**NIST CSF 2.0: DE.CM-09, ID.RA-09** **NIST CSF 1.1: PR.DS-8** **NIST SP 800-53r5: SA-10** **SNI ISO/IEC 27001:2022: 7.13**

Kriteria Pemenuhan Kontrol 2.3.5.e Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki dan menerapkan prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data.	Tidak ada kebijakan atau prosedur yang ditetapkan atau diterapkan terkait pemeliharaan, pembaruan, dan pengelolaan informasi data.	Tidak ada dokumen kebijakan/prosedur; tidak ada bukti pelaksanaan kegiatan pemeliharaan atau pengelolaan data.
1	Organisasi telah merancang dan menerapkan sebagian kecil prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data.	Terdapat sebagian kecil prosedur yang dirancang dan diterapkan, namun belum menyeluruh atau terbatas pada area tertentu.	Draf awal prosedur terbatas (misalnya hanya untuk sebagian data atau sistem); dokumentasi terbatas penerapan pada beberapa unit atau proyek.
2	Organisasi telah merancang dan menerapkan sebagian besar prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data	Mayoritas prosedur sudah dirancang dan diterapkan, namun belum sepenuhnya menyeluruh atau belum disahkan formal.	Dokumen prosedur lebih lengkap namun belum mencakup seluruh siklus hidup data; catatan penerapan di sebagian besar unit; belum ada pengesahan formal.
3	Organisasi telah mengesahkan dan menerapkan secara menyeluruh prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data	Semua prosedur telah dirancang, disahkan secara formal, dan diterapkan secara menyeluruh di seluruh organisasi.	Prosedur lengkap dan sudah disahkan secara formal; bukti penerapan menyeluruh di seluruh unit; catatan aktivitas pemeliharaan dan pembaruan tersedia.
4	Organisasi telah mengesahkan, menerapkan secara menyeluruh, memonitoring dan mereviu secara berkala prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data	Prosedur telah disahkan, diterapkan secara menyeluruh, dan dilakukan monitoring serta reviu berkala untuk efektivitasnya.	Terdapat bukti monitoring (log aktivitas, laporan audit internal); jadwal reviu rutin; dokumentasi hasil evaluasi berkala.
5	Organisasi telah mengesahkan, menerapkan secara menyeluruh, memonitoring dan mereviu secara berkala serta melakukan perbaikan prosedur pemeliharaan, pembaruan dan pengelolaan informasi pada siklus hidup data	Prosedur disahkan, diterapkan menyeluruh, dimonitor dan direviu berkala, serta ada mekanisme perbaikan berkelanjutan berdasarkan hasil evaluasi.	Selain semua bukti pada indeks 4, terdapat dokumen perbaikan atau penyempurnaan prosedur berdasarkan hasil evaluasi; catatan implementasi perubahan atau peningkatan.

2.3.6. Memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pencadangan dan sumber daya untuk melakukan pemeliharaan dan pengujian secara berkala.
Dampak	**Tinggi** – Dengan prosedur pencadangan yang efektif, organisasi dapat mengurangi risiko kehilangan data dan memastikan bahwa data dapat dipulihkan dengan cepat dan lengkap jika terjadi insiden.
Kompleksitas	**Sedang** – Memerlukan sistem pencadangan yang tepat dan prosedur pengujian yang terstruktur untuk memastikan bahwa pencadangan data dilakukan dengan benar dan diuji secara berkala.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-11, RC.RP-03** **NIST CSF 1.1: PR.IP-4** **NIST SP 800-53r5: CP-4, CP-6, CP-9** **SNI ISO/IEC 27001:2022: 5.29, 5.33, 8.13**

80 Kontrol 2.3.6.a:

Kontrol	Tersedianya dan diterapkannya prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem.
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa prosedur pencadangan sistem dilakukan secara berkala dan pengujian kehandalan komponen dilakukan untuk memastikan ketersediaan sistem. Prosedur ini bertujuan untuk melindungi sistem dari kehilangan data dan gangguan operasional dengan memastikan bahwa salinan data dan sistem yang dapat dipulihkan tersedia jika terjadi insiden. Pengujian kehandalan komponen juga penting untuk memastikan bahwa sistem berfungsi dengan baik dan siap menghadapi kegagalan komponen atau gangguan lainnya. Tujuan dari kontrol ini adalah untuk memastikan bahwa sistem memiliki tingkat ketahanan yang cukup untuk menjaga ketersediaan layanan yang tidak terputus.
Deskripsi Bukti Dukung	Bukti dukung yang dapat disediakan untuk menunjukkan tersedianya dan diterapkannya prosedur pencadangan sistem serta pengujian kehandalan komponen meliputi dokumen formal prosedur pencadangan dan pengujian, jadwal pelaksanaan pencadangan, log hasil pencadangan, bukti pelaksanaan uji kehandalan sistem (misalnya hasil simulasi failover atau recovery), laporan monitoring dan reviu berkala, serta dokumen tindak lanjut atau perbaikan atas hasil evaluasi tersebut. Bukti ini menunjukkan bahwa organisasi secara sistematis menjamin ketersediaan sistem dalam rangka menjaga kontinuitas layanan.
Ancaman/Risiko yang dimitigasi	TH007 TH009 TH011 TH014 TH023 TH008 TH010 TH013 TH015
Referensi Kontrol	**NIST CSF 2.0: PR.DS-11, RC.RP-03** **NIST CSF 1.1: PR.IP-4** **NIST SP 800-53r5: CP-4, CP-6, CP-9** **SNI ISO/IEC 27001:2022: 5.29, 5.33, 8.13**

Kriteria Pemenuhan Kontrol 2.3.6.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem.	Tidak ada dokumen, belum ada inisiatif pencadangan dan pengujian keandalan sistem. Sistem rentan terhadap gangguan tanpa mitigasi.	Tidak ada dokumen resmi atau bukti kegiatan pencadangan/ pengujian
1	Organisasi telah menyusun prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem dan menerapkan pada sebagian kecil aspek	Sudah ada dokumen awal/draf prosedur, dan mulai diterapkan terbatas pada unit/sistem tertentu. Belum menyeluruh dan belum formal.	Draft prosedur, dokumentasi pencadangan pada sistem minor, catatan kegiatan terbatas
2	Organisasi telah menyusun prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem dan menerapkan pada sebagian besar aspek	Prosedur mulai dijalankan lebih luas, mencakup sebagian besar sistem utama, namun belum semua bagian organisasi/sistem.	Prosedur formal, log pencadangan dari mayoritas sistem, hasil uji coba failover untuk sebagian besar komponen
3	Organisasi telah mengesahkan prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem dan menerapkan pada seluruh aspek	Prosedur formal dengan pengesahan manajemen. Implementasi sudah menyeluruh di seluruh sistem dan unit terkait.	Dokumen prosedur disahkan manajemen, log pencadangan lengkap, bukti pelaksanaan uji ke semua komponen
4	Organisasi telah mengesahkan prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem dan menerapkan pada seluruh aspek, dimonitoring dan direviu secara berkala	Selain implementasi menyeluruh, terdapat aktivitas monitoring dan evaluasi rutin untuk memastikan efektivitas.	Laporan monitoring berkala, notulen reviu prosedur, evaluasi hasil uji keandalan.
5	Organisasi telah mengesahkan prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem dan menerapkan pada seluruh aspek, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	Pendekatan berkelanjutan diterapkan. Hasil monitoring dan reviu digunakan untuk memperbarui dan menyempurnakan prosedur secara aktif.	Dokumen perbaikan/pembaruan prosedur, log perubahan, bukti implementasi hasil evaluasi

2.3.7. Menyediakan kebijakan pemusnahan data

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus menyediakan kebijakan pemusnahan data
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengimplementasikan kebijakan pemusnahan data, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan kebijakan pemusnahan data yang jelas, organisasi dapat mengurangi risiko kebocoran data dan memastikan bahwa data yang sudah tidak diperlukan lagi dimusnahkan dengan aman.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan sistem pemusnahan data yang tepat untuk memastikan bahwa data dimusnahkan dengan aman dan sesuai dengan kebijakan yang ditetapkan.
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08** **NIST CSF 1.1: PR.IP-6** **NIST SP 800-53r5: MP-6, SR-12** **SNI ISO/IEC 27001:2022: 7.10, 7.14, 8.8**

81 Kontrol 2.3.7.a:

Kontrol	Saat akan menghapuskan perangkat dan aset informasi, prosedur penghapusan data yang disimpan dari perangkat dan server serta informasi penting lainya (misalnya, kunci pribadi dan sertifikat digital), atau dibuat agar tidak dapat dibaca.
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa prosedur penghapusan data yang disimpan pada perangkat dan server dilakukan dengan cara yang aman, sehingga data dan informasi penting (misalnya, kunci pribadi dan sertifikat digital) tidak dapat dipulihkan atau dibaca setelah perangkat atau aset informasi dihapuskan. Penghapusan data ini bertujuan untuk melindungi informasi sensitif yang dapat disalahgunakan jika perangkat atau data yang disimpan jatuh ke tangan yang tidak berwenang. Prosedur ini harus mengacu pada standar penghapusan data yang diakui, seperti metode penghapusan data berbasis standar (misalnya, DoD 5220.22-M) atau menggunakan alat penghapusan yang dapat memastikan bahwa data tidak dapat dipulihkan. Tujuan dari kontrol ini adalah untuk memastikan perlindungan informasi sensitif dengan cara yang sesuai saat perangkat atau aset informasi dihapuskan.
Deskripsi Bukti Dukung	Sebagai bukti pemenuhan terhadap kontrol penghapusan data saat pemusnahan perangkat dan aset informasi, organisasi perlu menunjukkan dokumen kebijakan resmi, prosedur teknis, serta catatan penerapan penghapusan data yang mencakup media penyimpanan perangkat, server, dan informasi penting seperti kunci pribadi atau sertifikat digital. Bukti juga dapat berupa log penghapusan, hasil audit internal, bukti penerapan tool wiping/overwriting, laporan monitoring, serta bukti evaluasi dan perbaikan prosedur secara berkala untuk memastikan bahwa data yang dihapus tidak dapat dipulihkan kembali.
Ancaman/Risiko yang dimitigasi	TH031 TH035 TH054 TH075 TH032 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-08** **NIST CSF 1.1: PR.IP-6** **NIST SP 800-53r5: MP-6, SR-12** **SNI ISO/IEC 27001:2022: 7.10, 7.14, 8.8**

Kriteria Pemenuhan Kontrol 2.3.7.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki kebijakan dan menerapkan penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan.	Organisasi tidak memiliki kebijakan atau prosedur penghapusan data dari perangkat dan server yang akan dimusnahkan.	- Tidak tersedia kebijakan atau prosedur penghapusan data. - Tidak ada bukti implementasi.
1	Organisasi telah menyusun kebijakan dan menerapkan sebagian kecil mekanisme penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan	Organisasi telah menyusun kebijakan awal, namun baru menerapkan sebagian kecil mekanisme penghapusan data. Implementasi masih terbatas.	- Draft kebijakan/prosedur penghapusan data. - Bukti terbatas penerapan pada sebagian perangkat. - Dokumentasi manual proses tanpa standar.
2	Organisasi telah menyusun kebijakan dan menerapkan sebagian besar mekanisme penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan	Organisasi telah menyusun kebijakan dan menerapkan sebagian besar mekanisme penghapusan data, namun belum menyeluruh atau belum didukung pengesahan formal.	- Dokumen kebijakan/prosedur yang lebih lengkap. - Bukti penerapan pada sebagian besar perangkat. - Bukti penggunaan tool penghapusan data (misalnya software wiping).
3	Organisasi telah mengesahkan kebijakan dan menerapkan secara menyeluruh mekanisme penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan	Organisasi telah mengesahkan kebijakan dan menerapkan seluruh mekanisme penghapusan data secara menyeluruh, sesuai dengan standar yang berlaku.	- Kebijakan yang disahkan secara resmi. - Prosedur standar operasional (SOP) penghapusan data. - Bukti penerapan menyeluruh (log, laporan pelaksanaan, dokumentasi kegiatan).
4	Organisasi telah mengesahkan kebijakan, menerapkan secara menyeluruh mekanisme, memonitoring dan mereviu secara berkala penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan	Selain pengesahan dan implementasi menyeluruh, organisasi juga melakukan monitoring dan reviu berkala atas proses penghapusan data.	- Semua bukti pada indeks 3. - Laporan monitoring atau audit internal. - Jadwal dan hasil reviu berkala kebijakan/prosedur.
5	Organisasi telah mengesahkan kebijakan, menerapkan secara menyeluruh mekanisme, memonitoring dan mereviu secara berkala serta melakukan perbaikan penghapusan data yang disimpan dari perangkat dan server yang akan dimusnahkan	Organisasi secara proaktif memperbaiki dan meningkatkan proses penghapusan data berdasarkan hasil monitoring dan reviu berkala. Praktik ini sudah menjadi bagian dari siklus perbaikan berkelanjutan.	- Semua bukti pada indeks 4. - Bukti pelaksanaan perbaikan atau pembaruan prosedur. - Notulen rapat evaluasi, rekomendasi perbaikan, dan implementasi perubahan.

2.4. Melindungi aplikasi

Melindungi aplikasi merupakan bagian penting dalam menjaga keamanan operasional Infrastruktur Informasi Vital (IIV). Penyelenggara IIV wajib menerapkan prosedur konfigurasi dasar sistem dan pengendalian perubahan, menyusun serta mengimplementasikan rencana manajemen kerentanan, serta memastikan pemisahan lingkungan pengembangan, pengujian, dan produksi. Selain itu, juga perlu diterapkan prosedur pengembangan sistem yang aman agar aplikasi terhindar dari berbagai potensi ancaman siber.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi;
b) mengembangkan dan mengimplementasikan rencana manajemen kerentanan;
c) memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional; dan
d) mengimplementasikan prosedur pengembangan sistem yang aman.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melindungi aplikasi” secara efektif antara lain:

NIST CSF 2.0	**:**	**PR.PS-01, PR.PS-02, PR.PS-06, PR.IR-01, ID.AM-08, ID.RA-01**
NIST CSF 1.1	**:**	**PR.IP-1, PR.IP-2, PR.IP-12, PR.DS-7**
NIST SP 800-53r5	**:**	**CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-3, SA-4, SA-8, SA-10, SA-11, RA-1, RA-3, RA-5, SI-2**
SNI ISO/IEC 27001:2022	**:**	**5.8, 5.36, 8.8, 8.9, 8.19, 8.25, 8.27, 8.31, 8.32**

2.4.1. Menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi yang digunakan pada operasional Infrastruktur Informasi Vital.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengimplementasikan prosedur konfigurasi dan kendali perubahan.
Dampak	**Tinggi** – Dengan prosedur yang jelas, organisasi dapat memastikan bahwa semua perubahan pada sistem dilakukan dengan cara yang terkendali, sehingga mengurangi risiko kesalahan konfigurasi dan meningkatkan keamanan sistem.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mengelola dan mencatat semua perubahan konfigurasi secara efektif.
Referensi Kontrol	**NIST CSF 2.0: PR.PS-01** **NIST CSF 1.1: PR.IP-1** **NIST SP 800-53r5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** **SNI ISO/IEC 27001:2022: 8.9, 8.19, 8.32**

82 Kontrol 2.4.1.a:

Kontrol	Tersedianya dan diterapkannya prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses, dsb).
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa terdapat prosedur yang jelas dan diterapkan untuk mengatur keamanan sistem, termasuk prosedur terkait penerapan kata sandi yang kuat, kontrol izin akses, dan kebijakan keamanan lainnya. Prosedur ini bertujuan untuk mengurangi risiko penyalahgunaan akses atau serangan yang dapat merusak integritas dan kerahasiaan sistem. Pengaturan yang benar sejak awal akan membatasi potensi ancaman yang dapat muncul akibat pengaturan sistem yang kurang aman. Prosedur pengaturan ini harus mencakup standar terbaik yang sesuai dengan kebijakan organisasi serta pedoman industri dan peraturan yang berlaku. Tujuan dari kontrol ini adalah untuk memastikan bahwa pengaturan sistem dilakukan dengan langkah-langkah keamanan yang memadai untuk melindungi asset informasi dan mencegah akses yang tidak sah.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur yang mengatur pengaturan kata sandi (misalnya, panjang kata sandi, kompleksitas, waktu kedaluwarsa, dan penggantian kata sandi). - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan hak akses pengguna (misalnya, penerapan prinsip "least privilege", peninjauan hak akses secara berkala). - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan. - Catatan audit yang mencatat perubahan pengaturan sistem yang relevan, seperti pengaturan kata sandi dan hak akses, serta siapa yang membuat perubahan tersebut - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem.
Ancaman/Risiko yang dimitigasi	TH053 TH071 TH073 TH054 TH072
Referensi Kontrol	**NIST CSF 2.0: PR.PS-01** **NIST CSF 1.1: PR.IP-1** **NIST SP 800-53r5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** **SNI ISO/IEC 27001:2022: 8.9, 8.19, 8.32**

Kriteria Pemenuhan Kontrol 2.4.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Prosedur untuk keamanan pada saat pengaturan sistem belum ada.	Tidak ada	Tidak ada
1	Organisasi telah menyediakan prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses) dan diterapkan oleh sebagian kecil organisasi tapi belum diformalkan	Sebagian kecil unit kerja di organisasi telah menerapkan prosedur untuk keamanan pada saat pengaturan sistem yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur pengaturan kata sandi yang telah disediakan oleh organisasi namun belum diformalkan. - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan yang telah disediakan oleh organisasi namun belum diformalkan. - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan pada sebagian kecil unit kerja yang telah menerapkan kebijakan, - Catatan audit yang mencatat perubahan pengaturan sistem yang relevan pada sebagian kecil unit kerja yang telah menerapkan kebijakan. - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan pada sebagian kecil unit kerja yang telah menerapkan kebijakan. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem pada sebagian kecil unit kerja yang telah menerapkan kebijakan.
2	Organisasi telah menyediakan prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses) dan diterapkan oleh sebagian besar organisasi tapi belum diformalkan	Sebagian besar unit kerja di organisasi telah menerapkan prosedur untuk keamanan pada saat pengaturan sistem yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur pengaturan kata sandi yang telah disediakan oleh organisasi namun belum diformalkan. - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan yang telah disediakan oleh organisasi namun belum diformalkan. - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan pada sebagian besar unit kerja yang telah menerapkan kebijakan,

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Catatan audit yang mencatat perubahan pengaturan sistem yang relevan pada sebagian besar unit kerja yang telah menerapkan kebijakan. - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan pada sebagian besar unit kerja yang telah menerapkan kebijakan. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem pada sebagian besar unit kerja yang telah menerapkan kebijakan.
3	Organisasi telah menyediakan prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses), diterapkan oleh seluruh organisasi dan sudah diformalkan	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk keamanan pada saat pengaturan sistem yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja.	- Kebijakan atau prosedur yang mengatur pengaturan kata sandi yang telah disediakan oleh organisasi dan telah diformalkan. - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan yang telah disediakan oleh organisasi dan telah diformalkan. - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan pada seluruh unit kerja. - Catatan audit yang mencatat perubahan pengaturan sistem yang relevan pada seluruh unit kerja. - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan pada seluruh unit kerja. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem pada seluruh unit kerja.
4	Organisasi telah menyediakan prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses), diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring dan direviu berkala	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk keamanan pada saat pengaturan sistem yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu prosedur	- Kebijakan atau prosedur yang mengatur pengaturan kata sandi yang telah disediakan oleh organisasi dan telah diformalkan, dimonitoring dan direviu. - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan yang telah disediakan oleh

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		juga dimonitoring implementasinya dan direviu oleh organisasi.	organisasi dan telah diformalkan, dimonitoring dan direviu. - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan pada seluruh unit kerja. - Catatan audit yang mencatat perubahan pengaturan sistem yang relevan pada seluruh unit kerja. - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan pada seluruh unit kerja. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem pada seluruh unit kerja.
5	Organisasi telah menyediakan prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses), diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring dan direviu berkala, dan dilakukan perbaikan	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk keamanan pada saat pengaturan sistem yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu prosedur juga dimonitoring implementasinya, direviu dan diperbaiki oleh organisasi berdasarkan hasil reviu.	- Kebijakan atau prosedur yang mengatur pengaturan kata sandi yang telah disediakan oleh organisasi dan telah diformalkan, dimonitoring, direviu dan diperbaiki oleh organisasi. - Kebijakan atau prosedur yang mengatur izin akses dan pengelolaan yang telah disediakan oleh organisasi dan telah diformalkan, dimonitoring, direviu dan diperbaiki oleh organisasi. - Laporan implementasi kebijakan kata sandi dan akses yang menunjukkan penerapan kontrol sesuai kebijakan pada seluruh unit kerja. - Catatan audit yang mencatat perubahan pengaturan sistem yang relevan pada seluruh unit kerja. - Laporan pengujian atau audit keamanan yang menunjukkan apakah prosedur pengaturan sistem yang diterapkan memenuhi standar keamanan yang ditetapkan pada seluruh unit kerja. - Dokumen yang mencakup pelatihan keamanan yang diberikan kepada personel yang bertanggung jawab atas pengaturan dan pengelolaan sistem pada seluruh unit kerja.

83 Kontrol 2.4.1.b:

Kontrol	Tersedianya dan diterapkannya prosedur untuk melakukan perubahan pengaturan pada perangkat.
Deskripsi Kontrol	Penyelenggara Infrastruktur Informasi Vital harus memastikan bahwa terdapat prosedur yang jelas dan diterapkan untuk melakukan perubahan pengaturan pada perangkat. Prosedur ini bertujuan untuk mengendalikan perubahan pada sistem dan perangkat, serta untuk mencegah perubahan yang tidak sah atau tidak terkontrol yang dapat mengancam keamanan sistem dan data. Setiap perubahan harus dilakukan dengan cara yang terstruktur dan terdokumentasi untuk memastikan bahwa dampaknya dapat dipantau dan jika diperlukan, dapat dilakukan rollback kepengaturan sebelumnya. Tujuan dari prosedur ini adalah untuk menjaga integritas perangkat dan memastikan bahwa perubahan yang dilakukan tidak merusak fungsi keamanan atau operasi normal sistem.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat (misalnya, prosedur persetujuan perubahan, dokumentasi perubahan, uji coba perubahan sebelum penerapan). - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat. - Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko baru terhadap keamanan atau ketersediaan sistem - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan, jika diperlukan.
Ancaman/Risiko yang dimitigasi	TH053 TH071 TH073 TH054 TH072
Referensi Kontrol	**NIST CSF 2.0: PR.PS-01** **NIST CSF 1.1: PR.IP-1** **NIST SP 800-53r5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** **SNI ISO/IEC 27001:2022: 8.9, 8.19, 8.32**

Kriteria Pemenuhan Kontrol 2.4.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur untuk melakukan perubahan pengaturan pada perangkat	Tidak ada	Tidak ada
1	Organisasi telah menyediakan prosedur untuk melakukan perubahan pengaturan pada perangkat dan diterapkan oleh sebagian kecil organisasi tetapi belum diformalkan	Sebagian kecil unit kerja di organisasi telah menerapkan prosedur untuk perubahan pengaturan pada perangkat yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat yang disediakan oleh organisasi. - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan pada sebagian kecil unit kerja yang telah menerapkan. - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat pada sebagian kecil unit kerja yang telah menerapkan. - Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko baru terhadap keamanan atau ketersediaan sistem pada sebagian kecil unit kerja yang telah menerapkan. - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan pada sebagian kecil unit kerja yang telah menerapkan. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan pada sebagian kecil unit kerja yang telah menerapkan.
2	Organisasi telah menyediakan prosedur untuk melakukan perubahan pengaturan pada perangkat dan diterapkan oleh sebagian besar organisasi tetapi belum diformalkan	Sebagian besar unit kerja di organisasi telah menerapkan prosedur untuk perubahan pengaturan pada perangkat yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat yang disediakan oleh organisasi. - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan pada sebagian besar unit kerja yang telah menerapkan. - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat pada sebagian besar unit kerja yang telah menerapkan. - Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			baru terhadap keamanan atau ketersediaan sistem pada sebagian besar unit kerja yang telah menerapkan. - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan pada sebagian besar unit kerja yang telah menerapkan. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan pada sebagian besar unit kerja yang telah menerapkan.
3	Organisasi telah menyediakan prosedur untuk melakukan perubahan pengaturan pada perangkat dan diterapkan oleh seluruh organisasi dan sudah diformalkan	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk melakukan perubahan pengaturan pada perangkat yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja.	- Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat yang disediakan oleh organisasi dan telah diformalkan. - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan pada seluruh unit kerja. - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat pada seluruh unit kerja. - Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko baru terhadap keamanan atau ketersediaan sistem pada seluruh unit kerja. - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan pada seluruh unit kerja. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan pada seluruh unit kerja.
4	Organisasi telah menyediakan prosedur untuk melakukan perubahan pengaturan pada perangkat dan diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring dan direviu berkala	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk melakukan perubahan pengaturan pada perangkat yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu, prosedur juga dimonitoring implementasinya dan direviu oleh organisasi.	- Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat yang disediakan oleh organisasi dan telah diformalkan, dimonitoring dan direviu berkala oleh organisasi. - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan pada seluruh unit kerja. - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat pada seluruh unit kerja.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko baru terhadap keamanan atau ketersediaan sistem pada seluruh unit kerja. - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan pada seluruh unit kerja. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan pada seluruh unit kerja.
5	Organisasi telah menyediakan prosedur untuk melakukan perubahan pengaturan pada perangkat dan diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring, direviu berkala dan dilakukan perbaikan	Seluruh unit kerja di organisasi telah menerapkan prosedur untuk melakukan perubahan pengaturan pada perangkat yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu prosedur juga dimonitoring implementasinya dan direviu serta diperbaiki oleh organisasi.	- Kebijakan atau prosedur yang mengatur pengelolaan perubahan pengaturan perangkat yang disediakan oleh organisasi dan telah diformalkan, dimonitoring, direviu berkala dan diperbaiki oleh organisasi. - Catatan perubahan yang mencakup rincian perubahan yang dilakukan, siapa yang melakukan perubahan, dan alasan perubahan pada seluruh unit kerja. - Laporan audit atau reviu yang menunjukkan penerapan kontrol terhadap perubahan pengaturan perangkat pada seluruh unit kerja. - Laporan pengujian atau validasi yang memastikan bahwa perubahan pengaturan perangkat tidak menimbulkan risiko baru terhadap keamanan atau ketersediaan sistem pada seluruh unit kerja. - Protokol yang menunjukkan pelaksanaan perubahan yang terkoordinasi antara tim teknis dan pemangku kepentingan yang relevan pada seluruh unit kerja. - Prosedur rollback atau pemulihan untuk mengatasi masalah setelah perubahan yang diterapkan pada seluruh unit kerja.

84 Kontrol 2.4.1.c:

Kontrol	Tersedianya dan diterapkannya prosedur Pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server.
Deskripsi Kontrol	Penyelenggara Infrastruktur Informasi Vital harus memastikan bahwa terdapat prosedur yang jelas dan diterapkan untuk membatasi perangkat lunak yang dapat ditambahkan pada perangkat dan server. Prosedur ini bertujuan untuk mengendalikan instalasi perangkat lunak yang dapat mempengaruhi keamanan dan kinerja sistem. Pembatasan ini diperlukan untuk mencegah pemasangan perangkat lunak yang tidak sah atau berisiko, yang dapat menyebabkan kerentanannya terhadap ancaman siber atau mengganggu operasi sistem. Tujuan prosedur ini adalah untuk meminimalkan potensi celah keamanan dan memastikan bahwa hanya perangkat lunak yang terverifikasi dan sah yang dapat dijalankan pada perangkat dan server.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur yangmengatur jenis perangkat lunak yangdapat diinstal dan kriteria pemilihannya (misalnya, perangkat lunak yang telah diverifikasi, memiliki lisensi sah, atau telah diuji keamanannya). - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak. - Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal (misalnya, pengujian integritas, pemeriksaan tanda tangan digital, atau uji kerentanannya).
Ancaman/Risiko yang dimitigasi	TH054 TH072 TH074 TH071 TH073
Referensi Kontrol	**NIST CSF 2.0: PR.PS-01** **NIST CSF 1.1: PR.IP-1** **NIST SP 800-53r5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** **SNI ISO/IEC 27001:2022: 8.9, 8.19, 8.32**

Kriteria Pemenuhan Kontrol 2.4.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server	Tidak ada	Tidak ada
1	Organisasi telah menyediakan rancangan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server dan diterapkan oleh sebagian kecil organisasi tetapi belum diformalkan	Sebagian kecil unit kerja di organisasi telah menerapkan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur jenis perangkat lunak yang dapat diinstal dan kriteria pemilihannya yang disediakan oleh organisasi yang belum diformalkan. - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi yang belum diformalkan. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem yang belum diformalkan. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti pada sebagian kecil unit kerja yang telah menerapkan kebijakan. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak yang belum diformalkan. - Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal pada sebagian kecil unit kerja yang telah menerapkan kebijakan.
2	Organisasi telah menyediakan rancangan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server dan diterapkan oleh sebagian besar organisasi tetapi belum diformalkan	Sebagian besar unit kerja di organisasi telah menerapkan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server yang disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur yang mengatur jenis perangkat lunak yang dapat diinstal dan kriteria pemilihannya yang disediakan oleh organisasi yang belum diformalkan. - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi yang belum diformalkan. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem yang belum diformalkan. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti pada sebagian besar unit kerja yang telah menerapkan kebijakan. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak yang belum diformalkan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal pada sebagian besar unit kerja yang telah menerapkan kebijakan.
3	Organisasi telah menyediakan rancangan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server dan diterapkan oleh seluruh organisasi dan sudah diformalkan	Seluruh unit kerja di organisasi telah menerapkan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja.	- Kebijakan atau prosedur yang mengatur jenis perangkat lunak yang dapat diinstal dan kriteria pemilihannya yang disediakan oleh organisasi dan telah diformalkan. - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi yang telah diformalkan. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem yang telah diformalkan. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti pada seluruh unit kerja. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak yang telah diformalkan. - Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal pada seluruh unit kerja.
4	Organisasi telah menyediakan rancangan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server dan diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring, dan direviu secara berkala	Seluruh unit kerja di organisasi telah menerapkan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu, prosedur juga dimonitoring implementasinya dan direviu oleh organisasi.	- Kebijakan atau prosedur yang mengatur jenis perangkat lunak yang dapat diinstal dan kriteria pemilihannya yang disediakan oleh organisasi dan telah diformalkan, dimonitoring dan direviu secara berkala oleh organisasi.. - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi yang telah diformalkan, dimonitoring dan direviu secara berkala oleh organisasi. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem yang telah diformalkan, dimonitoring dan direviu secara berkala oleh organisasi. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti pada seluruh unit kerja. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak yang telah

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			diformalkan, dimonitoring dan direviu secara berkala oleh organisasi. - Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal pada seluruh unit kerja.
5	Organisasi telah menyediakan rancangan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server dan diterapkan oleh seluruh organisasi, sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	Seluruh unit kerja di organisasi telah menerapkan prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server yang disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja. Selain itu prosedur juga dimonitoring implementasinya dan direviu serta diperbaiki oleh organisasi.	- Kebijakan atau prosedur yang mengatur jenis perangkat lunak yang dapat diinstal dan kriteria pemilihannya yang disediakan oleh organisasi dan telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi. - Daftar perangkat lunak yang disetujui dan yang dilarang untuk digunakan dalam organisasi yang telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi. - Protokol atau proses persetujuan instalasi perangkat lunak, termasuk persetujuan dari pihak yang berwenang sebelum perangkat lunak diinstal pada sistem yang telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi.. - Laporan audit yang menunjukkan bahwa prosedur pembatasan perangkat lunak telah diterapkan dan diikuti pada seluruh unit kerja. - Prosedur untuk memantau dan mengevaluasi perangkat lunak yang ada di sistem untuk memastikan kepatuhan terhadap kebijakan pembatasan perangkat lunak yang telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi. - Dokumentasi yang menunjukkan proses verifikasi keamanan perangkat lunak baru sebelum diinstal pada seluruh unit kerja.

2.4.2. Mengembangkan dan mengimplementasikan rencana manajemen kerentanan

Kriteria	Detail
Deskripsi	Penyelenggara Infrastruktur Informasi Vital mengembangkan dan mengimplementasikan rencana manajemen kerentanan yang dapat terjadi pada infrastruktur informasi vital.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam alat manajemen kerentanan dan sumber daya untuk mengelola serta memperbaiki kerentanan yang ditemukan.
Dampak	**Tinggi** – Dengan manajemen kerentanan yang efektif, organisasi dapat mengurangi risiko eksploitasi kerentanan dan meningkatkan keamanan sistem.
Kompleksitas	**Sedang** – Memerlukan alat dan prosedur yang tepat untuk mengidentifikasi, menilai, dan memperbaiki kerentanan secara efektif.
Referensi Kontrol	**NIST CSF 2.0: PR.PS-02, ID.RA-01** **NIST CSF 1.1: PR.IP-12** **NIST SP 800-53r5: RA-1, RA-3, RA-5, SI-2** **SNI ISO/IEC 27001:2022: 5.36, 8.8**

85 Kontrol 2.4.2.a:

Kontrol	Mengembangkan dan mengimplementasikan rencana manajemen kerentanan.
Deskripsi Kontrol	Penyelenggara Infrastruktur Informasi Vital harus mengembangkan dan mengimplementasikan rencana manajemen kerentanan yang mencakup serangkaian langkah dari pengumpulan informasi tentang kerentanan, inventarisasi kerentanan yang teridentifikasi, hingga perbaikan kerentanan yang ditemukan. Proses ini penting untuk mengidentifikasi dan mengatasi kerentanan di sistem dan aplikasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Rencana manajemen kerentanan harus mencakup prosedur untuk melakukan pemindaian kerentanan secara berkala, mendokumentasikan kerentanannya, mengklasifikasikan tingkat keparahannya, dan kemudian menetapkan langkah mitigasi atau perbaikan yang diperlukan untuk mengurangi atau menghilangkan risiko yang ditimbulkan oleh kerentanannya. Tujuan dari rencana ini adalah untuk meminimalkan eksposur terhadap ancaman dan memastikan bahwa setiap kerentanannya diatasi sebelum dapat dimanfaatkan oleh pihak yang berpotensi merusak sistem.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur manajemen kerentanan yang mencakup langkah-langkah pengumpulan, inventarisasi, dan perbaikan kerentanan. - Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya. - Daftar kerentanan yang telah teridentifikasi, beserta status dan tindak lanjut perbaikannya. - Protokol pengujian dan pembaruan aplikasi atau sistem untuk memastikan bahwa kerentanan yang ditemukan sudah diperbaiki. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan untuk menanggulangi kerentanannya. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan, termasuk hasil tindak lanjut terhadap kerentanannya. - Catatan rapat atau komunikasi dengan tim terkait mengenai status perbaikan kerentanannya.
Ancaman/Risiko yang dimitigasi	TH050 TH071 TH073 TH054 TH072 TH074
Referensi Kontrol	**NIST CSF 2.0: PR.PS-02, ID.RA-01** **NIST CSF 1.1: PR.IP-12** **NIST SP 800-53r5: RA-1, RA-3, RA-5, SI-2** **SNI ISO/IEC 27001:2022: 5.36, 8.8**

Kriteria Pemenuhan Kontrol 2.4.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum mengembangkan dan mengimplementasikan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi.	Tidak ada	Tidak ada
1	Organisasi sudah mengembangkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi. diimplementasikan pada sebagian kecil organisasi dan belum diformalkan	Sebagian kecil unit kerja menerapkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi yang telah disediakan oleh organisasi. Prosedur belum diformalkan sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Kebijakan atau prosedur manajemen kerentanan yang disediakan oleh organisasi namun belum diformalkan. - Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya pada sebagian kecil unit kerja yang menerapkan kebijakan. - Daftar kerentanan yang telah teridentifikasi yang disediakan organisasi namun belum diformalkan. - Protokol pengujian dan pembaruan aplikasi atau sistem yang disediakan organisasi namun belum diformalkan. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan pada sebagian kecil unit kerja yang menerapkan kebijakan. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan pada sebagian kecil unit kerja yang menerapkan. - Catatan rapat atau komunikasi dengan tim terkait status perbaikan kerentanan pada sebagian kecil unit kerja yang menerapkan.
2	Organisasi sudah mengembangkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi. diimplementasikan pada sebagian besar organisasi dan belum diformalkan	Sebagian besar unit kerja menerapkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi yang telah disediakan oleh organisasi. Prosedur belum diformalkan	- Kebijakan atau prosedur manajemen kerentanan yang disediakan oleh organisasi namun belum diformalkan. - Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya pada sebagian besar unit kerja yang menerapkan kebijakan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		sehingga penerapan bergantung pada kesadaran masing-masing unit kerja.	- Daftar kerentanan yang telah teridentifikasi yang disediakan organisasi namun belum diformalkan. - Protokol pengujian dan pembaruan aplikasi atau sistem yang disediakan organisasi namun belum diformalkan. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan pada sebagian besar unit kerja yang menerapkan kebijakan. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan pada sebagian besar unit kerja yang menerapkan. - Catatan rapat atau komunikasi dengan tim terkait status perbaikan kerentanan pada sebagian besar unit kerja yang menerapkan.
3	Organisasi sudah mengembangkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi. diimplementasikan pada seluruh organisasi dan sudah diformalkan	Seluruh unit kerja menerapkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi yang telah disediakan oleh organisasi. Prosedur telah diformalkan sehingga harus diterapkan oleh seluruh unit kerja.	- Kebijakan atau prosedur manajemen kerentanan yang disediakan oleh organisasi yang telah diformalkan. - Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya pada seluruh unit kerja - Daftar kerentanan yang telah teridentifikasi yang disediakan organisasi yang telah diformalkan. - Protokol pengujian dan pembaruan aplikasi atau sistem yang disediakan organisasi yang telah diformalkan. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan pada seluruh unit kerja. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan pada seluruh unit kerja. - Catatan rapat atau komunikasi dengan tim terkait status perbaikan kerentanan pada seluruh unit kerja.
4	Organisasi sudah mengembangkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi. diimplementasikan	Seluruh unit kerja menerapkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi yang telah	- Kebijakan atau prosedur manajemen kerentanan yang disediakan oleh organisasi yang telah diformalkan, dimonitoring dan direviu secara berkala oleh organisasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	pada seluruh organisasi, sudah diformalkan, dimonitoring dan direviu secara berkala	disediakan oleh organisasi. Prosedur telah diformalkan dimonitoring, direviu secara berkala oleh organisasi.	- Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya pada seluruh unit kerja - Daftar kerentanan yang telah teridentifikasi yang disediakan organisasi yang telah diformalkan. - Protokol pengujian dan pembaruan aplikasi atau sistem yang disediakan organisasi yang telah diformalkan, dimonitoring dan direviu secara berkala oleh organisasi. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan pada seluruh unit kerja. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan pada seluruh unit kerja. - Catatan rapat atau komunikasi dengan tim terkait status perbaikan kerentanan pada seluruh unit kerja.
5	Organisasi sudah mengembangkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi. diimplementasikan pada seluruh organisasi, sudah diformalkan, dimonitoring, direviu secara berkala, dan diperbaiki	Seluruh unit kerja menerapkan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi yang telah disediakan oleh organisasi. Prosedur telah diformalkan dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi.	- Kebijakan atau prosedur manajemen kerentanan yang disediakan oleh organisasi yang telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi. - Laporan hasil pemindaian kerentanan yang mencatat temuan-temuan kerentanannya dan tingkat keparahannya pada seluruh unit kerja. - Daftar kerentanan yang telah teridentifikasi yang disediakan organisasi yang telah diformalkan. - Protokol pengujian dan pembaruan aplikasi atau sistem yang disediakan organisasi yang telah diformalkan, dimonitoring, direviu secara berkala dan diperbaiki oleh organisasi. - Dokumentasi terkait pembaruan perangkat lunak atau patch yang diterapkan pada seluruh unit kerja. - Catatan audit terkait implementasi dan pemantauan kebijakan manajemen kerentanan pada seluruh unit kerja. - Catatan rapat atau komunikasi dengan tim terkait status perbaikan kerentanan pada seluruh unit kerja.

2.4.3. Memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional

Kriteria	Detail
Deskripsi	Penyelenggara IIV memastikan pemisahan jelas antara lingkungan pengembangan/pengujian dan lingkungan produksi untuk menjaga keamanan dan stabilitas sistem. Pemisahan ini mencakup penggunaan media penyimpanan, jaringan, dan lingkungan kerja yang berbeda, dengan pembatasan akses ketat sesuai prinsip least privilege. Langkah ini mencegah gangguan operasional, kebocoran data, serta perubahan tidak sah, sekaligus memastikan setiap pengembangan atau pembaruan diuji terlebih dahulu sebelum diterapkan pada sistem produksi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan pengaturan dan pemeliharaan lingkungan yang terpisah untuk pengembangan, pengujian, dan produksi.
Dampak	**Tinggi** – Dengan lingkungan yang terpisah, organisasi dapat mengurangi risiko kesalahan dan memastikan bahwa perubahan diuji secara menyeluruh sebelum diterapkan ke lingkungan produksi.
Kompleksitas	**Sedang** – Memerlukan pengaturan dan pemeliharaan lingkungan yang terpisah serta prosedur untuk memindahkan kode dari pengembangan dan pengujian ke produksi.
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01** **NIST CSF 1.1: PR.DS-7** **NIST SP 800-53r5: CM-2** **SNI ISO/IEC 27001:2022: 8.31**

86 Kontrol 2.4.3.a:

Kontrol	Penggunaan lingkungan pengembangan sistem yang berbeda dari lingkungan produksi yang meliputi pemisahan terhadap media penyimpanan, jaringan, lingkungan kerja, dsb.
Deskripsi Kontrol	Penggunaan lingkungan pengembangan sistem yang terpisah dari lingkungan produksi adalah penting untuk mengurangi risiko gangguan atau kebocoran data antara pengembangan dan operasional sehari-hari. Pemisahan ini meliputi aspek-aspek seperti media penyimpanan, jaringan, dan lingkungan kerja untuk memastikan bahwa pengujian, pengembangan,dan pemeliharaan sistem tidak mengganggu operasi langsung yang berjalan di lingkungan produksi. Tujuan dari pemisahan ini adalah untuk menjaga kestabilan, keamanan, dan integritas sistem produksi dengan menghindari pengaruh negatif dari perubahan atau kesalahan dalam pengembangan. Selain itu, hal ini juga mengurangi risiko terhadap data sensitif dan menghindari potensi kebocoran informasi yang terjadi selama proses pengembangan atau pengujian.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi. - Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan. - Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personil yang berwenang. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi.
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH073 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01** **NIST CSF 1.1: PR.DS-7** **NIST SP 800-53r5: CM-2** **SNI ISO/IEC 27001:2022: 8.31**

Kriteria Pemenuhan Kontrol 2.4.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki pemisahan antara lingkungan pengembangan dan lingkungan produksi. Tidak ada upaya yang dilakukan untuk mengimplementasikan pemisahan tersebut.	Tidak ada	Tidak ada
1	Organisasi telah mulai menerapkan pemisahan antara lingkungan pengembangan dan lingkungan produksi pada sebagian kecil aspek, seperti media penyimpanan atau jaringan, tetapi belum ada formalitas atau kebijakan yang mendukung pemisahan ini secara keseluruhan.	Lingkungan pengembangan dan lingkungan produksi di organisasi telah dipisahkan pada sebagian kecil aspek. Karena belum diformalkan, pemisahan masih bersifat sukarela dan bergantung pada kesadaran setiap unit kerja di organisasi.	- Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi pada sebagian kecil aspek. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi pada sebagian kecil aspek - Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan pada sebagian kecil aspek. - Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi pada sebagian kecil aspek. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi pada sebagian kecil aspek. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personel yang berwenang di setiap unit kerja. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi di setiap unit kerja.
2	Pemisahan antara lingkungan pengembangan dan lingkungan produksi telah diterapkan pada sebagian besar aspek, termasuk media penyimpanan, jaringan, dan lingkungan kerja, tetapi belum ada kebijakan atau dokumentasi formal yang mengatur atau mendukung praktik ini.	Lingkungan pengembangan dan lingkungan produksi di organisasi telah dipisahkan pada sebagian besar aspek. Karena belum diformalkan, pemisahan masih bersifat sukarela dan bergantung pada kesadaran setiap unit kerja di organisasi.	- Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi pada sebagian besar aspek. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi pada sebagian besar aspek - Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan pada sebagian besar aspek.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi pada sebagian besar aspek. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi pada sebagian besar aspek. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personel yang berwenang di setiap unit kerja. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi di setiap unit kerja.
3	Organisasi telah menerapkan pemisahan lingkungan pengembangan dan produksi pada seluruh aspek, dan langkah ini sudah didukung oleh kebijakan, prosedur, dan dokumentasi formal. Pemisahan ini menjadi bagian dari standar operasi organisasi.	Lingkungan pengembangan dan lingkungan produksi di organisasi telah dipisahkan pada seluruh aspek. Pemisahan yang menjadi standar operasi organisasi, membuat setiap unit kerja harus menerapkan pemisahan tersebut.	- Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi pada seluruh aspek. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi pada seluruh aspek. - Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan pada seluruh aspek. - Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi pada seluruh aspek. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi pada seluruh aspek. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personel yang berwenang di setiap unit kerja. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi di setiap unit kerja.
4	Selain pemisahan yang sudah diterapkan dan diformalkan, organisasi juga melakukan monitoring dan reviu secara berkala untuk memastikan bahwa pemisahan antara lingkungan pengembangan dan produksi	Lingkungan pengembangan dan lingkungan produksi di organisasi telah dipisahkan pada seluruh aspek. Pemisahan yang menjadi standar operasi organisasi, membuat setiap unit kerja harus menerapkan pemisahan tersebut,	- Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi pada seluruh aspek. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi pada seluruh aspek.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	tetap efektif dan sesuai dengan kebijakan yang ada.	proses tersebut dimonitoring dan direviu secara berkala oleh organisasi.	- Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan pada seluruh aspek. - Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi pada seluruh aspek. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi pada seluruh aspek. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personel yang berwenang di setiap unit kerja. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi di setiap unit kerja.
5	Organisasi tidak hanya menerapkan dan memformalkan pemisahan antara lingkungan pengembangan dan produksi, tetapi juga melakukan monitoring, reviu berkala, serta perbaikan terus-menerus. Jika memungkinkan, otomatisasi teknis diterapkan untuk meningkatkan efisiensi dan keamanan dalam memisahkan kedua lingkungan tersebut.	Lingkungan pengembangan dan lingkungan produksi di organisasi telah dipisahkan pada seluruh aspek. Pemisahan yang menjadi standar operasi organisasi, membuat setiap unit kerja harus menerapkan pemisahan tersebut, proses tersebut dimonitoring, direviu secara berkala dan diperbaiki terus menerus oleh organisasi. Organisasi juga melakukan otomatisasi teknis jika memungkinkan.	- Dokumen arsitektur sistem yang menunjukkan pemisahan antara lingkungan pengembangan dan produksi pada seluruh aspek. - Kebijakan atau prosedur yang mengatur pemisahan lingkungan pengembangan dan produksi pada seluruh aspek. - Laporan audit atau penilaian keamanan yang memverifikasi pemisahan lingkungan pada seluruh aspek. - Protokol atau konfigurasi jaringan yang menunjukkan pemisahan antara jaringan pengembangan dan jaringan produksi pada seluruh aspek. - Daftar perangkat keras dan perangkat lunak yang digunakan secara terpisah untuk pengembangan dan produksi pada seluruh aspek. - Dokumentasi kontrol akses yang membatasi akses ke lingkungan produksi hanya untuk personel yang berwenang di setiap unit kerja. - Dokumentasi pengujian dan pemeliharaan yang dilakukan di lingkungan pengembangan tanpa mempengaruhi produksi di setiap unit kerja.

2.4.4. Mengimplementasikan prosedur pengembangan sistem yang aman

Kriteria	Detail
Deskripsi	Penyelenggara IIV menerapkan prosedur pengembangan sistem yang aman dengan memastikan setiap tahapan siklus hidup pengembangan perangkat lunak mempertimbangkan aspek keamanan. Prosedur ini mencakup perencanaan, perancangan, pengkodean, pengujian, hingga implementasi, dengan penerapan kontrol keamanan, pengujian kerentanan, dan mitigasi risiko secara berkelanjutan untuk menjaga kerahasiaan, integritas, dan ketersediaan sistem.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam pelatihan pengembang dan alat pengujian keamanan, tetapi tidak selalu membutuhkan teknologi tambahan yang mahal.
Dampak	**Tinggi** – Dengan prosedur pengembangan yang aman, organisasi dapat mengurangi risiko kerentanan keamanan dalam aplikasi dan memastikan bahwa perangkat lunak yang dikembangkan aman untuk digunakan.
Kompleksitas	**Sedang** – Memerlukan pengaturan proses pengembangan yang aman dan pengujian keamanan yang berkelanjutan.
Referensi Kontrol	**NIST CSF 2.0: PR.PS-06, ID.AM-08** **NIST CSF 1.1: PR.IP-2** **NIST SP 800-53r5: SA-3, SA-4, SA-8, SA-10, SA-11** **SNI ISO/IEC 27001:2022: 5.8, 8.25, 8.27**

87 Kontrol 2.4.4.a:

Kontrol	Tersedianya dan diterapkannya prosedur pengembangan perangkat lunak yang selalu memperhatikan aspek keamanan pada setiap tahapan siklus hidup pengembangannya.
Deskripsi Kontrol	Prosedur pengembangan perangkat lunak yang memperhatikan aspek keamanan pada setiap tahapan siklus hidup pengembangannya bertujuan untuk mengidentifikasi dan mengurangi potensi kerentanannya sejak dini. Keamanan harus dipertimbangkan dalam perencanaan, desain, pengembangan, pengujian, implementasi, dan pemeliharaan perangkat lunak. Hal ini melibatkan penerapan prinsip-prinsip seperti pengkodean aman (secure coding), uji penetrasi, penilaian kerentanannya, dan penerapan patch atau pembaruan keamanan secara berkala. Tujuan dari prosedur ini adalah untuk menghasilkan perangkat lunak yang aman, mencegah kerentanannya dieksploitasi, serta memastikan bahwa perangkat lunak dapat bertahan terhadap ancaman dan serangan siber yang terus berkembang.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak. - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi. - Laporan hasil pengujian kerentanannya (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya. - Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamananyang diterapkan dalampengembangan perangkat lunak (misalnya, ISO/IEC 27034 atau OWASP).
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH072 TH074 TH053 TH071 TH073
Referensi Kontrol	**NIST CSF 2.0: PR.PS-06, ID.AM-08** **NIST CSF 1.1: PR.IP-2** **NIST SP 800-53r5: SA-3, SA-4, SA-8, SA-10, SA-11** **SNI ISO/IEC 27001:2022: 5.8, 8.25, 8.27**

Kriteria Pemenuhan Kontrol 2.4.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pengembangan perangkat lunak yang memperhatikan aspek keamanan pada setiap tahapan siklus hidup pengembangannya. Tidak ada upaya yang dilakukan untuk mengintegrasikan keamanan dalam proses pengembangan.	Tidak ada	Tidak ada
1	Aspek keamanan mulai diperhatikan dalam sebagian kecil tahapan siklus hidup pengembangan perangkat lunak, tetapi belum ada prosedur formal yang mendokumentasikan atau mendukung penerapan tersebut. Keamanan belum menjadi bagian yang sistematis dalam proses pengembangan.	Organisasi memperhatikan aspek keamanan pada sebagian kecil tahapan siklus hidup pengembangan perangkat lunak, namun belum menjadi bagian sistematis dan tidak ada prosedur formal.	- Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak yang belum diformalkan. - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi yang belum diformalkan. - Laporan hasil pengujian kerentanan (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya. - Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi yang belum diformalkan. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamanan yang diterapkan dalam pengembangan perangkat lunak.
2	Keamanan sudah diperhatikan dalam sebagian besar tahapan siklus hidup pengembangan perangkat lunak, namun prosedur yang mengatur penerapan keamanan tersebut belum diformalkan. Semua aspek pengembangan sudah mencakup pertimbangan keamanan, tetapi tanpa dokumentasi resmi atau kebijakan yang mengaturnya.	Organisasi memperhatikan aspek keamanan pada sebagian besar tahapan siklus hidup pengembangan perangkat lunak, namun belum menjadi bagian sistematis dan tidak ada prosedur formal.	- Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak yang belum diformalkan. - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi yang belum diformalkan. - Laporan hasil pengujian kerentanan (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi yang belum diformalkan. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamanan yang diterapkan dalam pengembangan perangkat lunak.
3	Prosedur pengembangan perangkat lunak yang memperhatikan aspek keamanan sudah diterapkan di seluruh tahapan siklus hidup pengembangan dan telah diformalkan. Dokumentasi, kebijakan, dan prosedur yang mengatur keamanan dalam pengembangan perangkat lunak sudah tersedia dan diterapkan secara konsisten.	Organisasi memerhatikan aspek keamanan pada seluruh tahapan siklus hidup pengembangan perangkat lunak dan telah diformalkan.	- Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak dan telah diformalkan - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi dan telah diformalkan. - Laporan hasil pengujian kerentanan (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya. - Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi yang belum diformalkan. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamanan yang diterapkan dalam pengembangan perangkat lunak.
4	Selain penerapan dan formalisasi, prosedur pengembangan perangkat lunak yang memperhatikan aspek keamanan juga dimonitoring dan direviu secara berkala untuk memastikan efektivitasnya. Organisasi secara aktif mengevaluasi apakah prosedur tersebut masih relevan dan efisien seiring dengan perkembangan teknologi dan ancaman keamanan.	Organisasi memerhatikan aspek keamanan pada seluruh tahapan siklus hidup pengembangan perangkat lunak dan telah diformalkan. Organisasi juga mengevaluasi secara aktif prosedur tersebut.	- Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak dan telah diformalkan - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi dan telah diformalkan. - Laporan hasil pengujian kerentanan (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi yang belum diformalkan. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamanan yang diterapkan dalam pengembangan perangkat lunak.
5	Organisasi tidak hanya menerapkan, memformalkan, memonitoring, dan mereviu prosedur pengembangan perangkat lunak yang memperhatikan keamanan, tetapi juga secara aktif melakukan perbaikan berkelanjutan berdasarkan hasil reviu. Jika memungkinkan, otomatisasi proses keamanan dalam siklus hidup pengembangan diterapkan untuk meningkatkan efisiensi dan respons terhadap ancaman keamanan.	Organisasi memperhatikan aspek keamanan pada seluruh tahapan siklus hidup pengembangan perangkat lunak dan telah diformalkan. Organisasi juga mengevaluasi secara aktif prosedur tersebut dan melakukan otomatisasi jika memungkinkan.	- Kebijakan atau prosedur pengembangan perangkat lunak yang mencakup langkah-langkah keamanan di setiap tahapan siklus hidup perangkat lunak dan telah diformalkan - Panduan pengkodean aman (secure coding) yang diterapkan dalam organisasi dan telah diformalkan. - Laporan hasil pengujian kerentanan (vulnerability testing) yang dilakukan pada perangkat lunak selama pengembangan. - Dokumentasi proses pengujian keamanan seperti uji penetrasi danuji kerentanannya. - Protokol pemantauan dan pembaruan keamanan yang diterapkan pada perangkat lunak yang telah diproduksi yang belum diformalkan. - Catatan audit tentang evaluasi risiko dan mitigasi yang dilakukan selama siklus hidup perangkat lunak. - Sertifikasi atau standar keamanan yang diterapkan dalam pengembangan perangkat lunak.

2.5. Melindungi jaringan

Kategori ini berfokus pada penerapan kontrol dan mekanisme untuk menjaga keamanan jaringan organisasi dari akses yang tidak sah, serangan, maupun traffic jaringan yang berbahaya. Tujuannya adalah memastikan bahwa data yang dikirim dan diterima melalui jaringan tetap terjaga kerahasiaan, integritas, dan ketersediaannya. Upaya perlindungan jaringan mencakup penggunaan firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), segmentasi jaringan, pengamanan perangkat jaringan, serta pemantauan lalu lintas secara berkelanjutan. Melalui penerapan kebijakan dan teknologi yang tepat, organisasi dapat mengurangi risiko kompromi jaringan dan menjaga lingkungan TI tetap aman dari ancaman siber.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum;
b) menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali;
c) menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan;
d) memastikan integritas jaringan senantiasa dilindungi;
e) menerapkan prosedur dan teknologi pencegahan malware;
f) memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi; dan
g) memastikan bahwa informasi mengenai pelindungan terhadap teknologi dibagikan hanya kepada pihak tepercaya.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melindungi jaringan” secara efektif antara lain:

NIST CSF 2.0	**:**	**PR.DS-01, PR.PS-01, PR.IR-01, PR.IR-03, PR.PS-04, PR.AA-06, ID.IM-03**
NIST CSF 1.1	**:**	**PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4, PR.PT-5, PR.AC-5, PR.IP-8**
NIST SP 800-53r5	**:**	**AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16, AC-3, AC-4, AC-10, AC-12, AC-17, AC-18, AC-21, CM-7, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, CP-2, CP-7, CP-8, CP-11, CP-12, CP-13, SC-5, SC-6, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47, PE-11, PL-8, CA-7, IR-8, SI-4**
SNI ISO/IEC 27001:2022	**:**	**5.1, 5.10, 5.14, 5.15, 5.27, 5.29, 7.7, 7.10, 8.14, 8.15, 8.17, 8.20, 8.22, 8.34**

Peraturan BSSN Nomor 7 tahun 2024

Peraturan BSSN Nomor 11 Tahun 2024

2.5.1. Menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum

Kriteria	Detail
Deskripsi	Penyelenggara IIV menerapkan konfigurasi sistem berdasarkan prinsip fungsionalitas minimum dengan menonaktifkan atau memblokir secara fisik maupun logis port jaringan, USB, dan port serial yang tidak diperlukan untuk mencegah akses langsung ke komponen utama perangkat dan server. Selain itu, penggunaan removable media dibatasi dan dilindungi sesuai kebijakan keamanan yang berlaku guna mencegah penyalahgunaan, kebocoran data, dan potensi ancaman siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk mengidentifikasi dan menonaktifkan fungsi-fungsi yang tidak diperlukan, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan hanya mengaktifkan fungsi-fungsi yang diperlukan, organisasi dapat mengurangi risiko eksploitasi dan meningkatkan keamanan sistem.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif untuk menentukan fungsi-fungsi yang diperlukan dan menonaktifkan yang tidak diperlukan.
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.PS-01** **NIST CSF 1.1: PR.PT-2, PR.PT-3** **NIST SP 800-53r5: AC-3, CM-7, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8** **SNI ISO/IEC 27001:2022: 5.1, 5.10, 5.15, 7.7, 7.10**

88 Kontrol 2.5.1.a:

Kontrol	Minimalkan fungsi perangkat dan server dengan memblokir secara fisik dan logis port jaringan, USB, dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server.
Deskripsi Kontrol	Minimalkan fungsi perangkat dan server dengan memblokir secara fisik dan logis port yang tidak diperlukan untuk mengurangi potensi risiko keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Port yang tidak digunakan, seperti port jaringan, USB, dan port serial, harus diblokir baik secara fisik (misalnya dengan penutupan atau pengunci port) maupun secara logis (misalnya dengan konfigurasi firewall atau pengaturan sistem operasi untuk menonaktifkan port). Hal ini dilakukan untuk mencegah akses fisik maupun remote ke perangkat atau server yang dapat mengeksposnya terhadap ancaman. Tujuannya adalah untuk mengurangi permukaan serangan dan memastikan bahwa hanya port yang diperlukan yang dapat diakses oleh perangkat atau server tersebut.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan dan prosedur terkait pengelolaan port pada perangkat dan server. - Laporan audit yang menunjukkan status port yang telah diblokir atau dinonaktifkan pada perangkat dan server. - Konfigurasi perangkat jaringan, firewall, dan sistem operasi yang menunjukkan port mana yang diblokir atau dinonaktifkan. - Catatan pengujian kerentanannya yang dilakukan untuk memastikan bahwa port yang tidak digunakan benarbenar tidak dapat diakses. - Dokumentasi fisik terkait penguncian atau penutupan port perangkat, seperti catatan perawatan perangkat keras atau manual penggunaan perangkat. - Laporan yang mencatat pemantauan dan evaluasi terhadap akses perangkat secara berkala, serta tindakan yang diambil untuk menutup port yang tidak diperlukan
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH072 TH074 TH053 TH071 TH073
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.PS-01** **NIST CSF 1.1: PR.PT-2, PR.PT-3** **NIST SP 800-53r5: AC-3, CM-7, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8** **SNI ISO/IEC 27001:2022: 5.1, 5.10, 5.15, 7.7, 7.10**

Kriteria Pemenuhan Kontrol 2.5.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan pemblokiran secara fisik dan logis port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server	Tidak ada	Tidak ada
1	Organisasi sudah menerapkan pemblokiran secara fisik dan logis pada sebagian kecil port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server, tetapi kebijakan/prosedur penerapan pemblokiran tersebut belum diformalkan	Beberapa perangkat telah dikonfigurasi untuk menonaktifkan port USB atau port jaringan yang tidak digunakan namun belum ada kebijakan resmi.	- Dokumentasi konfigurasi menunjukkan perangkat telah dikonfigurasi untuk memblokir sebagian kecil port jaringan, USB, dan dan port serial yang tidak perlu. - Tidak ada SOP atau kebijakan hardening yang mendukung penerapan pemblokiran.
2	Organisasi sudah menerapkan pemblokiran secara fisik dan logis pada sebagian besar port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server, tetapi kebijakan/prosedur penerapan pemblokiran tersebut belum diformalkan	Sebagian besar perangkat telah dikonfigurasi untuk menonaktifkan port USB atau port jaringan yang tidak digunakan namun belum ada kebijakan resmi.	- Dokumentasi konfigurasi menunjukkan perangkat telah dikonfigurasi untuk memblokir sebagian besar port jaringan, USB, dan dan port serial yang tidak perlu. - Tidak ada kebijakan atau SOP yang terdokumentasi secara resmi.
3	Organisasi sudah menerapkan pemblokiran secara fisik dan logis pada seluruh port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server, dan kebijakan/prosedur penerapan pemblokiran tersebut sudah diformalkan.	- Semua port yang tidak diperlukan telah diblokir secara menyeluruh pada perangkat dan server. - Terdapat SOP atau kebijakan resmi yang mengatur pemblokiran port	- SOP atau kebijakan hardening perangkat telah tersedia dan diimplementasikan. - Dokumentasi konfigurasi menunjukkan semua port yang tidak perlu telah diblokir.
4	Organisasi sudah menerapkan pemblokiran secara fisik dan logis pada seluruh port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server, dan kebijakan/prosedur penerapan pemblokiran tersebut sudah diformalkan, dimonitoring, dan direviu secara berkala	- Semua port yang tidak diperlukan telah diblokir secara menyeluruh pada perangkat dan server. - Pemantauan berkala terhadap akses ke port. Salah satu metode yang dapat digunakan adalah dengan menggunakan SIEM (Security Information and Event Management). - Log akses port direkam untuk mendeteksi upaya akses yang mencurigakan	- SOP dan kebijakan telah mencantumkan mekanisme monitoring dan reviu berkala. - Dokumentasi konfigurasi perangkat mencatat pengaturan pemantauan akses ke port. - Log keamanan menunjukkan aktivitas akses ke port yang diblokir

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi sudah menerapkan pemblokiran secara fisik dan logis pada seluruh port jaringan, USB, dan dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server, dan kebijakan/prosedur penerapan pemblokiran tersebut sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan atau otomatisasi pemblokiran	- Semua port yang tidak diperlukan telah diblokir secara menyeluruh pada perangkat dan server. - Pemantauan berkala terhadap akses ke port. Salah satu metode yang dapat digunakan adalah dengan menggunakan SIEM (Security Information and Event Management). - Log akses port direkam untuk mendeteksi upaya akses yang mencurigakan. - Implementasi pemblokiran port dilakukan secara otomatis, misal dengan menggunakan GPO (Group Policy Object), NAC (Network Access Control), ataupun sistem lainnya. - Kebijakan terus diperbarui sesuai dengan hasil evaluasi dan tren ancaman terbaru	- SOP dan kebijakan hardening mencakup otomatisasi pemblokiran dan pembaruan berkala. - Dokumentasi konfigurasi menunjukkan penggunaan sistem otomatis untuk pemblokiran port. - Laporan audit mencatat perbaikan dan pembaruan konfigurasi secara berkala. - Log keamanan menunjukkan pemblokiran otomatis terhadap upaya akses tidak sah

89 Kontrol 2.5.1.b:

Kontrol	Memastikan Removable Media terlindungi dan penggunaannya terbatas sesuai dengan kebijakan
Deskripsi Kontrol	Memastikan removable media, seperti USB flash drive, CD/DVD, atau hard drive eksternal, terlindungi dan penggunaannya dibatasi sesuai kebijakan organisasi untuk mengurangi risiko terhadap data dan sistem organisasi. Kebijakan ini harus mencakup aturan tentang siapa yang dapat menggunakan media tersebut, jenis data apa yang dapat dipindahkan, dan langkah-langkah keamanan yang harus diterapkan, seperti enkripsi, penggunaan kata sandi, atau pembatasan akses hanya untuk perangkat yang terverifikasi. Tujuannya adalah untuk mencegah kehilangan, pencurian, atau penyebaran data yang tidak sah serta mengurangi risiko infeksi malware atau ancaman lainnya melalui media yang dapat dilepas
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan penggunaan removable media yang mengatur prosedur dan pembatasan terkait penggunaan perangkat tersebut. - Laporan pemantauan dan audit yang mencatat penggunaan removable media di lingkungan organisasi. - Protokol keamanan yang diterapkan, seperti enkripsi atau penggunaan kata sandi pada removable media. - Daftar perangkat yang telah diautentikasi atau disetujui untuk digunakan dengan sistem organisasi. - Dokumentasi prosedur pembersihan atau penghapusan data pada media yang telah digunakan. - Laporan dan bukti pengujian keamanan, seperti uji malware atau analisis keamanan terhadap removable media yang digunakan dalam organisasi
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH073 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.DS-01, PR.PS-01** **NIST CSF 1.1: PR.PT-2, PR.PT-3** **NIST SP 800-53r5: AC-3, CM-7, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8** **SNI ISO/IEC 27001:2022: 5.1, 5.10, 5.15, 7.7, 7.10**

Kriteria Pemenuhan Kontrol 2.5.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memastikan Removable Media terlindungi dan pembatasan penggunaannya	Tidak ada	Tidak ada
1	Organisasi sudah menerapkan pelindungan dan pembatasan penggunaan pada sebagian kecil Removable Media tetapi kebijakannya belum diformalkan	Beberapa perangkat removable media diberi pembatasan namun belum didukung kebijakan formal.	- Daftar removable media parsial - Log pembatasan - Bukti kontrol teknis sebagian perangkat
2	Organisasi sudah menerapkan pelindungan dan pembatasan penggunaan pada sebagian besar Removable Media tetapi kebijakannya belum diformalkan	Mayoritas removable media sudah dikendalikan, namun belum terdokumentasi dalam kebijakan resmi.	- Daftar removable media mencakup sebagian besar perangkat - Bukti konfigurasi pembatasan sebagian besar removable media. - Kebijakan masih berupa draft atau belum diresmikan
3	Organisasi sudah menerapkan pelindungan dan pembatasan penggunaan pada seluruh Removable Media sesuai dengan kebijakan yang sudah diformalkan	Kebijakan tertulis disahkan, mencakup semua jenis Removable media	- Kebijakan Removable media yang telah disahkan - Daftar seluruh removable media terkelola - Bukti konfigurasi pembatasan sebagian besar removable media
4	Organisasi sudah menerapkan pelindungan dan pembatasan penggunaan pada seluruh Removable Media sesuai dengan kebijakan yang sudah diformalkan, dimonitoring, dan direviu secara berkala	Kebijakan tertulis disahkan, mencakup semua jenis Removable media serta telah dilakukan monitoring dan evaluasi terhadap efektivitas pengendalian removable media.	- Kebijakan Removable media yang telah disahkan - Daftar seluruh removable media terkelola - Bukti konfigurasi kontrol (Misalnya Group Policy Object (GPO)) - Laporan monitoring (Contoh log monitoring removable media) - Evaluasi kepatuhan pengguna terhadap kebijakan
5	Organisasi sudah menerapkan pelindungan dan pembatasan penggunaan pada seluruh Removable Media sesuai dengan kebijakan yang sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	Kebijakan tertulis disahkan, mencakup semua jenis Removable media serta telah dilakukan monitoring dan evaluasi terhadap efektivitas pengendalian removable media. Selain melakukan monitoring dan reviu berkala, organisasi juga menerapkan perbaikan atau otomatisasi, seperti penggunaan endpoint security untuk membatasi akses removable media secara otomatis	- Kebijakan removable media yang telah disahkan dan senantiasa diperbarui sesuai kebutuhan dan kondisi organisasi - Daftar seluruh removable media terkelola - Bukti konfigurasi kontrol (Misalnya Group Policy Object (GPO)) - Laporan monitoring (Contoh log monitoring removable media) - Bukti penggunaan tools otomatisasi berupa endpoint security untuk membatasi akses removable media secara otomatis - Bukti peningkatan kepatuhan (contoh: penurunan pelanggaran penggunaan Removable media)

2.5.2. Menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali

Kriteria	Detail
Deskripsi	Penyelenggara IIV melindungi jaringan komunikasi, akses sistem informasi, dan sistem kendali dengan menerapkan segmentasi atau zonasi jaringan sesuai fungsi, seperti lingkungan pengembangan, pengujian, produksi, dan area lain dalam organisasi. Jaringan yang terhubung ke perangkat penting, termasuk SCADA atau ICS, diisolasi secara ketat untuk mencegah akses tidak sah dan mengurangi risiko gangguan terhadap operasi kritis.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pelindungan jaringan seperti firewall, IDS/IPS, dan sistem autentikasi.
Dampak	**Tinggi** – Melindungi komunikasi dan akses sistem dari ancaman dan akses tidak sah, sehingga menjaga integritas dan kerahasiaan data.
Kompleksitas	**Sedang** – Memerlukan pengaturan dan pemeliharaan sistem pelindungan jaringan yang efektif.
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01, PR.AA-06** **NIST CSF 1.1: PR.PT-4** **NIST SP 800-53r5: AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47** **SNI ISO/IEC 27001:2022: 5.14, 8.20**

90 Kontrol 2.5.2.a:

Kontrol	Organisasi menentukan dan menerapkan segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet. (misalnya dibagi menjadi lingkungan pengembangan, pengujian, lingkungan produksi, dan lingkungan lain dalam organisasi)
Deskripsi Kontrol	Segmentasi jaringan atau pembagian zonasi bertujuan untuk memisahkan berbagai bagian atau fungsi organisasi yang memiliki kebutuhan keamanan dan operasional yang berbeda, seperti lingkungan pengembangan, pengujian, dan produksi. Pembagian ini mengurangi kemungkinan dampak dari ancaman atau serangan yang dapat menyebar antar lingkungan yang berbeda, serta mempermudah implementasi kontrol keamanan yang spesifik pada masing-masing zona. Hal ini juga membantu dalam mengelola akses, pemantauan, dan mitigasi risiko yang lebih efisien. Segmentasi jaringan yang tepat dapat mengurangi kerentanannya terhadap potensi ancaman dan mengoptimalkan pemisahan tugas antara sistem kritis dan non-kritis.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur internal yang mengatur segmentasi atau pembagian zona jaringan dalam organisasi. - Diagram jaringan yang menunjukkan pembagian zona atau segmentasi lingkungan yang berbeda (misalnya pengembangan, pengujian, dan produksi). - Dokumentasi tentang penerapan kontrol akses dan pemantauan untuk setiap zona jaringan yang tersegmentasi. - Laporan audit dan pengujian yang menunjukkan bahwa pembagian zona telah diterapkan dengan benar dan aman. - Prosedur dan dokumentasi terkait dengan pengelolaan akses dan isolasi antar zona untuk mencegah pergerakan lateral antar lingkungan yang terpisah. - Analisis risiko yang mendokumentasikan alasan dan manfaat dari segmentasi jaringan yang diterapkan.
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH072 TH074 TH053 TH071 TH073
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01, PR.AA-06** **NIST CSF 1.1: PR.PT-4** **NIST SP 800-53r5: AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47** **SNI ISO/IEC 27001:2022: 5.14, 8.20**

Kriteria Pemenuhan Kontrol 2.5.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menerapkan segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet.	Tidak ada	Tidak ada
1	Organisasi sudah menentukan dan menerapkan sebagian kecil segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet, tetapi kebijakan/prosedurnya belum diformalkan	Hanya beberapa bagian dari jaringan, yang dipisahkan dari jaringan utama (contohnya telah dibentuk beberapa segmentasi jaringan (VLAN)), tetapi tidak ada aturan formal mengenai segmentasi ini	- Dokumentasi awal segmentasi jaringan. - Konfigurasi VLAN atau subnetting beberapa jaringan
2	Organisasi sudah menentukan dan menerapkan sebagian besar segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet, tetapi kebijakan/prosedurnya belum diformalkan	Sebagian besar jaringan telah dipisahkan dari jaringan utama (contohnya telah dibentuk beberapa segmentasi jaringan (VLAN)), tetapi tidak ada aturan formal mengenai segmentasi ini	- Topologi jaringan yang menunjukkan sebagian besar segmentasi. - Konfigurasi firewall atau VLAN yang mengatur sebagian besar jaringan - Kebijakan keamanan jaringan berbentuk draft/belum resmi.
3	Organisasi sudah menentukan dan menerapkan seluruh segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet, dan kebijakan/prosedurnya sudah diformalkan.	- Seluruh jaringan telah dibagi ke dalam zona yang jelas dengan aturan akses yang sesuai, dan kebijakan sudah terdokumentasi. - Kebijakan jaringan resmi disahkan, mencakup segmentasi lengkap (contohnya: DMZ untuk layanan publik) dengan aturan akses dan enkripsi data	- Topologi sistem/jaringan yang menunjukkan segmentasi dari keseluruhan jaringan. - Bukti konfigurasi teknis seluruh jaringan (Contoh VLAN, firewall, ACL, dll). - Kebijakan keamanan jaringan yang telah diformalkan.
4	Organisasi sudah menentukan dan menerapkan seluruh segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Seluruh jaringan telah dibagi ke dalam zona yang jelas dengan aturan akses yang sesuai, dan kebijakan sudah terdokumentasi. - Kebijakan jaringan resmi disahkan, mencakup segmentasi lengkap (contohnya: DMZ untuk layanan publik) dengan aturan akses dan enkripsi data - Organisasi telah melakukan pemantauan terhadap lalu lintas jaringan dan meninjau efektivitas segmentasi jaringan secara berkala	- Topologi sistem/jaringan yang menunjukkan segmentasi dari keseluruhan jaringan. - Bukti konfigurasi teknis seluruh jaringan (Contoh VLAN, firewall, ACL, dll). - Kebijakan keamanan jaringan yang telah diformalkan - Log monitoring jaringan untuk memantau lalu lintas antar zona. - Dokumen evaluasi segmentasi dan/atau pembagian zonasi jaringan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi sudah menentukan dan menerapkan seluruh segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Seluruh jaringan telah dibagi ke dalam zona yang jelas dengan aturan akses yang sesuai, dan kebijakan sudah terdokumentasi - Kebijakan jaringan resmi disahkan, mencakup segmentasi lengkap (contohnya: DMZ untuk layanan publik) dengan aturan akses dan enkripsi data - Organisasi telah melakukan pemantauan terhadap lalu lintas jaringan dan meninjau efektivitas segmentasi jaringan secara berkala serta melakukan perbaikan atau otomatisasi	- Topologi sistem/jaringan yang menunjukkan segmentasi dari keseluruhan jaringan. - Bukti konfigurasi teknis seluruh jaringan (Contoh VLAN, firewall, ACL, dll). - Kebijakan keamanan jaringan yang telah diformalkan - Log monitoring jaringan untuk memantau lalu lintas antar zona. - Dokumen evaluasi segmentasi dan/atau pembagian zonasi jaringan - Dokumen tindakan perbaikan (revisi kebijakan, update konfigurasi). - Bukti peningkatan keamanan (misalnya penurunan insiden intrusi antar-zona).

91 Kontrol 2.5.2.b:

Kontrol	Organisasi juga melakukan isolasi terhadap jaringan yang menghubungkan dengan perangkat penting, misalnya perangkat SCADA atau ICS (Industrial Control System).
Deskripsi Kontrol	Isolasi jaringan yang menghubungkan dengan perangkat penting, seperti SCADA atau ICS, bertujuan untuk meminimalkan potensi risiko terhadap sistem yang memiliki fungsi kritis. Dengan isolasi, perangkat-perangkat ini dipisahkan dari jaringan yang lebih luas untuk mencegah akses tidak sah dan mengurangi kemungkinan dampak dari serangan yang dapat mengganggu operasi penting. Isolasi ini bisa melibatkan penggunaan jaringan terpisah, firewall, atau kontrol akses yang ketat yang membatasi komunikasi antara sistem SCADA/ICS dan jaringan lainnya. Hal ini juga mencakup pembatasan akses fisik dan virtual, serta pemantauan dan pengujian yang intensif untuk memastikan keamanan sistem.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur yang mengatur isolasi jaringan untuk perangkat penting seperti SCADA atau ICS. - Diagram jaringan yang menunjukkan pemisahan antara jaringan perangkat penting dan jaringan lain dalam organisasi. - Laporan audit dan pengujian yang menunjukkan penerapan isolasi yang efektif pada sistem SCADA atau ICS. - Catatan konfigurasi dan pengaturan firewall atau perangkat keamanan lainnya yang digunakan untuk isolasi jaringan. - Dokumentasi tentang kontrol akses yang diterapkan untuk membatasi komunikasi antar jaringan, termasuk kontrol terhadap perangkat yang dapat terhubung ke perangkat ICS. - Analisis risiko yang menggambarkan pentingnya isolasi jaringan untuk mencegah ancaman yang dapat mengakses perangkat dan sistem kritis.
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH072 TH074 TH053 TH071 TH073
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01, PR.AA-06** **NIST CSF 1.1: PR.PT-4** **NIST SP 800-53r5: AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47** **SNI ISO/IEC 27001:2022: 5.14, 8.20**

Kriteria Pemenuhan Kontrol 2.5.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan isolasi terhadap jaringan yang menghubungkan dengan perangkat penting.	Tidak ada	Tidak ada
1	Organisasi sudah melakukan isolasi terhadap sebagian kecil jaringan yang menghubungkan dengan perangkat penting, tetapi kebijakan/prosedurnya belum diformalkan	Sebagian kecil perangkat penting (contoh: SCADA atau ICS) telah dipisahkan dari jaringan umum, tanpa standar yang terdokumentasi	- Topologi yang menunjukkan isolasi sebagian kecil jaringan - Tidak ada dokumen kebijakan tertulis atau terdapat dokumen kebijakan namun belum diformalkan
2	Organisasi sudah melakukan isolasi terhadap sebagian besar jaringan yang menghubungkan dengan perangkat penting, tetapi kebijakan/prosedurnya belum diformalkan	Sebagian besar perangkat penting (contoh: SCADA atau ICS) dipisahkan dari jaringan umum tetapi tanpa standar yang terdokumentasi	- Topologi yang menunjukkan isolasi sebagian besar jaringan - Tidak ada dokumen kebijakan tertulis atau terdapat dokumen kebijakan namun belum diformalkan
3	Organisasi sudah melakukan isolasi terhadap seluruh jaringan yang menghubungkan dengan perangkat penting, dan kebijakan/prosedurnya sudah diformalkan.	Semua perangkat kritikal telah dipisahkan dalam jaringan khusus, serta terdapat kebijakan yang mendukung implementasi ini	- Topologi jaringan lengkap menunjukkan isolasi total. - Kebijakan keamanan jaringan resmi.
4	Organisasi sudah melakukan isolasi terhadap seluruh jaringan yang menghubungkan dengan perangkat penting, dan kebijakan/prosedurnya sudah diformalkan, dan direviu secara berkala	- Semua perangkat kritikal telah dipisahkan dalam jaringan khusus, serta terdapat kebijakan yang mendukung implementasi ini. - Terdapat proses peninjauan rutin atas kebijakan dan kondisi jaringan kritikal.	- Topologi jaringan lengkap menunjukkan isolasi total. - Kebijakan keamanan jaringan resmi. - Dokumen hasil reviu kebijakan jaringan.
5	Organisasi sudah melakukan isolasi terhadap seluruh jaringan yang menghubungkan dengan perangkat penting, dan kebijakan/prosedurnya sudah diformalkan, direviu secara berkala, dan dilakukan perbaikan	- Semua perangkat kritikal telah dipisahkan dalam jaringan khusus, serta terdapat kebijakan yang mendukung implementasi ini. - Terdapat proses peninjauan rutin atas kebijakan dan kondisi jaringan kritikal. - Organisasi melakukan perbaikan atau adaptasi berdasarkan hasil evaluasi (misalnya segmentasi tambahan, penggunaan firewall industri, Intrusion Detection System (IDS), dll).	- Topologi jaringan lengkap menunjukkan isolasi total. - Kebijakan keamanan jaringan resmi. - Dokumen hasil reviu kebijakan jaringan. - Bukti implementasi kontrol tambahan (misalnya segmentasi tambahan, penggunaan firewall industri, Intrusion Detection System (IDS), dll).

2.5.3. Menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan

Kriteria	Detail
Deskripsi	Penyelenggara IIV memastikan penggunaan perangkat jaringan yang mendukung fungsi keamanan, termasuk mekanisme seperti fail safe, load balancing, atau hot swap, untuk menjamin ketahanan sistem baik dalam kondisi normal maupun situasi darurat. Fungsi keamanan pada perangkat tersebut dioptimalkan sesuai kebutuhan dan didukung dengan sertifikat keamanan yang valid, sehingga keandalan dan perlindungan jaringan tetap terjaga.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam perangkat jaringan yang memiliki fungsi keamanan seperti firewall, router dengan ACL, dan switch dengan VLAN.
Dampak	**Tinggi** – Dengan menggunakan perangkat jaringan yang memiliki fungsi keamanan, organisasi dapat mengurangi risiko serangan dan meningkatkan keamanan jaringan secara keseluruhan.
Kompleksitas	**Sedang** – Memerlukan pengaturan dan pemeliharaan perangkat jaringan dengan fitur keamanan yang tepat.
Referensi Kontrol	**NIST CSF 2.0: PR.IR-03** **NIST CSF 1.1: PR.PT-5** **NIST SP 800-53r5: CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6** **SNI ISO/IEC 27001:2022: 5.29, 8.14**

92 Kontrol 2.5.3.a:

Kontrol	Memastikan perangkat jaringan mampu menerapkan mekanisme (misalnya, fail safe, load balancer, atau hot swap) yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan
Deskripsi Kontrol	Perangkat jaringan harus mampu menerapkan mekanisme yang memastikan ketersediaan dan ketahanan sistem dalam situasi normal maupun situasi yang merugikan (seperti gangguan atau serangan). Mekanisme seperti failover, load balancing, dan hot swap berfungsi untuk menjaga kelangsungan operasi, mengurangi downtime, dan meningkatkan kinerja serta ketahanan infrastruktur jaringan. Failover memungkinkan perangkat untuk secara otomatis beralih ke perangkat cadangan saat terjadi kegagalan, load balancer membagi beban lalu lintas secara merata untuk meningkatkan kinerja, dan hot swap memungkinkan perangkat diganti tanpa menghentikan operasi sistem. Tujuan dari mekanisme ini adalah untuk memastikan bahwa jaringan tetap tersedia dan berfungsi dengan baik meskipun ada gangguan atau kerusakan
Deskripsi Bukti Dukung	- Dokumen kebijakan dan prosedur yang menggambarkan penerapan mekanisme ketahanan jaringan (failover, load balancer, hot swap). - Diagram arsitektur jaringan yang menunjukkan bagaimana mekanisme ketahanan diterapkan. - Catatan konfigurasi perangkat jaringan yang mendukung failover dan load balancing. - Laporan pengujian ketahanan (misalnya, pengujian failover dan load balancing) yang menunjukkan bagaimana perangkat menangani situasi merugikan. - Bukti implementasi hot swap pada perangkat jaringan yang digunakan. - Protokol pemantauan dan pelaporan kinerja jaringan untuk memastikan mekanisme ketahanan berfungsi dengan baik. - Audit laporan dari pengujian pemulihan bencana yang melibatkan perangkat jaringan
Ancaman/Risiko yang dimitigasi	TH013 TH015 TH017 TH024 TH077 TH014 TH016 TH023 TH070
Referensi Kontrol	**NIST CSF 2.0: PR.IR-03** **NIST CSF 1.1: PR.PT-5** **NIST SP 800-53r5: CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6** **SNI ISO/IEC 27001:2022: 5.29, 8.14**

Kriteria Pemenuhan Kontrol 2.5.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memastikan perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan	Tidak Ada	Tidak Ada
1	Organisasi telah memastikan sebagian kecil perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan, tetapi kebijakan/prosedurnya belum diformalkan	Sebagian kecil perangkat memiliki konfigurasi failover atau hot swap, belum disertai kebijakan atau prosedur formal	- Topologi yang menunjukkan failover pada sebagian kecil sistem/perangkat. - Belum ada kebijakan formal atau masih dalam bentuk draft
2	Organisasi telah memastikan sebagian besar perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan, tetapi kebijakan/prosedurnya belum diformalkan	Sebagian besar perangkat penting sudah memiliki konfigurasi ketahanan, namun kebijakan/prosedur belum tersedia	- Topologi yang menunjukkan failover pada sebagian besar sistem/perangkat. - Belum ada kebijakan formal atau masih dalam bentuk draft. - Daftar perangkat kritikal lengkap.
3	Organisasi telah memastikan seluruh perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan, dan kebijakan/prosedurnya sudah diformalkan	Seluruh perangkat kritikal telah mengimplementasikan fail safe/load balancer/hot swap, dan kebijakan formal sudah ditetapkan	- Topologi sistem menunjukkan ketahanan menyeluruh - Kebijakan Redundansi/HA berlaku aktif - Daftar perangkat kritikal lengkap dan terdokumentasi
4	Organisasi telah memastikan seluruh perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Seluruh perangkat kritikal telah mengimplementasikan fail safe/load balancer/hot swap, dan kebijakan formal sudah ditetapkan - Terdapat evaluasi periodik terhadap efektivitas ketahanan jaringan dan dokumentasi hasil evaluasi	- Topologi sistem menunjukkan ketahanan menyeluruh - Kebijakan Redundansi/HA berlaku aktif - Daftar perangkat kritikal lengkap dan terdokumentasi - Laporan hasil reviu kebijakan dan sistem ketahanan - Bukti pelaksanaan simulasi failover/load balancing

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi telah memastikan seluruh perangkat jaringan mampu menerapkan mekanisme yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan atau otomatisasi	- Seluruh perangkat kritikal telah mengimplementasikan fail safe/load balancer/hot swap, dan kebijakan formal sudah ditetapkan - Terdapat evaluasi periodik terhadap efektivitas ketahanan jaringan dan dokumentasi hasil evaluasi - Organisasi mengimplementasikan perbaikan dan otomatisasi (misal dynamic load balancing, self-healing network)	- Topologi sistem menunjukkan ketahanan menyeluruh - Kebijakan Redundansi/HA berlaku aktif - Daftar perangkat kritikal lengkap dan terdokumentasi - Laporan hasil reviu kebijakan dan sistem ketahanan - Bukti pelaksanaan simulasi failover/load balancing - Bukti penerapan sistem otomatis HA

93 Kontrol 2.5.3.b:

Kontrol	Memastikan fungsi keamanan pada perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan.
Deskripsi Kontrol	Fungsi keamanan pada perangkat jaringan harus dapat diakses dan digunakan sesuai dengan kebutuhan operasional organisasi serta sesuai dengan sertifikat keamanan yang dimiliki perangkat tersebut. Fungsi keamanan ini mencakup mekanisme perlindungan seperti firewall, sistem deteksi intrusi (IDS), enkripsi, kontrol akses, dan lainnya, yang diatur dan dipelihara agar dapat berfungsi dengan efektif. Sertifikat keamanan, seperti sertifikat SSL/TLS atau sertifikat kepatuhan industri, digunakan untuk memastikan bahwa perangkat jaringan telah memenuhi standar keamanan yang diakui. Tujuan dari pengelolaan fungsi keamanan ini adalah untuk memastikan bahwa perangkat jaringan tidak hanya aman, tetapi juga dapat diandalkan dalam memenuhi kebutuhan perlindungan data dan jaringan organisasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Dokumen sertifikat keamanan perangkat atau Surat keterangan Verifikasi dan/ atau Rekognisi - Catatan konfigurasi perangkat jaringan yang memastikan fungsi keamanan teraktifkan (misalnya, konfigurasi firewall, enkripsi, IDS/IPS). - Laporan audit keamanan yang menunjukkan penggunaan dan efektivitas fungsi keamanan pada perangkat jaringan. - Laporan pengujian fungsionalitas untuk memastikan bahwa mekanisme keamanan bekerja sesuai kebutuhan. - Dokumentasi prosedur pengelolaan dan pemeliharaan perangkat keamanan yang mencakup pembaruan perangkat lunak dan perangkat keras secara berkala. - Protokol pemantauan dan pelaporan yang mendokumentasikan status operasional dan efektivitas fungsi keamanan pada perangkat jaringan. - Hasil uji penetrasi atau evaluasi keamanan yang menunjukkan kepatuhan perangkat jaringan terhadap persyaratan keamanan
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH046 TH071 TH036 TH044 TH047
Referensi Kontrol	**NIST CSF 2.0: PR.IR-03** **NIST CSF 1.1: PR.PT-5** **NIST SP 800-53r5: CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6** **SNI ISO/IEC 27001:2022: 5.29, 8.14** **Peraturan BSSN Nomor 7 tahun 2024** **Peraturan BSSN Nomor 11 Tahun 2024**

Kriteria Pemenuhan Kontrol 2.5.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memastikan fungsi keamanan pada perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan	Tidak Ada	Tidak Ada
1	Organisasi telah memastikan fungsi keamanan pada sebagian kecil perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan, tetapi kebijakan/prosedurnya belum diformalkan	Fungsi keamanan hanya diterapkan pada sebagian kecil perangkat, belum ada kebijakan/prosedur formal	- Dokumentasi fungsi keamanan - Daftar spesifikasi pada sebagian kecil perangkat yang menunjukkan fitur keamanan. - Label atau sertifikat CC/SCCI pada sebagian kecil perangkat - Belum terdapat SOP yang disahkan atau diresmikan
2	Organisasi telah memastikan fungsi keamanan pada sebagian besar perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan, tetapi kebijakan/prosedurnya belum diformalkan	Fungsi keamanan diterapkan di sebagian besar perangkat, namun belum ada kebijakan/prosedur formal	- Dokumentasi fungsi keamanan - Daftar spesifikasi pada sebagian besar perangkat yang menunjukkan fitur keamanan. - Label atau sertifikat CC/SCCI pada sebagian besar perangkat - Belum terdapat SOP yang disahkan atau diresmikan
3	Organisasi telah memastikan fungsi keamanan pada seluruh perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan, dan kebijakan/prosedurnya sudah diformalkan	Fungsi keamanan sudah diterapkan di seluruh perangkat jaringan, dan terdapat kebijakan/prosedur formal	- Dokumentasi fungsi keamanan - Daftar spesifikasi seluruh perangkat mencakup fitur keamanan - Sertifikat CC/SCCI seluruh perangkat - Kebijakan Pengadaan Perangkat - SOP UAT Perangkat - SOP fungsi keamanan perangkat jaringan
4	Organisasi telah memastikan fungsi keamanan pada seluruh perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Fungsi keamanan sudah diterapkan di seluruh perangkat jaringan, dan terdapat kebijakan/prosedur formal - Fungsi keamanan dimonitor secara aktif dan dilakukan reviu berkala terhadap prosedur dan penerapan.	- Dokumentasi fungsi keamanan - Daftar spesifikasi seluruh perangkat mencakup fitur keamanan - Sertifikat CC/SCCI seluruh perangkat - Kebijakan Pengadaan Perangkat - SOP UAT Perangkat - SOP fungsi keamanan perangkat jaringan - Laporan hasil monitoring perangkat - Jadwal dan hasil reviu berkala

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi telah memastikan fungsi keamanan pada seluruh perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan, dan kebijakan/prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Fungsi keamanan sudah diterapkan di seluruh perangkat jaringan, dan terdapat kebijakan/prosedur formal - Fungsi keamanan dimonitor secara aktif dan dilakukan reviu berkala terhadap prosedur dan penerapan. - Evaluasi dan perbaikan dilakukan berdasarkan hasil monitoring/pentest/VA untuk meningkatkan efektivitas kontrol.	- Dokumentasi fungsi keamanan - Daftar spesifikasi seluruh perangkat mencakup fitur keamanan - Sertifikat CC/SCCI seluruh perangkat - Kebijakan Pengadaan Perangkat - SOP UAT Perangkat - SOP fungsi keamanan perangkat jaringan - Laporan hasil monitoring perangkat - Jadwal dan hasil reviu berkala - Bukti pelaksanaan VA/Pentest dan tindak lanjutnya - Hasil audit internal/eksternal - Revisi SOP atau kebijakan pengadaan berdasarkan evaluasi

2.5.4. Memastikan integritas jaringan senantiasa dilindungi

Kriteria	Detail
Deskripsi	Penyelenggara IIV memastikan integritas jaringan terlindungi melalui prosedur pengujian dan pemantauan berkala terhadap konfigurasi jaringan. Langkah ini mencakup verifikasi segmentasi jaringan agar sesuai dengan desain keamanan yang ditetapkan, sehingga potensi akses tidak sah dan risiko gangguan dapat diminimalkan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan teknologi pemantauan dan pelindungan jaringan, serta sumber daya untuk pemeliharaan berkala.
Dampak	**Tinggi** – Dengan melindungi integritas jaringan, organisasi dapat memastikan bahwa data yang dikirim tetap utuh dan tidak berubah selama pengiriman.
Kompleksitas	**Sedang** – Memerlukan sistem pemantauan yang tepat dan prosedur untuk melindungi integritas jaringan.
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01** **NIST CSF 1.1: PR.AC-5** **NIST SP 800-53r5: AC-4, AC-10, SC-7, SC-10, SC-20** **SNI ISO/IEC 27001:2022: 5.14, 8.20, 8.22**

94 Kontrol 2.5.4.a:

Kontrol	Tersedianya prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai.
Deskripsi Kontrol	Prosedur pelindungan terhadap integritas jaringan melibatkan pengujian dan pemantauan konfigurasi jaringan secara berkala untuk memastikan bahwa pengaturan jaringan, seperti segmentasi, telah diterapkan dengan benar dan berfungsi sebagaimana mestinya. Segmentasi jaringan adalah metode untuk membagi jaringan menjadi bagian-bagian yang lebih kecil untuk membatasi penyebaran ancaman dan mengisolasi aset yang lebih kritis. Pengujian dan monitoring ini bertujuan untuk mendeteksi dan mencegah perubahan atau pengaturan yang tidak sah serta mengidentifikasi potensi kerentanannya. Prosedur ini juga mencakup pemantauan kinerja jaringan, audit konfigurasi, dan pemeriksaan kontrol akses di setiap segmen jaringan untuk menjaga integritas dan keamanan data serta mencegah akses yang tidak sah.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan pengujian segmentasi jaringan, termasuk hasil evaluasi keamanan dari pengaturan segmentasi yang ada. - Dokumentasi konfigurasi jaringan yang mencakup segmentasi dan pembatasan akses antara segmen. - Protokol pengujian keamanan dan pengawasan yang mengidentifikasi dan mendokumentasikan potensi risiko terhadap integritas jaringan. - Catatan pemantauan yang menunjukkan analisis dan deteksi terhadap konfigurasi yang tidak sesuai atau perubahan konfigurasi yang tidak sah. - Laporan audit dan reviu terhadap pengaturan jaringan yang menunjukkan penerapan prinsip keamanan dalam desain dan implementasi jaringan. - Protokol pelaporan yang mencatat insiden terkait integritas jaringan dan tindak lanjut yang diambil untuk mengatasi masalah yang ditemukan. - Dokumentasi prosedur untuk memverifikasi konfigurasi jaringan dan pengujian segmentasi secara berkala
Ancaman/Risiko yang dimitigasi	TH025 TH037 TH040 TH044 TH036 TH038 TH043 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.IR-01** **NIST CSF 1.1: PR.AC-5** **NIST SP 800-53r5: AC-4, AC-10, SC-7, SC-10, SC-20** **SNI ISO/IEC 27001:2022: 5.14, 8.20, 8.22**

Kriteria Pemenuhan Kontrol 2.5.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai.	Tidak Ada	Tidak Ada
1	Organisasi telah menjalankan sebagian kecil penyediaan prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai, tetapi prosedurnya belum diformalkan	- Sudah mulai melakukan sebagian kecil pengujian dan monitoring, namun belum ada prosedur formal - Aktivitas terbatas, bersifat ad-hoc dan tidak terdokumentasi secara resmi	- Bukti pelaksanaan pentest - Belum ada SOP monitoring jaringan - Belum ada SOP Pentest dan VA
2	Organisasi telah menjalankan sebagian besar prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai, tetapi prosedurnya belum diformalkan	- Sebagian besar konfigurasi jaringan telah diuji dan dimonitor, namun prosedur masih belum diformalkan - Monitoring dan pengujian dilakukan lebih luas, tetapi belum didukung oleh SOP tertulis	- Laporan pelaksanaan pentest dan monitoring jaringan - SOP monitoring jaringan masih dalam bentuk draft atau belum disahkan - SOP pentest atau VA masih dalam bentuk draft atau belum disahkan
3	Organisasi telah menjalankan secara penuh prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai, dan prosedurnya sudah diformalkan	- Seluruh prosedur pelindungan terhadap integritas jaringan sudah diterapkan secara penuh dan telah diformalkan - Seluruh perangkat jaringan dipastikan memenuhi fungsi keamanan sesuai kebutuhan, didukung kebijakan dan prosedur tertulis - Terdapat SOP formal terkait monitoring jaringan dan pelaksanaan pentest serta VA	- SOP Monitoring Jaringan yang telah disahkan - SOP Pentest dan VA - Bukti pelaksanaan monitoring jaringan, Pentest, dan VA sesuai dengan SOP
4	Organisasi telah menjalankan secara penuh prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap	- Prosedur sudah diterapkan penuh, dimonitor, dan direviu secara berkala	- SOP Monitoring Jaringan (disahkan dan berlaku) - SOP Pentest dan VA (disahkan dan berlaku)

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Siklus pengujian dan monitoring dilakukan berkala dan ada proses evaluasi terhadap efektivitasnya	- Laporan hasil pelaksanaan monitoring jaringan dan pentest secara berkala - Jadwal kegiatan monitoring jaringan - Jadwal kegiatan pentest, dan VA - Dokumen hasil reviu periodik terhadap: • Efektivitas SOP monitoring jaringan • Efektivitas pelaksanaan pentest dan VA - Rekapitulasi log audit keamanan jaringan dan tindak lanjut monitoring
5	Organisasi telah menjalankan secara penuh prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Prosedur telah diformalkan, dimonitor, direviu berkala, dan dilakukan perbaikan berkelanjutan - Ada bukti perbaikan atau penguatan sistem berdasarkan hasil reviu atau temuan pengujian sebelumnya	- SOP Monitoring Jaringan (disahkan dan berlaku) - SOP Pentest dan VA (disahkan dan berlaku) - Laporan hasil pelaksanaan monitoring jaringan dan pentest secara berkala - Jadwal kegiatan monitoring jaringan - Jadwal kegiatan pentest, dan VA - Dokumen hasil reviu periodik terhadap: • Efektivitas SOP monitoring jaringan • Efektivitas pelaksanaan pentest dan VA - Dokumen perbaikan atau penyempurnaan SOP Monitoring Jaringan dan SOP Pentest/VA (Apabila Ada) - Daftar insiden keamanan dan langkah mitigasi/perbaikannya - Rencana Aksi atau Program Peningkatan Fungsi Keamanan Jaringan

2.5.5. Menerapkan prosedur dan teknologi pencegahan malware

Kriteria	Detail
Deskripsi	Penyelenggara IIV menerapkan prosedur dan teknologi pencegahan malware untuk menjaga ketersediaan dan keamanan data. Langkah ini mencakup pencadangan data secara berkala, pemindaian removable media sebelum digunakan, serta pembaruan rutin perangkat anti-malware seperti antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection/prevention system. Selain itu, sistem operasi dan aplikasi diperbarui melalui upgrade dan patch untuk menutup celah keamanan yang dapat dimanfaatkan oleh ancaman siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi antivirus, antimalware, dan prosedur pelindungan serta pemeliharaan berkala.
Dampak	**Tinggi** – Dengan pencegahan malware yang efektif, organisasi dapat mengurangi risiko infeksi malware dan melindungi sistem serta data dari kerusakan atau kehilangan.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem antimalware yang tepat dan pelatihan karyawan untuk mengenali serta mencegah ancaman malware.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

95 Kontrol 2.5.5.a:

Kontrol	Untuk melindungi ketersediaan data terhadap serangan malware, data organisasi harus di-rekam cadang secara berkala.
Deskripsi Kontrol	Rekaman cadangan data secara berkala merupakan langkah penting untuk melindungi ketersediaan data organisasi dari risiko kehilangan atau kerusakan akibat serangan malware. Proses pencadangan harus dilakukan secara teratur dan disimpan dalam lokasi yang aman, seperti sistem penyimpanan terisolasi atau cloud dengan enkripsi. Selain itu, pengujian terhadap cadangan harus dilakukan secara berkala untuk memastikan bahwa data dapat dipulihkan dengan benar jika diperlukan. Langkah ini membantu organisasi untuk meminimalkan dampak serangan siber dan memastikan keberlanjutan operasional meskipun terjadi insiden keamanan
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan pencadangan data organisasi. - Jadwal rutin pencadangan data. - Dokumentasi prosedur pencadangan, termasuk mekanisme enkripsi data. - Laporan hasil pengujian pemulihan data dari cadangan. - Log pencadangan data yang mencatat waktu, lokasi penyimpanan, dan hasil pencadangan. - Bukti penyimpanan cadangan data di lokasi terisolasi atau layanan cloud yang aman. - Audit laporan tentang efektivitas sistem pencadangan dan pemulihan data.
Ancaman/Risiko yang dimitigasi	TH023 TH050 TH077 TH048 TH065
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 2.5.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala.	Tidak Ada	Tidak Ada
1	Organisasi telah menjalankan sebagian kecil prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala, tetapi prosedurnya belum diformalkan	- Sebagian kecil prosedur pencadangan data dijalankan, namun belum terdokumentasi formal - Pencadangan dilakukan terbatas, hanya pada sebagian sistem, tanpa prosedur baku	- Bukti hasil backup sebagian sistem - Jadwal atau daftar backup tidak lengkap - Tidak tersedia SOP formal
2	Organisasi telah menjalankan sebagian besar prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala, tetapi prosedurnya belum diformalkan	- Sebagian besar sistem sudah dicadangkan, tetapi belum ada prosedur resmi - Proses backup lebih menyeluruh namun belum diformalkan atau distandardisasi	- Daftar data yang dicadangkan dan jadwal yang lebih lengkap - Hasil backup (log/rekaman) untuk sebagian besar sistem - SOP masih draft atau belum disahkan
3	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala, dan prosedurnya sudah diformalkan	- Prosedur pencadangan dan teknologi sudah berjalan penuh dan terdokumentasi - Terdapat SOP Backup Restore resmi dan backup dilakukan terhadap seluruh sistem penting	- SOP Backup dan Restore yang telah diresmikan dan berlaku - Daftar data dan jadwal backup lengkap - Bukti hasil backup dan Restore seluruh sistem
4	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Prosedur berjalan penuh, dimonitor, dan direviu secara berkala - Tersedia proses audit, monitoring, dan evaluasi terhadap efektivitas backup data	- SOP Backup dan Restore yang telah diresmikan dan berlaku - Daftar data dan jadwal backup lengkap - Bukti hasil backup dan Restore seluruh sistem - Laporan hasil monitoring backup - Jadwal reviu dan hasil evaluasinya - Log sistem pemantauan backup otomatis
5	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware untuk melindungi ketersediaan data berupa perekaman pencadangan data organisasi secara berkala, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Terdapat proses perbaikan berkelanjutan dari hasil evaluasi backup dan perlindungan malware - Hasil reviu ditindaklanjuti dengan peningkatan prosedur atau teknologi pencadangan	- SOP Backup dan Restore yang telah diresmikan dan berlaku - Daftar data dan jadwal backup lengkap - Bukti hasil backup dan Restore seluruh sistem - Laporan hasil monitoring backup - Jadwal reviu dan hasil evaluasinya - Log sistem pemantauan backup otomatis - Rencana peningkatan teknologi backup (opsional) - Laporan insiden dan tindak lanjutnya

96 Kontrol 2.5.5.b:

Kontrol	Pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya untuk mencegah masuknya virus dari luar ke dalam perangkat pengolah informasi dan jaringan komunikasi data milik Organisasi
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa semua media penyimpanan yang dapat dilepas (removable media) seperti USB drive, hard drive eksternal, atau kartu memori, dilakukan pemindaian menggunakan perangkat lunak keamanan sebelum digunakan pada perangkat organisasi. Pemindaian ini bertujuan untuk mencegah masuknya malware, virus, atau ancaman keamanan lainnya yang dapat merusak perangkat pengolah informasi atau jaringan komunikasi data organisasi. Tujuan dari kontrol ini adalah untuk menjaga integritas, kerahasiaan, dan ketersediaan aset informasi organisasi dengan menerapkan langkah pencegahan yang proaktif terhadap ancaman eksternal
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur organisasi yang mengatur kewajiban pemindaian removable media sebelum digunakan. - Log atau laporan hasil pemindaian removable media menggunakan perangkat lunak antivirus atau antimalware. - Daftar perangkat lunak keamanan yang digunakan untuk pemindaian, termasuk bukti pembaruan definisi virus secara berkala. - Dokumentasi pelatihan kepada staf mengenai pentingnya pemindaian removable media dan langkah-langkah operasionalnya. - Laporan insiden yang menunjukkan efektivitas pemindaian removable media dalam mencegah ancaman keamanan. - Catatan audit internal yang memeriksa kepatuhan terhadap kebijakan pemindaian removable media.
Ancaman/Risiko yang dimitigasi	TH031 TH036 TH045 TH048 TH034 TH039 TH047 TH050
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 2.5.5.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya.	Tidak Ada	Tidak Ada
1	Organisasi telah menjalankan sebagian kecil prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya, tetapi prosedurnya belum diformalkan	- Sebagian kecil perangkat sudah dilakukan pemindaian removable media, namun belum ada prosedur formal - Aktivitas terbatas pada beberapa perangkat dan tidak ada panduan tertulis	- Bukti antivirus terpasang pada sebagian perangkat - Tidak ada SOP atau kebijakan tertulis
2	Organisasi telah menjalankan sebagian besar prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya, tetapi prosedurnya belum diformalkan	- Sebagian besar perangkat telah menggunakan pemindaian, namun prosedur belum diformalkan - Kontrol teknis sudah berjalan pada sebagian besar sistem, tapi belum didukung oleh dokumen resmi	- Antivirus aktif pada hampir seluruh endpoint - Laporan hasil scanning berkala - SOP masih berupa draft atau belum ditetapkan resmi
3	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya, dan prosedurnya sudah diformalkan	- Seluruh perangkat telah dilengkapi pemindaian dan prosedur formal tersedia - SOP dan teknologi scanning sudah diterapkan penuh di seluruh lingkungan sistem	- SOP Penggunaan Removable media yang telah disahkan - Antivirus aktif dan dikonfigurasi untuk auto-scan - Bukti kebijakan otorisasi penggunaan media eksternal
4	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya, dan	- Prosedur formal telah dijalankan, dimonitor, dan direviu secara berkala - Aktivitas scanning dipantau, dievaluasi, dan dilakukan audit berkala	- SOP Penggunaan Removable media yang telah disahkan - Antivirus aktif dan dikonfigurasi untuk auto-scan - Bukti kebijakan otorisasi penggunaan media eksternal - Log monitoring antivirus/scanning

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala		- Jadwal reviu kebijakan removable media - Bukti laporan hasil evaluasi dan tindak lanjutnya
5	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pemindaian/scanning terhadap removable media yang akan digunakan pada perangkat komputer, notebook, server, atau perangkat pengolah informasi lainnya, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Prosedur telah dijalankan penuh, direviu, dan diperbaiki secara berkelanjutan - Hasil evaluasi digunakan untuk menyempurnakan kebijakan dan teknologi pengamanan media	- SOP Penggunaan Removable media yang telah disahkan - Antivirus aktif dan dikonfigurasi untuk auto-scan - Bukti kebijakan otorisasi penggunaan media eksternal - Log monitoring antivirus/scanning - Jadwal reviu kebijakan removable media - Bukti laporan hasil evaluasi dan tindak lanjutnya - Revisi SOP atau pembaruan kebijakan - Laporan audit keamanan removable media - Catatan insiden dan perbaikannya terkait removable media

97 Kontrol 2.5.5.c:

Kontrol	Mengunduh dan menginstalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system
Deskripsi Kontrol	Penyelenggara IIV harus secara rutin mengunduh dan menginstal pembaruan terbaru untuk perangkat lunak keamanan seperti antivirus, anti-spyware, spam filtering, web content filtering, dan sistem deteksi dan pencegahan intrusi (IDPS). Pembaruan ini penting untuk memastikan bahwa sistem keamanan tetap efektif melindungi organisasi terhadap ancaman keamanan terbaru yang terus berkembang. Tujuan dari kontrol ini adalah untuk menjaga keamanan aset informasi organisasi dengan mengantisipasi eksploitasi kerentanan dan mengurangi risiko masuknya ancaman siber yang dapat membahayakan operasi organisasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur organisasi terkait pembaruan perangkat lunak keamanan. - Log atau catatan aktivitas pembaruan perangkat lunak keamanan, termasuk waktu dan versi pembaruan. - Daftar perangkat lunak keamanan yang digunakan oleh organisasi, beserta status pembaruan terbaru. - Bukti pengaturan otomatis (auto-update) untuk perangkat lunak keamanan di sistem. - Laporan audit internal atau eksternal yang memeriksa kepatuhan terhadap pembaruan perangkat lunak keamanan. - Sertifikasi atau laporan dari vendor perangkat lunak keamanan yang menyatakan bahwa pembaruan terbaru telah diunduh dan diinstal. - Dokumentasi pelatihan personel terkait langkah-langkah pembaruan perangkat lunak keamanan
Ancaman/Risiko yang dimitigasi	TH024 TH038 TH040 TH047 TH050 TH036 TH039 TH046 TH048 TH065
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 2.5.5.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system.	Tidak ada	Tidak ada
1	Organisasi telah menjalankan sebagian kecil prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system, tetapi prosedurnya belum diformalkan	- Pembaruan dilakukan pada sebagian kecil sistem, namun tanpa prosedur formal - Sebagian perangkat memiliki software anti-malware aktif, tapi belum distandardisasi	- Antivirus aktif Sebagian - Tidak ada kebijakan formal - Auto-update aktif hanya pada beberapa perangkat
2	Organisasi telah menjalankan sebagian besar prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system, tetapi prosedurnya belum diformalkan	- Sebagian besar sistem menggunakan teknologi update anti-malware, namun belum diformalkan - Teknologi pembaruan sudah menyeluruh, tapi prosedur belum terdokumentasi resmi	- Antivirus dan anti-malware aktif pada hampir seluruh sistem - Auto-update berjalan - Kebijakan masih berupa draft
3	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system, dan prosedurnya sudah diformalkan	- Seluruh sistem memiliki update anti-malware otomatis dan prosedur telah diformalkan - Organisasi memiliki kebijakan antivirus dan sistem auto-update berjalan penuh	- Kebijakan Antivirus tertulis dan disahkan - Konfigurasi auto-update antivirus dan IDPS - Bukti hasil update atau log sistem keamanan
4	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Prosedur update berjalan penuh, dimonitor, dan direviu secara berkala - Monitoring terhadap update dilakukan dan hasilnya dievaluasi secara rutin	- Kebijakan Antivirus tertulis dan disahkan - Konfigurasi auto-update antivirus dan IDPS - Bukti hasil update atau log sistem keamanan - Laporan monitoring update antivirus

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Log sistem pembaruan otomatis
5	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa pengunduhan dan instalasi update anti malware terbaru, meliputi antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Prosedur dijalankan secara penuh, direviu, dan ditingkatkan secara berkala - Hasil evaluasi dijadikan dasar peningkatan teknologi atau kebijakan keamanan	- Kebijakan Antivirus tertulis dan disahkan - Konfigurasi auto-update antivirus dan IDPS - Bukti hasil update atau log sistem keamanan - Laporan monitoring antivirus - Log sistem pembaruan otomatis - Update kebijakan antivirus/IDPS - Laporan insiden dan tindak lanjut pembaruan sistem

98 Kontrol 2.5.5.d:

Kontrol	Meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa perangkat komputer, termasuk sistem operasi dan aplikasi yang digunakan, secara rutin di-update melalui upgrade dan patch. Proses ini bertujuan untuk memperbaiki kerentanan keamanan, meningkatkan kinerja, dan menjaga kompatibilitas dengan perangkat dan sistem lain. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi tetap terlindungi dari ancaman keamanan terbaru yang dapat mengeksploitasi kerentanan yang belum diperbaiki, serta menjaga keberlangsungan operasional organisasi melalui perangkat yang optimal.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan atau prosedur organisasi terkait proses upgrade dan patching sistem operasi dan aplikasi. - Log atau laporan pembaruan sistem operasi dan aplikasi, termasuk tanggal, versi patch, dan perangkat yang diperbarui. - Daftar perangkat komputer dan aplikasi organisasi beserta status pembaruannya. - Bukti pengaturan pembaruan otomatis (auto-update) untuk sistem operasi dan aplikasi. - Laporan hasil audit internal atau eksternal mengenai kepatuhan terhadap proses upgrade dan patching. - Dokumentasi komunikasi dengan vendor perangkat lunak terkait pembaruan atau patch terbaru. - Bukti pelaksanaan pelatihan kepada staf terkait pentingnya pembaruan sistem operasi dan aplikasi
Ancaman/Risiko yang dimitigasi	TH021 TH036 TH039 TH046 TH048 TH065 TH025 TH038 TH040 TH047 TH050 TH071
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 2.5.5.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi.	Tidak Ada	Tidak Ada
1	Organisasi telah menjalankan sebagian kecil prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi, tetapi prosedurnya belum diformalkan	- Sebagian kecil perangkat sudah di-patch atau di-upgrade, tapi tidak didukung prosedur formal - Aktivitas patch dilakukan sporadis dan tidak terdokumentasi secara konsisten	- Bukti upgrade manual pada beberapa perangkat - Belum ada SOP - Belum ada otorisasi atau jadwal patching
2	Organisasi telah menjalankan sebagian besar prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi, tetapi prosedurnya belum diformalkan	- Sebagian besar sistem telah dilakukan patch/upgrade namun belum diformalkan - Patch dilakukan rutin namun belum ada kebijakan atau prosedur resmi	- Patch log atau tool auto-update aktif - Bukti update di sebagian besar sistem - SOP belum tersedia
3	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi, dan prosedurnya sudah diformalkan	- Patch dan upgrade dilakukan menyeluruh dan sudah didukung SOP formal - Terdapat SOP dan kebijakan pembaruan, seluruh perangkat tunduk pada prosedur ini	- SOP Patching - Jadwal patching regular - Bukti pelaksanaan patching
4	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	- Seluruh sistem dipatch sesuai SOP dan dilakukan monitoring serta reviu berkala - Patch rutin dilaporkan, dimonitor, dan dilakukan peninjauan berkala efektivitasnya	- SOP Patching - Jadwal patching regular - Bukti atau laporan pelaksanaan patching - Log audit patching - Bukti reviu berkala terhadap pelaksanaan patching
5	Organisasi telah menjalankan secara penuh prosedur dan teknologi pencegahan malware berupa meng-update perangkat komputer dengan melakukan upgrade dan patch sistem operasi dan aplikasi, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	- Patch dan upgrade dilaksanakan menyeluruh, dimonitor, direviu, dan diperbaiki jika ada temuan - Hasil reviu digunakan untuk memperbaiki SOP/strategi patching agar lebih efektif	- SOP Patching - Jadwal patching regular - Bukti atau laporan pelaksanaan patching - Log audit patching - Bukti reviu berkala terhadap pelaksanaan patching - Dokumen evaluasi dan peningkatan dan perbaikan SOP patch

2.5.6. Memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi

Kriteria	Detail
Deskripsi	Penyelenggara IIV bertanggung jawab untuk memastikan bahwa catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau secara berkala sesuai dengan kebijakan organisasi. Tugas ini mencakup penetapan standar dan prosedur pencatatan aktivitas, penerapan mekanisme logging yang konsisten di seluruh sistem yang relevan, serta pelaksanaan tinjauan berkala guna mendeteksi anomali, memastikan kepatuhan, dan mendukung transparansi serta akuntabilitas dalam pengelolaan sistem informasi organisasi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem logging dan audit, serta sumber daya untuk pemeliharaan dan peninjauan berkala.
Dampak	**Tinggi** – Dengan log aktivitas yang lengkap dan teratur, organisasi dapat mendeteksi dan merespons insiden keamanan dengan cepat, serta memastikan kepatuhan terhadap kebijakan keamanan.
Kompleksitas	**Sedang** – Memerlukan sistem logging yang tepat dan prosedur untuk mendokumentasikan, mengimplementasikan, dan meninjau log aktivitas secara berkala.
Referensi Kontrol	**NIST CSF 2.0: PR.PS-04** **NIST CSF 1.1: PR.PT-1** **NIST SP 800-53r5: AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16** **SNI ISO/IEC 27001:2022: 8.15, 8.17, 8.34**

99 Kontrol 2.5.6.a:

Kontrol	Menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar.
Deskripsi Kontrol	Penyelenggara IIV perlu menentukan subjek atau ruang lingkup pencatatan log (audit trail) untuk memastikan semua aktivitas penting terkait keamanan siber tercatat dengan jelas dan relevan. Pencatatan ini mencakup informasi tentang akses, perubahan, atau aktivitas lain pada aset informasi yang penting. Catatan log harus ditinjau secara berkala untuk mendeteksi potensi insiden keamanan, khususnya yang berisiko tinggi, guna mendukung respons yang cepat dan tepat. Tujuan dari kontrol ini adalah untuk meningkatkan kemampuan organisasi dalam mendeteksi dan menangani insiden keamanan dengan memanfaatkan informasi log sebagai alat analisis dan investigasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Kebijakan dan prosedur organisasi terkait pengelolaan pencatatan log. - Daftar ruang lingkup pencatatan log yang telah ditentukan (misalnya, server, aplikasi kritis, perangkat jaringan). - Dokumentasi konfigurasi sistem pencatatan log (log management system). - Laporan hasil tinjauan log secara berkala yang mencakup potensi insiden yang terdeteksi. - Bukti penerapan alat analisis log, seperti laporan dari Security Information and Event Management (SIEM). - Dokumentasi pelatihan personel tentang analisis log untuk mendeteksi insiden keamanan. - Laporan investigasi insiden keamanan yang menggunakan data dari catatan log.
Ancaman/Risiko yang dimitigasi	TH025 TH037 TH040 TH044 TH053 TH055 TH036 TH038 TH043 TH052 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.PS-04** **NIST CSF 1.1: PR.PT-1** **NIST SP 800-53r5: AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16** **SNI ISO/IEC 27001:2022: 8.15, 8.17, 8.34**

Kriteria Pemenuhan Kontrol 2.5.6.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar	Tidak ada kebijakan, tidak ada sistem yang mencatat log, dan tidak ada bukti analisa log	Tidak ditemukan kebijakan atau bukti aktivitas log
1	Organisasi telah menjalankan sebagian kecil prosedur dalam menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar, tetapi prosedurnya belum diformalkan	Pencatatan log dilakukan pada sebagian sistem kritis secara terbatas dan belum terdokumentasi dalam kebijakan formal	- Log dari beberapa sistem - Bukti manual pencatatan - Tidak ada kebijakan tertulis
2	Organisasi telah menjalankan sebagian besar prosedur dalam menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar, tetapi prosedurnya belum diformalkan	Sistem log sudah cukup luas, tapi kebijakan dan proses belum terdokumentasi resmi	- Daftar sistem yang memiliki log - Bukti analisa log rutin - Belum ada kebijakan tertulis atau SOP log
3	Organisasi telah menjalankan secara Organisasi telah menjalankan secara penuh prosedur dalam menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar, dan prosedurnya sudah diformalkan	Seluruh prosedur berjalan dan terdokumentasi dalam kebijakan dan SOP formal	- Kebijakan log resmi - SOP pengelolaan log - Daftar sistem yang memiliki log lengkap - Bukti pelaksanaan pencatatan dan peninjauan log
4	Organisasi telah menjalankan secara penuh prosedur dalam menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	Terdapat jadwal monitoring dan laporan hasil reviu secara periodik	- Laporan monitoring log - Jadwal dan hasil reviu berkala - Dokumen pembaruan atau tindak lanjut dari hasil reviu log
5	Organisasi telah menjalankan secara penuh prosedur dalam menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	Bukti adanya tindakan korektif dan peningkatan sistem atau kebijakan log	- Bukti tindakan perbaikan dari hasil reviu - Revisi kebijakan atau SOP log - Notulen rapat evaluasi log dan hasil implementasi peningkatan

2.5.7. Memastikan bahwa informasi mengenai pelindungan terhadap teknologi dibagikan hanya kepada pihak tepercaya

Kriteria	Detail
Deskripsi	Penyelenggara IIV bertanggung jawab memastikan bahwa informasi terkait pelindungan terhadap teknologi hanya dibagikan kepada pihak yang tepercaya, sesuai dengan prinsip keamanan informasi. Hal ini dilakukan melalui penetapan kebijakan akses, verifikasi kredensial pihak penerima, serta penerapan prosedur klasifikasi dan pembatasan distribusi informasi agar tidak disalahgunakan oleh pihak yang tidak berwenang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan kebijakan dan prosedur untuk mengatur pembagian informasi, serta pelatihan karyawan tentang pentingnya menjaga kerahasiaan informasi.
Dampak	**Tinggi** – Dengan membatasi pembagian informasi hanya kepada pihak tepercaya, organisasi dapat mengurangi risiko kebocoran informasi dan meningkatkan keamanan secara keseluruhan.
Kompleksitas	**Sedang** – Memerlukan kebijakan yang jelas dan prosedur yang tepat untuk memastikan bahwa informasi dibagikan dengan aman dan hanya kepada pihak yang tepercaya.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: PR.IP-8** **NIST SP 800-53r5: AC-21, CA-7, CP-2, IR-8, SI-4** **SNI ISO/IEC 27001:2022: 5.27**

100 Kontrol 2.5.7.a:

Kontrol	Berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa informasi terkait efektivitas teknologi perlindungan data hanya dibagikan kepada mitra yang relevan dan terpercaya. Hal ini bertujuan untuk menjaga kerahasiaan informasi sensitif dan mencegah penyalahgunaan informasi oleh pihak yang tidak berwenang. Tujuan dari kontrol ini adalah memastikan bahwa proses berbagi informasi dilakukan dengan kontrol yang memadai untuk melindungi aset informasi organisasi sekaligus mendorong kolaborasi yang aman dan efisien dengan mitra strategis
Deskripsi Bukti Dukung	Bukti dapat dukung dapat berupa: - Kebijakan organisasi terkait berbagi informasi dengan pihak ketiga. - Daftar mitra yang disetujui untuk menerima informasi terkait perlindungan data. - Perjanjian kerahasiaan (NonDisclosure Agreement, NDA) dengan mitra. - Dokumentasi evaluasi dan kualifikasi mitra sebelum berbagi informasi. - Laporan audit terkait aktivitas berbagi informasi. - Bukti enkripsi atau mekanisme keamanan lainnya yang digunakan untuk berbagi informasi. - Catatan komunikasi yang mencakup informasi perlindungan data yang dibagikan.
Ancaman/Risiko yang dimitigasi	TH033 TH041 TH064 TH035 TH062 TH075
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: PR.IP-8** **NIST SP 800-53r5: AC-21, CA-7, CP-2, IR-8, SI-4** **SNI ISO/IEC 27001:2022: 5.27**

Kriteria Pemenuhan Kontrol 2.5.7.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan berbagi informasi mengenai efektivitas teknologi perlindungan data	Tidak ada kebijakan, SOP, atau bukti kerja sama dengan mitra terpercaya	Tidak ada
1	Organisasi telah menjalankan berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya namun belum secara menyeluruh (masih sebagian kecil) baik terhadap teknologi maupun terhadap mitra, tetapi prosedurnya belum diformalkan	Beberapa mitra menerima informasi secara informal, tanpa standar atau SOP	Ditemukan: - Bukti komunikasi atau laporan dengan sebagian mitra - Tidak ada kebijakan atau SOP resmi - Belum ada NDA formal
2	Organisasi telah menjalankan berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan sebagian besar mitra yang tepat dan terpercaya baik terhadap teknologi maupun terhadap mitra, tetapi prosedurnya belum diformalkan	Informasi dibagikan secara luas namun belum ada dokumen formal	Ditemukan: - Bukti komunikasi aktif dengan mitra utama - Sebagian NDA ditandatangani - Belum tersedia SOP atau kebijakan pertukaran informasi
3	Organisasi telah menjalankan berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya secara menyeluruh baik terhadap teknologi maupun terhadap mitra, dan prosedurnya sudah diformalkan	Tersedia kebijakan, SOP, dan seluruh mitra telah diverifikasi dan memiliki NDA	Verifikator dapat memeriksa: - Kebijakan pertukaran informasi - SOP pengadaan vendor - NDA lengkap dari seluruh mitra terpercaya
4	Organisasi telah menjalankan berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya secara menyeluruh baik terhadap teknologi maupun terhadap mitra, dan prosedurnya sudah diformalkan, dimonitoring, dan direviu secara berkala	Terdapat catatan monitoring, hasil evaluasi, dan pembaruan dokumen bila diperlukan	Diperiksa: - Laporan monitoring - Jadwal & hasil evaluasi mitra - Tinjauan rutin kebijakan/SOP
5	Organisasi telah menjalankan berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya secara menyeluruh baik terhadap teknologi maupun terhadap mitra, dan prosedurnya sudah diformalkan, dimonitoring, direviu secara berkala, dan dilakukan perbaikan	Bukti peningkatan dan tindak lanjut terhadap rekomendasi hasil reviu tersedia	Diperiksa: - Revisi SOP atau kebijakan - Bukti perbaikan pasca-reviu - Notulen pertemuan evaluasi dan rencana aksi

2.6. Melindungi sumber daya manusia

Penyelenggara IIV melindungi sumber daya manusia dengan menerapkan prosedur pengelolaan keamanan personel secara menyeluruh. Upaya ini meliputi penyelenggaraan pelatihan dan program peningkatan kesadaran keamanan siber untuk seluruh pegawai, sehingga mereka memahami risiko dan langkah mitigasi yang tepat. Selain itu, organisasi menyusun serta menerapkan kebijakan yang mengatur kompetensi dan keahlian personel keamanan siber, memastikan bahwa setiap individu memiliki kemampuan yang memadai untuk melindungi sistem dan informasi kritis yang dikelola.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menerapkan prosedur pengelolaan keamanan terhadap personel;
b) menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber; dan
c) menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di Penyelenggara IIV.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melindungi sumber daya manusia” secara efektif antara lain:

NIST CSF 2.0	**:**	**PR.AT-01, PR.AT-02, GV.RR-04**
NIST CSF 1.1	**:**	**PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, PR.IP-11**
NIST SP 800-53r5	**:**	**PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-9, SA-21, AT-2, AT-3, PM-3, PM-13, PM-14, CP-3, IR-2**
SNI ISO/IEC 27001:2022	**:**	**pasal 7, 5.2, 5.34, 6.1, 6.3, 6.4, 6.5, 7.4**

Peraturan BSSN No. 9 Tahun 2023 tentang Peningkatan Kapasitas SDM di Bidang Keamanan Siber dan Sandi

2.6.1. Menerapkan prosedur pengelolaan keamanan terhadap personel

Kriteria	Detail
Deskripsi	Penyelenggara IIV bertanggung jawab dalam memastikan penerapan prosedur pengelolaan keamanan terhadap personel guna meminimalkan risiko terhadap informasi dan sistem organisasi. Prosedur ini mencakup seleksi dan latar belakang personel, pemberian akses berdasarkan peran dan tanggung jawab, serta penegakan kebijakan keamanan selama dan setelah masa kerja. Hal ini dilakukan untuk memastikan bahwa setiap individu yang terlibat telah memenuhi standar keamanan yang ditetapkan organisasi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mengimplementasikan prosedur pengelolaan keamanan.
Dampak	**Tinggi** – Dengan prosedur yang jelas, organisasi dapat mengurangi risiko keamanan yang disebabkan oleh kesalahan manusia dan memastikan bahwa semua karyawan mematuhi praktik keamanan yang terbaik.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan pelatihan karyawan untuk memastikan bahwa semua orang memahami dan mematuhi kebijakan keamanan.
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

101 Kontrol 2.6.1.a:

Kontrol	Pemeriksaan verifikasi latar belakang terhadap semua calon personel harus dilakukan sebelum bergabung dengan Penyelenggara IIV dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa setiap calon personel yang akan bergabung dengan Penyelenggara IIV telah melalui proses pemeriksaan latar belakang secara menyeluruh. Pemeriksaan ini dilakukan sebelum perekrutan, dengan mempertimbangkan ketentuan hukum, etika, kebutuhan bisnis, serta tingkat risiko keamanan yang relevan. Tujuannya adalah untuk memastikan integritas, keandalan, dan kelayakan personel dalam mengakses informasi atau sistem yang sensitif.
Deskripsi Bukti Dukung	Sebagai bukti pelaksanaan kontrol terkait pengelolaan keamanan terhadap personel, organisasi telah menerapkan prosedur yang mencakup proses verifikasi latar belakang sebelum perekrutan. Bukti dukung tersebut antara lain berupa: - SOP manajemen SDM (Verifikasi latar belakang) - Hasil verifikasi personil
Ancaman/Risiko yang dimitigasi	TH026 TH041 TH056 TH064 TH033 TH053 TH062
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi belum menjalankan pemeriksaan latar belakang calon personel yang akan bergabung dengan organisasi	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi sudah melakukan pemeriksaan/verifikasi latar belakang kepada sebagian kecil calon personel yang akan bergabung dengan organisasi	Pemeriksaan latar belakang dilakukan secara ad-hoc atau hanya pada posisi tertentu	- Ditemukan: - SOP manajemen SDM mencantumkan verifikasi - Bukti verifikasi sebagian kecil personel
2	- Organisasi sudah memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi telah menjalankan kegiatan pemeriksaan verifikasi latar belakang terhadap sebagian besar calon personel yang akan bergabung dengan organisasi dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan namun belum secara menyeluruh	Organisasi mulai mempertimbangkan aspek hukum, etika, dan risiko, namun belum konsisten di seluruh rekrutmen	- Ditemukan: - SOP manajemen SDM - Hasil verifikasi sebagian besar calon personel - Checklist atau form standar pemeriksaan
3	- Organisasi sudah memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi telah menjalankan kegiatan kegiatan pemeriksaan verifikasi latar belakang terhadap semua calon personel yang akan bergabung dengan organisasi dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan secara menyeluruh	Verifikasi dilakukan penuh dengan prinsip proporsional dan sesuai peraturan yang berlaku	- Ditemukan: - SOP manajemen SDM lengkap - Bukti hasil verifikasi seluruh personel rekrutmen - Catatan pelaksanaan sistematis
4	- Organisasi sudah memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi telah menjalankan kegiatan kegiatan pemeriksaan verifikasi latar belakang terhadap semua calon personel yang	Terdapat proses monitoring awal terhadap personel pasca-penerimaan	- Ditemukan: - Laporan monitoring personel baru - Dokumentasi hasil observasi awal atau pengawasan khusus

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	akan bergabung dengan organisasi dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan secara menyeluruh serta melakukan pemantauan terhadap personel yang bergabung dengan organisasi		- Revisi data hasil rekrutmen jika diperlukan
5	- Organisasi sudah memiliki prosedur terorganisir dalam melakukan pemeriksaan verifikasi latar belakang calon personel yang akan bergabung dengan organisasi - Organisasi telah menjalankan kegiatan kegiatan pemeriksaan verifikasi latar belakang terhadap semua calon personel yang akan bergabung dengan organisasi dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan secara menyeluruh serta melakukan pemantauan secara berkala dan dilakukan perbaikan berkelanjutan terhadap pelaksanaan kegiatan verifikasi latar belakang personel	Monitoring dan verifikasi dilakukan berkala, dan hasilnya digunakan untuk perbaikan kebijakan/prosedur	- Revisi SOP manajemen SDM - Catatan evaluasi berkala - Bukti perbaikan (misal: update form, perubahan checklist, dll.) - Notulen atau laporan hasil reviu kebijakan verifikasi

102 Kontrol 2.6.1.b:

Kontrol	Perjanjian kontrak kerja harus menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa setiap perjanjian kontrak kerja mencantumkan secara jelas tanggung jawab personel dan organisasi dalam menjaga keamanan informasi. Dengan mencantumkan ketentuan tersebut, diharapkan seluruh pihak memahami dan mematuhi kewajiban serta batasan terkait perlindungan data dan informasi sensitif selama dan setelah masa kerja, guna meminimalkan risiko kebocoran atau penyalahgunaan informasi.
Deskripsi Bukti Dukung	Sebagai bukti pelaksanaan kontrol, organisasi telah mencantumkan tanggung jawab keamanan informasi dalam dokumen kontrak kerja personel. Bukti dukung ini menunjukkan Kontrak Kerja Personel
Ancaman/Risiko yang dimitigasi	TH033 TH053 TH059 TH062 TH041 TH056 TH060 TH064
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur terorganisir tentang penerapan perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi belum mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki prosedur terorganisir yang mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi sedang merencanakan membuat perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.	Tersedia rancangan prosedur atau template kontrak, belum diberlakukan ke personel	- Draft prosedur atau template kontrak - Dokumen rencana penerapan
2	- Organisasi sudah memiliki prosedur terorganisir yang mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi telah mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi namun belum secara menyeluruh	Klausul keamanan informasi sudah mulai digunakan dalam kontrak kerja sebagian personel	- SOP/standar kontrak kerja tersedia - Contoh kontrak kerja dengan klausul keamanan dari sebagian unit/personel
3	- Organisasi sudah memiliki prosedur terorganisir yang mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi telah mewajibkan dan menjalankan perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi secara menyeluruh	Klausul keamanan informasi diterapkan secara konsisten untuk semua personel	- SOP dan template kontrak kerja aktif - Kontrak kerja seluruh personel mencantumkan klausul keamanan informasi
4	- Organisasi sudah memiliki prosedur terorganisir yang mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi telah mewajibkan dan menjalankan perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi secara menyeluruh dan direviu secara berkala	Jadwal dan bukti reviu kontrak tersedia	- Bukti tinjauan berkala kontrak kerja - Notulen atau laporan evaluasi klausul keamanan informasi
5	- Organisasi sudah memiliki prosedur terorganisir yang mewajibkan adanya perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi - Organisasi telah mewajibkan dan menjalankan perjanjian kontrak kerja yang menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi secara menyeluruh dan dilakukan reviu secara berkala terhadap perjanjian kerja yang sudah ada serta diperbaiki secara berkelanjutan	Kontrak kerja diperbarui secara berkala dengan menyesuaikan kebutuhan keamanan informasi	- Dokumen revisi kontrak - Bukti perubahan klausul keamanan - Laporan audit atau reviu berkala terhadap kontrak kerja

103 Kontrol 2.6.1.c:

Kontrol	Proses pendisiplinan harus diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa organisasi memiliki proses pendisiplinan yang jelas, terdokumentasi, dan dikomunikasikan kepada seluruh personel serta pihak terkait. Proses ini digunakan sebagai dasar untuk mengambil tindakan yang tegas dan proporsional terhadap pelanggaran kebijakan keamanan informasi, guna menjaga kepatuhan, mencegah pelanggaran berulang, dan menumbuhkan budaya keamanan di lingkungan kerja.
Deskripsi Bukti Dukung	Sebagai bukti pelaksanaan kontrol terkait pendisiplinan atas pelanggaran kebijakan keamanan informasi, organisasi telah menetapkan mekanisme formal yang dituangkan dalam dokumen kebijakan atau prosedur. Bukti dukung tersebut berupa SOP/Kebijakan manajemen SDM (Tentang Pendisiplinan)
Ancaman/Risiko yang dimitigasi	TH026 TH041 TH053 TH064 TH033 TH049 TH062
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi belum merencanakan proses pendisiplinan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi.	Organisasi belum memiliki dokumentasi maupun rencana tindakan disipliner	Tidak ada
1	- Organisasi sudah memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi telah merencanakan proses pendisiplinan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi.	SOP pendisiplinan tersedia, belum diimplementasikan	- SOP manajemen SDM terkait pendisiplinan - Dokumen perencanaan penerapan atau sosialisasi
2	- Organisasi sudah memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi telah menjalankan proses pendisiplinan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi namun belum secara menyeluruh	Organisasi telah menindak sebagian pelanggaran, namun belum menyeluruh	- SOP pendisiplinan - Contoh kasus tindakan disipliner terbatas - Bukti internal memo atau peringatan
3	- Organisasi sudah memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi telah menjalankan proses pendisiplinan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi secara menyeluruh	Semua personel dan pihak terkait tunduk pada mekanisme disipliner formal	- SOP pendisiplinan aktif - Bukti pelaksanaan pada semua pelanggaran - Dokumentasi proses dan hasil keputusan disipliner
4	- Organisasi sudah memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi telah menjalankan proses pendisiplinan, diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi dan proses pendisiplinan tersebut direviu secara berkala	Tindakan disipliner ditinjau dan disesuaikan berdasarkan evaluasi rutin	- Bukti sosialisasi ke personel - Jadwal & hasil reviu kebijakan pendisiplinan - Laporan efektivitas prosedur disipliner
5	- Organisasi sudah memiliki prosedur terorganisir untuk melaksanakan pendislipan terhadap personel dan pihak berkepentingan lainnya - Organisasi telah menjalankan proses pendisiplinan, diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi dan proses pendisiplinan tersebut direviu secara berkala serta diperbaiki secara berkelanjutan	Tindakan disipliner ditinjau dan diperbaiki untuk meningkatkan efektivitas dan keadilan	- Revisi kebijakan atau SOP disiplin - Notulen evaluasi dan perbaikan sistem - Laporan efektivitas dan tindak lanjut implementasi

104 Kontrol 2.6.1.d:

Kontrol	Organisasi menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa organisasi memiliki mekanisme yang jelas dalam menetapkan dan mengomunikasikan kendali keamanan informasi kepada seluruh pegawai dan pihak ketiga yang mengalami penghentian atau perubahan jabatan, tugas, maupun tanggung jawab. Hal ini mencakup penyesuaian atau pencabutan akses, penyampaian kewajiban pasca-kerja, serta pengelolaan aset dan informasi, guna mencegah penyalahgunaan atau kebocoran informasi setelah perubahan status atau hubungan kerja.
Deskripsi Bukti Dukung	Sebagai bukti pelaksanaan kontrol terkait pengendalian keamanan informasi pasca penghentian atau perubahan jabatan pegawai dan pihak ketiga, organisasi telah menetapkan prosedur yang terdokumentasi dengan baik. Bukti dukung tersebut dapat berupa: - SOP Manajemen SDM (terkait pergantian/pemberhentian Pegawai) - Dokumentasi exit clearance dan serah terima
Ancaman/Risiko yang dimitigasi	TH033 TH053 TH062 TH041 TH054 TH064
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum merencanakan untuk menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi.	Tidak ada	Tidak ada
1	Organisasi sedang merencanakan untuk menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi.	Tersedia draft atau kerangka prosedur namun belum diberlakukan	- Draft SOP pergantian/ pemberhentian pegawai - Rencana komunikasi prosedur kepada personel
2	Organisasi telah menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi namun belum secara menyeluruh.	Exit clearance dan serah terima sudah dilakukan sebagian, namun belum konsisten di seluruh organisasi	- SOP manajemen SDM yang telah diberlakukan sebagian - Contoh dokumentasi exit clearance dan serah terima
3	Organisasi telah menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi secara menyeluruh.	Exit clearance dan serah terima dilakukan konsisten di seluruh organisasi	- SOP aktif dan berlaku untuk seluruh unit - Bukti pelaksanaan exit clearance dan serah terima dari berbagai unit/ personel
4	Organisasi telah menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi secara menyeluruh dan direviu secara berkala	Ada dokumentasi reviu dan hasil evaluasi kebijakan	- Jadwal dan hasil reviu berkala SOP dan pelaksanaannya - Notulen atau laporan evaluasi implementasi exit clearance
5	Organisasi telah menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi dan direviu secara berkala serta diperbaiki secara berkelanjutan	Bukti adanya revisi atau peningkatan prosedur berdasarkan evaluasi berkala	- SOP yang diperbarui - Bukti perubahan kebijakan/prosedur exit - Laporan audit internal atau temuan perbaikan berkala

105 Kontrol 2.6.1.e:

Kontrol	Perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa seluruh personel dan pihak berkepentingan lainnya yang memiliki akses terhadap informasi sensitif organisasi telah menandatangani perjanjian kerahasiaan (Non-Disclosure Agreement/NDA). Perjanjian ini harus mencerminkan kebutuhan organisasi dalam melindungi informasi, disusun secara terdokumentasi, ditinjau secara berkala, dan diperbarui sesuai dengan perubahan risiko atau kebijakan keamanan informasi yang berlaku. Hal ini dilakukan untuk mencegah kebocoran, penyalahgunaan, atau akses tidak sah terhadap informasi penting organisasi.
Deskripsi Bukti Dukung	Sebagai bukti pelaksanaan kontrol terkait perjanjian kerahasiaan, organisasi telah menetapkan kewajiban penandatanganan perjanjian tersebut melalui prosedur formal yang tertuang dalam SOP Manajemen SDM. Bukti dukung yang relevan dapat berupa: - SOP Manajemen SDM (Kewajiban perjanjian kerahasiaan) - Perjanjian kerahasiaan di tanda tangani personel
Ancaman/Risiko yang dimitigasi	TH035 TH049 TH064 TH041 TH062 TH075
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.e Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum merencanakan untuk membuat perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.	Tidak ada	Tidak ada
1	Organisasi telah merencanakan untuk membuat perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.	Tersedia draft perjanjian kerahasiaan dan/atau rencana penerapannya	- Draft SOP/NDA - Dokumen rencana sosialisasi/ implementasi NDA
2	Organisasi menjalankan perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya namun belum secara menyeluruh	NDA ditandatangani sebagian, belum semua pihak terkait	- SOP/NDA yang sudah berlaku - Contoh NDA yang ditandatangani sebagian personel/pihak ketiga
3	Organisasi menjalankan perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya secara menyeluruh	NDA diberlakukan kepada semua pihak dan terdokumentasi	- SOP aktif yang mewajibkan NDA - Bukti NDA ditandatangani seluruh personel & mitra
4	Organisasi menjalankan perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya secara menyeluruh dan direviu secara berkala	Reviu dilakukan secara periodik dan terdokumentasi	- Jadwal dan hasil reviu NDA - Revisi NDA atau SOP hasil evaluasi
5	Organisasi menjalankan perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya secara menyeluruh dan direviu secara berkala serta diperbaiki secara berkelanjutan	Tindakan perbaikan dilakukan atas temuan audit atau perubahan risiko	- Dokumen revisi NDA - Laporan audit internal - Notulen rapat perbaikan prosedur NDA

106 Kontrol 2.6.1.f:

Kontrol	Langkah-langkah keamanan harus diterapkan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa ketika personel bekerja dari jarak jauh (remote working), organisasi menerapkan langkah-langkah keamanan yang memadai guna melindungi informasi yang diakses, diproses, atau disimpan di luar lingkungan fisik organisasi. Langkah-langkah ini dapat mencakup penggunaan koneksi aman (seperti VPN), enkripsi perangkat, autentikasi ganda, kebijakan penggunaan perangkat pribadi, serta pengawasan terhadap aktivitas akses jarak jauh guna mencegah kebocoran atau penyalahgunaan data.
Deskripsi Bukti Dukung	Sebagai bukti penerapan langkah-langkah keamanan dalam mendukung kerja jarak jauh, organisasi telah menetapkan kebijakan atau SOP khusus terkait teleworking. Bukti dukung tersebut dapat berupa: - SOP / Kebijakan Teleworking - Permohonan Teleworking
Ancaman/Risiko yang dimitigasi	TH012 TH036 TH040 TH044 TH053 TH065 TH025 TH039 TH043 TH050 TH054
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.f Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum memiliki prosedur mengenai langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi	Tidak ada	Tidak ada
1	Telah membentuk tim penyusunan prosedur langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi	Tim internal atau komite telah dibentuk secara formal untuk menyusun prosedur	- Dokumen pembentukan tim atau surat tugas - Notulen/agenda penyusunan kebijakan
2	Telah menyusun prosedur langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi sudah dijadwalkan untuk diterapkan namun belum disahkan	Prosedur telah dirancang secara lengkap tetapi belum berlaku secara formal	- Draft SOP/Kebijakan teleworking - Jadwal/surat edaran internal terkait rencana implementasi
3	Telah mengesahkan prosedur langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi sudah diterapkan	Dokumen teleworking telah resmi berlaku dan digunakan dalam aktivitas organisasi	- SOP/Kebijakan teleworking yang sudah disahkan - Bukti permohonan kerja jarak jauh oleh pegawai
4	Telah mewajibakan seluruh pegawai untuk menjalankan prosedur langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi	Implementasi sudah berjalan menyeluruh dan bersifat mandatory	- Sosialisasi dan pemberitahuan resmi ke seluruh pegawai - Bukti kepatuhan (e.g., form permohonan dengan checklist keamanan)
5	Telah mewajibkan seluruh pegawai untuk menjalankan prosedur langkah-langkah keamanan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi serta terdapat mekanisme untuk menampung saran/masukan pegawai terhadap prosedur tersebut guna perbaikan berkelanjutan	Sistem keamanan kerja jarak jauh terus disesuaikan dengan kondisi dan umpan balik pegawai	- Bukti mekanisme umpan balik (form evaluasi/feedback pegawai) - Revisi kebijakan berdasarkan saran pegawai - Notulen/rekap perbaikan prosedur

107 Kontrol 2.6.1.g:

Kontrol	Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.
Deskripsi Kontrol	Kontrol ini bertujuan agar organisasi memiliki mekanisme yang jelas dan mudah diakses oleh personel untuk melaporkan setiap kejadian keamanan informasi yang mereka amati atau curigai. Mekanisme ini dapat berupa saluran pelaporan formal seperti email khusus, portal internal, atau hotline yang dijaga kerahasiaannya. Tujuannya adalah untuk mempercepat deteksi insiden, meminimalkan dampak, serta mendorong budaya sadar keamanan di lingkungan kerja.
Deskripsi Bukti Dukung	Sebagai bagian dari implementasi kontrol pelaporan insiden keamanan informasi, organisasi telah menyediakan saluran pelaporan resmi yang dapat diakses oleh seluruh personel. Bukti dukungnya mencakup Email / No telp / Chat terkait channel pelaporan kelemahan
Ancaman/Risiko yang dimitigasi	TH026 TH033 TH036 TH044 TH053 TH055 TH027 TH035 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: GV.RR-04** **NIST CSF 1.1: PR.IP-11** **NIST SP 800-53r5: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21** **SNI ISO/IEC 27001:2022: 5.34, 6.1, 6.5**

Kriteria Pemenuhan Kontrol 2.6.1.g Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum terdapat mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Tidak ada	Tidak ada
1	Telah membentuk tim untuk merumuskan mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Tim kerja atau penanggung jawab mekanisme pelaporan telah ditetapkan	- Surat tugas atau notulen pembentukan tim - Agenda kerja penyusunan mekanisme pelaporan
2	Telah menyusun mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Terdapat draft SOP atau panduan pelaporan, kanal sudah dirancang	- Draft SOP pelaporan insiden - Rencana implementasi kanal pelaporan (email/telepon/chat)
3	Telah mengesahkan mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Kanal pelaporan aktif dan digunakan personel untuk melaporkan insiden	- SOP pelaporan insiden yang berlaku - Email/nomor/chat aktif dan terdokumentasi
4	Telah mengesahkan dan mereviu mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat namun belum dilakukan tindakan perbaikan.	Proses pelaporan dievaluasi untuk efektivitas dan kendala teknis/ organisasional	- Laporan reviu internal - Feedback pengguna kanal pelaporan
5	Telah mengesahkan dan mereviu mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat dan dilakukan tindakan perbaikan berkelanjutan.	Perubahan/perbaikan dilakukan untuk meningkatkan kecepatan, aksesibilitas, dan kejelasan pelaporan	- Dokumentasi perbaikan (revisi SOP/penambahan kanal) - Notulen atau laporan hasil evaluasi dan tindak lanjutnya

2.6.2. Menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber

Kriteria	Detail
Deskripsi	Penyelenggara Identitas dan Informasi Verifikasi (IIV) yang efektif dalam menjalankan kontrol pelatihan dan peningkatan kesadaran keamanan siber adalah organisasi yang secara rutin menyelenggarakan program edukasi terstruktur kepada seluruh personel dan pihak terkait. Program ini mencakup pelatihan dasar hingga lanjutan mengenai ancaman siber, kebijakan keamanan, serta prosedur penanganan insiden. Pelatihan dilengkapi dengan dokumentasi, jadwal berkala, serta evaluasi untuk memastikan seluruh individu memahami tanggung jawab mereka dalam menjaga keamanan informasi organisasi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam program pelatihan dan sumber daya untuk menyelenggarakan pelatihan secara berkala.
Dampak	**Tinggi** – Dengan peningkatan kesadaran dan pemahaman tentang keamanan siber, organisasi dapat mengurangi risiko serangan siber yang disebabkan oleh kesalahan manusia.
Kompleksitas	**Sedang** – Memerlukan program pelatihan yang terstruktur dan materi yang sesuai untuk meningkatkan kesadaran keamanan siber di seluruh organisasi.
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01, PR.AT-02** **NIST CSF 1.1: PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5** **NIST SP 800-53r5: AT-2, AT-3, PM-3, PM-13, PM-14, PS-7, SA-9, CP-3, IR-2** **SNI ISO/IEC 27001:2022: 5.2, 6.3, 7.4**

108 Kontrol 2.6.2.a:

Kontrol	Memberikan pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa seluruh individu dalam organisasi dibekali dengan pelatihan dan pendidikan yang sesuai guna memahami serta menjalankan peran dan tanggung jawab mereka dalam mencegah dan menangani insiden keamanan informasi. Pelatihan ini mencakup pemahaman ancaman, prosedur tanggap insiden, serta praktik terbaik keamanan informasi. Selain itu, organisasi juga diwajibkan mengelola catatan pelatihan secara tertib sebagai bukti partisipasi dan acuan evaluasi kompetensi secara berkala.
Deskripsi Bukti Dukung	Untuk mendukung implementasi kontrol pelatihan dan pendidikan dalam mencegah serta menangani insiden keamanan, organisasi telah menyusun dokumentasi formal dan teknis yang relevan. Bukti dukung mencakup: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait insiden - Jadwal Pelatihan Insiden - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH027 TH039 TH044 TH047 TH053 TH057 TH036 TH043 TH046 TH052 TH056 TH060
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01, PR.AT-02** **NIST CSF 1.1: PR.AT-1, PR.AT-2** **NIST SP 800-53r5: AT-2, PM-3, PM-13, PM-14** **SNI ISO/IEC 27001:2022: 5.2, 6.3**

Kriteria Pemenuhan Kontrol 2.6.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi - Organisasi belum mengidentifikasi jenis-jenis pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi - Organisasi belum memiliki perencanaan yang tepat dalam pelaksanaan program pelatihan dan pendidikan kaitannya dengan insiden keamanan	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi - Organisasi belum memiliki perencanaan yang tepat dalam pelaksanaan program pelatihan dan pendidikan kaitannya dengan insiden keamanan	SOP tersedia, identifikasi awal sudah dimulai, namun pelatihan belum dilaksanakan secara menyeluruh	- SOP Pelatihan dan Induksi - Draft jadwal pelatihan - Identifikasi kebutuhan awal pelatihan
2	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi - Organisasi sudah melakukan identifikasi jenis-jenis pelatihan dan pendidikan yang dibutuhkan semua individu dalam organisasi untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan - Secara sah terdapat dokumen identifikasi jenis-jenis pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi - Organisasi sudah memiliki perencanaan yang tepat dalam pelaksanaan program pelatihan dan pendidikan kaitannya dengan insiden keamanan	Ada dokumen rencana pelatihan, dan jenis pelatihan yang sesuai dengan peran telah ditetapkan	- SOP pelatihan - Dokumen perencanaan pelatihan - Matriks jenis pelatihan berdasarkan jabatan
3	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi - Secara sah terdapat dokumen identifikasi jenis-jenis pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi - Organisasi mengelola catatan kebutuhan pelatihan berdasarkan hasil identifikasi pelatihan dan pendidikan	Pelatihan telah dilaksanakan, peserta sesuai klasifikasi telah mengikuti, catatan tersimpan	- Dokumentasi pelatihan (absensi, notulensi) - Jadwal & daftar hadir pelatihan insiden - Matriks kompetensi vs realisasi
4	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi	Proses klasifikasi personil dan jenis pelatihan sesuai peran telah diterapkan	- Matriks klasifikasi personil - Daftar pelatihan berdasarkan jabatan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Organisasi sudah melakukan identifikasi jenis-jenis pelatihan dan pendidikan yang dibutuhkan oleh semua individu dalam organisasi untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan - Organisasi telah memiliki dan mengelola dokumen identifikasi jenis-jenis pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi serta terdapat klasifikasi personil dengan kriteria yang sesuai dengan jenis-jenis pelatihan yang dibutuhkan. - Seluruh pegawai sesuai klasifikasi kriteria mengikuti pelatihan dan pendidikan yang tepat dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan.		- Evaluasi pemahaman pasca pelatihan
5	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi - Organisasi telah memiliki dan mengelola dokumen identifikasi jenis-jenis pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi serta terdapat klasifikasi personil dengan kriteria yang sesuai dengan jenis-jenis pelatihan yang dibutuhkan. - Seluruh pegawai sesuai klasifikasi kriteria mengikuti pelatihan dan pendidikan yang tepat - Organisasi mengelola catatan pelatihan dan pendidikan yang sudah diberikan serta terdapat mekanisme evaluasi kemampuan SDM pasca pendidikan dan pelatihan sebagai bahan perbaikan berkelanjutan organisasi.	Pelatihan dilakukan terus-menerus, ada umpan balik dan perbaikan terhadap pelaksanaan pelatihan	- Hasil evaluasi pelatihan - Laporan peningkatan/penyesuaian materi - Perbandingan hasil pre-post test pelatihan

109 Kontrol 2.6.2.b:

Kontrol	Memberikan pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. Kemudian, kelola catatan pelatihan dan pendidikan keamanan tersebut.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa semua anggota organisasi dan pihak terkait yang berperan penting dalam manajemen keamanan informasi dibekali dengan pelatihan dan pendidikan yang relevan dan sesuai. Pelatihan ini mencakup pemahaman terhadap potensi ancaman, pencegahan, serta penanganan insiden keamanan. Selain itu, organisasi juga wajib mengelola dan memelihara catatan pelatihan secara terstruktur untuk memastikan bahwa kompetensi personel terjaga dan dapat ditinjau serta dievaluasi secara berkala.
Deskripsi Bukti Dukung	Untuk mendukung pelaksanaan kontrol terkait pelatihan dan pendidikan keamanan bagi anggota organisasi dan pihak terkait, organisasi telah menetapkan prosedur formal dan dokumentasi pendukung. Bukti dukung yang tersedia dapat berupa: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait - Jadwal Pelatihan indisen - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH027 TH039 TH044 TH047 TH053 TH057 TH036 TH043 TH046 TH052 TH056 TH060
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01, PR.AT-02** **NIST CSF 1.1: PR.AT-3** **NIST SP 800-53r5: AT-3, PS-7, SA-9** **SNI ISO/IEC 27001:2022: 5.2, 6.3**

Kriteria Pemenuhan Kontrol 2.6.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Belum mengidentifikasi pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. - Belum ada mekanisme pengelolaan catatan pelatihan dan pendidikan keamanan tersebut.	Tidak ada	Tidak Ada
1	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi dan pihak terkait - Telah membentuk tim untuk mengidentifikasi pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. - Telah membentuk tim penyusunan mekanisme pengelolaan catatan pelatihan dan pendidikan keamanan tersebut.	Ada notulen pembentukan tim atau TOR penyusunan SOP pelatihan	- Draft awal SOP - Daftar tim kerja - Risalah rapat perencanaan
2	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi dan pihak terkait - Secara sah terdapat dokumen identifikasi pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. - Secara sah telah terdapat dokumen mekanisme pengelolaan catatan pelatihan dan pendidikan keamanan tersebut.	SOP tersedia, terdapat daftar pelatihan dan kebutuhan kompetensi	- SOP Pelatihan, - Dokumen Identifikasi Kompetensi, - Matriks Kompetensi
3	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi dan pihak terkait - 50% anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan sudah mendapatkan pendidikan dan pelatihan keamanan, - Pengelolaan catatan pelatihan dan pendidikan keamanan tersebut belum dilaksanakan namun telah direncanakan untuk dilaksanakan.	Daftar peserta pelatihan, dokumentasi pelatihan sebagian personel	- Jadwal pelatihan, - Dokumentasi pelatihan parsial, - Rencana pengelolaan catatan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi dan pihak terkait - Seluruh anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan sudah mendapatkan pendidikan dan pelatihan keamanan, - Melakukan pengelolaan catatan pelatihan dan pendidikan keamanan tersebut telah dilaksanakan.	Bukti pelatihan menyeluruh, catatan kehadiran, dokumentasi evaluasi	- Matriks pelatihan, - Daftar hadir pelatihan, - Dokumentasi pelatihan lengkap
5	- Organisasi sudah memiliki prosedur dalam melakukan identifikasi dan pengelolaan data kebutuhan pelatihan yang diberikan kepada semua individu dalam organisasi dan pihak terkait lainnya - Organisasi sudah mengidentifikasi jenis-jenis pelatihan dan pendidikan namun belum kepada semua individu dalam organisasi dan pihak terkait - Seluruh anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan sudah mendapatkan pendidikan dan pelatihan keamanan, dan terdapat mekanisme evaluasi kemampuan SDM pasca pendidikan dan pelatihan sebagai bahan perbaikan berkelanjutan organisasi. - Mekanisme pengelolaan catatan pelatihan dan pendidikan keamanan tersebut telah dilaksanakan dan menjadi dasar evaluasi perbaikan pengelolaan SDM organisasi berkelanjutan.	Dokumen hasil evaluasi, laporan peningkatan SDM, rencana pelatihan lanjutan	- SOP evaluasi pelatihan, - Laporan hasil evaluasi, - Dokumentasi perbaikan program

110 Kontrol 2.6.2.c:

Kontrol	Meningkatkan isi pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan organisasi.
Deskripsi Kontrol	Kontrol ini bertujuan untuk memastikan bahwa materi pelatihan dan pendidikan keamanan informasi yang diberikan kepada anggota organisasi dan pihak terkait lainnya senantiasa diperbarui dan ditingkatkan secara berkala. Peningkatan dilakukan agar materi tetap relevan, kontekstual, dan sesuai dengan perkembangan ancaman keamanan, teknologi, regulasi, serta kebutuhan organisasi, khususnya bagi individu yang memiliki peran strategis dalam mencegah, mendeteksi, dan menanggulangi insiden keamanan informasi.
Deskripsi Bukti Dukung	Untuk mendukung pelaksanaan kontrol terkait peningkatan isi pelatihan dan pendidikan keamanan, organisasi telah menyediakan sejumlah dokumen pendukung yang relevan. Bukti-bukti ini mencakup: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait - Jadwal Pelatihan keamanan informasi - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH027 TH039 TH044 TH047 TH053 TH057 TH036 TH043 TH046 TH052 TH056 TH060
Referensi Kontrol	**NIST CSF 2.0: PR.AT-02** **NIST CSF 1.1: PR.AT-4, PR.AT-5** **NIST SP 800-53r5: AT-3, CP-3, IR-2, PM-13** **SNI ISO/IEC 27001:2022: 5.2, 6.3, 7.4**

Kriteria Pemenuhan Kontrol 2.6.2.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi belum melaksanakan evaluasi peningkatan isi pelatihan dan pendidikan teentang keamanan yang diberikan kepada anggota organisasi dan pihak trkait lainnya	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi telah merencanakan evaluasi peningkatan materi/isi pendidikan dan pelatihan dengan membentuk tim evaluasi	- Mulai membentuk mekanisme evaluasi - Organisasi telah menyusun prosedur dan membentuk tim evaluasi	- SOP Pelatihan dan Induksi - SK Tim Evaluasi
2	- Organisasi sudah memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi telah melaksanakan evaluasi terhadap materi/isi pelatihan dan pendidikan tentang keamanan yang diberikan kepaa anggota dan pihak terkait lainnya	- Evaluasi telah dilakukan sekali - Organisasi telah melaksanakan satu kali evaluasi terhadap materi pelatihan	- Laporan Evaluasi Materi - Dokumentasi Materi Pelatihan Lama & Baru
3	- Organisasi sudah memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi telah melakukan evaluasi secara berkala untuk meningkatkan materi/isi pelatihan dan pendidikan yang diberikan kepada anggota dan pihak terkait lainnya	- Evaluasi dilakukan secara berkala - Evaluasi dilakukan rutin (misal: tahunan atau per siklus pelatihan)	- Jadwal Evaluasi - Laporan Evaluasi Berkala
4	- Organisasi sudah memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi telah melakukan evaluasi secara berkala untuk meningkatkan materi/isi pelatihan dan pendidikan yang diberikan kepada anggota dan pihak terkait lainnya dan melaksanakan perbaikan berkelanjutan terhadap hasil evaluasi	- Evaluasi digunakan untuk perbaikan materi - Evaluasi bukan hanya dilakukan, tetapi sudah menghasilkan peningkatan isi pelatihan	- Dokumentasi revisi materi - Notulen/surat tindak lanjut hasil evaluasi
5	- Organisasi sudah memiliki prosedur dan mekanisme evaluasi peningkatan pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya - Organisasi telah melakukan evaluasi secara berkala untuk meningkatkan materi/isi pelatihan dan pendidikan yang diberikan kepada anggota dan pihak terkait lainnya dan melaksanakan perbaikan berkelanjutan terhadap hasil evaluasi secara konsisten dan menyeluruh	- Evaluasi & peningkatan dilakukan menyeluruh dan berkelanjutan - Evaluasi dan peningkatan dilakukan secara menyeluruh pada semua materi, rutin dan terdokumentasi	- Rekap perbaikan isi pelatihan tahunan - Form feedback pelatihan - Matriks Kompetensi terbaru

2.6.3. Menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di Penyelenggara IIV

Kriteria	Detail
Deskripsi	Penyelenggara Identitas dan Informasi Verifikasi (IIV) yang menjalankan kontrol ini adalah organisasi yang menyusun dan menerapkan kebijakan formal terkait kompetensi serta keahlian sumber daya manusia di bidang keamanan siber. Kebijakan ini mencakup standar kualifikasi, pelatihan berkelanjutan, serta pengembangan keahlian teknis dan non-teknis yang dibutuhkan untuk menjaga keamanan sistem informasi. Penyelenggara juga memastikan bahwa personel yang bertugas memiliki sertifikasi atau pengalaman yang relevan, dan melakukan evaluasi rutin guna menjamin kesesuaian kompetensi dengan perkembangan ancaman siber dan kebutuhan operasional.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun serta mengimplementasikan kebijakan kompetensi dan keahlian.
Dampak	**Tinggi** – Dengan kebijakan yang jelas, organisasi dapat memastikan bahwa staf keamanan siber memiliki keterampilan dan pengetahuan yang diperlukan untuk melindungi organisasi dari ancaman siber.
Kompleksitas	**Sedang** – Memerlukan kebijakan yang terstruktur dan sistem pelatihan yang tepat untuk memastikan bahwa staf keamanan siber memiliki kompetensi yang memadai.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: pasal 7, 6.1, 6.3, 6.4** **Peraturan BSSN No. 9 Tahun 2023 tentang Peningkatan Kapasitas SDM di Bidang Keamanan Siber dan Sandi**

111 Kontrol 2.6.3.a:

Kontrol	Organisasi perlu menetapkan kebijakan terkait Kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya dengan mengacu kepada Peta Okupasi Keamanan Siber Nasional Indonesia.
Deskripsi Kontrol	Kontrol ini bertujuan memastikan bahwa organisasi memiliki kebijakan tertulis dan terstruktur mengenai kompetensi yang dibutuhkan untuk menjalankan fungsi keamanan siber secara efektif. Kebijakan ini harus mengacu pada Peta Okupasi Keamanan Siber Nasional Indonesia, yang menjadi acuan nasional dalam mengidentifikasi peran, kualifikasi, dan standar kompetensi SDM keamanan siber. Dengan adanya kebijakan ini, organisasi dapat menyelaraskan kebutuhan kompetensi dengan standar nasional dan memastikan bahwa personel yang terlibat dalam keamanan siber memiliki kemampuan yang sesuai untuk mengantisipasi, mencegah, dan menangani insiden keamanan informasi.
Deskripsi Bukti Dukung	Untuk memastikan kesesuaian kompetensi personel keamanan siber dengan Peta Okupasi Keamanan Siber Nasional Indonesia, organisasi telah menetapkan kebijakan yang mendukung pemenuhan standar kompetensi melalui pelatihan dan pengembangan. Bukti dukung atas implementasi kontrol ini mencakup: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait - Jadwal Pelatihan keamanan informasi - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH044 TH053 TH057 TH052 TH056 TH060
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: pasal 7, 6.1** **Peraturan BSSN No. 9 Tahun 2023 tentang Peningkatan Kapasitas SDM di Bidang Keamanan Siber dan Sandi**

Kriteria Pemenuhan Kontrol 2.6.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi belum merencanakan atau menyusun kebutuhan kompetensi dan keahlian sumber daya manusia yang melaksanakan tugas dibidang keamanan siber	Tidak ada	Tidak ada
1	- Organisasi sudah memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi telah memiliki atau membuat draf dokumen kebutuhan kompetensi sumber daya manusia yang melaksanakan tugas dibidang keamanan siber	Tersedia kebijakan atau draft dokumen kebutuhan kompetensi keamanan siber	- Draft kebijakan kompetensi, - Draft SOP pelatihan, - Draft matriks kompetensi SDM
2	- Organisasi sudah memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi telah memiliki atau membuat draf dokumen kebutuhan kompetensi sumber daya manusia yang melaksanakan tugas dibidang keamanan siber	Terdapat dokumen resmi kompetensi keamanan siber internal organisasi	- SOP Pelatihan & Induksi, - Jobdesc SDM keamanan, - Matriks kompetensi belum mengacu ke peta nasional
3	- Organisasi sudah memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi telah memiliki dan mengesahkan dokumen kompetensi sumber daya manusia bidang keamanan siber dan telah mengacu pada Peta okupasi Keamanan Siber	Dokumen kompetensi sudah mengacu ke Peta Okupasi Keamanan Siber Nasional Indonesia	- SOP pelatihan, - Jobdesc keamanan siber, - Matriks kompetensi yang terstandarisasi nasional
4	- Organisasi sudah memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi telah memiliki dan mengesahkan dokumen kompetensi sumber daya manusia bidang keamanan siber yang mengacu pada Peta Okupasi Keamanan Siber dan telah ditinjau secara berkala	Ada bukti reviu berkala kebijakan dan dokumen kompetensi keamanan siber	- Notulen rapat/reviu berkala, - Versi dokumen terdahulu dan terkini, - Laporan evaluasi pelatihan
5	- Organisasi sudah memiliki kebijakan terkait kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya sesuai dengan Peta Okupasi Keamanan Siber Nasional Indonesia - Organisasi telah memiliki dan mengesahkan dokumen kebutuhan sumber daya manusia bidang keamanan siber yang mengacu pada Peta Okupasi Keamanan Siber dan diterapkan dan telah ditinjau serta dilakukan perbaikan secara berkelanjutan.	Organisasi memiliki mekanisme perbaikan berkelanjutan terhadap kompetensi SDM keamanan siber	- SOP pelatihan yang terus diperbarui, - Hasil evaluasi pelatihan, - Update matriks kompetensi berdasarkan hasil evaluasi dan kebutuhan baru

112 Kontrol 2.6.3.b:

Kontrol	Organisasi perlu menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/workshop.
Deskripsi Kontrol	Kontrol ini menekankan bahwa organisasi harus memiliki kebijakan formal yang mengatur pengembangan kompetensi sumber daya manusia (SDM) di bidang keamanan siber, yang dapat dilakukan melalui pelatihan, pendidikan, atau workshop. Kebijakan ini bertujuan untuk memastikan bahwa seluruh personel yang terlibat dalam pengelolaan keamanan informasi memiliki pengetahuan, keterampilan, dan kemampuan yang memadai untuk menghadapi ancaman dan risiko siber yang terus berkembang. Dengan demikian, kebijakan tersebut menjadi dasar strategis untuk peningkatan kapasitas SDM secara berkelanjutan.
Deskripsi Bukti Dukung	Untuk mendukung implementasi kontrol terkait kebijakan pengembangan kompetensi SDM keamanan siber, organisasi telah menyediakan sejumlah dokumen pendukung. Dokumen-dokumen ini mencakup: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait - Jadwal Pelatihan keamanan informasi - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH027 TH039 TH046 TH052 TH056 TH060 TH036 TH044 TH047 TH053 TH057
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: 6.3**

Kriteria Pemenuhan Kontrol 2.6.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Organisasi belum menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/ *workshop*. - Organisasi belum merencanakan atau melakukan penghitungan kebutuhan sumber daya manusia bidang keamanan siber	Tidak ada	Tidak ada
1	- Organisasi sudah menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/*workshop* - Organisasi telah memiliki atau membuat draf dokumen perencanaan peningkatan kapasitas sumber daya manusia bidang keamanan siber namun belum mencakup: 1. Peningkatan kompetensi dan/ atau sertifikasi kompetensi 2. Alih Teknologi dan Alih Keahlian 3. Peningkatan budaya kesadaran keamanan informasi	Adanya dokumen kebijakan dan rencana awal peningkatan SDM namun belum menyeluruh	- Draf kebijakan, - Draf dokumen perencanaan pelatihan, - SOP pelatihan
2	- Organisasi sudah menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/*workshop* - Organisasi telah memiliki atau membuat draf dokumen perencanaan peningkatan kapasitas sumber daya manusia bidang keamanan siber yang mencakup paling sedikit melalui: 1. Peningkatan kompetensi dan/ atau sertifikasi kompetensi 2. Alih Teknologi dan Alih Keahlian 3. Peningkatan budaya kesadaran keamanan informasi	Rencana pelatihan lebih lengkap, namun belum disahkan	- SOP Pelatihan, - Matriks Kompetensi, - Jadwal pelatihan yang mengarah pada 3 aspek tersebut
3	- Organisasi sudah menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/*workshop* - Organisasi telah memiliki dan mengesahkan dokumen peningkatan kapasitas sumber daya manusia bidang keamanan siber yang mencakup paling sedikit melalui: 1. Peningkatan kompetensi dan/ atau sertifikasi kompetensi 2. Alih Teknologi dan Alih Keahlian 3. Peningkatan budaya kesadaran keamanan informasi yang telah diimplemetasikan dan dilakukan evaluasi terhadap pelaksanaan peningkatan kapasitas	Pelatihan telah diberikan dan ada bukti pelaksanaan kepada personel terkait	- Dokumentasi pelatihan, - Daftar peserta, - Sertifikat pelatihan, - Jadwal realisasi
4	- Organisasi sudah menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/*workshop*	Tersedia laporan evaluasi hasil pelatihan	- Laporan evaluasi, - Feedback peserta, - Dokumen revisi pelatihan berdasarkan hasil evaluasi

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Organisasi telah memiliki dan mengesahkan dokumen peningkatan kapasitas sumber daya manusia bidang keamanan siber yang mencakup paling sedikit melalui : 1. Peningkatan kompetensi dan/ atau sertifikasi kompetensi 2. Alih Teknologi dan Alih Keahlian 3. Peningkatan budaya kesadaran keamanan informasi yang telah diimplemetasikan dan dilakukan evaluasi terhadap pelaksanaan peningkatan kapasitas		
5	- Organisasi sudah menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/*workshop* - Organisasi telah memiliki dan mengesahkan dokumen peningkatan kapasitas sumber daya manusia bidang keamanan siber yang mencakup paling sedikit melalui: 1. Peningkatan kompetensi dan/ atau sertifikasi kompetensi 2. Alih Teknologi dan Alih Keahlian 3. Peningkatan budaya kesadaran keamanan informasi yang telah diimplemetasikan, dievaluasi dan diperbaiki secara berkelanjutan	Kebijakan dan pelaksanaan pelatihan direvisi secara rutin dengan bukti tertulis	- Catatan perbaikan berkelanjutan, - Hasil evaluasi tahunan, - Revisi SOP & materi pelatihan

113 Kontrol 2.6.3.c:

Kontrol	Organisasi sektor Pemerintah harus meningkatkan keterampilan dan kompetensi teknis dalam keamanan siber serta perilaku personel terhadap keamanan siber secara berkala dan sesuai dengan perkembangan teknologi dan pemanfaatan TIK.
Deskripsi Kontrol	Kontrol ini menekankan bahwa organisasi sektor Pemerintah wajib secara berkala meningkatkan keterampilan teknis dan kompetensi personel dalam bidang keamanan siber, sejalan dengan perkembangan teknologi dan pemanfaatan TIK (Teknologi Informasi dan Komunikasi). Peningkatan ini tidak hanya mencakup kemampuan teknis, tetapi juga mencakup perilaku dan kesadaran keamanan siber agar personel mampu mengenali, mencegah, dan merespons ancaman siber dengan baik sesuai standar terkini.
Deskripsi Bukti Dukung	Berikut ini disampaikan bukti dukung yang menunjukkan upaya organisasi dalam meningkatkan keterampilan teknis dan kompetensi personel di bidang keamanan siber secara berkala: - SOP Pelatihan dan Induksi Personil - Jobdesc terkait - Jadwal Pelatihan Kompetensi Teknikal - Dokumentasi Pelatihan - Matriks Kompetensi
Ancaman/Risiko yang dimitigasi	TH027 TH039 TH046 TH052 TH056 TH060 TH036 TH044 TH047 TH053 TH057
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: 6.3, 6.4**

Kriteria Pemenuhan Kontrol 2.6.3.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi sektor pemerintah belum memiliki dokumen perencanaan peningkatan kompetensi SDM keamanan siber melalui pendidikan formal dan/atau informal	Tidak ada	Tidak ada
1	Organisasi sektor pemerintah sudah memiliki dokumen perencanaan yang telah ditetapkan terkait peningkatan kompetensi SDM keamanan siber yang telah melalui pendidikan formal dan/atau informal namun belum mengacu pada Standar Kompetensi Bidang Keamanan Siber yang terdiri atas: 1. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang keamanan siber, 2. Standar kompetensi jabatan bidang keamanan siber, atau 3. Standar kompetensi bidang keamanan siber lainnya	Dokumen perencanaan peningkatan kompetensi sudah ditetapkan tetapi belum menjelaskan acuan pada standar nasional	- SOP Pelatihan & Induksi - Draf dokumen perencanaan pelatihan - Jadwal pelatihan umum
2	Organisasi sektor pemerintah sudah memiliki dokumen perencanaan yang telah ditetapkan terkait peningkatan kompetensi SDM keamanan siber yang telah melalui pendidikan formal dan/atau informal yang mengacu pada Standar Kompetensi Bidang Keamanan Siber yang terdiri atas: 1. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang keamanan siber, 2. Standar kompetensi jabatan bidang keamanan siber, atau 3. Standar kompetensi bidang keamanan siber lainnya	Tersedia rencana pelatihan dan kompetensi dengan referensi pada: SKKNI, standar jabatan, atau standar lain yang diakui	- SOP Pelatihan - Dokumen perencanaan - Matriks Kompetensi - Referensi ke SKKNI
3	Organisasi sektor pemerintah telah melaksanakan peningkatan kompetensi SDM keamanan siber sesuai dokumen perencanaan yang telah ditetapkan melalui pendidikan formal dan/atau informal yang mengacu pada Standar Kompetensi Bidang Keamanan Siber yang terdiri atas: 1. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang keamanan siber, 2. Standar kompetensi jabatan bidang keamanan siber, atau 3. Standar kompetensi bidang keamanan siber lainnya	Dokumentasi pelaksanaan pelatihan sesuai rencana yang mengacu pada standar kompetensi nasional	- Jadwal & daftar hadir pelatihan - Laporan pelatihan - Dokumentasi materi pelatihan
4	Organisasi sektor pemerintah melaksanakan dan melakukan evaluasi terhadap peningkatan kompetensi SDM keamanan siber sesuai dokumen perencanaan peningkatan kompetensi SDM keamanan siber	Bukti adanya evaluasi terhadap efektivitas pelatihan (formulir umpan balik, laporan evaluasi, revisi rencana)	- Laporan hasil evaluasi pelatihan - Kuesioner/feedback peserta - Notulen evaluasi berkala
5	Organisasi sektor pemerintah melaksanakan dan melakukan evaluasi terhadap peningkatan kompetensi SDM keamanan siber sesuai dokumen perencanaan dan dilakukan evaluasi dan perbaikan secara berkelanjutan	Ditemukan siklus evaluasi dan perbaikan yang terdokumentasi secara berkelanjutan	- Revisi dokumen pelatihan - Bukti penyesuaian materi berdasarkan evaluasi - Perbandingan hasil kompetensi tahun ke tahun





III DOMAIN DETEKSI

"Domain Deteksi merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam mengembangkan dan menerapkan aktivitas yang sesuai untuk memantau secara tepat waktu terjadinya Peristiwa Siber"

3.1. Mengelola deteksi Peristiwa Siber

Penyelenggara IIV melaksanakan serangkaian proses dan aktivitas yang bertujuan untuk secara efektif dan efisien mengidentifikasi, memvalidasi, menganalisis, dan merespons indikasi potensi atau terjadinya insiden keamanan siber dalam suatu sistem, jaringan, atau lingkungan infrastruktur informasi vital.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber;
b) melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku;
c) menguji prosedur pendeteksian Peristiwa Siber secara berkala; dan
d) menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Mengelola deteksi Peristiwa Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**GV.RR-02, ID.IM-02, DE.AE, DE.AE-06, DE.CM-01**
NIST CSF 1.1	**:**	**DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.CM-1**
NIST SP 800-53r5	**:**	**CA-1, CA-2, CA-7, PM-14, SI-1, SI-3, SI-4, SR-1, SR-9, SR-10, AU-12, CM-3, SC-5, SC-7, AU-6, RA-5**
SNI ISO/IEC 27001:2022	**:**	**5.2, 5.34, 6.8, 8.16, 8.29**

3.1.1. Menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV mendefinisikan secara jelas dan terdokumentasi peran, tanggung jawab, dan akuntabilitas setiap unit, tim, atau individu dalam organisasi terkait dengan implementasi dan operasional kebijakan pendeteksian peristiwa siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menetapkan dan mengomunikasikan peran serta tanggung jawab, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan peran dan tanggung jawab yang jelas, organisasi dapat mengurangi kebingungan dan memastikan respons yang cepat dan efektif terhadap peristiwa siber.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen untuk memastikan bahwa peran dan tanggung jawab ditetapkan dan dipahami dengan jelas.
Referensi Kontrol	**NIST CSF 2.0: GV.RR-02** **NIST CSF 1.1: DE.DP-1** **NIST SP 800-53r5: CA-2, CA-7, PM-14** **SNI ISO/IEC 27001:2022: 5.2**

114 Kontrol 3.1.1.a:

Kontrol	Memperjelas peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan.
Deskripsi Kontrol	Penyelenggara IIV perlu mendefinisikan secara jelas siapa yang bertanggung jawab untuk memantau, menganalisis, dan melaporkan peristiwa keamanan. Penyedia layanan juga harus diberikan peran dalam mendeteksi ancaman pada sistem yang mereka kelola, serta melakukan komunikasi yang efektif dengan organisasi jika ada indikasi peristiwa keamanan. Tujuan dari kontrol ini adalah untuk memastikan bahwa peran dalam deteksi ancaman dibagi dengan jelas antara Penyelenggara IIV dan penyedia layanan, dan semua pihak memiliki prosedur yang telah ditetapkan untuk menangani peristiwa keamanan secara cepat dan tepat.
Deskripsi Bukti Dukung	Dapat berupa dokumen kebijakan dan prosedur keamanan yang menguraikan tanggung jawab masing-masing pihak dalam pemantauan dan deteksi ancaman, serta mekanisme pelaporan dan eskalasi insiden. Selain itu, perjanjian formal seperti Service Level Agreement (SLA) atau Memorandum of Understanding (MoU) dapat digunakan untuk mendefinisikan kewajiban penyedia layanan terkait pemantauan keamanan, waktu respons, serta tindakan yang harus diambil dalam menghadapi peristiwa keamanan. Bukti lainnya dapat mencakup hasil audit kepatuhan, laporan pemantauan keamanan, serta rekaman koordinasi atau komunikasi antara organisasi dan penyedia layanan terkait deteksi ancaman dan penanganannya.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH043 TH050 TH054 TH077 TH036 TH040 TH044 TH053 TH071
Referensi Kontrol	**NIST CSF 2.0: GV.RR-02** **NIST CSF 1.1: DE.DP-1** **NIST SP 800-53r5: CA-2, CA-7, PM-14** **SNI ISO/IEC 27001:2022: 5.2**

Kriteria Pemenuhan Kontrol 3.1.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum adanya kejelasan tentang peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan	Belum ada upaya mendefinisikan dan mendokumentasikan peran serta tanggung jawab terkait deteksi peristiwa keamanan, baik untuk internal organisasi maupun untuk pihak ketiga (penyedia layanan) yang mungkin terlibat.	Tidak ada dokumen atau bukti yang mendukung
1	Peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk mendefinisikan peran dan tanggung jawab, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, email, atau diskusi yang menunjukkan upaya awal dalam mendefinisikan peran dan tanggung jawab.
2	Peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan.	Peran dan tanggung jawab sudah diterapkan secara luas, tetapi belum terdokumentasi secara formal atau disetujui oleh semua pihak.	Dokumen draft yang mencakup sebagian besar aspek peran dan tanggung jawab, tetapi belum disahkan.
3	Peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan	Peran dan tanggung jawab sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti kebijakan keamanan, perjanjian tingkat layanan (SLA), atau kontrak dengan penyedia layanan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	Peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring secara rutin, dan di reviu secara berkala meninjau kembali dan mengevaluasi efektivitasnya. Ada upaya untuk memastikan bahwa proses ini tetap relevan dan efisien seiring waktu.	Selain terdokumentasi dan disetujui, peran dan tanggung jawab dimonitor secara rutin dan di-reviu berkala untuk mengevaluasi efektivitasnya.	Laporan monitoring, catatan reviu, dan dokumen evaluasi yang menunjukkan proses monitoring dan reviu berkala.
5	Peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dilakukan monitoring secara rutin, dan di reviu secara berkala meninjau kembali dan mengevaluasi efektivitasnya, proaktif melakukan perbaikan berkelanjutan dan adaptif terhadap perubahan lingkungan dan ancaman keamanan.	Selain semua kriteria Level 4, organisasi secara proaktif melakukan perbaikan berkelanjutan dan adaptif terhadap perubahan lingkungan dan ancaman keamanan.	Dokumen perbaikan berkelanjutan, catatan adaptasi terhadap ancaman baru, dan bukti implementasi perubahan berdasarkan hasil reviu.

115 Kontrol 3.1.1.b:

Kontrol	Penyelenggara IIV menyiapkan sistem dalam organisasi untuk mendeteksi, menganalisis, dan merespons peristiwa keamanan.
Deskripsi Kontrol	Penyelenggara IIV perlu menyiapkan sistem yang mampu mendeteksi, menganalisis, dan merespons peristiwa keamanan untuk memastikan keamanan informasi yang memadai di seluruh organisasi. Sistem ini harus mencakup alat dan proses untuk mengidentifikasi potensi ancaman, menganalisis dampaknya, dan mengambil langkah yang tepat untuk merespons insiden dengan cepat dan efektif. Langkah- langkah ini meliputi penggunaan sistem deteksi intrusi (IDS), sistem informasi manajemen keamanan (SIEM), dan prosedur operasi standar (SOP) untuk respon insiden. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi memiliki sistem yang terintegrasi dan efisien untuk menangani peristiwa keamanan, baik yang terdeteksi secara otomatis maupun yang dilaporkan oleh personel
Deskripsi Bukti Dukung	Dapat berupa dokumentasi arsitektur dan konfigurasi sistem keamanan, seperti Security Information and Event Management (SIEM), Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS) yang digunakan untuk pemantauan ancaman secara real-time. Selain itu, bukti lain dapat mencakup kebijakan dan prosedur deteksi serta respons insiden, laporan hasil analisis peristiwa keamanan, catatan log keamanan dari sistem pemantauan, serta rekaman uji coba atau simulasi respons terhadap insiden keamanan siber. Audit kepatuhan terhadap standar keamanan yang berlaku, seperti ISO 27001 atau NIST, serta pelatihan staf terkait deteksi dan respons insiden juga dapat menjadi bukti dukung yang relevan.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 3.1.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada sistem untuk mendeteksi peristiwa kamanan - Belum ada sistem untuk menganalisis peristiwa kamanan - Belum ada sistem untuk merespons peristiwa keamanan	Tidak ada upaya untuk menyiapkan sistem deteksi, analisis, atau respons terhadap peristiwa keamanan.	Tidak ada dokumen atau bukti yang mendukung.
1	- Sistem untuk mendeteksi peristiwa keamanan sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Sistem untuk menganalisis peristiwa keamanan sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Sistem untuk merespons peristiwa keamanan sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk menyiapkan sistem deteksi, analisis, dan respons, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam menyiapkan sistem.
2	- Sistem untuk mendeteksi peristiwa keamanan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Sistem untuk menganalisis peristiwa keamanan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Sistem untuk merespons peristiwa keamanan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Sistem sudah diterapkan secara luas, tetapi belum terdokumentasi secara formal atau disetujui oleh semua pihak.	Dokumen draf yang mencakup sebagian besar aspek sistem deteksi, analisis, dan respons, tetapi belum disahkan.
3	- Sistem untuk mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan - Sistem untuk menganalisis peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan - Sistem untuk merespons peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan	Sistem sudah terdokumentasi secara formal dan disetujui oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti kebijakan keamanan, prosedur deteksi, analisis, dan respons, serta panduan operasional.
4	- Sistem untuk mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala - Sistem untuk menganalisis peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala	Selain terdokumentasi dan disetujui, sistem dimonitor secara rutin dan di-*reviu* berkala untuk mengevaluasi efektivitasnya.	Laporan *monitoring*, catatan *reviu*, dan dokumen evaluasi yang menunjukkan proses *monitoring* dan *reviu* berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Sistem untuk merespons peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala		
5	- Sistem untuk mendeteksi peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala serta dilakukan otomatisasi - Sistem untuk menganalisis peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala serta dilakukan otomatisasi - Sistem untuk merespons peristiwa keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala serta dilakukan otomatisasi	Selain semua kriteria Level 4, sistem telah diotomatisasi untuk meningkatkan efisiensi dan efektivitas deteksi, analisis, dan respons terhadap peristiwa keamanan.	Dokumen otomatisasi sistem, catatan implementasi teknologi otomatisasi, dan bukti peningkatan efisiensi dan efektivitas.

3.1.2. Melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku

Kriteria	Detail
Deskripsi	Upaya proaktif dan terstruktur oleh organisasi pengelola infrastruktur informasi vital untuk secara terus menerus memantau, menganalisis, dan mengidentifikasi potensi ancaman dan insiden keamanan siber yang dapat berdampak pada layanan atau aset kritikal mereka. Pelaksanaan ini didasarkan pada kepatuhan terhadap regulasi yang ketat, kebijakan internal yang komprehensif, dan kebutuhan untuk mendeteksi ancaman yang canggih, dengan memanfaatkan teknologi yang tepat, tim yang kompeten, dan kolaborasi yang efektif dengan pihak terkait.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam alat deteksi dan pemantauan, serta pelatihan untuk memastikan kepatuhan terhadap kebijakan yang berlaku.
Dampak	**Tinggi** – Dengan melaksanakan pendeteksian sesuai kebijakan, organisasi dapat mengidentifikasi dan merespons ancaman dengan lebih efektif dan mengurangi risiko serangan siber.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem pemantauan yang efektif dan pelatihan karyawan untuk memastikan kepatuhan terhadap kebijakan pendeteksian.
Referensi Kontrol	**NIST CSF 2.0: DE.AE, DE.CM-01** **NIST CSF 1.1: DE.DP-2, DE.CM-1** **NIST SP 800-53r5: CA-1, CA-2, CA-7, PM-14, SI-1, SI-4, SR-1, SR-9, SR-10, AU-12, CM-3, SC-5, SC-7** **SNI ISO/IEC 27001:2022: 5.34, 8.16**

116 Kontrol 3.1.2.a:

Kontrol	Melakukan proses pemantauan peristiwa keamanan siber, sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku.
Deskripsi Kontrol	Penyelenggara IIV harus melakukan proses pemantauan peristiwa keamanan siber secara berkelanjutan untuk memastikan bahwa ancaman dan insiden yang terjadi dapat dideteksi dan ditangani secara efektif. Proses ini mencakup pemantauan terhadap aktivitas yang mencurigakan, serta pemantauan terhadap sistem dan perangkat yang digunakan dalam organisasi. Pemantauan tersebut harus dilakukan dengan merujuk pada peraturan, arahan, standar industri, dan aturan yang berlaku di sektor terkait. Tujuan dari pemantauan ini adalah untuk memberikan wawasan yang mendalam tentang potensi risiko yang dapat mempengaruhi keamanan siber, serta untuk memastikan kepatuhan terhadap regulasi yang ada.
Deskripsi Bukti Dukung	Dapat berupa dokumentasi kebijakan dan prosedur pemantauan keamanan yang mengacu pada standar seperti ISO 27001, NIST, atau regulasi lokal yang berlaku. Selain itu, laporan hasil pemantauan dari sistem *Security Information and Event Management* (SIEM), *Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS) yang menunjukkan aktivitas deteksi ancaman secara berkelanjutan juga menjadi bukti kuat. Rekaman log keamanan yang dihasilkan oleh perangkat dan aplikasi kritis, hasil audit kepatuhan terhadap standar industri, serta laporan insiden dan tindak lanjutnya dapat menunjukkan bahwa organisasi telah menerapkan pemantauan keamanan yang sesuai. Bukti lainnya mencakup hasil evaluasi efektivitas pemantauan, notulen rapat tim keamanan siber, serta pelatihan staf terkait pemantauan dan deteksi ancaman sesuai dengan regulasi yang berlaku.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE** **NIST CSF 1.1: DE.DP-2** **NIST SP 800-53r5: CA-1, CA-2, CA-7, PM-14, SI-1, SI-4, SR-1, SR-9, SR-10** **SNI ISO/IEC 27001:2022: 5.34**

Kriteria Pemenuhan Kontrol 3.1.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum dilakukan proses pemantauan peristiwa keamanan siber, sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Tidak ada upaya untuk melakukan pemantauan peristiwa keamanan siber.	Tidak ada dokumen atau bukti yang mendukung.
1	Proses pemantauan peristiwa keamanan siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Ada upaya informal untuk melakukan pemantauan, tetapi belum terdokumentasi atau disesuaikan dengan peraturan, arahan, standar industri, dan aturan yang berlaku.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam pemantauan.
2	Proses pemantauan peristiwa keamanan siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Pemantauan sudah dilakukan secara luas, tetapi belum terdokumentasi secara formal atau disesuaikan sepenuhnya dengan peraturan, arahan, standar industri, dan aturan yang berlaku.	Dokumen draf yang mencakup sebagian besar aspek pemantauan, tetapi belum disahkan atau disesuaikan sepenuhnya dengan standar yang berlaku.
3	Proses pemantauan peristiwa keamanan siber sudah diterapkan pada seluruh aspek dan sudah diformalkan sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Pemantauan sudah terdokumentasi secara formal dan disesuaikan dengan peraturan, arahan, standar industri, dan aturan yang berlaku.	Dokumen resmi yang disetujui, seperti kebijakan pemantauan keamanan siber, prosedur pemantauan, dan laporan pemantauan yang sesuai dengan standar industri.
4	Proses pemantauan peristiwa keamanan siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Selain terdokumentasi dan disesuaikan dengan standar, pemantauan dimonitor secara rutin dan di*reviu* berkala untuk mengevaluasi efektivitasnya.	Laporan monitoring, catatan reviu, dan dokumen evaluasi yang menunjukkan proses *monitoring* dan reviu berkala sesuai dengan standar yang berlaku.
5	Proses pemantauan peristiwa keamanan siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala serta dilakukan otomatisasi sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku	Selain semua kriteria Level 4, proses pemantauan telah diotomatisasi untuk meningkatkan efisiensi dan efektivitas, serta tetap mematuhi peraturan, arahan, standar industri, dan aturan yang berlaku.	Dokumen otomatisasi sistem, catatan implementasi teknologi otomatisasi, dan bukti peningkatan efisiensi dan efektivitas pemantauan yang sesuai dengan standar industri.

117 Kontrol 3.1.2.b:

Kontrol	Melakukan pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi.
Deskripsi Kontrol	Penyelenggara IIV harus melakukan pemantauan dan kontrol yang ketat terhadap jaringan pada setiap titik masuk ke dalam jaringan organisasi, seperti *firewall*, *gateway*, *router*, dan perangkat lainnya yang terhubung ke jaringan eksternal. Tujuan dari pemantauan ini adalah untuk mendeteksi adanya potensi ancaman atau akses yang tidak sah, serta memastikan bahwa hanya trafik yang sah yang dapat mengakses sistem dan data organisasi. Proses ini juga melibatkan pengaturan aturan akses dan deteksi intrusi untuk meminimalkan potensi risiko keamanan. Pemantauan dan kontrol ini harus dilakukan secara berkelanjutan untuk mencegah serangan dari luar yang dapat merusak integritas, kerahasiaan, dan ketersediaan informasi dalam organisasi.
Deskripsi Bukti Dukung	Dapat berupa dokumentasi kebijakan dan prosedur keamanan jaringan yang mencakup pemantauan serta pengendalian akses di setiap titik masuk, seperti *firewall*, *gateway*, VPN, dan *proxy server*. Selain itu, laporan dari sistem *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) yang menunjukkan aktivitas pemantauan dan respons terhadap ancaman juga menjadi bukti penting. Rekaman *log* lalu lintas jaringan yang dihasilkan oleh SIEM (*Security Information and Event Management*) serta hasil audit kepatuhan terhadap standar keamanan jaringan, seperti ISO 27001 atau NIST, dapat menunjukkan bahwa pemantauan dilakukan secara efektif. Bukti lainnya mencakup laporan hasil uji penetrasi terhadap jaringan organisasi, hasil konfigurasi *firewall* dan sistem keamanan lainnya, serta dokumentasi evaluasi dan perbaikan terhadap potensi celah keamanan di titik masuk jaringan.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01** **NIST CST 1.1.: DE.CM-1** **NIST SP 800-53r5: AU-12, CA-7, CM-3, SC-5, SC-7, SI-4** **SNI ISO/IEC 27001:2022: 8.16**

Kriteria Pemenuhan Kontrol 3.1.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum dilakukan proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi	Tidak ada upaya untuk melakukan pemantauan dan kontrol jaringan pada titik masuk.	Tidak ada dokumen atau bukti yang mendukung.
1	Proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk melakukan pemantauan dan kontrol jaringan pada titik masuk, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam pemantauan dan kontrol jaringan.
2	Proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Pemantauan dan kontrol jaringan sudah dilakukan secara luas, tetapi belum terdokumentasi secara formal atau disepakati oleh semua pihak.	Dokumen draft yang mencakup sebagian besar aspek pemantauan dan kontrol jaringan, tetapi belum disahkan.
3	Proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi sudah diterapkan pada seluruh aspek dan sudah diformalkan	Pemantauan dan kontrol jaringan sudah terdokumentasi secara formal dan disepakati oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti kebijakan pemantauan jaringan, prosedur kontrol jaringan, dan laporan pemantauan.
4	Proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala	Selain terdokumentasi dan disepakati, pemantauan dan kontrol jaringan dimonitor secara rutin dan di*reviu* berkala untuk mengevaluasi efektivitasnya.	Laporan *monitoring*, catatan *reviu*, dan dokumen evaluasi yang menunjukkan proses monitoring dan *reviu* berkala.
5	Proses pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala serta dilakukan otomatisasi	Selain semua kriteria Level 4, proses pemantauan dan kontrol jaringan telah diotomatisasi untuk meningkatkan efisiensi dan efektivitas.	Dokumen otomatisasi sistem, catatan implementasi teknologi otomatisasi, dan bukti peningkatan efisiensi dan efektivitas pemantauan dan kontrol jaringan.

3.1.3. Menguji prosedur pendeteksian Peristiwa Siber secara berkala

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan pengujian sebagai kegiatan terencana dan sistematis untuk memvalidasi efektivitas dan keandalan mekanisme deteksi yang telah diimplementasikan dalam organisasi, yang bertujuan untuk mengidentifikasi kelemahan, celah, atau inefisiensi dalam prosedur deteksi sebelum insiden keamanan siber yang sebenarnya terjadi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan pengujian secara berkala dan menilai efektivitas prosedur pendeteksian.
Dampak	**Tinggi** – Dengan pengujian yang rutin, organisasi dapat memastikan bahwa prosedur pendeteksian tetap efektif dan dapat mengidentifikasi serta merespons ancaman dengan cepat.
Kompleksitas	**Sedang** – Memerlukan prosedur pengujian yang terstruktur dan sumber daya untuk melakukan pengujian secara berkala.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-02** **NIST CSF 1.1: DE.DP-3** **NIST SP 800-53r5: CA-2, CA-7, SI-3, SI-4, PM-14** **SNI ISO/IEC 27001:2022: 8.29**

118 Kontrol 3.1.3.a:

Kontrol	Penyelenggara IIV melakukan pengujian secara periodik tentang efektifitas perangkat dan prosedur untuk mendeteksi peristiwa keamanan sebagaimana mestinya.
Deskripsi Kontrol	Pengujian periodik terhadap efektivitas perangkat dan prosedur untuk mendeteksi peristiwa keamanan bertujuan untuk memastikan bahwa sistem deteksi yang diterapkan dapat mengenali dan merespons ancaman atau insiden keamanan dengan cepat dan tepat. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi tidak hanya mengimplementasikan alat dan prosedur deteksi, tetapi juga secara rutin mengujinya untuk memastikan keberhasilannya dalam mendeteksi peristiwa yang berisiko tinggi bagi keamanan informasi dan infrastruktur organisasi.
Deskripsi Bukti Dukung	Dapat berupa dokumentasi kebijakan dan prosedur pengujian yang mencakup metode, frekuensi, serta parameter evaluasi efektivitas sistem deteksi. Selain itu, laporan hasil uji coba dari *penetration testing*, *Security Monitoring System* (SIEM), *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan *log* analisis anomali jaringan dapat menunjukkan tingkat efektivitas deteksi ancaman. Bukti lainnya mencakup catatan hasil audit keamanan siber, laporan simulasi insiden keamanan (*tabletop exercise*), serta dokumentasi tindakan perbaikan berdasarkan hasil evaluasi dari pengujian yang telah dilakukan. Hal ini memastikan bahwa perangkat dan prosedur deteksi peristiwa keamanan terus diperbarui dan ditingkatkan sesuai dengan ancaman terbaru.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-02** **NIST CSF 1.1: DE.DP-3** **NIST SP 800-53r5: CA-2, CA-7, SI-3, SI-4, PM-14** **SNI ISO/IEC 27001:2022: 8.29**

Kriteria Pemenuhan Kontrol 3.1.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada SOP Pengujian Perangkat IIV - Belum ada SOP Pendeteksian Peristiwa Keamanan Siber	Tidak ada upaya untuk membuat atau menerapkan SOP Pengujian Perangkat IIV dan SOP Pendeteksian Peristiwa Keamanan Siber.	Tidak ada dokumen atau bukti yang mendukung.
1	- SOP Pengujian Perangkat IIV sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - SOP Pendeteksian Peristiwa Keamanan Siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk membuat dan menerapkan SOP Pengujian Perangkat IIV dan SOP Pendeteksian Peristiwa Keamanan Siber, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam pembuatan dan penerapan SOP.
2	- SOP Pengujian Perangkat IIV sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - SOP Pendeteksian Peristiwa Keamanan Siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	SOP sudah diterapkan secara luas, tetapi belum terdokumentasi secara formal atau disepakati oleh semua pihak.	Dokumen draf yang mencakup sebagian besar aspek SOP Pengujian Perangkat IIV dan SOP Pendeteksian Peristiwa Keamanan Siber, tetapi belum disahkan.
3	- SOP Pengujian Perangkat IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan - SOP Pendeteksian Peristiwa Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan	SOP sudah terdokumentasi secara formal dan disepakati oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti SOP Pengujian Perangkat IIV dan SOP Pendeteksian Peristiwa Keamanan Siber.
4	- SOP Pengujian Perangkat IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala - SOP Pendeteksian Peristiwa Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala	Selain terdokumentasi dan disepakati, SOP dimonitor secara rutin dan di-*reviu* berkala untuk mengevaluasi efektivitasnya.	Laporan *monitoring*, catatan *reviu*, dan dokumen evaluasi yang menunjukkan proses *monitoring* dan *reviu* berkala.
5	- SOP Pengujian Perangkat IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan direviu secara berkala serta dilakukan perbaikan - SOP Pendeteksian Peristiwa Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala serta dilakukan perbaikan	Selain semua kriteria Level 4, dilakukan perbaikan berkelanjutan berdasarkan hasil *monitoring* dan *reviu* untuk meningkatkan efektivitas SOP.	Dokumen perbaikan berkelanjutan, catatan implementasi perbaikan, dan bukti peningkatan efektivitas SOP.

3.1.4. Menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak

Kriteria	Detail
Deskripsi	Proses terstruktur untuk memberitahukan temuan deteksi insiden keamanan siber kepada individu, tim, atau unit organisasi yang memiliki kebutuhan dan wewenang untuk menerima informasi tersebut. dan memastikan bahwa pihak yang tepat mendapatkan informasi yang relevan dan tepat waktu agar dapat mengambil tindakan yang sesuai.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem untuk mendokumentasikan dan menyampaikan informasi hasil pendeteksian, serta pelatihan karyawan tentang prosedur komunikasi yang tepat.
Dampak	**Tinggi** – Dengan komunikasi yang efektif, organisasi dapat memastikan bahwa respons terhadap peristiwa siber dilakukan dengan cepat dan tepat oleh pihak yang berwenang.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang terstruktur untuk mendokumentasikan dan menyampaikan informasi hasil pendeteksian secara efektif.
Referensi Kontrol	**NIST CSF 2.0: DE.AE-06** **NIST CSF 1.1: DE.DP-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, RA-5, SI-4** **SNI ISO/IEC 27001:2022: 6.8**

119 Kontrol 3.1.4.a:

Kontrol	Informasi hasil pendeteksian kejadian keamanan diberitahukan kepada pihak yang terkait sesuai dengan persetujuan manajemen organisasi.
Deskripsi Kontrol	Informasi hasil pendeteksian kejadian keamanan perlu diberitahukan kepada pihak yang terkait, sesuai dengan persetujuan manajemen organisasi. Proses ini memastikan bahwa informasi yang relevan dapat segera diambil tindakan oleh pihak yang berwenang, baik di dalam maupun di luar organisasi, untuk mencegah atau mengurangi dampak dari kejadian tersebut. Tujuan dari kontrol ini adalah untuk menjamin komunikasi yang efektif dan respons yang cepat terhadap insiden keamanan yang terjadi, sesuai dengan kebijakan dan prosedur yang telah disetujui oleh manajemen.
Deskripsi Bukti Dukung	Dapat berupa dokumentasi kebijakan dan prosedur pelaporan insiden keamanan yang mengatur mekanisme, pihak yang berwenang, serta tingkat eskalasi dalam penyampaian informasi. Selain itu, bukti dapat mencakup log komunikasi atau notifikasi insiden, seperti laporan dari *Security Information and Event Management* (SIEM), sistem *ticketing* keamanan, atau *email* resmi yang menunjukkan bahwa hasil deteksi kejadian keamanan telah dilaporkan kepada pihak terkait. Rekaman hasil rapat atau notulen diskusi tentang insiden, termasuk daftar penerima informasi serta tindak lanjut yang disepakati, juga dapat menjadi bukti pendukung. Selain itu, adanya audit *trail* dari sistem keamanan yang menunjukkan riwayat penyampaian informasi kepada pihak internal maupun eksternal yang relevan dapat memperkuat kepatuhan terhadap kebijakan organisasi.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE-06** **NIST CSF 1.1: DE.DP-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, RA-5, SI-4** **SNI ISO/IEC 27001:2022: 6.8**

Kriteria Pemenuhan Kontrol 3.1.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan - Belum ada dokumen NDA	Tidak ada upaya untuk membuat atau menerapkan SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan dan dokumen NDA.	Tidak ada dokumen atau bukti yang mendukung.
1	- SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan sudah diterapkan pada sebagian aspek tapi belum diformalkan - Dokumen NDA sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk membuat dan menerapkan SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan dan dokumen NDA, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam pembuatan dan penerapan SOP dan NDA.
2	- SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Dokumen NDA sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	SOP dan NDA sudah diterapkan secara luas, tetapi belum terdokumentasi secara formal atau disepakati oleh semua pihak.	Dokumen draf yang mencakup sebagian besar aspek SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan dan dokumen NDA, tetapi belum disahkan.
3	- SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan - Dokumen NDA sudah diterapkan pada seluruh aspek dan sudah diformalkan	SOP dan NDA sudah terdokumentasi secara formal dan disepakati oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan dan dokumen NDA.
4	- SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala - Dokumen NDA sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala	Selain terdokumentasi dan disepakati, SOP dan NDA dimonitor secara rutin dan di-*reviu* berkala untuk mengevaluasi efektivitasnya.	Laporan *monitoring*, catatan *reviu*, dan dokumen evaluasi yang menunjukkan proses monitoring dan *reviu* berkala.
5	- SOP Penyampaian Informasi hasil pendeteksian kejadian keamanan sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan di*reviu* secara berkala serta dilakukan perbaikan - Dokumen NDA sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring* dan di*reviu* secara berkala serta dilakukan perbaikan	Selain semua kriteria Level 4, dilakukan perbaikan berkelanjutan berdasarkan hasil *monitoring* dan *reviu* untuk meningkatkan efektivitas SOP dan NDA.	Dokumen perbaikan berkelanjutan, catatan implementasi perbaikan, dan bukti peningkatan efektivitas SOP dan NDA.

120 Kontrol 3.1.4.b:

Kontrol	Penyelenggara IIV melakukan reviu dan peningkatan prosedur pendeteksian peristiwa keamanan secara berkala.
Deskripsi Kontrol	Penyelenggara IIV harus melakukan reviu dan peningkatan prosedur pendeteksian peristiwa keamanan secara berkala untuk memastikan bahwa prosedur yang ada tetap efektif dalam mendeteksi peristiwa atau ancaman keamanan yang mungkin terjadi. Reviu ini bertujuan untuk menyesuaikan prosedur dengan perubahan dalam lanskap ancaman, perkembangan teknologi, dan kebutuhan organisasi. Peningkatan dapat mencakup perubahan dalam metode deteksi, penggunaan alat pendeteksi terbaru, atau pelatihan personel terkait prosedur yang ada. Tujuan dari reviu dan peningkatan ini adalah untuk memastikan sistem pendeteksian selalu optimal dan mampu mengenali ancaman dengan cepat dan akurat. Proses ini juga membantu dalam identifikasi dan penghapusan celah yang mungkin ada dalam sistem pendeteksian yang ada.
Deskripsi Bukti Dukung	Dapat berupa dokumentasi kebijakan dan prosedur yang menetapkan jadwal serta metode evaluasi sistem pendeteksian insiden keamanan. Selain itu, laporan hasil reviu yang mencakup analisis efektivitas alat deteksi, seperti *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan *Security Information and Event Management* (SIEM), serta rekomendasi peningkatan berdasarkan tren ancaman terbaru dapat menjadi bukti. Catatan hasil audit keamanan siber, notulen rapat evaluasi dengan pemangku kepentingan terkait, serta dokumentasi implementasi perbaikan termasuk pembaruan konfigurasi sistem, peningkatan kebijakan deteksi, atau pelatihan tim keamanan juga memperkuat bukti adanya upaya peningkatan berkelanjutan dalam prosedur pendeteksian peristiwa keamanan.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE-06** **NIST CSF 1.1: DE.DP-4** **NIST SP 800-53r5: AU-6, CA-2, CA-7, RA-5, SI-4** **SNI ISO/IEC 27001:2022: 6.8**

Kriteria Pemenuhan Kontrol 3.1.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum ada *Reviu* prosedur secara berkala	Tidak ada upaya untuk melakukan *reviu* prosedur pendeteksian peristiwa keamanan secara berkala.	Tidak ada dokumen atau bukti yang mendukung.
1	*Reviu* prosedur secara berkala sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Ada upaya informal untuk melakukan *reviu* prosedur, tetapi belum terdokumentasi atau disepakati secara resmi.	Catatan informal, *email*, atau diskusi yang menunjukkan upaya awal dalam melakukan *reviu* prosedur.
2	*Reviu* prosedur secara berkala sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	*Reviu* prosedur sudah dilakukan secara luas, tetapi belum terdokumentasi secara formal atau disepakati oleh semua pihak.	Dokumen draft yang mencakup sebagian besar aspek *reviu* prosedur, tetapi belum disahkan.
3	*Reviu* prosedur secara berkala sudah diterapkan pada seluruh aspek dan sudah diformalkan	*Reviu* prosedur sudah terdokumentasi secara formal dan disepakati oleh semua pihak terkait.	Dokumen resmi yang disetujui, seperti laporan *reviu* prosedur dan catatan hasil *reviu* yang terdokumentasi.
4	*Reviu* prosedur secara berkala sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan dikaji secara berkala	Selain terdokumentasi dan disepakati, *reviu* prosedur dimonitor secara rutin dan dikaji berkala untuk mengevaluasi efektivitasnya.	Laporan monitoring, catatan kajian, dan dokumen evaluasi yang menunjukkan proses *monitoring* dan kajian berkala.
5	*Reviu* prosedur secara berkala sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring dan dikaji secara berkala serta dilakukan perbaikan	Selain semua kriteria Level 4, dilakukan perbaikan berkelanjutan berdasarkan hasil *monitoring* dan kajian untuk meningkatkan efektivitas *reviu* prosedur.	Dokumen perbaikan berkelanjutan, catatan implementasi perbaikan, dan bukti peningkatan efektivitas *reviu* prosedur.

3.2. Menganalisis anomali dan Peristiwa Siber

Organisasi wajib melakukan analisis anomali dan peristiwa siber untuk mendeteksi, memahami, dan merespons aktivitas yang mencurigakan atau berpotensi mengancam keamanan sistem informasi serta melaporkan kepada pihak manajemen sesuai ketentuan. Kontrol ini bertujuan untuk meningkatkan kesiapsiagaan terhadap ancaman siber dengan mengidentifikasi pola tidak normal dalam aktivitas jaringan, sistem, dan aplikasi, serta mengambil tindakan mitigasi yang diperlukan sebelum insiden untuk eskalasi lebih lanjut.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data;
b) melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi;
c) menentukan dampak dari Peristiwa Siber yang terdeteksi; dan
d) mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Menganalisis anomali dan Peristiwa Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-07, ID.AM-03**
NIST CSF 1.1	**:**	**DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4**
NIST SP 800-53r5	**:**	**AC-4, CA-3, CA-7, CM-2, SC-16, SI-4, AU-6, RA-3, RA-5, IR-4, IR-5, IR-8, CP-2**
SNI ISO/IEC 27001:2022	**:**	**5.24, 5.25, 8.16**

3.2.1. Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data

Kriteria	Detail
Deskripsi	Penyelenggara IIV wajib menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang dapat mempengaruhi kinerja jaringan komputer dan alur data. Kontrol ini bertujuan untuk memastikan adanya deteksi dini terhadap potensi gangguan operasional, sehingga langkah mitigasi dapat dilakukan sebelum insiden berkembang menjadi gangguan yang lebih besar atau menyebabkan kegagalan layanan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menetapkan serta mendokumentasikan ambang batas peringatan, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan ambang batas yang jelas, organisasi dapat mendeteksi ancaman dan insiden dengan lebih tepat dan meresponsnya dengan cepat serta efektif.
Kompleksitas	**Sedang** – Memerlukan analisis yang komprehensif untuk menetapkan ambang batas dan dokumentasi yang tepat untuk mencatat serta mengomunikasikan ambang batas tersebut.
Referensi Kontrol	**NIST CSF 2.0: ID.AM-03** **NIST CSF 1.1: DE.AE-1** **NIST SP 800-53r5: AC-4, CA-3, CM-2, SC-16, SI-4** **SNI ISO/IEC 27001:2022: 8.16**

121 Kontrol 3.2.1.a:

Kontrol	Penyelenggara IIV menetapkan dan menerapkan prosedur untuk mengidentifikasi dan mengelola ambang batas terhadap operasional jaringan dan arus informasi yang diharapkan antara pengguna, penyelenggara, dan sistem.
Deskripsi Kontrol	Penyelenggara IIV perlu menetapkan dan menerapkan prosedur untuk mengidentifikasi dan mengelola ambang batas yang berkaitan dengan operasional jaringan dan arus informasi antara pengguna, penyelenggara, dan sistem. Hal ini penting untuk memastikan bahwa aliran data dan komunikasi jaringan tetap sesuai dengan ketentuan yang berlaku dan tidak melebihi kapasitas atau batas yang telah ditetapkan, guna menjaga performa jaringan serta mencegah terjadinya gangguan atau kebocoran data. Tujuan dari kontrol ini adalah untuk mengelola dan mengatur trafik informasi yang ada, serta meminimalkan potensi risiko yang mungkin timbul akibat beban operasional yang tidak terkelola dengan baik.
Deskripsi Bukti Dukung	Data dukung berupa kebijakan dan prosedur yang mengatur ambang batas operasional jaringan dan arus informasi antara pengguna, penyelenggara, dan sistem yang sudah disahkan oleh pimpinan organisasi dan dilakukan reviu dan perbaikan secara berkala. Serta melakukan pemantauan kapasitas mencakup seluruh infrastruktur dari jaringan, penyimpanan, hingga sumber daya sistem dan dievaluasi secara rutin untuk memastikan sistem selalu berada dalam kondisi optimal dan sesuai kebutuhan organisasi.
Ancaman/Risiko yang dimitigasi	TH036 TH040 TH044 TH053 TH065 TH077 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.AM-03** **NIST CSF 1.1: DE.AE-1** **NIST SP 800-53r5: AC-4, CA-3, CM-2, SC-16, SI-4** **SNI ISO/IEC 27001:2022: 8.16**

Kriteria Pemenuhan Kontrol 3.2.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada SOP Identifikasi Operasional IIV - Belum ada SOP Pengelolaan Operasional IIV - Belum ada Dokumen *Monitoring* Kapasitas IIV	Tidak ada data dukung berupa kebijakan dan prosedur terkait.	- Tidak ditemukan dokumen kebijakan atau prosedur terkait - Tidak ada bukti komunikasi atau penerapan prosedur pengelolaan kapasitas jaringan dan informasi
1	- SOP Identifikasi Operasional IIV sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - SOP Pengelolaan Operasional IIV sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Dokumen *Monitoring* Kapasitas IIV sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Organisasi sudah melakukan proses identifikasi operasional IIV tetapi belum mencakup keseluruhan sistem, dan melakukan pengelolaan operasional IIV pada sebagian kecil aspek serta melakukan pencatatan dan pelaporan kapasitas tanpa standar yang ditentukan dan tidak disahkan.	- Draft awal SOP yang belum mendapat persetujuan manajemen - Email, memo, atau catatan rapat yang membahas sebagian kecil aspek operasional - Dokumentasi terbatas terkait monitoring kapasitas jaringan.
2	- SOP Identifikasi Operasional IIV sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - SOP Pengelolaan Operasional IIV sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Dokumen *Monitoring* Kapasitas IIV sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Organisasi sudah melakukan proses identifikasi operasional IIV tetapi belum mencakup keseluruhan sistem, dan melakukan pengelolaan operasional IIV pada sebagian besar aspek serta melakukan pencatatan dan pelaporan kapasitas namun dilakukan tanpa standar yang ditentukan dan tidak disahkan.	- SOP yang telah disusun tetapi belum ditetapkan secara resmi. - Notulensi rapat yang menunjukkan pembahasan aspek operasional jaringan secara luas. - Hasil monitoring kapasitas jaringan yang belum terdokumentasi secara sistematis.
3	- SOP Identifikasi Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan - SOP Pengelolaan Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan - Dokumen *Monitoring* Kapasitas IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan	Organisasi sudah melakukan proses identifikasi operasional IIV yang mencakup keseluruhan sistem, dan melakukan pengelolaan operasional IIV pada seluruh aspek serta melakukan pencatatan dan pelaporan kapasitas sesuai standar yang ditentukan dan sudah disahkan.	- Dokumen SOP yang sudah mendapatkan persetujuan resmi dari pimpinan. - SOP tersedia dalam sistem dokumentasi organisasi dan dapat diakses oleh pihak terkait. - Dokumen monitoring kapasitas jaringan telah diformalkan dan digunakan secara aktif.
4	- SOP Identifikasi Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring,* dan di*reviu* secara berkala	- Organisasi sudah melakukan proses identifikasi operasional IIV yang mencakup keseluruhan sistem, dan melakukan pengelolaan operasional IIV pada seluruh aspek serta melakukan pencatatan dan	- Bukti laporan audit internal mengenai kepatuhan terhadap SOP. - Hasil evaluasi rutin terhadap SOP dan rekomendasi perbaikannya.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- SOP Pengelolaan Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, dan direviu secara berkala - Dokumen *Monitoring* Kapasitas IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, dan di*reviu* secara berkala	pelaporan kapasitas sesuai standar yang ditentukan dan sudah disahkan. - Memastikan proses operasional berjalan sesuai prosedur dan dikaji ulang secara berkala untuk meningkatkan efisiensi dan mengakomodasi perubahan kebutuhan operasional organisasi.	- Dokumen *monitoring* kapasitas jaringan yang diperbarui secara berkala berdasarkan evaluasi.
5	- SOP Identifikasi Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis - SOP Pengelolaan Operasional IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis. - Dokumen *Monitoring* Kapasitas IIV sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis	- Organisasi sudah melakukan proses identifikasi operasional IIV yang mencakup keseluruhan sistem, dan melakukan pengelolaan operasional IIV pada seluruh aspek serta melakukan pencatatan dan pelaporan kapasitas sesuai standar yang ditentukan dan sudah disahkan. - Memastikan proses operasional berjalan sesuai prosedur dan dikaji ulang dan dilakukan perbaikan secara berkala untuk meningkatkan efisiensi dan mengakomodasi perubahan kebutuhan operasional organisasi.	- Bukti perubahan SOP berdasarkan hasil evaluasi dan implementasi teknologi baru. - Laporan otomatisasi proses *monitoring* kapasitas jaringan (misalnya penggunaan SIEM, NMS, atau AI-*based monitoring*). - Laporan perbaikan kebijakan berdasarkan tren perkembangan teknologi atau insiden keamanan.

3.2.2. Melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan analisis terhadap peristiwa siber yang terdeteksi untuk mengidentifikasi, memahami, dan merespons insiden siber secara efektif. Proses ini mencakup pengumpulan data dari berbagai sumber, seperti *log* sistem, jaringan, dan *endpoint security*, kemudian mengorelasikan informasi untuk mendeteksi pola anomali atau indikasi serangan. Analisis lebih lanjut dilakukan menggunakan teknik forensik digital dan *framework* keamanan siber untuk mengidentifikasi taktik dan metode serangan. Hasil analisis digunakan untuk menilai dampak insiden, menentukan langkah mitigasi, serta memperkuat kebijakan dan sistem keamanan agar lebih baik terhadap ancaman yang sama kedepannya. Dengan pendekatan ini, organisasi dapat merespons insiden dengan cepat, mengurangi risiko kerugian, dan meningkatkan ketahanan terhadap ancaman siber yang terus berkembang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan alat analisis yang canggih dan tim analis keamanan yang terlatih.
Dampak	**Sangat Tinggi** – Analisis yang tepat dapat mengungkapkan ancaman tersembunyi dan membantu dalam perencanaan mitigasi yang efektif.
Kompleksitas	**Tinggi** – Memerlukan kemampuan analitis yang mendalam dan teknologi yang canggih untuk menganalisis data keamanan.
Referensi Kontrol	**NIST CSF 2.0: DE.AE-02, DE.AE-03, DE.AE-07** **NIST CSF 1.1: DE.AE-2, DE.AE-3** **NIST SP 800-53r5: AU-6, CA-7, RA-5, IR-4, IR-5, IR-8, SI-4, CP-2** **SNI ISO/IEC 27001:2022: 5.24, 5.25**

122 Kontrol 3.2.2.a:

Kontrol	Kejadian keamanan yang terdeteksi dianalisis untuk memahami target dan metode serangan
Deskripsi Kontrol	Penyelenggara IIV harus melakukan analisis terhadap kejadian-kejadian keamanan yang terdeteksi untuk memahami tujuan serangan, metode yang digunakan oleh penyerang, serta dampak yang mungkin ditimbulkan. Proses analisis ini penting untuk memastikan pemahaman yang mendalam mengenai pola serangan, sehingga organisasi dapat meningkatkan sistem pertahanan dan respon terhadap insiden di masa depan. Tujuan kontrol ini adalah untuk memberikan wawasan yang lebih baik tentang ancaman yang dihadapi dan untuk memperbaiki respons keamanan di organisasi.
Deskripsi Bukti Dukung	Data dukung berupa dokumentasi yang menunjukkan bahwa organisasi secara sistematis melakukan analisis terhadap kebijakan keamanan yang ada untuk mengidentifikasi potensi ancaman. Data dukung dapat berupa analisis insiden siber, dokumentasi investigasi forensik digital, serta rekaman *log* dari sistem pemantauan keamanan seperti SIEM, IDS/IPS, dan *firewall*. Bukti dukung ini menunjukkan bahwa organisasi tidak hanya mendeteksi ancaman, tetapi juga memahami pola serangan, mengevaluasi dampaknya, dan memperkuat kebijakan keamanan untuk mencegah insiden serupa di masa depan.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE-02** **NIST CSF 1.1: DE.AE-2** **NIST SP 800-53r5: AU-6, CA-7, RA-5, IR-4, SI-4** **SNI ISO/IEC 27001:2022: 5.24, 5.25**

Kriteria Pemenuhan Kontrol 3.2.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada *tools* untuk melaksanakan analisis terhadap peristiwa siber - Belum ada Petunjuk Teknis Analisis terhadap Peristiwa Siber - Belum ada laporan analisis terhadap peristiwa siber yang terdeteksi	- Tidak ada *tools* yang digunakan untuk analisis peristiwa siber. - Tidak ada petunjuk teknis atau prosedur terkait analisis insiden. - Tidak ada laporan analisis insiden siber yang terdokumentasi.	- Tidak ada *log* keamanan atau catatan insiden siber. - Tidak ada kebijakan atau SOP terkait analisis insiden. - Tidak ada dokumentasi investigasi forensik digital atau hasil analisis serangan
1	- *Tools* untuk melaksanakan analisis terhadap peristiwa siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Petunjuk Teknis Analisis terhadap Peristiwa Siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Laporan analisis terhadap peristiwa siber yang terdeteksi sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	- *Tools* untuk analisis peristiwa siber sudah digunakan tetapi hanya mencakup sebagian kecil aspek, seperti pemantauan log atau deteksi anomali dasar, tanpa adanya prosedur baku atau integrasi yang menyeluruh. - Petunjuk teknis analisis telah diterapkan secara terbatas, hanya dalam bentuk panduan internal atau praktik informal tanpa standar yang terdokumentasi secara resmi. - Selain itu, laporan analisis terhadap peristiwa siber sudah mulai dibuat tetapi belum konsisten dalam penyusunan, format, maupun mekanisme pelaporannya	- Bukti penggunaan beberapa *tools* seperti SIEM atau IDS/IPS, namun belum terdokumentasi dan tanpa adanya prosedur baku atau integrasi yang menyeluruh. - Draf atau dokumen tidak resmi mengenai panduan analisis insiden. - Contoh laporan analisis insiden tetapi belum konsisten dalam penyusunan, format, maupun mekanisme pelaporannya.
2	- *Tools* untuk melaksanakan analisis terhadap peristiwa siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Petunjuk Teknis Analisis terhadap Peristiwa Siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Laporan analisis terhadap peristiwa siber yang terdeteksi sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	- *Tools* analisis siber telah diterapkan pada sebagian besar aspek, tetapi belum diatur secara formal dalam kebijakan organisasi. - Petunjuk teknis analisis peristiwa siber mulai diterapkan di berbagai bagian organisasi, namun masih dalam tahap sosialisasi. - Laporan analisis insiden dibuat secara lebih terstruktur, namun belum menjadi kewajiban.	- Bukti penggunaan tools di lebih banyak aspek, misalnya implementasi SIEM pada beberapa *server* kritis. - Dokumen petunjuk teknis sudah mulai diterapkan, namun belum menjadi SOP resmi atau disahkan. - Beberapa laporan analisis insiden sudah mencantumkan pola serangan dan dampaknya.
3	- *Tools* untuk melaksanakan analisis terhadap peristiwa siber sudah diterapkan pada seluruh aspek dan sudah diformalkan. - Petunjuk Teknis analisis terhadap peristiwa siber sudah diterapkan pada seluruh aspek dan sudah diformalkan. - Laporan analisis terhadap peristiwa siber yang terdeteksi sudah diterapkan pada seluruh aspek dan sudah diformalkan	- *Tools* untuk analisis peristiwa siber sudah digunakan di seluruh aspek yang relevan dan telah diatur dalam kebijakan atau SOP organisasi. - Petunjuk teknis sudah menjadi standar dan wajib diikuti dalam setiap analisis insiden. - Laporan analisis insiden dibuat secara konsisten dan terdokumentasi dengan baik	- SOP yang mengatur penggunaan tools analisis insiden, seperti tata cara penggunaan SIEM, IDS/IPS, dan forensik digital. - Dokumentasi resmi petunjuk teknis analisis insiden, termasuk langkah-langkah investigasi dan metode korelasi data.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Laporan insiden siber yang terdokumentasi dalam format standar organisasi.
4	- *Tools* untuk melaksanakan analisis terhadap peristiwa siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring, dan direviu secara berkala - Petunjuk Teknis Analisis terhadap Peristiwa Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, dan di*reviu* secara berkala - Laporan analisis terhadap peristiwa siber yang terdeteksi sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, dan di*reviu* secara berkala	- *Tools* analisis siber sudah digunakan secara menyeluruh, dengan pemantauan dan evaluasi berkala untuk meningkatkan efektivitasnya. - Petunjuk teknis tidak hanya diterapkan, tetapi juga dimonitoring dan direviu secara berkala agar tetap relevan dengan ancaman terbaru. - Laporan analisis insiden dikaji secara berkala untuk mengidentifikasi tren serangan dan kelemahan keamanan yang perlu diperbaiki.	- Laporan *monitoring* efektivitas tools analisis insiden. - Bukti pelaksanaan *reviu* berkala terhadap petunjuk teknis, seperti notulen rapat atau hasil evaluasi. - Dokumentasi tren serangan berdasarkan hasil analisis insiden sebelumnya.
5	- *Tools* untuk melaksanakan analisis terhadap peristiwa siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis - Petunjuk Teknis Analisis terhadap Peristiwa Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis - Laporan analisis terhadap peristiwa siber yang terdeteksi sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis	- *Tools* analisis siber tidak hanya diterapkan dan dimonitor, tetapi juga terus diperbaiki atau diotomatisasi jika memungkinkan. - Petunjuk teknis terus diperbarui berdasarkan hasil *reviu* dan perkembangan teknologi keamanan siber. - Laporan analisis insiden digunakan untuk perbaikan berkelanjutan, termasuk integrasi *threat intelligence* dan otomatisasi respons insiden.	- Bukti peningkatan atau otomatisasi dalam analisis insiden, seperti implementasi SOAR (*Security Orchestration*, *Automation*, and *Response*). - Dokumentasi perubahan atau perbaikan petunjuk teknis berdasarkan evaluasi berkala. - Penggunaan *threat intelligence* dalam laporan analisis untuk memahami pola serangan yang lebih kompleks.

123 Kontrol 3.2.2.b:

Kontrol	Identifikasi peristiwa keamanan secara akurat dengan menerapkan prosedur untuk melakukan analisis korelasi insiden keamanan dan analisis komparatif dengan informasi ancaman yang diperoleh dari luar organisasi.
Deskripsi Kontrol	Penyelenggara IIV harus mengidentifikasi peristiwa keamanan dengan akurat dengan menggunakan prosedur yang mencakup analisis korelasi insiden keamanan internal dan perbandingan dengan informasi ancaman yang diperoleh dari sumber eksternal. Tujuan dari kontrol ini adalah untuk memastikan bahwa setiap peristiwa yang terdeteksi dapat dianalisis dengan tepat, dengan memanfaatkan data eksternal seperti laporan dari lembaga keamanan atau *platform* berbagi informasi ancaman untuk mendapatkan pemahaman yang lebih komprehensif dan mendalam mengenai ancaman yang dihadapi oleh organisasi. Proses ini juga membantu dalam mempercepat respons terhadap ancaman yang relevan.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencakup dokumentasi prosedur dan SOP yang mengatur analisis korelasi insiden keamanan serta integrasi informasi ancaman eksternal dalam proses identifikasi insiden. Penggunaan SIEM (*Security Information and Event Management*) untuk mengorelasikan log dari berbagai sumber terintegrasi dengan *Threat Intelligence Feeds*, serta penerapan IDS/IPS sebagai sistem deteksi dini menjadi bukti teknis yang mendukung implementasi kontrol ini. Selain itu, laporan analisis insiden yang mencantumkan hasil korelasi dengan indikator serangan eksternal, notulen rapat evaluasi ancaman, serta bukti pelaksanaan monitoring dan pembaruan sistem secara berkala. Dengan adanya bukti dukung ini, organisasi dapat memastikan bahwa setiap insiden keamanan dianalisis secara menyeluruh menggunakan pendekatan berbasis data dan ancaman terkini, sehingga memungkinkan respons yang lebih cepat dan akurat terhadap potensi serangan siber.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE-03, DE.AE-07** **NIST CSF 1.1: DE.AE-3** **NIST SP 800-53r5: AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 3.2.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Belum ada SOP Investigasi Insiden Keamanan Siber - Belum ada Laporan Investigasi Insiden Keamanan Siber	- Tidak ada SOP Investigasi Insiden Keamanan Siber - Tidak ada Laporan Investigasi Insiden Keamanan Siber	- Tidak ditemukan dokumen atau prosedur terkait investigasi insiden keamanan siber - Tidak ada rekam jejak atau Laporan Investigasi Insiden Keamanan Siber
1	- SOP Investigasi Insiden Keamanan Siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan - Laporan Investigasi Insiden Keamanan Siber sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Organisasi mulai menerapkan prosedur investigasi insiden keamanan siber, namun masih dalam tahap awal dan belum memiliki standar yang terdokumentasi secara resmi. Implementasi tersebut terbatas pada beberapa sistem atau unit kerja tertentu, tanpa adanya kebijakan yang mengatur penerapan secara menyeluruh. Selain itu, laporan hasil investigasi insiden telah dibuat untuk beberapa kejadian, tetapi belum memiliki format baku atau mekanisme validasi formal.	- Draft SOP Investigasi Insiden Keamanan ada, tetapi belum mendapatkan persetujuan resmi. - Laporan insiden tersedia namun tidak mengikuti format baku. - Investigasi hanya dilakukan terhadap insiden tertentu tanpa dokumentasi sistematis.
2	- SOP Investigasi Insiden Keamanan Siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan - Laporan Investigasi Insiden Keamanan Siber sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Organisasi telah memiliki prosedur investigasi insiden yang diterapkan secara luas di berbagai sistem, unit kerja, atau infrastruktur keamanan siber, namun masih belum terdokumentasi secara resmi sebagai kebijakan standar. Prosedur tersebut telah digunakan secara konsisten dalam menangani insiden keamanan, tetapi belum memiliki persetujuan formal atau mekanisme kontrol yang mengatur penerapannya secara menyeluruh. Laporan investigasi insiden juga sudah dibuat untuk sebagian besar kejadian yang terjadi, namun format, proses validasi, serta mekanisme pelaporan dan penyimpanan masih bersifat fleksibel dan belum ditetapkan dalam kebijakan resmi.	- Draft SOP telah diterapkan lebih luas tetapi belum ditandatangani atau disahkan oleh manajemen. - Laporan investigasi tersedia dengan format yang lebih sistematis tetapi belum menjadi standar resmi. - Analisis insiden sudah mulai dilakukan tetapi masih bersifat manual dan belum menggunakan *tools* khusus.
3	- SOP Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan - Laporan Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan	Organisasi telah memiliki prosedur investigasi insiden yang terdokumentasi secara resmi dan diterapkan secara menyeluruh di seluruh sistem, unit kerja, dan infrastruktur keamanan siber. SOP tersebut telah ditetapkan sebagai kebijakan formal yang mengatur langkah-langkah investigasi insiden secara sistematis, mulai dari identifikasi, analisis, mitigasi, hingga pelaporan hasil investigasi. Selain itu, laporan investigasi insiden telah dibuat dengan format	- SOP telah disahkan dan didokumentasikan secara resmi. - Semua insiden keamanan yang terdeteksi memiliki laporan resmi yang sesuai dengan prosedur standar.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		standar, menggunakan metodologi yang telah ditetapkan, serta disimpan dalam repositori resmi untuk keperluan audit dan evaluasi.	- Penggunaan alat bantu seperti SIEM mulai diterapkan untuk mendukung investigasi.
4	- SOP Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring, dan direviu secara berkala - Laporan Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring, dan direviu secara berkala	Organisasi tidak hanya memiliki prosedur investigasi insiden yang terdokumentasi dan diterapkan secara menyeluruh, tetapi juga telah menerapkan mekanisme pengawasan dan evaluasi secara berkala. SOP yang ada telah ditetapkan sebagai kebijakan formal dan diterapkan secara konsisten di seluruh sistem dan unit kerja, dengan proses monitoring yang memastikan kepatuhan terhadap prosedur yang telah ditetapkan. Selain itu, laporan investigasi insiden dibuat secara sistematis, dikaji ulang secara berkala, dan digunakan untuk menganalisis tren insiden keamanan serta meningkatkan efektivitas prosedur yang ada.	- SOP telah diterapkan secara menyeluruh dengan mekanisme evaluasi berkala. - Hasil reviu dan monitoring investigasi terdokumentasi dalam laporan berkala. - Investigasi dilakukan dengan integrasi Threat Intelligence dan sistem deteksi otomatis.
5	- SOP Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis - Laporan Investigasi Insiden Keamanan Siber sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis	Organisasi tidak hanya memiliki prosedur investigasi insiden yang terdokumentasi dan diterapkan secara menyeluruh, tetapi juga telah menerapkan mekanisme pengawasan, evaluasi dan perbaikan secara berkala. SOP yang ada telah ditetapkan sebagai kebijakan formal dan diterapkan secara konsisten di seluruh sistem dan unit kerja, dengan proses *monitoring* yang memastikan kepatuhan terhadap prosedur yang telah ditetapkan. Selain itu, laporan investigasi insiden dibuat secara sistematis, dikaji ulang secara berkala, dan digunakan untuk menganalisis tren insiden keamanan serta meningkatkan efektivitas prosedur yang ada. Jika memungkinkan secara teknis, otomatisasi telah diterapkan dalam aspek investigasi insiden, seperti penggunaan SIEM (*Security Information and Event Management*) untuk korelasi *log* dan *Threat Intelligence Feeds* untuk deteksi ancaman lebih cepat.	- SOP dan laporan investigasi dikembangkan dengan pendekatan berkelanjutan menggunakan *feedback* dari insiden sebelumnya. - Sistem investigasi insiden telah diotomatisasi dengan teknologi seperti *Threat Intelligence* otomatis. - Hasil analisis insiden digunakan untuk memperbarui kebijakan keamanan organisasi.

3.2.3. Menentukan dampak dari Peristiwa Siber yang terdeteksi

Kriteria	Detail
Deskripsi	Penyelenggara Infrastruktur Informasi Vital (IIV) harus menentukan dampak dari Peristiwa Siber yang terdeteksi untuk menilai tingkat keparahan dan konsekuensi yang ditimbulkan terhadap sistem, data, serta operasional layanan. Penentuan dampak ini mencakup aspek teknis, operasional, hukum, dan reputasi, sehingga dapat digunakan sebagai dasar dalam pengambilan keputusan terkait respons dan mitigasi. Dengan memahami dampaknya secara menyeluruh, penyelenggara IIV dapat merancang strategi penanggulangan yang tepat, memprioritaskan sumber daya, serta meningkatkan kesiapsiagaan dalam menghadapi ancaman siber di masa mendatang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan penilaian dampak, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan penilaian dampak yang tepat, organisasi dapat merencanakan langkah-langkah mitigasi dan pemulihan yang sesuai untuk mengurangi dampak negatif dari insiden siber.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan metodologi yang tepat untuk menentukan dampak dari peristiwa siber.
Referensi Kontrol	**NIST CSF 2.0: DE.AE-04** **NIST CSF 1.1: DE.AE-4** **NIST SP 800-53r5: CP-2, IR-4, RA-3, SI-4** **SNI ISO/IEC 27001:2022: -**

124 Kontrol 3.2.3.a:

Kontrol	Identifikasi dampak peristiwa keamanan, termasuk dampaknya terhadap organisasi lain yang relevan.
Deskripsi Kontrol	Penyelenggara IIV perlu melakukan identifikasi terhadap dampak peristiwa keamanan, baik yang terjadi di dalam organisasi maupun yang mempengaruhi organisasi lain yang relevan. Dampak ini mencakup kerugian finansial, reputasi, kerusakan operasional, serta ancaman terhadap integritas, kerahasiaan, dan ketersediaan informasi. Identifikasi ini penting untuk memahami luasnya peristiwa keamanan dan menentukan langkah mitigasi yang tepat. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi dapat menilai dan merespons dampak peristiwa keamanan secara efektif, dengan mempertimbangkan hubungan dan ketergantungan terhadap organisasi lain yang terlibat.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencangkup berbagai dokumentasi dan alat analisis yang digunakan dalam proses evaluasi dampak insiden. Bukti tersebut dapat berupa SOP dan pedoman analisis dampak insiden yang menjelaskan langkah-langkah dalam mengidentifikasi dan menilai dampak keamanan terhadap sistem internal maupun pihak eksternal. Selain itu, laporan investigasi insiden keamanan yang mencangkup hasil analisis dampak operasional, reputasi, finansial serta dampak ke organisasi lain.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.AE-04** **NIST CSF 1.1: DE.AE-4** **NIST SP 800-53r5: CP-2, IR-4, RA-3, SI-4** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 3.2.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum ada dokumen Manajemen Risiko berupa dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning*), DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*)	- Tidak ada dokumen SOP yang mengatur langkah-langkah dalam mengidentifikasi, menganalisis, dan merespons insiden keamanan. - Belum memiliki laporan investigasi insiden yang mendokumentasikan kejaidan keamanan siber yang pernah terjadi, termasuk penyebab, dampak, dan tindakan perbaikannya.	- Tidak ada dokumen kebijakan atau pedoman formal terkait penanganan insiden keamanan siber. - Belum memiliki laporan investigasi insiden yang terdokumentasi.
1	Dokumen Manajemen Risiko (dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning),* DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*) sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Organisasi telah mulai menerapkan SOP Investigasi Insiden Keamanan Siber, tetapi hanya pada sebagian kecil aspek yang relevan dengan keamanan siber, dan belum diformalkan dalam dokumen resmi. Implementasi masih bersifat *ad-hoc* atau hanya diterapkan di beberapa unit atau sistem tertentu tanpa standarisasi yang jelas. Laporan investigasi insiden sudah mulai dibuat, tetapi masih dalam skala terbatas dan belum mengikuti format baku atau prosedur yang terdokumentasi dengan baik. Selain itu, belum ada mekanisme *reviu* atau validasi terhadap laporan yang dibuat, sehingga kualitas dan konsistensi investigasi masih bervariasi.	- Dokumen SOP Investigasi Insiden Keamanan Siber sementara atau panduan internal yang digunakan oleh tim keamanan dalam menganani insiden belum disahkan - Laporan investigasi insiden sudah mulai dibuat untuk beberapa kasus keamanan tertentu, tetapi belum konsisten dan belum menjadi bagian dari prosedur standar yang terdokumentasi dengan baik. - Bukti lainnya dapat berupa catatan manual, rekaman investigasi insiden dalam bentuk notulen rapat atau email, serta adanya personel yang telah menjalankan investigasi insiden meskipun tanpa panduan yang terstruktur secara formal.
2	Dokumen Manajemen Risiko (dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning),* DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*) sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Organisasi telah menerapkan SOP Investigasi Insiden Keamanan Siber pada sebagian besar aspek yang relevan, mencakup berbagai unit kerja, sistem, dan infrastruktur TI, tetapi belum diformalkan dalam kebijakan atau prosedur standar yang terdokumentasi secara resmi. Implementasi sudah lebih luas dibandingkan tingkat sebelumnya, memungkinkan proses investigasi insiden lebih terstruktur dan sistematis di berbagai bagian organisasi. Laporan investigasi insiden keamanan siber juga telah diterapkan secara lebih konsisten di sebagian besar kejadian, meskipun belum memiliki format baku atau prosedur yang terdokumentasi dengan baik.	- SOP Investigasi Insiden Keamanan Siber mencangkup berbagai skenario insiiden keamanan dan mulai digunakan oleh tim keamanan siber, meskipun belum terdapat persetujuan formal dari pimpinan. - Laporan investigasi insiden sudah dibuat secara lebih konsisten dan mencakup sebagian besar kejadian yang terjadi, tetapi format dan tata cara pelaporannya mungkin masih bervariasi karena belum terstandarisasi secara resmi. - Selain itu, dapat ditemukan bukti dalam bentuk log insiden yang terdokumentasi dalam sistem manajemen insiden, rekaman komunikasi internal

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			mengenai investigasi insiden, serta penerapan prosedur analisis insiden yang mulai dilakukan oleh berbagai unit terkait dalam organisasi.
3	Dokumen Manajemen Risiko (dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning),* DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*) sudah diterapkan pada seluruh aspek dan sudah diformalkan	SOP Investigasi Insiden Keamanan Siber telah diterapkan secara menyeluruh di seluruh aspek organisasi dan telah diformalkan dalam bentuk kebijakan atau prosedur standar yang terdokumentasi dengan jelas. Semua unit kerja yang relevan telah mengikuti standar operasional yang sama dalam menangani insiden keamanan siber, memastikan konsistensi dalam proses identifikasi, analisis, mitigasi, dan pelaporan insiden. Laporan investigasi insiden keamanan siber juga telah diterapkan pada seluruh kejadian yang relevan, menggunakan format yang baku dan terdokumentasi dengan baik, sehingga memungkinkan organisasi untuk melakukan analisis historis dan evaluasi tren insiden	- Prosedur investigasi insiden keamanan siber telah diterapkan di seluruh aspek organisasi dan diformalkan sebagai kebijakan resmi. Bukti dukung yang dapat ditemukan mencakup dokumen SOP Investigasi Insiden Keamanan Siber yang telah ditandatangani oleh pimpinan, disosialisasikan kepada seluruh pihak terkait, dan digunakan secara konsisten dalam setiap investigasi insiden. - Selain itu, laporan investigasi insiden keamanan telah memiliki format yang baku dan digunakan untuk setiap insiden yang terjadi, dengan dokumentasi yang lengkap, termasuk analisis akar penyebab, dampak, serta langkah mitigasi yang dilakukan. - Bukti lainnya meliputi catatan investigasi insiden yang terdokumentasi dalam sistem manajemen insiden, rekaman rapat evaluasi insiden, serta audit kepatuhan internal yang memastikan bahwa prosedur telah dijalankan sesuai dengan SOP yang ditetapkan.
4	Dokumen Manajemen Risiko (dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning),* DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*) sudah diterapkan pada seluruh aspek dan sudah diformalkan, dimonitoring, dan direviu secara berkala	- SOP Investigasi Insiden Keamanan Siber telah diterapkan secara menyeluruh di seluruh aspek organisasi, diformalkan dalam kebijakan tertulis, serta diterapkan secara konsisten dalam setiap investigasi insiden. Selain itu, dilakukan *monitoring* untuk menilai kepatuhan terhadap SOP dan *reviu* berkala untuk menyesuaikan prosedur sesuai dengan perubahan teknologi, regulasi, atau pola serangan siber terbaru. - Laporan investigasi insiden juga telah diterapkan dengan standar yang seragam dan ditinjau secara berkala guna memastikan bahwa semua insiden tercatat, dianalisis dengan baik, serta memberikan	- Dokumen SOP yang telah disahkan oleh pimpinan dan terdokumentasi dalam sistem manajemen kebijakan keamanan informasi. - *Monitoring* dan *reviu* berkala dibuktikan dengan jadwal evaluasi SOP, hasil *reviu* berkala yang terdokumentasi, serta laporan hasil audit internal atau eksternal yang menilai kepatuhan dan efektivitas pelaksanaan SOP. - Selain itu, terdapat laporan investigasi insiden yang telah diformalkan dengan format baku, mencakup analisis akar penyebab, dampak, dan langkah mitigasi yang dilakukan. - Bukti lainnya meliputi log aktivitas *monitoring* insiden keamanan, rapat evaluasi berkala terkait

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		wawasan yang berharga bagi peningkatan strategi keamanan organisasi.	investigasi insiden, serta tindakan perbaikan yang diterapkan berdasarkan hasil *reviu* untuk meningkatkan efektivitas prosedur investigasi.
5	Dokumen Manajemen Risiko (dokumen Penilaian Risiko (*Risk Assessment*), IRP (*Incident Response Program and Planning),* DRP (*Disaster Recovery Planning*), dan BIA (*Business Impact Analysis*) sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis	- SOP Investigasi Insiden Keamanan Siber telah diterapkan secara menyeluruh, terdokumentasi dengan baik, dan diformalkan oleh pimpinan organisasi. Proses ini tidak hanya di*monitoring* dan di*reviu* secara berkala untuk memastikan efektivitasnya, tetapi juga dilakukan perbaikan secara berkelanjutan berdasarkan hasil evaluasi dan tren ancaman terbaru. - Jika memungkinkan, aspek teknis dari investigasi insiden telah diotomatisasi menggunakan teknologi seperti *Security Information and Event Management* (SIEM), *Threat Intelligence Platform*, atau *Automated Incident Response Systems* untuk meningkatkan kecepatan dan akurasi dalam mendeteksi serta menanggapi insiden. - Laporan investigasi insiden juga telah dikembangkan dengan sistematis, dianalisis menggunakan metode yang lebih baik, dan secara otomatis dikorelasikan dengan data historis serta informasi ancaman eksternal untuk meningkatkan ketepatan dalam penilaian dampak serta rekomendasi perbaikan.	- Dokumen SOP yang telah disahkan dan diperbaharui secara berkala berdasarkan hasil *reviu* dan audit internal atau eksternal - *Monitoring* dan *reviu* berkala dibuktikan dengan jadwal evaluasi SOP, laporan hasil *reviu*, serta *log* perubahan atau perbaikan prosedur berdasarkan temuan sebelumnya. - Laporan investigasi insiden yang terdokumentasi dengan format baku, mencakup analisis akar penyebab, dampak, langkah mitigasi, serta rekomendasi perbaikan yang telah diimplementasikan. - Penggunaan teknologi otomatisasi, seperti SIEM (*Security Information and Event Management*) untuk korelasi *log*, *playbook* otomatis untuk investigasi insiden, atau sistem ticketing yang terintegrasi untuk respons insiden. Selain itu, dashboard pemantauan insiden secara *real-time*, laporan efektivitas perbaikan, serta dokumentasi implementasi perubahan sistem atau kebijakan berdasarkan hasil *reviu* juga menjadi bagian dari bukti dukung.

3.2.4. Mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi

Kriteria	Detail
Deskripsi	Penyelenggara Infrastruktur Informasi Vital (IIV) wajib mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi untuk memastikan transparansi, akuntabilitas, dan efektivitas dalam penanganan insiden. Dokumentasi ini mencakup identifikasi sumber, jenis, dan dampak peristiwa, serta langkah-langkah mitigasi yang telah atau akan diambil. Dengan pencatatan yang sistematis, penyelenggara IIV dapat mengevaluasi pola serangan, meningkatkan strategi pertahanan, serta memperkuat koordinasi dengan pihak terkait dalam rangka meningkatkan keamanan siber secara keseluruhan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem pencatatan yang efektif dan sumber daya untuk mendokumentasikan hasil analisis, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan dokumentasi yang lengkap, organisasi dapat mengakses informasi yang relevan untuk merespons insiden di masa depan dan melakukan perbaikan berkelanjutan.
Kompleksitas	**Sedang** – Memerlukan sistem pencatatan yang tepat dan prosedur untuk mendokumentasikan hasil analisis secara efektif.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

125 Kontrol 3.2.4.a:

Kontrol	Hasil analisis peristiwa siber didokumentasikan, serta dilaporkan kepada pihak manajemen sesuai ketentuan.
Deskripsi Kontrol	Penyelenggara IIV harus mendokumentasikan hasil analisis terhadap peristiwa siber yang terjadi, termasuk penyebab, dampak, dan respons yang dilakukan. Analisis ini juga harus dilaporkan kepada pihak manajemen sesuai dengan ketentuan yang berlaku di organisasi, agar manajemen dapat mengambil keputusan yang tepat berdasarkan informasi yang akurat dan terkini. Tujuan dari kontrol ini adalah untuk memastikan transparansi dalam proses penanganan insiden siber, serta memberikan gambaran yang jelas kepada manajemen mengenai peristiwa siber yang terjadi dan langkah-langkah yang telah diambil untuk mitigasi atau pemulihan.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencakup dokumentasi hasil analisis peristiwa siber dalam bentuk laporan insiden yang mencakup kronologi, analisis teknis, dampak, serta rekomendasi mitigasi. Laporan ini harus tersimpan dalam sistem yang aman dan memiliki histori perubahan untuk memastikan transparansi. Selain itu, terdapat bukti pelaporan kepada pihak manajemen, seperti notulen rapat, *e-mail* resmi, atau sistem *ticketing* yang mencatat eskalasi insiden sesuai dengan prosedur yang ditetapkan. Jika ada ketentuan regulasi atau kebijakan internal, maka bukti dukung juga meliputi konfirmasi penerimaan laporan oleh manajemen serta tindakan yang diambil sebagai respons terhadap laporan tersebut. Contoh data dukung berupa dokumen hasil analisis peristiwa siber, dokumentasi hasil analisis siber, dan pelaporan insiden siber ke manajemen.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 3.2.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum ada proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan.	Organisasi belum memiliki kebijakan, prosedur, atau mekanisme yang jelas terkait dokumentasi dan pelaporan hasil analisis insiden siber.	Tidak ada dokumen formal SOP investigasi insiden, laporan insiden keamanan siber, dan sistem pencacatan insiden yang menunjukkan adanya proses pelaporan.
1	Proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan sudah diterapkan pada sebagian kecil aspek tapi belum diformalkan	Organisasi telah mulai melakukan dokumeentasi dan pelaporan insiden siber tetapi masih dalam lingkup terbatas dan belum memiliki standar yang baku.	Bukti dukung dapat berupa laporan insiden siber yang telah dibuat namun belum konsisten dalam format atau strukturnya, catatan atau rekam jejak komunikasi internal terkait insiden yang disampaikan ke manajemen, seperti email atau notulen rapat, serta adanya inisiatif penerapan prosedur investigasi insiden meskipun belum terdokumentasi dalam bentuk SOP resmi.
2	Proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan sudah diterapkan pada sebagian besar aspek tapi belum diformalkan	Organisasi telah secara aktif melakukan dokumentasi dan pelaporan hasil analisis insiden siber pada berbagai aspek, namun belum memiliki prosedur formal yang baku.	- Bukti dukung dapat berupa laporan insiden siber yang telah dibuat secara rutin dengan format yang mulai seragam tetapi belum sepenuhnya terdokumentasi dalam kebijakan resmi. - Selain itu, catatan komunikasi internal seperti *e-mail*, notulen rapat, atau memo terkait pelaporan insiden ke manajemen juga dapat menjadi bukti. - Adanya *tools* atau sistem yang digunakan untuk mencatat dan melacak insiden, meskipun belum diatur dalam SOP formal, menunjukkan bahwa proses telah berjalan dengan cukup luas. - Bukti lain bisa berupa hasil audit internal atau eksternal yang mencatat bahwa proses dokumentasi dan pelaporan telah diterapkan di sebagian besar unit atau divisi, tetapi masih memerlukan standarisasi formal dalam kebijakan organisasi.
3	Proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan sudah diterapkan pada seluruh aspek dan sudah diformalkan	Organisasi telah melakukan proses dokumentasi dan pelaporan analisis peristiwa siber secara menyeluruh serta diatur dalam kebijakan formal.	- Bukti dukung dapat berupa SOP atau kebijakan resmi yang mengatur mekanisme dokumentasi dan pelaporan hasil analisis insiden siber, termasuk format laporan, pihak yang bertanggung jawab, serta prosedur eskalasi. - Selain itu, adanya laporan insiden siber yang terdokumentasi secara konsisten sesuai ketentuan yang berlaku menunjukkan bahwa prosedur ini telah diterapkan dengan baik. - Sistem atau *platform* manajemen insiden yang digunakan untuk mencatat, menganalisis, dan melaporkan peristiwa siber secara terstruktur. - Hasil audit internal atau eksternal yang mengonfirmasi bahwa proses ini telah berjalan sesuai regulasi serta adanya notulen rapat atau laporan evaluasi rutin terkait insiden yang dilaporkan kepada manajemen semakin memperkuat bukti pemenuhan indeks ini.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	Proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, dan di*reviu* secara berkala	Proses dokumentasi dan pelaporan telah terstandarisasi dan diimplementasikan secara menyeluruh, serta terdapat mekanisme pemantauan dan peninjauan berkala untuk memastikan efektivitasnya.	- Bukti dukung dapat berupa dokumen SOP resmi yang mengatur prosedur dokumentasi dan pelaporan insiden, laporan insiden siber yang konsisten dan terstruktur, serta hasil audit atau *reviu* berkala yang mengevaluasi kepatuhan terhadap prosedur yang telah ditetapkan. - Selain itu, keberadaan sistem manajemen insiden siber (SIEM/IR *Platform*) yang mencatat dan memonitor insiden serta laporan hasil pemantauan dan notulen rapat evaluasi insiden menjadi indikator bahwa proses ini terus diawasi dan ditingkatkan. - Tindakan perbaikan yang diterapkan berdasarkan hasil *reviu* juga menjadi bukti bahwa proses ini tidak hanya berjalan tetapi juga dikembangkan untuk meningkatkan efektivitas manajemen insiden siber secara berkelanjutan.
5	Proses dokumentasi hasil analisis peristiwa siber yang dilaporkan kepada pihak manajemen sesuai ketentuan sudah diterapkan pada seluruh aspek dan sudah diformalkan, di*monitoring*, di*reviu* secara berkala, dan dilakukan perbaikan, atau otomatisasi jika teknis	Proses dokumentasi hasil analisis peristiwa siber telah diterapkan secara menyeluruh, terdokumentasi dalam SOP yang telah diformalkan, serta di*monitoring* dan di*reviu* secara berkala untuk memastikan efektivitasnya.	- Bukti dukung dapat berupa dokumen SOP resmi yang mengatur prosedur dokumentasi dan pelaporan insiden, laporan insiden siber yang tersusun secara sistematis dan konsisten, serta hasil audit atau *reviu* berkala yang mengevaluasi kepatuhan terhadap prosedur yang telah ditetapkan. - Selain itu, adanya sistem otomatisasi, seperti *Security Information and Event Management* (SIEM) atau *Incident Response Platform*, yang mendukung dokumentasi dan pelaporan insiden secara real-time menjadi bukti bahwa organisasi telah mengimplementasikan teknologi untuk meningkatkan efisiensi dan akurasi dalam proses ini. - Bukti lainnya mencakup laporan hasil pemantauan, catatan evaluasi perbaikan berdasarkan *reviu* berkala, serta rekaman implementasi perbaikan yang diterapkan, baik dalam bentuk penyempurnaan prosedur maupun peningkatan sistem otomatisasi untuk mendukung pengelolaan insiden secara lebih efektif dan efisien.

3.3. Memantau Peristiwa Siber berkelanjutan

Dalam melakukan pelindungan terhadap IIV yang dimilikinya, Penyelenggara IIV perlu melakukan pemantauan terhadap peristiwa siber yang terjadi secara berkelanjutan. Pemantauan dilakukan terhadap perangkat, jaringan, aplikasi, serta aktivitas personel dan pihak ketiga. Hal ini diperlukan agar peristiwa anomali yang ditimbulkan oleh infeksi *malware*, pemerolehan akses tidak sah, eksploitasi kerentanan, atau aktivitas tidak wajar lainnya dapat dideteksi lebih dini. Pemantauan dapat dilakukan dengan memanfaatkan alat atau teknologi terotomatisasi dan pencatatan log, dengan tetap disupervisi oleh personel yang berkompeten dan bertanggung jawab. Pemantauan peristiwa siber yang berkelanjutan diharapkan dapat mendukung respons insiden yang lebih tanggap serta meningkatkan keamanan sistem secara keseluruhan.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menerapkan prosedur pendeteksi kode berbahaya dan tak berizin;
b) memonitor kegiatan personel yang berada di dalam lingkup sistem IIV;
c) memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV; dan
d) menerapkan teknologi pemindaian kerentanan terhadap sistem IIV.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Memantau Peristiwa Siber berkelanjutan” secara efektif antara lain:

NIST CSF 2.0	**:**	**DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, ID.RA-01, PR.PS-05**
NIST CSF 1.1	**:**	**DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8**
NIST SP 800-53r5	**:**	**AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, SC-18, SC-44, SI-3, SI-4, SI-8, PS-7, SA-4, SA-9, RA-5**
SNI ISO/IEC 27001:2022	**:**	**5.22, 8.7, 8.8, 8.15, 8.16, 8.19, 8.30**

3.3.1. Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin

Kriteria	Detail
Deskripsi	Salah satu aspek penting dalam pemantauan terhadap IIV adalah mendeteksi keberadaan kode berbahaya yang beroperasi tanpa izin, seperti *malware*, *trojan,* atau *ransomware*. Untuk memastikan deteksi dilakukan secara konsisten dan efektif, diperlukan prosedur teknis yang mengacu pada standar keamanan yang berlaku sebagai acuan pelaksanaan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pendeteksi kode berbahaya serta sumber daya untuk menjalankan dan memelihara sistem pendeteksian.
Dampak	**Tinggi** – Dengan pendeteksian yang tepat, organisasi dapat mengidentifikasi dan menghapus kode berbahaya sebelum dapat menyebabkan kerusakan atau kehilangan data.
Kompleksitas	**Sedang** – Memerlukan pengaturan sistem pendeteksian yang efektif serta pelatihan karyawan untuk mengenali dan merespons ancaman kode berbahaya.
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-09** **NIST CSF 1.1: DE.CM-4, DE.CM-5** **NIST SP 800-53r5: SC-18, SC-44, SI-3, SI-4, SI-8** **SNI ISO/IEC 27001:2022: 8.7, 8.16, 8.19**

126 Kontrol 3.3.1.a:

Kontrol	Gunakan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan. (misalnya perangkat *intrustion detection and prevention systems*, *next-generation firewall*, *endpoint detection and response*, dll)
Deskripsi Kontrol	Teknologi atau alat deteksi otomatis diperlukan untuk deteksi awal kode berbahaya dan tidak berizin. Organisasi perlu menetapkan pemanfaatan teknologi tersebut sebagai prosedur agar menjadi standar minimum dalam melakukan deteksi terhadap kode berbahaya dan tidak berizin. Jika diperlukan, susun petunjuk teknis dari pemasangan hingga pengambilan data untuk memastikan pemanfaatannya optimal. Prosedur berkaitan dengan pemanfaatan teknologi deteksi dapat mencakup peninjauan konfigurasi secara berkala, pembaruan konfigurasi apabila diperlukan, penentuan ambang batas deteksi, kriteria hasil deteksi yang disampaikan ke pihak terkait, serta langkah-langkah lain untuk memastikan efektivitas dan optimalisasi penggunaan perangkat.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini di antaranya adalah dokumen Standar Operasional Prosedur (SOP) deteksi pada sistem dan jaringan, perangkat deteksi sistem dan jaringan, kebijakan anti-malware, penggunaan perangkat pendeteksi perilaku abnormal atau dokumen SOP atau dokumen lain yang menunjukkan penggunaan dan pemanfaatan teknologi deteksi kode berbahaya dan tak berizin.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-09** **NIST CSF 1.1: DE.CM-4, DE.CM-5** **NIST SP 800-53r5: SC-18, SC-44, SI-3, SI-4, SI-8** **SNI ISO/IEC 27001:2022: 8.7, 8.16, 8.19**

Kriteria Pemenuhan Kontrol 3.3.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menggunakan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan.	Tidak ada perangkat teknologi yang digunakan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi telah menerapkan penggunaan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan di sebagian kecil aspek tapi belum diformalkan	- Sudah ada perangkat teknologi yang digunakan. - Perangkat teknologi diterapkan pada sebagian kecil infrastruktur sistem dan jaringan organisasi. - Penggunaan dan pemanfaatan perangkat teknologi tidak tertulis dalam prosedur deteksi yang telah ditetapkan.	- Topologi sistem dan jaringan organisasi dan titik-titik pemasangan perangkat. - SOP deteksi pada sistem dan jaringan organisasi yang didalamnya tidak tertulis penggunaan dan pemanfaatan perangkat teknologi deteksi.
2	Organisasi telah menerapkan penggunaan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan di sebagian besar aspek tapi belum diformalkan	- Sudah ada perangkat teknologi yang digunakan. - Perangkat teknologi diterapkan pada sebagian besar infrastruktur sistem dan jaringan organisasi. - Penggunaan dan pemanfaatan perangkat teknologi tidak tertulis dalam prosedur deteksi yang telah ditetapkan.	- Topologi sistem dan jaringan organisasi dan titik-titik pemasangan perangkat. - SOP deteksi pada sistem dan jaringan organisasi yang didalamnya tidak tertulis penggunaan dan pemanfaatan perangkat teknologi deteksi.
3	Organisasi sudah menerapkan penggunaan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan di seluruh aspek dan sudah diformalkan	- Sudah ada perangkat teknologi yang digunakan. - Perangkat teknologi diterapkan pada seluruh infrastruktur sistem dan jaringan organisasi. - Penggunaan dan pemanfaatan perangkat teknologi tertulis dalam prosedur deteksi yang telah ditetapkan.	- Topologi sistem dan jaringan organisasi dan titik-titik pemasangan perangkat. - SOP deteksi pada sistem dan jaringan organisasi yang didalamnya tertulis penggunaan dan pemanfaatan perangkat teknologi deteksi.
4	Organisasi sudah menerapkan penggunaan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan di seluruh aspek dan sudah diformalkan, melakukan *monitoring* dan dilakukan *reviu* prosedur secara berkala.	- Sudah ada perangkat teknologi yang digunakan. - Perangkat teknologi diterapkan pada seluruh infrastruktur sistem dan jaringan organisasi. - Penggunaan dan pemanfaatan perangkat teknologi tertulis dalam prosedur deteksi yang telah ditetapkan. - Pelaksanaan prosedur terpantau.	- Topologi sistem dan jaringan organisasi dan titik-titik pemasangan perangkat. - SOP deteksi pada sistem dan jaringan organisasi yang didalamnya tertulis penggunaan dan pemanfaatan perangkat teknologi deteksi. - Dokumentasi peninjauan prosedur.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		- Prosedur ditinjau secara berkala.	
5	Organisasi sudah menerapkan penggunaan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan di seluruh aspek dan sudah diformalkan, melakukan *monitoring* dan dilakukan *reviu* prosedur secara berkala, serta dilakukan perbaikan prosedur dan pembaruan perangkat secara berkelanjutan.	- Sudah ada perangkat teknologi yang digunakan. - Perangkat teknologi diterapkan pada seluruh infrastruktur sistem dan jaringan organisasi. - Penggunaan dan pemanfaatan perangkat teknologi tertulis dalam prosedur deteksi yang telah ditetapkan. - Pelaksanaan prosedur terpantau. - Prosedur ditinjau secara berkala. - Dilakukan pembaruan prosedur apabila diperlukan.	- Topologi sistem dan jaringan organisasi dan titik-titik pemasangan perangkat. - SOP deteksi pada sistem dan jaringan organisasi yang didalamnya tertulis penggunaan dan pemanfaatan perangkat teknologi deteksi. - Dokumentasi peninjauan dan/atau pembaruan prosedur.

127 Kontrol 3.3.1.b:

Kontrol	Memvalidasi apakah informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan.
Deskripsi Kontrol	Selain mendeteksi perilaku abnormal, perlu juga untuk mendeteksi informasi atau file yang diterima. Sebelum informasi dan file tersebut diakses, perlu dilakukan deteksi apakah informasi dan file tersebut merupakan informasi dan file yang aman tidak mengandung kode berbahaya. Kontrol ini dapat diterapkan dengan menerapkan perangkat deteksi pada sistem.
Deskripsi Bukti Dukung	Bukti dukung dari diterapkannya kontrol ini dapat berupa dokumen hasil pemindaian antivirus/antimalware, SOP anti-malware, SOP penggunaan file dari internet, dokumentasi otorisasi menggunakan file dari dunia maya pada sistem kritikal, atau dapat ditunjukkannya penggunaan teknologi auto scan pada email, cloud atau aset lainnya di dunia maya.
Ancaman/Risiko yang dimitigasi	TH036 TH050 TH039 TH065
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-09** **NIST CSF 1.1: DE.CM-4, DE.CM-5** **NIST SP 800-53r5: SC-18, SC-44, SI-3, SI-4, SI-8** **SNI ISO/IEC 27001:2022: 8.7, 8.16, 8.19**

Kriteria Pemenuhan Kontrol 3.3.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan.	Tidak ada SOP yang diterapkan dan tidak ada perangkat teknologi yang digunakan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi sudah menerapkan prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan, pada sebagian kecil aspek tapi belum diformalkan	- Prosedur belum diformalkan menjadi dokumen resmi. - Baru sebagian kecil personel yang memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur baru diterapkan pada sebagian kecil bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa baru sebagian kecil personel yang memahami prosedur yang harus dilakukan ketika menerima informasi atau file dari dunia maya, atau bahwa prosedur hanya diterapkan pada sebagian kecil sistem
2	Organisasi sudah menerapkan prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan, pada sebagian besar aspek tapi belum diformalkan	- Prosedur belum diformalkan menjadi dokumen resmi. - Sebagian besar personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada sebagian besar bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa sudah sebagian besar personel yang memahami prosedur yang harus dilakukan ketika menerima informasi atau file dari dunia maya, atau bahwa prosedur sudah diterapkan pada sebagian besar sistem.
3	Organisasi sudah menerapkan prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan, pada seluruh aspek dan sudah diformalkan	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan ketika menerima informasi atau file dari dunia maya, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem.
4	Organisasi sudah menerapkan prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan, pada seluruh aspek dan sudah	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan ketika menerima informasi atau file dari dunia maya,

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	diformalkan, dilakukan *monitoring* dan *reviu* prosedur secara berkala.	- Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut.	atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan.
5	Organisasi sudah menerapkan prosedur validasi informasi atau *file* yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan, pada seluruh aspek dan sudah diformalkan, dilakukan *monitoring* dan *reviu* prosedur secara berkala, serta melakukan perbaikan prosedur secara berkelanjutan, dan mengarah pada otomatisasi	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan. - Organisasi menerapkan teknologi deteksi yang secara otomatis memindai informasi atau file yang didapat dari dunia maya.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan ketika menerima informasi atau file dari dunia maya, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada). - Dokumen yang menunjukkan penerapan teknologi deteksi yang secara otomatis memindai informasi atau file yang didapat dari dunia maya pada sistem IIV.

128 Kontrol 3.3.1.c:

Kontrol	Memvalidasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan.
Deskripsi Kontrol	Apabila informasi dan/atau data yang didapat dari dunia maya sudah terbukti aman dan tidak mengandung kode berbahaya, hal yang selanjutnya harus dipastikan adalah mengenai kebenaran dan keaslian informasi dan/atau file tersebut. Salah satu cara yang dapat dilakukan untuk menerapkan kontrol ini adalah dengan menerapkan prosedur untuk melakukan validasi terhadap informasi dan/atau file yang diterima dari dunia maya. Organisasi harus memastikan setiap personel memahami dan menerapkan prosedur tersebut serta dilakukan peninjauan dan perbaikan secara berkala.
Deskripsi Bukti Dukung	Bukti dukung dari diterapkannya kontrol ini dapat berupa dokumen laporan validasi hash, SOP Penggunaan file dari internet, dokumentasi otorisasi menggunakan file dari dunia maya pada sistem kritis, atau dokumen yang menunjukkan penggunaan teknologi yang dapat otomatis memeriksa validitas dari informasi dan/atau file yang didapat.
Ancaman/Risiko yang dimitigasi	TH036 TH040 TH054 TH038 TH050
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-09** **NIST CSF 1.1: DE.CM-4, DE.CM-5** **NIST SP 800-53r5: SC-18, SC-44, SI-3, SI-4, SI-8** **SNI ISO/IEC 27001:2022: 8.7, 8.16, 8.19**

Kriteria Pemenuhan Kontrol 3.3.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur untuk melakukan validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan	Tidak ada SOP yang diterapkan dan tidak ada perangkat teknologi yang digunakan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi sudah menerapkan prosedur validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan pada sebagian kecil aspek tapi belum diformalkan	- Prosedur belum diformalkan menjadi dokumen resmi. - Baru sebagian kecil personel yang memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur baru diterapkan pada sebagian kecil bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa baru sebagian kecil personel yang memahami prosedur yang harus dilakukan untuk memvalidasi informasi atau file yang diterima dari dunia maya, atau bahwa prosedur hanya diterapkan pada sebagian kecil sistem.
2	Organisasi sudah menerapkan prosedur validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan pada sebagian besar aspek tapi belum diformalkan	- Prosedur belum diformalkan menjadi dokumen resmi. - Sebagian besar personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada sebagian besar bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa sudah sebagian besar personel yang memahami prosedur yang harus dilakukan untuk memvalidasi informasi atau file yang diterima dari dunia maya, atau bahwa prosedur sudah diterapkan pada sebagian besar sistem.
3	Organisasi sudah menerapkan prosedur validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan pada seluruh aspek dan sudah diformalkan	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan untuk memvalidasi informasi atau file yang diterima dari dunia maya, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem.
4	Organisasi sudah menerapkan prosedur validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan dan dilakukan pada seluruh	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan untuk memvalidasi informasi atau file yang diterima dari dunia

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	aspek dan sudah diformalkan, dilakukan *monitoring* dan *reviu* prosedur secara berkala.	- Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut.	maya, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan.
5	Organisasi sudah menerapkan prosedur validasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan pada seluruh aspek dan sudah diformalkan, dilakukan *monitoring* dan *reviu* prosedur secara berkala, serta melakukan perbaikan prosedur secara berkelanjutan, dan mengarah pada otomatisasi	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan. - Organisasi menerapkan teknologi deteksi yang secara otomatis memvalidasi informasi atau file yang didapat dari dunia maya.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur yang harus dilakukan untuk memvalidasi informasi atau file yang diterima dari dunia maya, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada). - Dokumen yang menunjukkan penerapan teknologi deteksi yang secara otomatis memvalidasi informasi atau file yang didapat dari dunia maya pada sistem IIV.

3.3.2. Memonitor kegiatan personel yang berada di dalam lingkup sistem IIV

Kriteria	Detail
Deskripsi	Apabila deteksi terhadap kode berbahaya yang beroperasi tanpa izin telah dilakukan, yang perlu dilakukan selanjutnya adalah melakukan deteksi terhadap kegiatan personel yang beroperasi di dalam lingkup sistem IIV. Hal ini penting karena sumber daya manusia seringkali menjadi rantai terlemah dari pelindungan sistem yang telah diterapkan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem pemantauan dan pencatatan aktivitas serta sumber daya untuk melakukan pemantauan berkala.
Dampak	**Tinggi** – Dengan pemantauan yang tepat, organisasi dapat mengidentifikasi dan mengatasi tindakan yang tidak sesuai dengan kebijakan keamanan, sehingga mengurangi risiko kesalahan manusia atau penyalahgunaan akses.
Kompleksitas	**Sedang** – Memerlukan sistem pemantauan yang tepat serta prosedur untuk memantau dan mencatat aktivitas personel secara efektif.
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, PR.PS-05** **NIST CSF 1.1: DE.CM-3, DE.CM-7** **NIST SP 800-53r5: AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, SI-4** **SNI ISO/IEC 27001:2022: 8.15, 8.16**

129 Kontrol 3.3.2.a:

Kontrol	Memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.
Deskripsi Kontrol	Kontrol ini dapat dilakukan dengan menerapkan prosedur yang dapat memastikan bahwa personel tidak melakukan hal-hal yang berisiko bagi sistem IIV. Prosedur tersebut perlu dievaluasi secara berkala. Organisasi perlu memastikan prosedur tersebut dipahami dan dilaksanakan oleh seluruh personel.
Deskripsi Bukti Dukung	Bukti dukung yang ditunjukkan untuk menunjukkan kontrol ini dapat berupa kebijakan akses dan koneksi ke sistem kritikal, SOP manajemen akses, SOP pemasangan perangkat lunak, dokumen otoritasi ke sistem kritikal, dan lain-lain.
Ancaman/Risiko yang dimitigasi	TH043 TH046 TH050 TH071 TH044 TH047 TH053
Referensi Kontrol	**NIST CSF 2.0: DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, PR.PS-05** **NIST CSF 1.1: DE.CM-3, DE.CM-7** **NIST SP 800-53r5: AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, SI-4** **SNI ISO/IEC 27001:2022: 8.15, 8.16**

Kriteria Pemenuhan Kontrol 3.3.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	Tidak ada SOP yang diterapkan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi sudah menerapkan prosedur pada sebagian kecil aspek tapi belum diformalkan untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV	- Prosedur belum diformalkan menjadi dokumen resmi. - Baru sebagian kecil personel yang memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur baru diterapkan pada sebagian kecil bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa baru sebagian kecil personel yang memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV, atau bahwa prosedur hanya diterapkan pada sebagian kecil sistem.
2	Organisasi sudah menerapkan prosedur pada sebagian besar aspek tapi belum diformalkan untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV	- Prosedur belum diformalkan menjadi dokumen resmi. - Sebagian besar personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada sebagian besar bagian sistem.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa sudah sebagian besar personel yang memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV, atau bahwa prosedur sudah diterapkan pada sebagian besar sistem.
3	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem.
4	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur tidak boleh dilakukannya koneksi

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV, dilakukan *monitoring* dan di*reviu* secara berkala.	dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut.	dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan.
5	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV, dilakukan *monitoring* dan di*reviu* secara berkala, serta diperbaiki prosedurnya secara berkelanjutan.	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh personel memahami dan melaksanakan prosedur yang perlu dilakukan, atau prosedur telah diterapkan pada seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan.	- SOP yang telah diformalkan. - Wawancara terhadap personel yang beroperasi di sistem IIV menunjukkan bahwa seluruh personel telah memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV, atau bahwa prosedur sudah diterapkan pada seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada).

3.3.3. Memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV

Kriteria	Detail
Deskripsi	Apabila teknologi dan sumber daya manusia internal sudah dalam kontrol, hal lain yang perlu dikontrol adalah pihak ketiga. Keterlibatan pihak ketiga dapat memunculkan risiko baru pada lingkup sistem IIV sehingga diperlukan kontrol khusus untuk memonitor kegiatan pihak ketiga agar tidak menjadi titik lemah rantai yang dapat dieksploitasi pihak tidak berwenang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem pemantauan dan pencatatan aktivitas serta sumber daya untuk melakukan pemantauan berkala terhadap pihak ketiga.
Dampak	**Tinggi** – Dengan pemantauan yang tepat, organisasi dapat mengidentifikasi dan mengatasi tindakan yang tidak sesuai dengan kebijakan keamanan yang dilakukan oleh pihak ketiga, sehingga mengurangi risiko keamanan dari ketergantungan eksternal.
Kompleksitas	**Sedang** – Memerlukan sistem pemantauan yang tepat serta prosedur untuk memantau dan mencatat aktivitas pihak ketiga secara efektif.
Referensi Kontrol	**NIST CSF 2.0: DE.CM-06** **NIST CSF 1.1: DE.CM-6** **NIST SP 800-53r5: CA-7, PS-7, SA-4, SA-9, SI-4** **SNI ISO/IEC 27001:2022: 5.22, 8.30**

130 Kontrol 3.3.3.a:

Kontrol	Memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.
Deskripsi Kontrol	Kontrol ini dapat dilakukan dengan menerapkan prosedur yang dapat memastikan bahwa pihak ketiga tidak melakukan hal-hal yang berisiko bagi sistem IIV. Prosedur tersebut perlu dievaluasi secara berkala. Organisasi perlu memastikan prosedur tersebut dipahami dan dilaksanakan oleh semua pihak ketiga yang terlibat dalam menyelenggarakan sistem IIV.
Deskripsi Bukti Dukung	Bukti dukung yang dapat digunakan untuk menunjukkan diterapkannya kontrol ini adalah dokumen kebijakan akses dan koneksi ke sistem kritikal, SOP Manajemen Akses, SOP Pemasangan Perangkat Lunak, dokumen otorisasi ke sistem kritikal, dokumen yang menunjukkan diselenggarakannya kegiatan sosialisasi prosedur kepada vendor, daftar dan hasil identifikasi vendor beserta personil dan hak aksesnya, dan lain-lain.
Ancaman/Risiko yang dimitigasi	TH043 TH046 TH050 TH071 TH044 TH047 TH053
Referensi Kontrol	**NIST CSF 2.0: DE.CM-06** **NIST CSF 1.1: DE.CM-6** **NIST SP 800-53r5: CA-7, PS-7, SA-4, SA-9, SI-4** **SNI ISO/IEC 27001:2022: 5.22, 8.30**

Kriteria Pemenuhan Kontrol 3.3.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur untuk memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	Tidak ada SOP yang diterapkan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi sudah menerapkan prosedur pada sebagian kecil aspek tapi belum diformalkan untuk memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV	- Prosedur belum diformalkan menjadi dokumen resmi. - Baru sebagian kecil dari pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV yang memahami dan melaksanakan prosedur yang perlu dilakukan.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel vendor/pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV menunjukkan bahwa baru sebagian kecil pihak ketiga yang terlibat memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV.
2	Organisasi sudah menerapkan prosedur pada sebagian besar aspek tapi belum diformalkanuntuk memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV	- Prosedur belum diformalkan menjadi dokumen resmi. - Sebagian besar dari pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV memahami dan melaksanakan prosedur yang perlu dilakukan.	- Belum adanya SOP yang diformalkan. - Wawancara terhadap personel vendor/pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV menunjukkan bahwa sudah sebagian besar pihak ketiga yang terlibat memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV.
3	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV memahami dan melaksanakan prosedur yang perlu dilakukan.	- SOP yang telah diformalkan. - Wawancara terhadap personel vendor/pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV menunjukkan bahwa seluruh pihak ketiga yang terlibat telah memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV.
4	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa pihak ketiga yang berada	- Prosedur sudah diformalkan menjadi dokumen resmi.	- SOP yang telah diformalkan. - Wawancara terhadap personel vendor/pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV, dilakukan *monitoring* dan di*reviu* secara berkala.	- Seluruh pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV memahami dan melaksanakan prosedur yang perlu dilakukan. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut.	menunjukkan bahwa seluruh pihak ketiga yang terlibat telah memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan.
5	Organisasi sudah menerapkan prosedur pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV, dilakukan *monitoring* dan di*reviu* secara berkala, serta diperbaiki prosedurnya secara berkelanjutan.	- Prosedur sudah diformalkan menjadi dokumen resmi. - Seluruh pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV memahami dan melaksanakan prosedur yang perlu dilakukan. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur tersebut. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan.	- SOP yang telah diformalkan. - Wawancara terhadap personel vendor/pihak ketiga yang terlibat dalam penyelenggaraan sistem IIV menunjukkan bahwa seluruh pihak ketiga yang terlibat telah memahami prosedur tidak boleh dilakukannya koneksi dan pemasangan perangkat keras atau perangkat lunak tak berizin pada lingkup sistem IIV. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada).

3.3.4. Menerapkan teknologi pemindaian kerentanan terhadap sistem IIV

Kriteria	Detail
Deskripsi	Risiko tidak hanya dapat timbul dikarenakan adanya ancaman dari luar organisasi, tetapi juga dari adanya kelemahan pada sistem yang dimiliki organisasi. Oleh karena itu, perlu adanya langkah preventif dengan mengidentifikasi kerentanan sistem sedini mungkin agar kelemahan pada sistem dapat segera diatasi sebelum kelemahan atau kerentanan tersebut dieksploitasi oleh pihak yang tidak berwenang. Salah satu hal yang dapat dilakukan adalah dengan memanfaatkan teknologi pemindaian kerentanan pada sistem IIV.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pemindaian kerentanan serta sumber daya untuk menjalankan dan memelihara sistem pemindaian.
Dampak	**Tinggi** – Dengan pemindaian yang rutin, organisasi dapat mengidentifikasi dan memperbaiki kerentanan sebelum dapat dieksploitasi, sehingga meningkatkan keamanan sistem secara keseluruhan.
Kompleksitas	**Sedang** – Memerlukan teknologi pemindaian yang tepat serta prosedur untuk mengidentifikasi dan memperbaiki kerentanan secara efektif.
Referensi Kontrol	**NIST CSF 2.0: ID.RA-01** **NIST CSF 1.1: DE.CM-8** **NIST SP 800-53r5: RA-5** **SNI ISO/IEC 27001:2022: 8.8**

131 Kontrol 3.3.4.a:

Kontrol	Memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanannya melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.
Deskripsi Kontrol	Salah satu kontrol yang dapat dilakukan untuk memindai kerentanan pada sistem IIV adalah dengan memastikan bahwa semua perangkat yang digunakan dalam penyelenggaraan sistem IIV telah diuji keamanannya dengan penilaian kerentanan, uji penetrasi, dan/atau audit keamanan. Pengujian tersebut dapat dilakukan dengan memanfaatkan teknologi yang dapat secara otomatis mengenali kerentanan pada sistem.
Deskripsi Bukti Dukung	Bukti dukung yang dapat ditunjukkan untuk mendukung kontrol ini adalah SOP *penetration testing* dan *vulnerability assessment* atau SOP uji keamanan lain yang harus dilakukan sebelum sistem masuk produksi (digunakan oleh khalayak umum).
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH047 TH053 TH065 TH077 TH036 TH039 TH043 TH046 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.RA-01** **NIST CSF 1.1: DE.CM-8** **NIST SP 800-53r5: RA-5** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 3.3.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki teknologi untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	Tidak ada SOP penerapan teknologi uji keamanan yang diformalkan dan belum ada teknologi uji keamanan yang diterapkan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi telah menerapkan teknologi pada sebagian kecil aspek tapi belum diformalkan untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	- Belum ada SOP penerapan teknologi uji keamanan yang diformalkan. - Penerapan teknologi uji keamanan dilakukan di sebagian kecil sistem.	- Dokumen laporan hasil uji keamanan atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan di sebagian kecil sistem.
2	Organisasi telah menerapkan teknologi pada sebagian besar aspek tapi belum diformalkan untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	- Belum ada SOP penerapan teknologi uji keamanan yang diformalkan. - Penerapan teknologi uji keamanan dilakukan di sebagian besar sistem.	- Dokumen laporan hasil uji keamanan atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan di sebagian besar sistem.
3	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	- SOP penerapan teknologi uji keamanan telah diformalkan. - Penerapan teknologi uji keamanan dilakukan di seluruh bagian sistem.	- SOP penerapan teknologi uji keamanan yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan di seluruh bagian sistem.
4	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan, dilakukan *monitoring* dan *reviu* prosedur secara berkala.	- SOP penerapan teknologi uji keamanan telah diformalkan. - Penerapan teknologi uji keamanan dilakukan di seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur uji keamanan.	- SOP penerapan teknologi uji keamanan yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan di seluruh bagian sistem.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur uji keamanan yang diterapkan.
5	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanan melalui penilaian kerentanan, uji penetrasi, atau audit keamanan, dilakukan *monitoring* dan *reviu* prosedur secara berkala serta dilakukan perbaikan prosedur secara berkelanjutan, dan mengarah pada otomatisasi.	- SOP penerapan teknologi uji keamanan telah diformalkan. - Penerapan teknologi uji keamanan dilakukan di seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur uji keamanan. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan. - Organisasi menerapkan teknologi yang secara otomatis melakukan uji keamanan pada sistem IIV.	- SOP penerapan teknologi uji keamanan yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan di seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur uji keamanan yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada). - Dokumen yang menunjukkan penerapan teknologi yang secara otomatis melakukan uji keamanan pada sistem IIV.

132 Kontrol 3.3.4.b:

Kontrol	Penyelenggara IIV memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi.
Deskripsi Kontrol	Selain perlunya dilakukan uji keamanan pada sistem IIV sebelum sistem masuk produksi, sistem IIV juga perlu diuji kembali keamanannya secara rutin dan berkala. Hal ini diperlukan dengan pertimbangan adanya kemungkinan berkembangnya teknologi atau modus serangan seiring berjalannya waktu.
Deskripsi Bukti Dukung	Bukti Dukung yang dapat menunjukkan diterapkannya kontrol ini adalah adanya SOP pemeliharaan sistem, SOP penetration testing dan vulnerability assessment, dan SOP pengujian keamanan lainnya, disertai dengan jadwal pelaksanaannya.
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH047 TH053 TH065 TH077 TH036 TH039 TH043 TH046 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.RA-01** **NIST CSF 1.1: DE.CM-8** **NIST SP 800-53r5: RA-5** **SNI ISO/IEC 27001:2022: 8.8**

Kriteria Pemenuhan Kontrol 3.3.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki prosedur pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi	Tidak ada SOP yang diterapkan.	Tidak ada bukti dukung yang dapat ditunjukkan.
1	Organisasi telah menerapkan teknologi pada sebagian kecil aspek tapi belum diformalkan untuk memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi	- Belum ada SOP pengujian keamanan atau pemeliharaan rutin yang diformalkan. - Pengujian keamanan atau pemeliharaan rutin dilakukan di sebagian kecil sistem.	- Dokumen laporan hasil uji keamanan atau pemeliharaan sistem atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan atau pemeliharaan sistem di sebagian kecil sistem.
2	Organisasi telah menerapkan teknologi pada sebagian besar aspek tapi belum diformalkan untuk memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi	- Belum ada SOP pengujian keamanan atau pemeliharaan rutin yang diformalkan. - Pengujian keamanan atau pemeliharaan rutin dilakukan di sebagian besar sistem.	- Dokumen laporan hasil uji keamanan atau pemeliharaan sistem atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan atau pemeliharaan sistem di sebagian besar sistem.
3	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi	- SOP pengujian keamanan atau pemeliharaan rutin telah diformalkan. - Pengujian keamanan atau pemeliharaan rutin dilakukan di seluruh bagian sistem.	- SOP pengujian keamanan atau pemeliharaan rutin yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau pemeliharaan sistem atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan atau pemeliharaan sistem di seluruh bagian sistem.
4	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi dan dilakukan *monitoring* dan *reviu* prosedur secara berkala.	- SOP pengujian keamanan atau pemeliharaan rutin telah diformalkan. - Pengujian keamanan atau pemeliharaan rutin dilakukan di seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur uji keamanan dan pemeliharan sistem rutin.	- SOP pengujian keamanan atau pemeliharaan rutin yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau pemeliharaan sistem atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan atau pemeliharaan sistem di seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur uji

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			keamanan dan pemeliharaan sistem rutin yang diterapkan.
5	Organisasi telah menerapkan teknologi pada seluruh aspek dan sudah diformalkan untuk memastikan adanya pemeriksaan rutin di perangkat dan *server* yang dikelola dalam organisasi dan dilakukan *monitoring* dan *reviu* prosedur secara berkala serta dilakukan perbaikan prosedur secara berkelanjutan, dan mengarah pada otomatisasi	- SOP pengujian keamanan atau pemeliharaan rutin telah diformalkan. - Pengujian keamanan atau pemeliharaan rutin dilakukan di seluruh bagian sistem. - Organisasi secara rutin melakukan monitoring dan peninjauan terhadap pelaksanaan prosedur uji keamanan dan pemeliharan sistem rutin. - Organisasi melakukan pembaruan terhadap prosedur yang ada berdasarkan hasil monitoring dan peninjauan yang dilakukan apabila diperlukan. - Organisasi menerapkan teknologi yang secara otomatis melakukan uji keamanan dan pemeliharaan sistem secara rutin pada sistem IIV yang dimilikinya.	- SOP pengujian keamanan atau pemeliharaan rutin yang telah diformalkan. - Dokumen laporan hasil uji keamanan atau pemeliharaan sistem atau dokumen lain yang dapat menunjukkan telah dilakukannya uji keamanan atau pemeliharaan sistem di seluruh bagian sistem. - Dokumen laporan pelaksanaan atau dokumen lain yang menunjukkan kegiatan monitoring dan peninjauan secara berkala terhadap prosedur uji keamanan dan pemeliharaan sistem rutin yang diterapkan. - Dokumen yang menunjukkan pembaruan SOP atas hasil monitoring dan peninjauan yang dilakukan (jika ada). - Dokumen yang menunjukkan penerapan teknologi yang secara otomatis melakukan uji keamanan dan pemeliharaan sistem rutin pada sistem IIV organisasi.





IV DOMAIN PENANGGULANGAN DAN PEMULIHAN

"Domain Penanggulangan dan Pemulihan merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam menyusun dokumen rencana penanggulangan dan pemulihan Insiden Siber, menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait Insiden Siber yang terdeteksi, menahan meluasnya dampak dari Insiden Siber, memulihkan layanan yang terganggu karena Insiden Siber serta mengurangi dampak dari Insiden Siber"

4.1. Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber

Perencanaan penanggulangan dan pemulihan insiden siber dilakukan dengan menyusun dan menetapkan rencana tanggap insiden serta rencana keberlangsungan kegiatan yang disetujui pimpinan organisasi. Kedua rencana ini harus dijalankan dan disimulasikan secara berkala agar efektif saat diterapkan. Personel pengelola Infrastruktur Informasi Vital juga dipastikan memahami peran, prosedur penanggulangan, serta penggunaan rekam cadang sehingga organisasi siap merespons insiden dengan cepat dan menjaga keberlangsungan layanan.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi;
b) menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi;
c) memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala;
d) memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan; dan
e) memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**RS.MA-01, RS.MA-05, RC.RP-01, RC.RP-02, PR.AT-01, ID.IM-02, ID.IM-04**
NIST CSF 1.1	**:**	**RS.RP-1, RS.CO-1, RC.RP-1, PR.IP-9, PR.IP-10**
NIST SP 800-53r5	**:**	**CP-1, CP-2, CP-3, CP-4, CP-7, CP-10, IR-1, IR-3, IR-4, IR-7, IR-8, IR-9, PM-14**
SNI ISO/IEC 27001:2022	**:**	**5.2, 5.3, 5.24, 5.26, 5.29**

4.1.1. Menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi

Kriteria	Detail
Deskripsi	Menyusun dan menetapkan rencana tanggap insiden siber yang disetujui oleh pimpinan organisasi merupakan langkah krusial dalam menjaga keamanan dan kelangsungan sistem informasi. Proses ini dimulai dengan pembentukan tim yang bertugas mengidentifikasi potensi risiko dan ancaman siber yang mungkin dihadapi organisasi, serta menentukan prioritas berdasarkan dampaknya. Rencana tanggap insiden juga harus mencakup strategi komunikasi yang efektif, baik internal maupun eksternal, untuk memastikan informasi yang akurat dan relevan tersampaikan kepada pihak yang tepat pada waktu yang tepat. Setelah rancangan rencana selesai, pimpinan organisasi akan melakukan peninjauan dan memberikan persetujuan. Proses ini melibatkan evaluasi terhadap efektivitas rencana, ketersediaan sumber daya yang dibutuhkan, dan keselarasan dengan tujuan bisnis organisasi. Setelah disetujui, rencana tanggap insiden siber akan disosialisasikan kepada seluruh karyawan dan pihak terkait, serta diuji secara berkala melalui simulasi dan latihan untuk memastikan kesiapan tim dalam menghadapi insiden siber yang sebenarnya.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mendapatkan persetujuan dari pimpinan organisasi, tetapi tidak selalu membutuhkan teknologi tambahan
Dampak	**Tinggi** – Dengan rencana yang jelas dan disetujui, organisasi dapat merespons insiden siber dengan cepat dan efektif, sehingga mengurangi dampak negatif pada operasional dan reputasi organisasi.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen untuk menyusun rencana yang mencakup semua aspek tanggap insiden.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-01, RS.MA-05, RC.RP-01, RC.RP-02, ID.IM-04** **NIST CSF 1.1: RS.RP-1, RC.RP-1, PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-4, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.26, 5.29**

133 Kontrol 4.1.1.a:

Kontrol	Menentukan dan menetapkan prosedur tanggap insiden beserta pembagian peran yang jelas antara pihak manajemen, personel pengelola IIV,, dan pihak lainnya yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber
Deskripsi Kontrol	Penyelenggara IIV harus menetapkan prosedur tanggap insiden yang mencakup pembagian peran yang jelas antara manajemen, personel pengelola IIV, dan pihak terkait lainnya. Prosedur ini harus mencakup langkah-langkah yang harus diambil setelah mendeteksi adanya insiden siber, termasuk identifikasi, pengendalian, pemulihan, dan pelaporan insiden. Pembagian peran yang jelas penting untuk memastikan bahwa setiap pihak yang terlibat mengetahui tanggung jawab dan tindakan yang harus dilakukan sesuai dengan peran masingmasing, guna meminimalisir dampak insiden terhadap operasional IIV dan keamanan data. Tujuan dari kontrol ini adalah untuk memastikan kesiapan organisasi dalam menghadapi insiden siber dengan prosedur yang terstruktur dan respons yang cepat
Deskripsi Bukti Dukung	Bukti Dukung yang berkaitan dengan kontrol tersebut antara lain: - Dokumen prosedur tanggap insiden yang mencakup langkah-langkah yang harus diambil, seperti identifikasi, pengendalian, dan pemulihan insiden. - Daftar peran dan tanggung jawab yang jelas untuk setiap pihak terkait, baik manajemen, personel pengelola IIV, maupun pihak lainnya. - Laporan pelatihan atau simulasi insiden siber yang telah dilaksanakan untuk memastikan bahwa semua pihak yang terlibat memahami prosedur dan peran mereka. - Dokumen komunikasi insiden yang mencakup format pelaporan insiden dan prosedur eskalasi. - Laporan hasil evaluasi dan perbaikan prosedur tanggap insiden setelah dilakukan penanganan insiden sebelumnya
Ancaman/Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: RS.MA-01** **NIST CSF 1.1: RS.RP-1** **NIST SP 800-53r5: CP-2, CP-10, IR-4, IR-8** **SNI ISO/IEC 27001:2022: 5.26**

Kriteria Pemenuhan Kontrol 4.1.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menetapkan prosedur tanggap insiden serta belum ada pembagian peran yang jelas antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber	Organisasi belum menentukan dan menetapkan prosedur tanggap insiden serta belum ada pembagian peran yang jelas antara pihak manajemen, personil pengelola IIV, dan pihak lainnya. Tidak ada tindakan yang dilakukan setelah mendeteksi insiden siber.	- Tidak adanya dokumen prosedur tanggap insiden. - Tidak ada catatan atau bukti pembagian peran dalam penanganan insiden siber. - Tidak ada bukti pelatihan atau sosialisasi terkait penanganan insiden siber. - Pernyataan dari pihak manajemen dan personel terkait yang mengkonfirmasi belum adanya prosedur dan pembagian peran.
1	Organisasi belum memformalkan penentuan dan penetapan prosedur tanggap insiden namun penerapan dan pembagian peran sudah diterapkan pada sebagian kecil aspek antara lain pihak manajemen, personel pengelola IIV, dan pihak lainnya, yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber.	Organisasi belum memformalkan prosedur tanggap insiden, namun penerapan pembagian peran sudah diterapkan pada sebagian kecil aspek antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. Tindakan pasca deteksi insiden siber telah dilakukan pada sebagian kecil.	- Draf atau catatan awal terkait prosedur tanggap insiden, meskipun belum final atau disahkan. - Beberapa catatan atau bukti parsial terkait pembagian peran dalam penanganan insiden, namun belum lengkap atau formal. - Beberapa bukti penerapan sebagian kecil aspek dari prosedur tanggap insiden, seperti tindakan identifikasi atau pelaporan insiden. - Keterangan dari beberapa personel terkait yang menunjukkan adanya pemahaman tentang peran mereka dalam beberapa aspek penanganan insiden.
2	Organisasi belum memformalkan penentuan dan penetapan prosedur tanggap insiden namun penerapan dan pembagian peran sudah diterapkan pada sebagian besar aspek antara lain pihak manajemen, personel pengelola IIV, dan pihak lainnya, yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber.	Organisasi belum memformalkan prosedur tanggap insiden, namun penerapan pembagian peran sudah diterapkan pada sebagian besar aspek antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. Tindakan pasca deteksi insiden siber sudah dilakukan pada sebagian besar aspek.	- Dokumen prosedur tanggap insiden yang masih dalam tahap pengembangan atau belum disahkan sepenuhnya. - Bagan atau daftar peran dan tanggung jawab dalam penanganan insiden yang belum lengkap atau belum disosialisasikan secara luas. - Bukti penerapan sebagian besar aspek dari prosedur tanggap insiden, seperti tindakan analisis, penanggulangan, atau pemulihan. - Keterangan dari sebagian besar personel terkait yang menunjukkan pemahaman tentang peran mereka dalam sebagian besar aspek penanganan insiden.
3	Organisasi telah memformalkan penentuan dan penetapan prosedur tanggap insiden beserta pembagian peran yang jelas serta sudah diterapkan pada seluruh aspek antara pihak manajemen, personel pengelola IIV, dan pihak lainnya.	Organisasi telah memformalkan prosedur tanggap insiden dan membagi peran dengan jelas antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. Tindakan pasca deteksi insiden siber sudah diterapkan pada seluruh aspek.	- Dokumen prosedur tanggap insiden yang telah disahkan dan didistribusikan kepada pihak terkait. - Bagan atau daftar peran dan tanggung jawab yang jelas dan lengkap dalam penanganan insiden, serta telah disosialisasikan kepada seluruh pihak terkait.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber.		- Bukti penerapan prosedur tanggap insiden pada seluruh aspek, termasuk tindakan deteksi, analisis, penanggulangan, pemulihan, dan komunikasi. - Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah diikuti. - Keterangan dari seluruh personel terkait yang menunjukkan pemahaman dan kesiapan mereka dalam menjalankan peran masing-masing dalam penanganan insiden.
4	Organisasi telah memformalkan penentuan dan penetapan serta melakukan reviu terhadap prosedur tanggap insiden beserta pembagian peran yang jelas dan sudah diterapkan pada seluruh aspek antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber.	Organisasi telah memformalkan prosedur tanggap insiden dan melakukan reviu terhadap prosedur tersebut. Pembagian peran yang jelas sudah diterapkan pada seluruh aspek, termasuk antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. Tindakan pasca deteksi insiden siber sudah dilakukan dengan baik.	- Dokumen prosedur tanggap insiden yang telah direviu dan diperbarui secara berkala. - Bukti pelaksanaan reviu prosedur, seperti notulen rapat atau laporan evaluasi. - Bukti pelatihan atau simulasi yang melibatkan seluruh pihak terkait untuk menguji efektivitas prosedur tanggap insiden. - Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah dievaluasi dan diperbaiki berdasarkan pengalaman.
5	Organisasi telah memformalkan penentuan dan penetapan serta melakukan reviu terhadap prosedur tanggap insiden beserta pembagian peran yang jelas dan sudah diterapkan pada seluruh aspek antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya Insiden Siber. yang diperbaiki secara berkala	Organisasi telah memformalkan prosedur tanggap insiden, melakukan reviu secara berkala terhadap prosedur tersebut, dan pembagian peran yang jelas sudah diterapkan pada seluruh aspek. Prosedur tanggap insiden serta pembagian peran diperbaiki secara berkala untuk meningkatkan respons terhadap insiden siber.	- Dokumen prosedur tanggap insiden yang telah direviu, diperbarui, dan diperbaiki secara berkala berdasarkan hasil evaluasi dan umpan balik. - Bukti adanya mekanisme umpan balik dari personel terkait dan pihak eksternal untuk perbaikan prosedur. - Bukti adanya inovasi atau peningkatan berkelanjutan dalam prosedur tanggap insiden. - Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah dioptimalkan berdasarkan pembelajaran dan praktik terbaik.

134 Kontrol 4.1.1.b:

Kontrol	Menyusun dan menetapkan prosedur rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradikasi, pemulihan, dan peningkatan berkelanjutan
Deskripsi Kontrol	Penyelenggara IIV harus menyusun dan menetapkan prosedur rencana tanggap insiden siber yang mencakup seluruh tahapan, mulai dari persiapan, identifikasi, kontainmen, eradikasi, pemulihan, hingga peningkatan berkelanjutan. Prosedur ini harus menyeluruh dan jelas dalam mendefinisikan langkah-langkah yang harus diambil dalam setiap fase untuk memastikan respons yang cepat dan terkoordinasi terhadap insiden siber. Tahapan ini meliputi: 1. Persiapan: Menyiapkan tim tanggap insiden, perangkat, dan sumber daya yang diperlukan untuk merespons insiden dengan efektif. 2. Identifikasi: Mendeteksi dan mengidentifikasi potensi insiden siber yang terjadi di organisasi. 3. Kontainmen: Mengisolasi insiden untuk mencegah penyebaran lebih lanjut. 4. Eradikasi: Menghilangkan penyebab insiden dan memastikan tidak ada jejak yang tersisa. 5. Pemulihan: Memulihkan sistem dan operasi ke kondisi normal. 6. Peningkatan Berkelanjutan: Menganalisis insiden untuk mengidentifikasi area perbaikan dalam prosedur dan sistem keamanan yang ada. Tujuan dari prosedur ini adalah untuk meminimalisir dampak dari insiden siber dan meningkatkan ketahanan sistem informasi organisasi.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini mencakup dokumen-dokumen yang menunjukkan keberadaan dan implementasi prosedur rencana tanggap insiden siber: - Dokumen prosedur rencana tanggap insiden yang mendetail, mencakup langkah-langkah persiapan hingga peningkatan berkelanjutan. - Daftar tim tanggap insiden yang mencakup peran, tanggung jawab, dan kontak darurat. - Laporan hasil pelatihan dan simulasi insiden siber yang melibatkan tim terkait. - Catatan identifikasi insiden sebelumnya, termasuk tipe insiden yang terjadi dan respon yang diterapkan. - Laporan tindak lanjut dan evaluasi dari insiden yang sudah terjadi, termasuk perubahan dan perbaikan prosedur tanggap insiden berdasarkan pembelajaran yang diperoleh. - Dokumen alat dan prosedur yang digunakan untuk mengisolasi dan mengatasi insiden siber (misalnya software atau perangkat keamanan yang diterapkan).
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: RS.MA-05, RC.RP-01, RC.RP-02** **NIST CSF 1.1: RC.RP-1** **NIST SP 800-53r5: CP-10, IR-4, IR-8** **SNI ISO/IEC 27001:2022: 5.26**

Kriteria Pemenuhan Kontrol 4.1.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menetapkan rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan	Organisasi belum memiliki prosedur rencana tanggap insiden siber yang terdokumentasi dan tidak ada tahapan yang jelas, mulai dari persiapan, identifikasi, kontainmen, eradikasi, pemulihan, dan peningkatan berkelanjutan.	- Tidak adanya dokumen prosedur rencana tanggap insiden siber. - Tidak ada catatan atau bukti tahapan-tahapan penanganan insiden yang jelas (persiapan, identifikasi, kontainmen, eradikasi, pemulihan, dan peningkatan berkelanjutan). - Tidak ada bukti pelatihan atau sosialisasi terkait penanganan insiden siber. - Pernyataan dari pihak manajemen dan personel terkait yang mengonfirmasi belum adanya prosedur dan tahapan yang jelas.
1	Organisasi sudah menentukan dan menetapkan sebagian kecil aspek dari rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan namun belum diformalkan.	Organisasi belum memformalkan prosedur rencana tanggap insiden siber dalam bentuk dokumen, tetapi sebagian kecil aspek dari tahapan-tahapan tersebut sudah diterapkan. Misalnya, mungkin ada tindakan identifikasi insiden, tetapi tidak ada prosedur kontainmen atau pemulihan yang jelas.	- Draf atau catatan awal terkait prosedur rencana tanggap insiden siber, meskipun belum final atau disahkan. - Beberapa catatan atau bukti parsial terkait tahapan-tahapan penanganan insiden, namun belum lengkap atau formal. - Beberapa bukti penerapan sebagian kecil aspek dari prosedur tanggap insiden, seperti tindakan identifikasi atau pelaporan insiden. - Keterangan dari beberapa personel terkait yang menunjukkan adanya pemahaman tentang peran mereka dalam beberapa aspek penanganan insiden.
2	Organisasi sudah menentukan dan menetapkan sebagian besar aspek dari rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan namun belum diformalkan.	Organisasi belum memformalkan prosedur rencana tanggap insiden siber, tetapi sebagian besar aspek dari tahapan-tahapan tersebut sudah diterapkan. Namun, mungkin ada beberapa tahapan yang belum lengkap atau belum terstruktur dengan baik.	- Dokumen prosedur rencana tanggap insiden siber yang masih dalam tahap pengembangan atau belum disahkan sepenuhnya. - Bagan atau daftar peran dan tanggung jawab dalam penanganan insiden yang belum lengkap atau belum disosialisasikan secara luas. - Bukti penerapan sebagian besar aspek dari prosedur tanggap insiden, seperti tindakan analisis, penanggulangan, atau pemulihan. - Keterangan dari sebagian besar personel terkait yang menunjukkan pemahaman tentang peran mereka dalam sebagian besar aspek penanganan insiden.
3	Organisasi sudah menentukan dan menetapkan keseluruhan aspek serta memformalkan rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan..	Organisasi telah memformalkan prosedur rencana tanggap insiden siber dalam bentuk dokumen dan telah memiliki tahapan-tahapan yang jelas, mulai dari persiapan, identifikasi, kontainmen, eradikasi, pemulihan, dan peningkatan berkelanjutan. Prosedur ini telah diterapkan pada seluruh aspek	- Dokumen prosedur rencana tanggap insiden siber yang telah disahkan dan didistribusikan kepada pihak terkait. - Bagan atau daftar peran dan tanggung jawab yang jelas dan lengkap dalam penanganan insiden, serta telah disosialisasikan kepada seluruh pihak terkait. - Bukti penerapan prosedur tanggap insiden pada seluruh tahapan, termasuk persiapan, identifikasi, kontainmen, eradikasi, pemulihan, dan peningkatan berkelanjutan.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah diikuti. - Keterangan dari seluruh personel terkait yang menunjukkan pemahaman dan kesiapan mereka dalam menjalankan peran masing-masing dalam penanganan insiden.
4	Organisasi sudah menentukan dan menetapkan keseluruhan aspek serta memformalkan rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan yang direviu secara berkala.	Organisasi telah memformalkan prosedur rencana tanggap insiden siber dan telah melakukan reviu terhadap prosedur tersebut secara berkala. Prosedur mencakup tahapan-tahapan yang lengkap dan diterapkan pada seluruh aspek	- Dokumen prosedur rencana tanggap insiden siber yang telah direviu dan diperbarui secara berkala. - Bukti pelaksanaan reviu prosedur, seperti notulen rapat atau laporan evaluasi. - Bukti pelatihan atau simulasi yang melibatkan seluruh pihak terkait untuk menguji efektivitas prosedur tanggap insiden. - Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah dievaluasi dan diperbaiki berdasarkan pengalaman.
5	Organisasi sudah menentukan dan menetapkan keseluruhan aspek serta memformalkan rencana tanggap Insiden Siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan yang direviu dan diperbaiki secara berkala	Organisasi telah memformalkan prosedur rencana tanggap insiden siber, telah melakukan reviu terhadap prosedur tersebut secara berkala, dan secara berkala melakukan perbaikan terhadap prosedur tersebut. Prosedur mencakup tahapan-tahapan yang lengkap dan diterapkan pada seluruh aspek.	- Dokumen prosedur rencana tanggap insiden siber yang telah direviu, diperbarui, dan diperbaiki secara berkala berdasarkan hasil evaluasi dan umpan balik. - Bukti adanya mekanisme umpan balik dari personel terkait dan pihak eksternal untuk perbaikan prosedur. - Bukti adanya inovasi atau peningkatan berkelanjutan dalam prosedur tanggap insiden. - Catatan atau laporan insiden sebelumnya yang menunjukkan bahwa prosedur tanggap insiden telah dioptimalkan berdasarkan pembelajaran dan praktik terbaik.

135 Kontrol 4.1.1.c:

Kontrol	Menentukan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber.
Deskripsi Kontrol	Penyelenggara IIV harus menentukan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap insiden siber. Skenario ini mencakup potensi insiden yang dapat mempengaruhi kerahasiaan, integritas, dan ketersediaan informasi serta layanan IIV seperti serangan siber (DDoS, malware, ransomware), kebocoran data, atau kegagalan sistem. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi siap menghadapi berbagai jenis insiden yang dapat terjadi, serta memiliki prosedur yang jelas dan terstruktur untuk menanggapi dan mengelola insiden tersebut secara efektif dan cepat.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini berfokus pada keberadaan dokumentasi yang menunjukkan identifikasi dan analisis skenario insiden keamanan yang relevan dengan layanan IIV. Dokumen-dokumen tersebut dapat berupa: - Dokumen rencana tanggap insiden siber yang mencakup daftar skenario insiden keamanan yang telah diidentifikasi, dengan penjelasan tentang dampaknya terhadap layanan IIV. - Daftar prosedur yang telah disusun untuk merespon setiap skenario insiden, termasuk langkah-langkah pengamanan dan pemulihan. - Laporan hasil analisis risiko yang menunjukkan insiden yang paling mungkin terjadi berdasarkan evaluasi terhadap ancaman yang ada. - Bukti simulasi atau uji coba tanggap insiden yang mencakup skenario yang telah ditambahkan ke dalam rencana. - Dokumentasi hasil evaluasi dan perbaikan dari rencana tanggap insiden setelah pengujian atau latihan yang dilakukan.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

Kriteria Pemenuhan Kontrol 4.1.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber	Organisasi belum mengidentifikasi skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan belum menambahkannya pada dokumen rencana tanggap insiden siber.	- Tidak adanya dokumen yang mengidentifikasi skenario insiden keamanan untuk layanan IIV. - Tidak ada catatan atau bukti analisis risiko terkait dengan layanan IIV. - Tidak ada bukti bahwa skenario insiden keamanan dipertimbangkan dalam dokumen rencana tanggap insiden siber.
1	Organisasi telah menentukan sebagian kecil skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber namun belum diformalkan.	Organisasi belum memformalkan identifikasi skenario insiden keamanan, tetapi sebagian kecil skenario sudah diidentifikasi dan dipertimbangkan dalam beberapa aspek tanggap insiden. Dokumentasi mungkin berupa catatan atau draf awal.	- Catatan atau draf awal yang berisi daftar sebagian kecil skenario insiden keamanan yang mungkin terjadi pada layanan IIV. - Analisis risiko awal atau parsial yang mencakup beberapa aspek layanan IIV. - Beberapa skenario insiden keamanan disebutkan secara singkat dalam dokumen rencana tanggap insiden siber, tetapi belum dijelaskan.
2	Organisasi telah menentukan sebagian besar skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber namun belum diformalkan.	Organisasi belum memformalkan identifikasi skenario insiden keamanan, tetapi sebagian besar skenario sudah diidentifikasi dan dipertimbangkan dalam sebagian besar aspek tanggap insiden. Dokumentasi mungkin belum lengkap atau final.	- Dokumen yang berisi daftar sebagian besar skenario insiden keamanan yang mungkin terjadi pada layanan IIV. - Analisis risiko yang mencakup sebagian besar aspek layanan IIV dan mengidentifikasi potensi ancaman dan dampaknya. - Dokumen rencana tanggap insiden siber yang mencakup beberapa prosedur khusus untuk beberapa skenario insiden keamanan yang telah diidentifikasi.
3	Organisasi telah menentukan dan memformalkan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber.	Organisasi telah mengidentifikasi dan mendokumentasikan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan telah menambahkannya pada dokumen rencana tanggap insiden siber. Skenario yang diidentifikasi mencakup berbagai jenis ancaman dan dampaknya.	- Dokumen lengkap yang berisi daftar skenario insiden keamanan yang mungkin terjadi pada layanan IIV, mencakup berbagai jenis ancaman dan dampaknya. - Analisis risiko yang komprehensif untuk layanan IIV, termasuk identifikasi ancaman, kerentanan, dan dampak potensial.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Dokumen rencana tanggap insiden siber yang secara rinci menjelaskan prosedur untuk setiap skenario insiden keamanan yang telah diidentifikasi.
4	Organisasi telah menentukan, memformalkan serta melakukan reviu terhadap skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber	Organisasi telah mengidentifikasi, mendokumentasikan, dan melakukan reviu terhadap skenario insiden keamanan yang mungkin terjadi pada layanan IIV. Skenario-skenario ini telah ditambahkan pada dokumen rencana tanggap insiden siber dan diuji efektivitasnya	- Dokumen yang sama seperti indeks 3, tetapi dengan bukti tambahan bahwa daftar skenario insiden keamanan telah ditinjau dan diperbarui secara berkala. - Laporan pengujian dan evaluasi terhadap rencana tanggap insiden siber, termasuk pengujian terhadap skenario insiden keamanan yang berbeda
5	Organisasi telah menentukan, memformalkan serta melakukan reviu terhadap skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap Insiden Siber yang diperbaiki secara berkala.	Organisasi telah mengidentifikasi, mendokumentasikan, melakukan reviu, dan secara berkala memperbarui skenario insiden keamanan yang mungkin terjadi pada layanan IIV. Skenario-skenario ini telah ditambahkan pada dokumen rencana tanggap insiden siber, diuji efektivitasnya, dan diperbaiki berdasarkan umpan balik serta perubahan lingkungan.	- Dokumen yang sama seperti indeks 4, tetapi dengan bukti tambahan bahwa daftar skenario insiden keamanan terus diperbarui dan ditingkatkan berdasarkan umpan balik dan perubahan lingkungan. - Bukti adanya mekanisme untuk mengumpulkan informasi tentang ancaman dan kerentanan baru yang relevan dengan layanan IIV

136 Kontrol 4.1.1.d:

Kontrol	Memastikan rencana tanggap Insiden Siber dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa rencana tanggap insiden siber dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan yang berlaku. Ini melibatkan penyampaian rencana kepada personel internal yang terlibat dalam penanganan insiden, serta pihak eksternal yang relevan seperti penyedia layanan pihak ketiga, otoritas yang berwenang, dan mitra bisnis yang terkait. Komunikasi ini harus mencakup pemahaman yang jelas mengenai prosedur tanggap insiden, peran masing-masing pihak, dan langkah-langkah yang harus diambil dalam menghadapi berbagai skenario insiden. Tujuan dari kontrol ini adalah untuk memastikan bahwa seluruh pihak yang terlibat dalam respons insiden memiliki pemahaman yang seragam tentang bagaimana menghadapi insiden siber
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini menunjukkan bahwa rencana tanggap insiden siber telah disosialisasikan dan tersedia bagi pihak-pihak yang berkepentingan. Bukti-bukti tersebut dapat berupa: - Dokumen rencana tanggap insiden siber yang mencakup daftar pihak yang terlibat dalam tanggap insiden, serta peran dan tanggung jawab masing-masing pihak. - Catatan komunikasi atau pemberitahuan yang mengonfirmasi bahwa rencana telah dikomunikasikan kepada pihak-pihak terkait. - Laporan hasil pelatihan atau simulasi tanggap insiden yang diikuti oleh pihak-pihak terkait. - Bukti penerimaan atau konfirmasi dari pihak eksternal yang berwenang bahwa mereka telah menerima dan memahami rencana tanggap insiden
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: RS.MA-01** **NIST CSF 1.1: RS.RP-1** **NIST SP 800-53r5: CP-2, CP-10, IR-4, IR-8** **SNI ISO/IEC 27001:2022: 5.26**

Kriteria Pemenuhan Kontrol 4.1.1.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Rencana tanggap Insiden Siber belum dikomunikasikan secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan - Tidak ada kebijakan/panduan/pedoman terkait komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan	Organisasi belum mengomunikasikan rencana tanggap insiden siber kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. Tidak ada bukti bahwa pihak-pihak terkait mengetahui atau memiliki akses ke rencana tersebut.	- Tidak ada bukti komunikasi rencana tanggap insiden siber kepada pihak-pihak yang berkepentingan. - Tidak ada catatan atau dokumen yang menunjukkan bahwa pihak-pihak terkait mengetahui keberadaan atau isi rencana tersebut.
1	- Rencana tanggap Insiden Siber sudah dikomunikasikan secara khusus ke sebagian kecil pihak yang berkepentingan dan berhak sesuai ketentuan - Belum ada kebijakan/panduan/pedoman terkait komunikasi secara khusus kepada beberapa pemangku kepentingan tentang pembelajaran tersebut.	Organisasi belum memformalkan komunikasi rencana tanggap insiden siber, tetapi sebagian kecil pihak terkait sudah mengetahui atau memiliki akses ke rencana tersebut melalui jalur informal.	- Beberapa bukti informal bahwa rencana tanggap insiden siber telah dibagikan kepada sebagian kecil pihak terkait, misalnya melalui percakapan lisan atau email informal. - Tidak ada daftar distribusi dokumen atau catatan sosialisasi yang terdokumentasi.
2	- Rencana tanggap Insiden Siber sudah dikomunikasikan kepada sebagian besar pihak yang berkepentingan dan berhak sesuai ketentuan. - Belum ada kebijakan/panduan/pedoman terkait komunikasi secara khusus kepada beberapa pemangku kepentingan tentang pembelajaran tersebut.	Organisasi belum memformalkan komunikasi rencana tanggap insiden siber, tetapi sebagian besar pihak terkait sudah mengetahui atau memiliki akses ke rencana tersebut. Namun, komunikasi mungkin belum terstruktur atau terdokumentasi dengan baik.	- Bukti bahwa rencana tanggap insiden siber telah dibagikan kepada sebagian besar pihak terkait, tetapi tidak ada proses formal yang terdokumentasi. - Mungkin ada daftar distribusi atau catatan sosialisasi yang tidak lengkap atau tidak mutakhir.
3	- Rencana tanggap Insiden Siber sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki kebijakan/panduan/pedoman terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan dalam bentuk	Organisasi telah mengomunikasikan rencana tanggap insiden siber kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. Terdapat bukti bahwa pihak-pihak terkait telah menerima informasi tentang rencana tersebut dan memahami peran mereka	- Daftar distribusi dokumen rencana tanggap insiden siber yang lengkap dan mutakhir, mencantumkan semua pihak yang berhak dan berkepentingan. - Catatan sosialisasi dan pelatihan yang terdokumentasi, menunjukkan bahwa pihak-pihak terkait telah menerima informasi tentang rencana tersebut dan memahami peran mereka. - Bukti ketersediaan dokumen rencana tanggap insiden siber bagi pihak-pihak

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			yang berhak, misalnya melalui intranet atau sistem manajemen dokumen.
4	- Rencana tanggap Insiden Siber sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki kebijakan/panduan/pedoman tertulis terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. - Telah dilakukan reviu terkait kebijakan komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Organisasi telah mengomunikasikan rencana tanggap insiden siber kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan, dan secara berkala melakukan reviu terhadap efektivitas komunikasi tersebut. Terdapat mekanisme untuk memastikan bahwa informasi tetap relevan dan mudah diakses	- Bukti yang sama seperti indeks 3, ditambah dengan bukti bahwa komunikasi rencana tanggap insiden siber dievaluasi secara berkala. - Notulen rapat atau survei yang menunjukkan bahwa umpan balik dari pihak-pihak terkait dipertimbangkan untuk meningkatkan komunikasi.
5	- Rencana tanggap Insiden Siber sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki kebijakan tertulis terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. - Telah dilakukan reviu dan diperbaiki secara berkala terkait kebijakan komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Organisasi telah mengomunikasikan rencana tanggap insiden siber kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan, secara berkala melakukan reviu, dan secara berkala melakukan perbaikan terhadap proses komunikasi tersebut berdasarkan umpan balik dan perubahan kebutuhan	- Bukti yang sama seperti indeks 4, ditambah dengan bukti bahwa proses komunikasi rencana tanggap insiden siber terus diperbaiki berdasarkan umpan balik dan perubahan kebutuhan. - Bukti adanya mekanisme untuk mengumpulkan umpan balik dari pihak-pihak terkait secara berkala

4.1.2. Menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi

Kriteria	Detail
Deskripsi	Proses penyusunan dan penetapan rencana keberlangsungan kegiatan merupakan langkah kritis dalam memastikan bahwa organisasi dapat mempertahankan operasionalnya secara berkelanjutan, terutama dalam menghadapi gangguan atau krisis. Rencana ini harus dirancang secara sistematis, mencakup identifikasi risiko, prosedur mitigasi, serta mekanisme pemulihan, dan harus mendapatkan persetujuan resmi dari pimpinan organisasi untuk memastikan keselarasan dengan tujuan strategis serta ketersediaan sumber daya. Dengan adanya rencana keberlangsungan kegiatan yang disetujui pimpinan, organisasi dapat meminimalkan dampak gangguan, mempercepat pemulihan, dan menjaga stabilitas operasional dalam jangka panjang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun dan mendapatkan persetujuan dari pimpinan organisasi, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan rencana yang jelas dan disetujui, organisasi dapat menjaga keberlangsungan operasional bahkan saat terjadi insiden, sehingga mengurangi dampak negatif pada bisnis dan layanan.
Kompleksitas	**Sedang** – Memerlukan koordinasi antara berbagai departemen untuk menyusun rencana yang mencakup semua aspek keberlangsungan kegiatan.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

137 Kontrol 4.1.2.a:

Kontrol	Menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.
Deskripsi Kontrol	Penyelenggara IIV perlu menentukan dan menetapkan daftar fungsi dan layanan vital yang mendukung penyelenggaraan IIV, untuk memastikan bahwa elemen-elemen yang paling kritis dalam operasional layanan dilindungi dengan baik. Penentuan ini meliputi pemetaan berbagai fungsi dan layanan yang esensial dalam sistem IIV, serta identifikasi siapa saja yang terlibat dalam masing-masing fungsi, termasuk pihak internal dan eksternal. Selain itu, perlu juga ditetapkan pembagian peran dan tanggung jawab antara pihak-pihak yang berhubungan langsung atau tidak langsung dengan operasional layanan IIV, untuk memastikan koordinasi yang efektif dan respons yang cepat dalam mengelola risiko atau insiden yang mungkin terjadi. Tujuan dari kontrol ini adalah untuk memastikan bahwa fungsi-fungsi yang vital bagi layanan IIV terkelola dengan baik dan aman, serta bahwa ada kejelasan dalam pembagian peran dan tanggung jawab antara berbagai pihak yang terlibat
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini berfokus pada dokumentasi yang secara jelas mengidentifikasi fungsi dan layanan vital IIV serta pembagian peran dan tanggung jawab terkait. Dokumen-dokumen tersebut dapat berupa: - Daftar fungsi dan layanan vital yang meliputi deskripsi layanan, pemilik fungsi, dan prioritasnya. - Rencana kontinuitas bisnis yang mencakup daftar fungsi kritis dan prosedur untuk menjaga kelangsungan operasional. - Daftar pembagian peran dan tanggung jawab yang menunjukkan siapa yang bertanggung jawab atas masing-masing fungsi atau layanan vital. - Prosedur dokumentasi dan pemeliharaan daftar fungsi dan layanan vital. - Bukti koordinasi dengan pihak terkait, seperti perjanjian kerjasama (MoU) atau surat keputusan (SK) yang mendefinisikan tanggung jawab pihak ketiga
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

Kriteria Pemenuhan Kontrol 4.1.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menetapkan daftar fungsi dan layanan vital bgai penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	Organisasi belum mengidentifikasi dan belum menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, serta belum memiliki daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	- Tidak ada dokumen yang mengidentifikasi fungsi dan layanan vital bagi penyelenggaraan IIV. - Tidak ada dokumen yang menetapkan pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV. - Tidak ada bukti bahwa fungsi dan layanan vital serta pembagian peran dan tanggung jawab dipertimbangkan dalam operasional layanan IIV.
1	- Organisasi telah menentukan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV. - Belum ada penetapan tertulis diorganisasi terkait daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV	Organisasi belum memformalkan identifikasi fungsi dan layanan vital, tetapi sebagian kecil fungsi dan layanan sudah diidentifikasi dan dipertimbangkan dalam beberapa aspek operasional. Pembagian peran dan tanggung jawab juga belum formal dan hanya mencakup beberapa pihak terkait.	- Catatan atau draf awal yang berisi daftar sebagian kecil fungsi dan layanan vital bagi penyelenggaraan IIV. - Catatan atau draf awal yang berisi pembagian peran dan tanggung jawab dengan beberapa pihak terkait, tetapi belum lengkap. - Beberapa fungsi dan layanan vital serta pembagian peran dan tanggung jawab disebutkan secara singkat dalam dokumen operasional, tetapi belum dijelaskan.
2	- Organisasi telah menentukan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV. - Penetapan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV sedang disusun/masih dalam bentuk draf/belum diresmikan.	Organisasi belum memformalkan identifikasi fungsi dan layanan vital, tetapi sebagian besar fungsi dan layanan sudah diidentifikasi dan dipertimbangkan dalam sebagian besar aspek operasional. Pembagian peran dan tanggung jawab juga belum formal, tetapi sudah mencakup sebagian besar pihak terkait.	- Dokumen yang berisi daftar sebagian besar fungsi dan layanan vital bagi penyelenggaraan IIV. - Dokumen yang berisi pembagian peran dan tanggung jawab dengan sebagian besar pihak terkait, tetapi belum formal atau lengkap. - Dokumen operasional yang mencakup beberapa prosedur khusus untuk beberapa fungsi dan layanan vital serta pembagian peran dan tanggung jawab yang telah diidentifikasi.
3	- Organisasi telah menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	Organisasi telah mengidentifikasi dan mendokumentasikan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, serta telah menetapkan daftar pembagian peran dan tanggung jawab yang jelas	- Dokumen lengkap yang berisi daftar fungsi dan layanan vital bagi penyelenggaraan IIV, mencakup berbagai aspek dan dampaknya. - Dokumen lengkap yang berisi pembagian peran dan tanggung jawab yang jelas dan rinci dengan semua pihak yang berhubungan dengan operasional layanan IIV.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Penetapan daftar fungsi dan layanan vital bagi penyelenggaraan IIV,, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV telah disusun dan telah diresmikan/diformalkan	dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	- Dokumen operasional yang secara rinci menjelaskan prosedur untuk setiap fungsi dan layanan vital serta peran dan tanggung jawab yang terkait.
4	- Organisasi telah Menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV. - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan penentuan penetapan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	Organisasi telah mengidentifikasi, mendokumentasikan, dan melakukan reviu terhadap daftar fungsi dan layanan vital, serta daftar pembagian peran dan tanggung jawab. Daftar-daftar ini telah ditetapkan dan diterapkan dalam operasional layanan IIV.	- Dokumen yang sama seperti indeks 3, tetapi dengan bukti tambahan bahwa daftar fungsi dan layanan vital serta pembagian peran dan tanggung jawab telah ditinjau dan diperbarui secara berkala. - Laporan pengujian dan evaluasi terhadap operasional layanan IIV, termasuk pengujian terhadap fungsi dan layanan vital yang berbeda.
5	- Organisasi telah Menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan perasional layanan IIV. - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan proses penentuan penetapan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV serta dilakukan perbaikan secara berkala.	Organisasi telah mengidentifikasi, mendokumentasikan, melakukan reviu, dan secara berkala memperbarui daftar fungsi dan layanan vital, serta daftar pembagian peran dan tanggung jawab. Daftar-daftar ini telah ditetapkan, diterapkan, dan secara berkala diperbaiki berdasarkan umpan balik dan perubahan lingkungan	- Dokumen yang sama seperti indeks 4, tetapi dengan bukti tambahan bahwa daftar fungsi dan layanan vital serta pembagian peran dan tanggung jawab terus diperbarui dan ditingkatkan berdasarkan umpan balik dan perubahan lingkungan. - Bukti adanya mekanisme untuk mengumpulkan informasi tentang perubahan kebutuhan dan risiko yang relevan dengan layanan IIV.

138 Kontrol 4.1.2.b:

Kontrol	Menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal
Deskripsi Kontrol	Penyelenggara IIV harus menentukan dan menetapkan strategi, tahapan, serta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi serta layanan vital secara penuh atau kembali normal setelah terjadi gangguan atau insiden. Ini bertujuan untuk memastikan bahwa organisasi dapat dengan cepat dan efisien mengembalikan operasional pentingnya, meminimalkan dampak gangguan terhadap layanan, serta menjaga kontinuitas layanan vital. Tujuan dari kontrol ini adalah untuk memastikan bahwa ada perencanaan yang jelas dan terstruktur dalam menghadapi kemungkinan insiden, sehingga meminimalisir waktu henti dan kerugian yang mungkin timbul
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini menunjukkan bahwa organisasi telah memiliki rencana yang jelas dan terukur untuk memulihkan fungsi dan layanan vital setelah terjadi gangguan. Bukti-bukti tersebut dapat berupa: - Rencana pemulihan bencana (Disaster Recovery Plan, DRP) yang mencakup strategi, tahapan, dan waktu pemulihan untuk setiap fungsi dan layanan vital. - Protokol pemulihan untuk layanan kritis, mencakup prosedur pemulihan dan tahapan yang harus diikuti. - Target waktu pemulihan (Recovery Time Objective, RTO) yang jelas untuk setiap layanan yang diprioritaskan. - Laporan evaluasi risiko dan dampak yang menunjukkan tahapan pemulihan yang disesuaikan dengan tingkat kritisitas layanan. - Laporan uji coba pemulihan atau simulasi insiden yang menunjukkan kesiapan organisasi untuk mengembalikan operasional setelah insiden.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

Kriteria Pemenuhan Kontrol 4.1.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal..	Organisasi belum menentukan dan belum menetapkan strategi, tahapan, dan target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal.	- Tidak ada dokumen yang mendefinisikan strategi, tahapan, dan target waktu pemulihan untuk fungsi dan layanan vital. - Tidak ada catatan atau bukti bahwa pertimbangan telah diberikan untuk pemulihan layanan.
1	- Organisasi telah menentukan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal. - Belum ada penetapan tertulis diorganisasi terkait daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV	Organisasi belum memformalkan penentuan strategi, tahapan, dan target waktu pemulihan, tetapi sebagian kecil aspek sudah diidentifikasi dan dipertimbangkan. Misalnya, mungkin ada perkiraan waktu pemulihan untuk beberapa layanan, tetapi belum terdokumentasi dengan baik.	- Catatan atau draf awal yang berisi beberapa elemen strategi, tahapan, atau target waktu pemulihan untuk beberapa fungsi dan layanan vital. - Bukti informal bahwa beberapa aspek pemulihan telah dipertimbangkan, tetapi belum ada rencana yang terdokumentasi secara formal.
2	- Organisasi telah menentukan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal. - Penetapan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal sedang disusun/masih dalam bentuk draf/belum diresmikan	Organisasi belum memformalkan penentuan strategi, tahapan, dan target waktu pemulihan, tetapi sebagian besar aspek sudah diidentifikasi dan dipertimbangkan. Namun, rencana pemulihan mungkin belum lengkap atau belum mencakup semua layanan vital.	- Dokumen yang berisi strategi, tahapan, dan target waktu pemulihan untuk sebagian besar fungsi dan layanan vital, tetapi mungkin belum lengkap atau belum mencakup semua skenario. - Beberapa prosedur pemulihan mungkin ada, tetapi belum terintegrasi atau belum diuji secara menyeluruh.
3	- Organisasi telah menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal. - Penetapan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal telah disusun dan telah diresmikan/diformalkan	Organisasi telah menentukan dan menetapkan strategi, tahapan, dan target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal. Rencana pemulihan ini terdokumentasi dengan baik dan mencakup semua layanan vital.	- Dokumen lengkap yang berisi strategi, tahapan, dan target waktu yang jelas dan terukur untuk memulihkan dan menjalankan semua fungsi dan layanan vital secara penuh/kembali normal. - Prosedur pemulihan yang rinci dan terdokumentasi untuk setiap tahapan, termasuk alokasi sumber daya dan tanggung jawab.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	- Organisasi telah Menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal. - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal	Organisasi telah menentukan, menetapkan, dan melakukan reviu terhadap strategi, tahapan, dan target waktu pemulihan secara berkala. Rencana pemulihan telah diuji dan dievaluasi efektivitasnya.	- Dokumen yang sama seperti indeks 3, tetapi dengan bukti tambahan bahwa strategi, tahapan, dan target waktu pemulihan telah ditinjau dan diperbarui secara berkala. - Laporan pengujian dan evaluasi terhadap rencana pemulihan, termasuk simulasi atau latihan yang dilakukan secara berkala
5	- Organisasi telah Menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal.. - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal serta dilakukan perbaikan secara berkala.	Organisasi telah menentukan, menetapkan, melakukan reviu, dan secara berkala memperbarui strategi, tahapan, dan target waktu pemulihan. Rencana pemulihan telah diuji, dievaluasi, dan ditingkatkan berdasarkan umpan balik dan perubahan kebutuhan.	- Dokumen yang sama seperti indeks 4, tetapi dengan bukti tambahan bahwa strategi, tahapan, dan target waktu pemulihan terus diperbarui dan ditingkatkan berdasarkan umpan balik dan perubahan lingkungan. - Bukti adanya mekanisme untuk mengumpulkan informasi tentang ancaman dan kerentanan baru yang relevan dengan layanan IIV

139 Kontrol 4.1.2.c:

Kontrol	Menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.
Deskripsi Kontrol	Penyelenggara IIV harus menentukan daftar sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan fungsi dan layanan vital. Hal ini penting untuk memastikan bahwa semua elemen yang diperlukan untuk operasi kritis organisasi tersedia dan dapat diakses dengan cepat saat terjadi gangguan. Tujuan dari kontrol ini adalah untuk mengidentifikasi dan mempersiapkan segala sesuatu yang diperlukan untuk memulihkan operasional vital dengan efisien dan tepat waktu. Ini mencakup peralatan TI, perangkat keras, perangkat lunak, serta tenaga kerja yang memiliki kemampuan dan keahlian untuk menangani pemulihan layanan.
Deskripsi Bukti Dukung	Bukti Dukung untuk kontrol ini berfokus pada dokumentasi yang secara jelas mengidentifikasi sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan fungsi dan layanan vital. Dokumen-dokumen tersebut dapat berupa: - Daftar sumber daya yang diperlukan untuk mendukung layanan kritis, seperti perangkat keras, perangkat lunak, dan sistem TI. - Daftar personel yang terlibat dalam pemulihan layanan, termasuk keterampilan dan peran mereka dalam proses pemulihan. - Inventarisasi perangkat dan sistem pendukung yang diperlukan untuk menjaga layanan vital. - Protokol akses darurat untuk personel yang berwenang dan alat yang diperlukan dalam situasi kritis. - Dokumentasi terkait pelatihan personel dalam menjalankan prosedur pemulihan dan pemeliharaan infrastruktur penting
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

Kriteria Pemenuhan Kontrol 4.1.2.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menentukan dan menetapkan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	Organisasi belum mengidentifikasi dan belum mendokumentasikan daftar sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	- Tidak ada dokumen yang mengidentifikasi sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Tidak ada catatan atau bukti bahwa pertimbangan telah diberikan untuk kebutuhan sumber daya.
1	- Organisasi telah menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Belum ada penetapan tertulis diorganisasi terkait daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	Organisasi belum memformalkan identifikasi kebutuhan sumber daya, peralatan, dan personel, tetapi sebagian kecil kebutuhan sudah diidentifikasi dan dipertimbangkan. Misalnya, mungkin ada daftar awal beberapa peralatan penting, tetapi belum lengkap atau belum mencakup semua kebutuhan.	- Catatan atau draf awal yang berisi beberapa elemen sumber daya, peralatan, atau personel yang dibutuhkan untuk beberapa fungsi dan layanan vital. - Bukti informal bahwa beberapa aspek kebutuhan sumber daya telah dipertimbangkan, tetapi belum ada rencana yang terdokumentasi secara formal.
2	- Organisasi telah menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Penetapan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. sedang disusun/masih dalam bentuk draf/belum diresmikan Organisasi telah menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Penetapan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. sedang disusun/masih dalam bentuk draf/belum diresmikan	Organisasi belum memformalkan identifikasi kebutuhan sumber daya, peralatan, dan personel, tetapi sebagian besar kebutuhan sudah diidentifikasi dan dipertimbangkan. Namun, dokumentasi mungkin belum lengkap atau belum mencakup semua aspek.	- Dokumen yang berisi sumber daya, peralatan, dan personel yang dibutuhkan untuk sebagian besar fungsi dan layanan vital, tetapi mungkin belum lengkap atau belum mencakup semua skenario. - Beberapa kebutuhan mungkin telah diidentifikasi, tetapi belum ada alokasi atau pengaturan yang jelas.
3	- Organisasi telah menentukan dan menetapkan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Penetapan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital telah disusun dan telah diresmikan/diformalkan	Organisasi telah mengidentifikasi dan mendokumentasikan daftar lengkap sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan fungsi dan layanan vital. Daftar ini mencakup semua kebutuhan yang relevan dan mutakhir.	- Dokumen lengkap yang berisi daftar rinci sumber daya, peralatan, dan personel yang dibutuhkan untuk menjalankan semua fungsi dan layanan vital. - Matriks ketergantungan yang menunjukkan hubungan antara

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			fungsi/layanan vital dan sumber daya, peralatan, dan personel yang dibutuhkan
4	- Organisasi telah Menentukan dan menetapkan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	Organisasi telah mengidentifikasi, mendokumentasikan, dan melakukan reviu terhadap daftar kebutuhan sumber daya, peralatan, dan personel secara berkala. Daftar ini telah diuji dan dievaluasi kecukupannya	- Dokumen yang sama seperti indeks 3, tetapi dengan bukti tambahan bahwa daftar kebutuhan sumber daya, peralatan, dan personel telah ditinjau dan diperbarui secara berkala. - Laporan pengujian dan evaluasi terhadap ketersediaan dan kecukupan sumber daya, peralatan, dan personel untuk mendukung fungsi dan layanan vital.
5	- Organisasi telah Menentukan dan menetapkan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. . - Organisasi sudah memiliki kebijakan yang telah disusun dan telah diresmikan/diformalkan dan melakukan reviu secara berkala yang berkaitan dengan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital. yang sudah diresmikan serta dilakukan perbaikan secara berkala	Organisasi telah mengidentifikasi, mendokumentasikan, melakukan reviu, dan secara berkala memperbarui daftar kebutuhan sumber daya, peralatan, dan personel. Daftar ini telah diuji, dievaluasi, dan ditingkatkan berdasarkan umpan balik dan perubahan kebutuhan.	- Dokumen yang sama seperti indeks 4, tetapi dengan bukti tambahan bahwa daftar kebutuhan sumber daya, peralatan, dan personel terus diperbarui dan ditingkatkan berdasarkan umpan balik dan perubahan lingkungan. - Bukti adanya mekanisme untuk mengumpulkan informasi tentang perubahan kebutuhan dan risiko yang relevan dengan layanan IIV.

140 Kontrol 4.1.2.d:

Kontrol	Memastikan rencana keberlangsungan layanan dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa rencana keberlangsungan layanan dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. Hal ini bertujuan untuk memastikan semua pihak yang relevan mengetahui peran mereka dalam keberlangsungan layanan dan memahami langkah-langkah yang harus diambil dalam situasi darurat atau gangguan. Tujuan dari kontrol ini adalah untuk menjamin koordinasi yang tepat antara pemangku kepentingan internal dan eksternal agar respons terhadap gangguan dapat dilakukan dengan cepat dan efektif. Komunikasi yang jelas akan mempercepat pemulihan dan mencegah kebingungannya ketika situasi darurat terjadi.
Deskripsi Bukti Dukung	Bukti Dukung yang dapat dilampirkan antara lain: - Dokumen rencana keberlangsungan layanan (BCP - Business Continuity Plan) yang mencakup informasi penting bagi pemangku kepentingan terkait. - Catatan rapat atau komunikasi yang mendokumentasikan penyampaian rencana kepada pihak-pihak yang berkepentingan. - Bukti pelatihan atau sosialisasi yang diadakan untuk pihak yang berkepentingan dalam rangka memastikan pemahaman terhadap rencana. - Surat atau dokumen yang menunjukkan persetujuan dan pemahaman dari pihak-pihak yang terlibat. - Protokol komunikasi yang digunakan untuk memberitahukan pemangku kepentingan terkait dalam keadaan darurat atau saat gangguan layanan.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-04** **NIST CSF 1.1: PR.IP-9** **NIST SP 800-53r5: CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9** **SNI ISO/IEC 27001:2022: 5.3, 5.24, 5.29**

Kriteria Pemenuhan Kontrol 4.1.2.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Rencana keberlangsungan layanan belum dikomunikasikan secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan - Tidak ada kebijakan/panduan/ pedoman terkait komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan	Organisasi tidak memiliki sistem atau prosedur untuk memastikan bahwa informasi tentang rencana keberlangsungan layanan disampaikan kepada pihak-pihak yang relevan.	Tidak ada dokumen atau catatan yang menunjukkan adanya upaya komunikasi tentang rencana keberlangsungan layanan
1	- Rencana keberlangsungan tersebut sudah dikomunikasikan secara khusus ke sebagian kecil pihak yang berkepentingan dan berhak sesuai ketentuan - Belum ada kebijakan/panduan/ pedoman terkait komunikasi secara khusus kepada beberapa pemangku kepentingan tentang pembelajaran tersebut	Organisasi telah melakukan beberapa upaya untuk mengomunikasikan rencana keberlangsungan layanan, tetapi upaya tersebut tidak terstruktur dan tidak mencakup semua pihak yang berkepentingan.	- Beberapa email atau pesan singkat yang dikirim ke beberapa pihak terkait, tetapi tidak ada daftar distribusi yang jelas atau catatan formal tentang komunikasi tersebut. - Informasi tentang rencana keberlangsungan layanan hanya tersedia di beberapa tempat terbatas dan tidak mudah diakses oleh semua pihak yang berkepentingan.
2	- Rencana keberlangsungan tersebut sudah dikomunikasikan kepada sebagian besar pihak yang berkepentingan dan berhak sesuai ketentuan. - Belum ada kebijakan/panduan/ pedoman terkait komunikasi secara khusus kepada beberapa pemangku kepentingan tentang pembelajaran tersebut	Organisasi telah mengomunikasikan rencana keberlangsungan layanan kepada sebagian besar pihak yang relevan, tetapi tidak ada catatan atau dokumentasi yang menunjukkan bahwa komunikasi tersebut telah dilakukan.	- Daftar distribusi dokumen yang tidak lengkap atau tidak diperbarui. - Beberapa tanda terima dokumen yang tidak lengkap atau tidak ada sama sekali. - Materi presentasi atau pelatihan yang tidak terdokumentasi dengan baik.
3	- Rencana keberlangsungan tersebut sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki draf kebijakan/ panduan/pedoman terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan dalam bentuk	Organisasi telah mengomunikasikan rencana keberlangsungan layanan kepada semua pihak yang relevan, tetapi tidak ada cara untuk memastikan bahwa mereka memahami informasi tersebut.	- Daftar distribusi dokumen yang lengkap dan diperbarui. - Tanda terima dokumen dari semua pihak yang relevan. - Materi presentasi atau pelatihan yang terdokumentasi dengan baik. - Namun, tidak ada kuesioner, survei, atau mekanisme lain untuk mengukur pemahaman peserta tentang rencana keberlangsungan layanan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
4	- Rencana keberlangsungan tersebut sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki kebijakan/ panduan/pedoman tertulis terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah dilakukan reviu terkait kebijakan komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Organisasi telah mengomunikasikan rencana keberlangsungan layanan kepada semua pihak yang relevan dan memiliki mekanisme untuk memastikan pemahaman mereka, tetapi tidak ada proses untuk mengevaluasi apakah komunikasi tersebut efektif	- Semua bukti dari indeks 3. - Kuesioner atau survei yang dibagikan kepada peserta setelah sosialisasi atau pelatihan. - Namun, tidak ada laporan atau analisis tentang hasil kuesioner atau survei tersebut
5	- Rencana keberlangsungan tersebut sudah dikomunikasikan kepada seluruh pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah memiliki kebijakan/ panduan/pedoman tertulis terkait komunikasi secara khusus kepada kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan. - Sudah dilakukan reviu dan diperbaiki secara berkala terkait kebijakan komunikasi secara khusus kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Organisasi telah mengomunikasikan rencana keberlangsungan layanan kepada semua pihak yang relevan, memiliki mekanisme untuk memastikan pemahaman mereka, dan telah mengevaluasi efektivitas komunikasi, serta menemukan bahwa informasi tersebut dipahami dengan baik oleh semua pihak yang berkepentingan.	- Semua bukti dari indeks 4. - Laporan atau analisis tentang hasil kuesioner atau survei yang menunjukkan bahwa sebagian besar peserta memahami rencana keberlangsungan layanan dengan baik. - Tindak lanjut atau perbaikan berdasarkan hasil evaluasi komunikasi.

4.1.3. Memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala

Kriteria	Detail
Deskripsi	Pelaksanaan dan simulasi berkala terhadap Rencana Tanggap Insiden Siber (Incident Response Plan/IRP) dan Rencana Keberlangsungan Kegiatan (Business Continuity Plan/BCP) merupakan indikator kritis dari kesiapan organisasi dalam menghadapi gangguan operasional, serangan siber, atau krisis lainnya. Tanpa pengujian rutin, rencana-rencana ini berisiko menjadi tidak relevan, tidak efektif, atau bahkan tidak dapat dijalankan saat dibutuhkan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk menyelenggarakan simulasi secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan simulasi yang rutin, organisasi dapat memastikan bahwa rencana tanggap dan keberlangsungan tetap relevan dan efektif dalam menghadapi insiden yang sebenarnya.
Kompleksitas	**Sedang** – Memerlukan koordinasi dan perencanaan yang komprehensif untuk menyelenggarakan simulasi secara berkala.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-02, ID.IM-04** **NIST CSF 1.1: PR.IP-10** **NIST SP 800-53r5: CP-4, IR-3, PM-14** **SNI ISO/IEC 27001:2022: 5.3**

141 Kontrol 4.1.3.a:

Kontrol	Memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. (misalnya dalam kegiatan simulasi kesiapsiagaan Insiden Siber)
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa rencana tanggap insiden siber dan rencana keberlangsungan kegiatan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. Simulasi ini bertujuan untuk menguji kesiapsiagaan dan respons organisasi terhadap potensi insiden siber yang dapat mempengaruhi layanan vital. Tujuan dari simulasi adalah untuk memastikan bahwa semua pihak yang terlibat memahami peran dan prosedur mereka, serta dapat merespons dengan cepat dan efektif dalam menghadapi insiden siber. Simulasi juga berfungsi untuk mengidentifikasi kelemahan dalam rencana tanggap insiden dan meningkatkan koordinasi antar pihak terkait.
Deskripsi Bukti Dukung	Berikut adalah penjelasan bukti dukung untuk memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV - Laporan hasil simulasi tanggap insiden siber dan keberlangsungan kegiatan, termasuk evaluasi dan rekomendasi perbaikan. - Jadwal dan dokumentasi kegiatan simulasi, termasuk daftar peserta dan peran mereka. - Protokol simulasi dan instruksi yang digunakan untuk mengarahkan simulasi. - Dokumentasi tentang umpan balik dan analisis dari simulasi, termasuk perbaikan yang diterapkan untuk meningkatkan kesiapan dan respons. - Catatan pelatihan dan evaluasi terkait personel yang terlibat dalam simulasi, serta pengukuran efektivitas pelatihan.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: ID.IM-02, ID.IM-04** **NIST CSF 1.1: PR.IP-10** **NIST SP 800-53r5: CP-4, IR-3, PM-14** **SNI ISO/IEC 27001:2022: 5.3**

Kriteria Pemenuhan Kontrol 4.1.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan belum disusun dan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. - Belum ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan	Organisasi tidak memiliki sistem atau prosedur untuk melakukan simulasi terhadap rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.	Tidak ada dokumen atau catatan yang menunjukkan adanya upaya simulasi.
1	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan sudah disimulasikan namun belum secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. - Belum ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.	Organisasi telah melakukan beberapa upaya untuk melakukan simulasi, tetapi upaya tersebut tidak terstruktur, tidak terjadwal secara berkala, dan tidak melibatkan seluruh pihak yang terkait.	- Beberapa email atau pesan singkat yang dikirim ke beberapa pihak terkait, tetapi tidak ada jadwal simulasi yang jelas atau catatan formal tentang pelaksanaan simulasi. - Simulasi hanya dilakukan pada sebagian kecil dari rencana atau tidak melibatkan seluruh pihak yang terkait.
2	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan sudah disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. - Belum ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.	Organisasi telah melakukan simulasi, tetapi tidak ada catatan atau dokumentasi yang menunjukkan bahwa simulasi tersebut telah dilakukan, siapa saja yang terlibat, dan apa hasil dari simulasi tersebut.	- Daftar hadir peserta yang tidak lengkap atau tidak ada sama sekali. - Materi simulasi yang tidak terdokumentasi dengan baik. - Laporan hasil simulasi yang tidak ada atau tidak lengkap.
3	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan sudah disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. - Sudah ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.	Organisasi telah melakukan simulasi secara berkala, tetapi tidak ada mekanisme untuk mengevaluasi apakah simulasi tersebut efektif dalam meningkatkan kesiapsiagaan dan pemahaman seluruh pihak yang terlibat.	- Jadwal simulasi yang teratur. - Daftar hadir peserta yang lengkap. - Materi simulasi yang terdokumentasi dengan baik. - Namun, tidak ada kuesioner, survei, atau mekanisme lain untuk mengukur efektivitas simulasi dalam meningkatkan pemahaman dan kesiapsiagaan peserta
4	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan sudah disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV.	Organisasi telah melakukan simulasi secara berkala dan memiliki mekanisme untuk mengevaluasi efektivitas simulasi, tetapi tidak	- Semua bukti dari indeks 3. - Kuesioner atau survei yang dibagikan kepada peserta setelah simulasi.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- Sudah ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan. - Telah dilakukan reviu terkait kebijakan simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.	ada tindak lanjut atau perbaikan berdasarkan hasil evaluasi simulasi.	- Namun, tidak ada laporan atau analisis tentang hasil kuesioner atau survei tersebut. - Tidak ada bukti bahwa hasil simulasi digunakan untuk memperbaiki rencana atau prosedur.
5	- Rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan sudah disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. - Sudah ada kebijakan/panduan/ pedoman terkait simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan. - Telah dilakukan reviu dan perbaikan secara berkala terkait kebijakan simulasi rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan	Organisasi telah melakukan simulasi secara berkala, memiliki mekanisme untuk mengevaluasi efektivitas simulasi, dan menindaklanjuti hasil evaluasi simulasi dengan perbaikan dan peningkatan yang berkelanjutan.	- Semua bukti dari indeks 4. - Laporan atau analisis tentang hasil kuesioner atau survei yang menunjukkan bahwa sebagian besar peserta memahami dan siap melaksanakan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan. - Bukti bahwa hasil simulasi digunakan untuk memperbaiki rencana, prosedur, atau pelatihan.

4.1.4. Memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan

Kriteria	Detail
Deskripsi	Kesiapan personel yang mengelola Infrastruktur Informasi Vital (IIV) dalam memahami peran, tanggung jawab, dan prosedur penanggulangan/pemulihan insiden merupakan faktor penentu efektivitas Rencana Tanggap Insiden Siber (IRP) dan Rencana Keberlangsungan Kegiatan (BCP). Tanpa pelatihan yang memadai, rencana-rencana tersebut tidak dapat dioperasionalkan secara optimal, bahkan berpotensi menimbulkan kesalahan kritis saat terjadi krisis.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk pelatihan personel dan penyebaran informasi, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan pemahaman yang jelas, personel dapat merespons insiden dengan cepat dan efektif, mengurangi dampak negatif pada operasional dan keamanan data.
Kompleksitas	**Sedang** – Memerlukan pelatihan dan komunikasi yang efektif untuk memastikan bahwa semua personel memahami peran dan prosedur mereka.
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01** **NIST CSF 1.1: RS.CO-1** **NIST SP 800-53r5: CP-2, CP-3, IR-3, IR-8** **SNI ISO/IEC 27001:2022: 5.2, 5.24**

142 Kontrol 4.1.4.a:

Kontrol	Penyelenggara IIV menentukan dan menetapkan personel yang ditugaskan dalam Tim Tanggap Insiden Siber.
Deskripsi Kontrol	Penyelenggara IIV harus menentukan dan menetapkan personel yang akan ditugaskan dalam Tim Tanggap Insiden Siber (Cyber Incident Response Team, CIRT). Tim ini memiliki tanggung jawab untuk menangani, merespons, dan menyelesaikan insiden keamanan siber yang terjadi, dengan tujuan untuk meminimalkan dampak dan mencegah kerusakan lebih lanjut. Penetapan personel ini penting untuk memastikan adanya kejelasan peran, keahlian yang relevan, serta respons yang cepat dan terkoordinasi saat insiden terjadi. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi memiliki tim yang siap dan terlatih dalam menangani insiden siber secara efektif.
Deskripsi Bukti Dukung	Berikut Bukti Dukung yang diperlukan antara lain: - Daftar personel yang ditugaskan dalam Tim Tanggap Insiden Siber, termasuk nama, jabatan, dan peran mereka dalam tim. - Deskripsi tugas dan tanggung jawab masing-masing anggota tim CIRT. - Prosedur pelatihan dan pengujian kesiapan tim untuk menangani insiden siber. - Struktur organisasi dan diagram alur komunikasi untuk Tim Tanggap Insiden Siber. - Laporan pelatihan atau simulasi respons insiden yang telah dilakukan oleh tim CIRT.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01** **NIST CSF 1.1: RS.CO-1** **NIST SP 800-53r5: CP-2, CP-3, IR-3, IR-8** **SNI ISO/IEC 27001:2022: 5.2, 5.24**

Kriteria Pemenuhan Kontrol 4.1.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum adanya dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dan/atau belum adanya pembagian peran yang ditetapkan oleh Organisasi	Organisasi tidak memiliki Tim Tanggap Insiden Siber yang terstruktur atau personel yang ditunjuk untuk menangani insiden siber.	Tidak ada dokumen atau catatan yang menunjukkan adanya Tim Tanggap Insiden Siber yang dibentuk.
1	Dokumen rencana tanggap Insiden Siber sudah memiliki penanggung jawab, namun belum spesifik, dokumen tersebut belum ditetapkan/diformalkan	Organisasi telah menentukan personel yang akan ditugaskan dalam Tim Tanggap Insiden Siber, tetapi tidak ada dokumen atau catatan yang menunjukkan bahwa penetapan tersebut telah dilakukan.	- Beberapa email atau pesan singkat yang dikirim ke beberapa pihak terkait, tetapi tidak ada daftar anggota tim yang jelas atau catatan formal tentang penetapan tim. - Beberapa orang mungkin secara informal ditugaskan untuk menangani insiden, tetapi tidak ada peran atau tanggung jawab yang didefinisikan secara jelas.
2	Dokumen rencana tanggap Insiden Siber sudah memiliki penanggung jawab yang ditugaskan secara spesifik namun belum diresmikan	Organisasi telah menentukan personel yang akan ditugaskan dalam Tim Tanggap Insiden Siber, tetapi tidak ada dokumen atau catatan yang menunjukkan bahwa penetapan tersebut telah dilakukan.	- Daftar nama personel yang dianggap sebagai anggota tim, tetapi tidak ada dokumen resmi yang menetapkan mereka sebagai anggota Tim Tanggap Insiden Siber. - Tidak ada deskripsi tugas atau peran yang terdokumentasi
3	Dokumen rencana tanggap Insiden Siber sudah memiliki penanggung jawab yang ditugaskan secara spesifik dan sudah diresmikan	Organisasi telah menetapkan personel dalam Tim Tanggap Insiden Siber dan memiliki dokumentasi formal, tetapi deskripsi tugas dan tanggung jawab masing-masing anggota tim tidak jelas atau tidak terdokumentasi.	- Surat keputusan atau dokumen resmi lainnya yang menetapkan personel yang ditugaskan dalam Tim Tanggap Insiden Siber. - Namun, tidak ada dokumen yang menjelaskan tugas dan tanggung jawab masing-masing anggota tim.
4	Dokumen rencana tanggap Insiden Siber sudah memiliki penanggung jawab yang ditugaskan secara spesifik, sudah diresmikan, dan direviu secara berkala	Organisasi telah menetapkan personel dalam Tim Tanggap Insiden Siber dengan deskripsi tugas yang jelas, tetapi tidak ada proses untuk mengevaluasi apakah personel tersebut memiliki kompetensi yang sesuai untuk melaksanakan tugas mereka.	- Semua bukti dari indeks 3. - Deskripsi tugas yang jelas untuk setiap anggota tim. - Namun, tidak ada catatan pelatihan, sertifikasi, atau penilaian kompetensi lainnya untuk anggota tim.
5	Dokumen rencana tanggap Insiden Siber sudah memiliki penanggung jawab yang ditugaskan secara spesifik, sudah diresmikan, direviu, dan dilakukan perbaikan secara berkala	Organisasi telah menetapkan personel dalam Tim Tanggap Insiden Siber dengan deskripsi tugas yang jelas, dan telah melakukan evaluasi terhadap kompetensi personel yang menunjukkan bahwa mereka memiliki pengetahuan, keterampilan, dan pengalaman yang sesuai untuk menangani insiden siber.	- Semua bukti dari indeks 4. - Profil anggota tim yang mencantumkan kualifikasi, sertifikasi, dan pengalaman yang relevan. - Catatan pelatihan atau sertifikasi yang relevan dengan keamanan siber yang telah diikuti oleh anggota Tim Tanggap Insiden Siber. - Hasil evaluasi kompetensi yang menunjukkan bahwa anggota tim memiliki pengetahuan, keterampilan, dan pengalaman yang sesuai untuk menangani insiden siber.

143 Kontrol 4.1.4.b:

Kontrol	Penyelenggara IIV memastikan personel mengetahui perannya dan urutan pengoperasian bila respons diperlukan
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa setiap personel yang terlibat dalam Tim Tanggap Insiden Siber (CIRT) mengetahui dengan jelas peran dan tanggung jawab mereka dalam merespons insiden siber. Hal ini mencakup pemahaman tentang urutan pengoperasian yang harus dilakukan jika respons diperlukan, seperti langkah-langkah untuk mengidentifikasi, menganalisis, dan mengatasi insiden, serta bagaimana berkoordinasi dengan pihak-pihak terkait. Tujuan dari kontrol ini adalah untuk memastikan bahwa personel dapat bertindak cepat, tepat, dan terkoordinasi ketika insiden terjadi, sehingga dampaknya dapat diminimalkan.
Deskripsi Bukti Dukung	Berikut adalah penjelasan Bukti Dukung untuk memastikan personel mengetahui perannya dna urutan pengoperasian bila respon diperlukan: - Daftar peran dan tanggung jawab masing-masing anggota Tim Tanggap Insiden Siber (CIRT). - Prosedur respons insiden yang mendetail, mencakup urutan pengoperasian dan langkahlangkah yang harus diambil oleh setiap personel. - Laporan atau dokumentasi yang menunjukkan pemahaman personel terhadap prosedur dan peran mereka (misalnya, hasil pelatihan atau simulasi respons insiden). - Penilaian kesiapan tim, termasuk pengujian pemahaman terhadap prosedur respons insiden melalui latihan atau ujian. - Dokumen alur komunikasi dan koordinasi dalam tim CIRT selama respons insiden
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01** **NIST CSF 1.1: RS.CO-1** **NIST SP 800-53r5: CP-2, CP-3, IR-3, IR-8** **SNI ISO/IEC 27001:2022: 5.2, 5.24**

Kriteria Pemenuhan Kontrol 4.1.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Seluruh personel belum mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan, baik karena belum tersampaikannya pembagian peran maupun karena belum adanya pembagian peran	Organisasi tidak memiliki sistem atau prosedur untuk memastikan bahwa personel memahami peran dan tanggung jawab mereka dalam situasi respons. Tidak ada upaya untuk melatih atau mengomunikasikan informasi ini kepada personel.	Tidak ada dokumen atau catatan yang menunjukkan adanya pelatihan atau sosialisasi tentang peran dan prosedur respons
1	Sebagian kecil personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan, namun tidak dapat mempraktikkannya	Organisasi telah melakukan beberapa upaya untuk memberikan informasi kepada personel tentang peran dan prosedur respons, tetapi upaya tersebut tidak terstruktur atau komprehensif. Personel mungkin hanya memahami sebagian dari peran mereka atau tidak mengetahui urutan tindakan yang harus diambil.	- Beberapa email atau pesan singkat yang dikirim ke beberapa pihak terkait, tetapi tidak ada jadwal pelatihan yang jelas atau catatan formal tentang pelaksanaan pelatihan. - Materi pelatihan yang tidak lengkap atau tidak mencakup semua aspek penting dari peran dan prosedur respons.
2	Sebagian besar personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan namun tidak dapat mempraktikkannya	Organisasi telah mengomunikasikan informasi tentang peran dan prosedur respons kepada personel, tetapi tidak ada catatan atau dokumentasi yang menunjukkan bahwa informasi tersebut telah disampaikan atau dipahami.	- Daftar hadir peserta pelatihan yang tidak lengkap atau tidak ada sama sekali. - Materi pelatihan yang tidak terdokumentasi dengan baik. - Tidak ada catatan evaluasi atau umpan balik dari peserta.
3	Seluruh personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan dan dapat mempraktikkannya Seluruh personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan dan dapat mempraktikkannya	Organisasi telah memberikan informasi tentang peran dan prosedur respons kepada personel, tetapi tidak ada cara untuk memastikan bahwa mereka benar-benar memahami informasi tersebut. Tidak ada evaluasi atau umpan balik untuk mengukur pemahaman personel.	- Jadwal pelatihan yang teratur. - Daftar hadir peserta yang lengkap. - Materi pelatihan yang terdokumentasi dengan baik. - Namun, tidak ada kuesioner, survei, atau mekanisme lain untuk mengukur pemahaman peserta tentang peran dan prosedur respons.
4	Seluruh personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan, dan dapat mempraktikkannya serta direviu secara berkala	Organisasi telah memberikan informasi tentang peran dan prosedur respons kepada personel dan memiliki mekanisme untuk mengukur pemahaman mereka, tetapi tidak ada evaluasi tentang efektivitas pelatihan atau komunikasi tersebut. Tidak ada	- Semua bukti dari indeks 3. - Kuesioner atau survei yang dibagikan kepada peserta setelah pelatihan. - Namun, tidak ada laporan atau analisis tentang hasil kuesioner atau survei tersebut.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
		umpan balik atau perbaikan berdasarkan hasil evaluasi.	- Tidak ada bukti bahwa hasil evaluasi digunakan untuk memperbaiki pelatihan atau prosedur.
5	Seluruh personel mengetahui peran dan urutan pengoperasian dalam proses penanggulangan dan pemulihan serta dapat mempraktikkannya serta direviu dan dilakukan perbaikan secara berkala	Organisasi telah memberikan informasi tentang peran dan prosedur respons kepada personel, memiliki mekanisme untuk mengukur pemahaman mereka, dan telah mengevaluasi efektivitas pelatihan atau komunikasi tersebut. Hasil evaluasi menunjukkan bahwa personel memahami dengan baik peran dan tanggung jawab mereka dalam situasi respons.	- Semua bukti dari indeks 4. - Laporan atau analisis tentang hasil kuesioner atau survei yang menunjukkan bahwa sebagian besar peserta memahami peran dan prosedur respons dengan baik. - Bukti bahwa hasil evaluasi digunakan untuk memperbaiki pelatihan, prosedur, atau komunikasi.

144 Kontrol 4.1.4.c:

Kontrol	Penyelenggara IIV mengidentifikasi siapa saja pihak-pihak pihak-pihak terkait dalam proses penanggulangan dan pemulihan insiden, misalnya aparat penegak hukum, regulator, maupun tim TTIS nasional
Deskripsi Kontrol	Penyelenggara IIV perlu mengidentifikasi dan menentukan pihak-pihak terkait yang akan dilibatkan dalam proses penanggulangan dan pemulihan insiden siber. Ini mencakup aparat penegak hukum, regulator yang mengatur sektor atau industri terkait, tim Tanggap Tindak Lanjut Insiden Siber (TTIS) nasional, serta pihak-pihak lain yang relevan, seperti vendor atau penyedia layanan, yang mungkin terlibat dalam pemulihan atau investigasi insiden. Identifikasi ini penting agar respons insiden dapat dilakukan secara terkoordinasi dengan melibatkan pihak yang memiliki kewenangan, informasi, atau keahlian untuk mendukung pemulihan dan mengatasi dampak insiden secara efektif
Deskripsi Bukti Dukung	Berikut adalah penjelasan bukti dukung yang dapat dilampirkan antara lain: - Daftar pihak terkait yang harus terlibat dalam penanggulangan insiden (misalnya, penegak hukum, regulator, TTIS, penyedia layanan terkait). - Prosedur komunikasi dan koordinasi dengan pihak-pihak terkait, termasuk protokol yang harus diikuti ketika melibatkan pihak eksternal. - Bukti koordinasi yang dilakukan dengan pihak-pihak terkait (misalnya, surat resmi, notifikasi, atau rapat koordinasi). - Rencana pemulihan yang mencakup peran dan tanggung jawab masing-masing pihak terkait dalam pemulihan pascainsiden. - Evaluasi atau laporan dari insiden yang menunjukkan partisipasi dan peran pihak-pihak terkait dalam pemulihan insiden.
Ancaman/ Risiko yang dimitigasi	TH025 TH038 TH040 TH044 TH053 TH065 TH077 TH036 TH039 TH043 TH050 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01** **NIST CSF 1.1: RS.CO-1** **NIST SP 800-53r5: CP-2, CP-3, IR-3, IR-8** **SNI ISO/IEC 27001:2022: 5.2, 5.24**

Kriteria Pemenuhan Kontrol 4.1.4.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Tidak melibatkan siapapun dalam proses penanggulangan dan pemulihan insiden, termasuk tidak adanya mekanisme eskalasi	Tidak ada identifikasi pihak-pihak terkait dalam proses penanggulangan dan pemulihan insiden.	Tidak ada dokumen, catatan, atau bukti yang menunjukkan upaya identifikasi pihak-pihak terkait.
1	Terdapat mekanisme eskalasi sehingga memungkinkan untuk melibatkan TTIS sektoral atau TTIS nasional dalam proses penanggulangan dan pemulihan insiden namun belum diformalkan/diresmikan	Identifikasi pihak-pihak terkait sangat minimal, hanya mencakup satu pihak (misalnya, hanya aparat penegak hukum).	Dokumen atau catatan yang menunjukkan identifikasi minimal, misalnya hanya mencantumkan satu pihak terkait (contoh: aparat penegak hukum).
2	- Terdapat mekanisme eskalasi sehingga memungkinkan untuk melibatkan TTIS sektoral atau TTIS nasional dalam proses penanggulangan dan pemulihan insiden namun belum diformalkan/diresmikan - Terdapat mekanisme dalam melibatkan aparat, penegak hukum, regulator, dan pihak lain yang diperlukan, namun kontak narahubung pihak lain tidak tercantum dalam dokumen rencana.	Identifikasi pihak-pihak terkait sebagian, mencakup dua pihak (misalnya, aparat penegak hukum dan regulator).	Dokumen atau catatan yang menunjukkan identifikasi sebagian, mencantumkan dua pihak terkait (contoh: aparat penegak hukum dan regulator).
3	- Terdapat mekanisme eskalasi sudah diformalkan/diresmikan sehingga memungkinkan untuk melibatkan TTIS sektoral atau TTIS nasional dalam proses penanggulangan dan pemulihan insiden. - Terdapat mekanisme yang sudah diformalkan/diresmikan dalam melibatkan aparat, penegak hukum, regulator, dan pihak lain yang diperlukan dan kontak narahubung pihak lain tercantum dalam dokumen rencana.	Identifikasi pihak-pihak terkait cukup lengkap, mencakup tiga pihak (misalnya, aparat penegak hukum, regulator, dan tim TTIS nasional).	Dokumen atau catatan yang menunjukkan identifikasi cukup lengkap, mencantumkan tiga pihak terkait (contoh: aparat penegak hukum, regulator, dan tim TTIS nasional).
4	- Terdapat mekanisme eskalasi yang sudah diformalkan/diresmikan dan direviu secara berkala sehingga memungkinkan untuk melibatkan TTIS sektoral atau TTIS nasional dalam proses penanggulangan dan pemulihan insiden. - Terdapat mekanisme yang sudah diformalkan/diresmikan dan direviu secara berkala dalam melibatkan aparat, penegak hukum, regulator,	Identifikasi pihak-pihak terkait hampir lengkap, mencakup semua pihak utama dan beberapa pihak pendukung.	Dokumen atau catatan yang menunjukkan identifikasi hampir lengkap, mencantumkan semua pihak utama dan beberapa pihak pendukung.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	dan pihak lain yang diperlukan dan kontak narahubung pihak lain tercantum dalam dokumen rencana. - - TTIS melibatkan komunitas, ahli hukum atau akademisi.		
5	- Terdapat mekanisme eskalasi yang sudah diformalkan/diresmikan serta direviu dan diperbaiki secara berkala sehingga memungkinkan untuk melibatkan TTIS sektoral atau TTIS nasional dalam proses penanggulangan dan pemulihan insiden. - Terdapat mekanisme yang diformalkan/diresmikan serta direviu dan diperbaiki secara berkala dalam melibatkan aparat, penegak hukum, regulator, dan pihak lain yang diperlukan dan kontak narahubung pihak lain tercantum dalam dokumen rencana. - TTIS melibatkan komunitas, ahli hukum dan akademisi	Identifikasi pihak-pihak terkait sangat lengkap, mencakup semua pihak utama, pihak pendukung, dan pihak lain yang relevan secara komprehensif.	Dokumen atau catatan yang menunjukkan identifikasi sangat lengkap, mencantumkan semua pihak utama, pihak pendukung, dan pihak lain yang relevan secara komprehensif.

145 Kontrol 4.1.4.d:

Kontrol	Penyelenggara IIV perlu mengembangkan dan mengelola aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan. sehingga informasi organisasi hanya boleh keluar melalui personel yang berwenang saja.
Deskripsi Kontrol	Penyelenggara IIV perlu mengembangkan dan mengelola aturan yang mengatur penerbitan dan distribusi informasi setelah terjadinya insiden keamanan. Tujuan dari kebijakan ini adalah untuk memastikan bahwa informasi terkait insiden hanya dibagikan kepada pihak yang berwenang, sesuai dengan protokol yang telah ditetapkan. Hal ini penting untuk mencegah kebocoran informasi yang dapat merugikan organisasi, mematuhi peraturan perlindungan data, dan memastikan bahwa informasi yang dibagikan tidak memperburuk situasi atau memberi keuntungan kepada pihak yang tidak bertanggung jawab. Kontrol ini bertujuan untuk memastikan bahwa organisasi memiliki kontrol yang ketat atas aliran informasi terkait insiden keamanan.
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat berupa dokumen atau catatan resmi yang menunjukkan bahwa penyelenggara IIV telah mengembangkan dan mengelola aturan terkait penerbitan dan distribusi informasi setelah terjadinya insiden keamanan diantaranya: - Kebijakan dan prosedur tentang penerbitan dan distribusi informasi pasca insiden keamanan, termasuk siapa yang berwenang untuk memberikan informasi dan dalam konteks apa informasi tersebut dapat dibagikan. - Daftar personel yang memiliki kewenangan untuk mengeluarkan informasi terkait insiden keamanan dan rincian tanggung jawab mereka. - Contoh laporan insiden yang menunjukkan bagaimana informasi dikelola dan dibagikan sesuai dengan kebijakan. - Protokol komunikasi internal dan eksternal yang mengatur aliran informasi terkait insiden siber. - Laporan audit atau pengawasan terhadap penerbitan dan distribusi informasi pasca insiden
Ancaman/ Risiko yang dimitigasi	TH053 TH071 TH054
Referensi Kontrol	**NIST CSF 2.0: PR.AT-01** **NIST CSF 1.1: RS.CO-1** **NIST SP 800-53r5: CP-2, CP-3, IR-3, IR-8** **SNI ISO/IEC 27001:2022: 5.2, 5.24**

Kriteria Pemenuhan Kontrol 4.1.4.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum adanya aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan	Tidak ada aturan atau prosedur yang dikembangkan atau dikelola terkait penerbitan dan distribusi informasi setelah insiden keamanan.	Tidak ada dokumen, catatan, atau bukti yang menunjukkan adanya aturan atau prosedur.
1	Sudah ada aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan, namun seluruh personel belum mengetahuinya serta belum mempraktikkannya	Aturan atau prosedur telah dikembangkan, tetapi belum sepenuhnya dikelola atau diterapkan.	Dokumen awal seperti draf kebijakan atau SOP yang belum final, tetapi belum ada bukti implementasi atau pelaksanaan.
2	Sudah ada aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan dan sebagian personel sudah mengetahuinya, namun aturan belum dipraktikkan	Aturan atau prosedur telah dikembangkan dan mulai dikelola, tetapi masih terbatas dalam penerapannya.	Dokumen kebijakan atau SOP yang sudah final, serta bukti awal implementasi seperti pelatihan atau sosialisasi terbatas kepada personel.
3	Sudah ada aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan dan sebagian personel sudah mengetahuinya dan sebagian sudah mempraktikkannya	Aturan atau prosedur telah dikembangkan, dikelola, dan diterapkan secara memadai.	Dokumen kebijakan atau SOP yang lengkap, bukti implementasi seperti pelatihan reguler, daftar personel yang berwenang, dan catatan distribusi informasi yang terbatas.
4	Sudah ada aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan dan seluruh personel sudah mengetahui dan mempraktikkannya	Aturan atau prosedur telah dikembangkan, dikelola, dan diterapkan dengan baik, mencakup hampir semua aspek yang diperlukan.	Dokumen kebijakan atau SOP yang komprehensif, bukti implementasi seperti pelatihan berkala, daftar personel yang berwenang, log distribusi informasi, dan mekanisme monitoring yang terstruktur.
5	Sudah ada aturan yang telah direviu dan diperbaiki secara berkala mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan dan seluruh personel sudah mengetahui dan mempraktikkannya	Aturan atau prosedur telah dikembangkan, dikelola, dan diterapkan secara optimal dan menyeluruh.	Dokumen kebijakan atau SOP yang sangat detail, bukti implementasi seperti pelatihan intensif, daftar personel yang berwenang, log distribusi informasi yang teraudit, serta sistem monitoring dan evaluasi yang efektif.

4.1.5. Memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang

Kriteria	Detail
Deskripsi	Pemahaman personel terhadap prosedur penggunaan rekam cadang (backup) merupakan komponen kritis dalam menjaga ketahanan data dan kelangsungan operasional organisasi. Tanpa penguasaan yang memadai terhadap proses backup (pencadangan), restorasi (pemulihan), dan validasi data, risiko kehilangan data atau kegagalan pemulihan pasca-insiden (seperti serangan siber, kegagalan sistem, atau bencana alam) akan meningkat signifikan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan pelatihan dan dokumentasi yang jelas tentang prosedur penggunaan rekam cadang.
Dampak	**Tinggi** – Dengan pemahaman yang jelas, personel dapat memastikan bahwa data yang dicadangkan dapat dipulihkan dengan cepat dan lengkap, mengurangi risiko kehilangan data.
Kompleksitas	**Sedang** – Memerlukan pelatihan yang terstruktur dan dokumentasi yang jelas tentang prosedur penggunaan rekam cadang.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

146 Kontrol 4.1.5.a:

Kontrol	Penyelenggara IIV memastikan personel yang mengelola IIV melakukan prosedur rekam cadang untuk mengamankan aset informasi berupa sistem/data yang tersimpan di dalam sistem IIV, serta memastikan bahwa media yang digunakan untuk menyimpan data tersebut telah diamankan
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa personel yang mengelola IIV melakukan prosedur rekam cadang (backup) yang sesuai untuk mengamankan aset informasi, termasuk sistem dan data yang tersimpan dalam sistem IIV. Prosedur ini bertujuan untuk melindungi data dari kehilangan, kerusakan, atau ancaman lainnya. Selain itu, organisasi juga perlu memastikan bahwa media yang digunakan untuk menyimpan data cadangan telah diamankan dengan tepat, misalnya dengan mengenkripsi data cadangan dan memastikan akses yang terbatas hanya untuk pihak yang berwenang. Tujuan dari kontrol ini adalah untuk memastikan bahwa data yang penting bagi organisasi terlindungi melalui rekam cadang yang aman dan efektif
Deskripsi Bukti Dukung	Bukti dukung untuk kontrol ini dapat mencakup: - Kebijakan dan prosedur backup yang mencakup frekuensi, media yang digunakan, serta mekanisme enkripsi data cadangan. - Laporan audit yang menunjukkan status implementasi prosedur backup pada sistem IIV. - Bukti pengujian pemulihan data (data recovery testing) yang mengonfirmasi bahwa prosedur backup dapat diandalkan untuk pemulihan data. - Laporan pemantauan yang menunjukkan bahwa media penyimpanan cadangan (misalnya tape, cloud storage) telah diamankan secara fisik dan logis. - Laporan hasil evaluasi dan pengujian sistem backup dan pemulihan (Disaster Recovery Test) yang mencakup jaminan ketersediaan data cadangan yang valid dan aman.
Ancaman/ Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.1.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Belum ada prosedur rekam cadang yang ditetapkan.	Tidak ada prosedur rekam cadang (backup) yang dilakukan, dan media penyimpanan data tidak diamankan.	Tidak ada dokumen, catatan, atau bukti yang menunjukkan adanya prosedur backup atau pengamanan media penyimpanan.
1	- Sudah ada prosedur rekam cadang yang disusun, namun belum ada pihak yang menjadi penanggung jawab. - Prosedur tersebut belum dilaksanakan sebagaimana direncanakan.	Prosedur rekam cadang telah diidentifikasi, tetapi belum sepenuhnya diterapkan atau dikelola.	Draf prosedur backup atau catatan awal yang menunjukkan rencana backup, tetapi belum ada bukti pelaksanaan atau pengamanan media penyimpanan.
2	- Sudah ada prosedur rekam cadang yang disusun dan sudah ada pihak yang menjadi penanggung jawab,dan terdapat penanggung jawab spesifik ke personel tertentu. - Prosedur tersebut belum dilaksanakan sesuai dengan rencana	Prosedur rekam cadang telah diterapkan sebagian, tetapi belum konsisten atau lengkap.	Dokumen prosedur backup yang sudah final, bukti pelaksanaan backup yang terbatas (misalnya, hanya untuk sebagian data), dan upaya pengamanan media penyimpanan yang masih minimal.
3	- Sudah ada prosedur rekam cadang yang ditetapkan/diformalkan dan sudah ada pihak yang menjadi penanggung jawab,dan terdapat penanggung jawab spesifik ke personel tertentu. - Prosedur tersebut sudah dilaksanakan sesuai dengan rencana	Prosedur rekam cadang telah diterapkan secara memadai, dan media penyimpanan telah diamankan.	Dokumen prosedur backup yang lengkap, bukti pelaksanaan backup yang teratur (misalnya, jadwal backup), serta bukti pengamanan media penyimpanan seperti enkripsi atau kontrol akses fisik.
4	- Sudah ada prosedur rekam cadang yang ditetapkan dan sudah ac pihak yang menjadi penanggung jawab,dan terdapat penanggur jawab spesifik ke personel tertentu Prosedur tersebut suda dilaksanakan sesuai dengan rencana - Media yang digunakan untuk menyimpan data belum disimpan sedemikian rupa sehingga aman.	Prosedur rekam cadang telah diterapkan dengan baik, dan media penyimpanan diamankan secara komprehensif.	Dokumen prosedur backup yang detail, bukti pelaksanaan backup yang konsisten dan teraudit, serta pengamanan media penyimpanan yang kuat (misalnya, enkripsi, penyimpanan cloud aman, dan kontrol akses ketat).
5	- Sudah ada prosedur rekam cadang yang ditetapkan dan sudah ada pihak yang menjadi penanggung jawab,dan terdapat penanggung jawab spesifik ke personel tertentu - Prosedur tersebut sudah dilaksanakan sesuai dengan rencana - Media yang digunakan untuk menyimpan data telah diamankan	Prosedur rekam cadang telah diterapkan secara optimal, dan media penyimpanan diamankan dengan tingkat keamanan tertinggi.	Dokumen prosedur backup yang sangat rinci, bukti pelaksanaan backup yang terotomatisasi dan teraudit secara berkala, serta pengamanan media penyimpanan yang mencakup enkripsi tingkat tinggi, redundansi, dan pemantauan keamanan 24 jam setiap harinya.

4.2. Menganalisis dan melaporkan Insiden Siber

Penyelenggara IIV melakukan analisis dan pelaporan insiden siber yang terjadi untuk mendapatkan informasi terkait penyebab, dampak, dan lingkup insiden siber, serta tersedianya informasi yang akurat dan tepat waktu kepada pihak-pihak yang berkepentingan dalam mengambil tindakan lebih lanjut. Proses analisis insiden siber mencakup identifikasi dan investigasi insiden, teknik yang digunakan, klasifikasi insiden berdasarkan tingkat keparahan dan jenis serangan, pemetaan dampak insiden, serta pengumpulan bukti forensik. Pelaporan insiden siber mencakup pembuatan laporan yang komprehensif terkait insiden meliputi waktu, deskripsi, dampak, dan langkah-langkah yang diambil; komunikasi dengan stakeholder internal dan eksternal serta otoritas terkait; pembaruan status penanganan insiden secara berkala.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal, maupun sumber informasi eksternal;
b) mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber;
c) memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan; dan
d) memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Menganalisis dan melaporkan Insiden Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08, RS.CO-02, RS.CO-03, RC.CO-04**
NIST CSF 1.1	**:**	**RS.AN-2, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5**
NIST SP 800-53r5	**:**	**CP-2, IR-4, IR-6, IR-8, RA-3, AU-6, PE-6, SI-5, PM-15**
SNI ISO/IEC 27001:2022	**:**	**5.27, 6.8**

4.2.1. Mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal maupun sumber informasi eksternal

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengumpulkan data dan informasi terkini tentang kondisi IIV dari sumber internal dan eksternal untuk mendukung deteksi, analisis, dan respon terhadap insiden siber. Pengumpulan informasi tersebut dilakukan untuk memperoleh gambaran menyeluruh mengenai kondisi sistem yang terdampak insiden. Pengumpulan informasi dari hasil deteksi internal dapat bersumber dengan menggunakan alamat pemantauan keamanan seperti SIEM, IDS/IPS untuke mendeteksi anomali; mengumpulkan dan menganalisis log sistem, aplikasi, dan jaringan; laporan dari tim internal atau user terkait potensi insiden. Sedangkan pengumpulan informasi dari sumber eksternal didapatkan dengan memanfaatkan threat intelligence seperti CERT/CSIRT/forum keamanan; berkolaborasi dengan mitra, pihak ketiga, atau otoritas keamanan siber; memantau berita, laporan publik, atau platform komunitas keamanan siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam alat dan sumber daya untuk mengumpulkan serta menganalisis informasi dari berbagai sumber.
Dampak	**Tinggi** – Dengan informasi yang lengkap, organisasi dapat mengidentifikasi potensi ancaman dan meresponsnya dengan cepat serta efektif.
Kompleksitas	**Sedang** – Memerlukan sistem dan prosedur yang tepat untuk mengumpulkan, menganalisis, dan mengintegrasikan informasi dari berbagai sumber.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

147 Kontrol 4.2.1.a:

Kontrol	Penyelenggara IIV memastikan hasil analisis deteksi peristiwa siber diperiksa untuk menilai ada atau tidaknya anomali pada sistem.
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa hasil analisis deteksi peristiwa siber (seperti log aktivitas sistem, alarm dari perangkat keamanan, dan hasil pemantauan jaringan) diperiksa secara menyeluruh untuk menilai apakah ada anomali yang menunjukkan potensi ancaman atau gangguan pada sistem. Anomali ini bisa mencakup aktivitas yang tidak biasa, pola akses yang mencurigakan, atau kegagalan sistem yang tidak dapat dijelaskan. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi secara proaktif mendeteksi potensi serangan atau gangguan keamanan melalui analisis yang mendalam dan dapat segera mengambil tindakan mitigasi yang diperlukan
Deskripsi Bukti Dukung	Berikut beberapa contoh Bukti Dukung: - Laporan hasil analisis log dan deteksi peristiwa yang mengidentifikasi anomali pada sistem. - Dokumen prosedur atau panduan internal tentang cara menganalisis peristiwa siber untuk mendeteksi anomali. - Hasil dari pemeriksaan atau audit yang dilakukan terhadap perangkat deteksi dan sistem pemantauan untuk memastikan bahwa anomali teridentifikasi secara tepat. - Laporan pemantauan yang menunjukkan adanya tindak lanjut yang diambil terhadap anomali yang terdeteksi. - Bukti pelatihan personel tentang cara mendeteksi dan menilai anomali dalam data peristiwa siber.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

Kriteria Pemenuhan Kontrol 4.2.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi tidak memeriksa hasil analisis deteksi peristiwa siber.	Tidak ada bukti kegiatan pemeriksaan hasil analisis deteksi peristiwa siber.	Tidak ada dokumentasi pemeriksaan atau analisis yang dilakukan terhadap peristiwa siber
1	- Organisasi melakukan deteksi peristiwa siber - Hasil deteksi tidak dianalisis lebih lanjut	Organisasi melakukan deteksi terhadap peristiwa siber, namun tidak ada analisis lanjutan terhadap hasil deteksi tersebut.	Dokumentasi hasil deteksi peristiwa siber yang tidak menunjukkan adanya analisis lanjutan. Dokumentasi ini dapat berupa Laporan deteksi peristiwa siber; Log deteksi yang tidak mencatat analisis lebih lanjut.
2	- Organisasi melakukan deteksi peristiwa siber - Hasil deteksi dianalisis lebih lanjut secara manual oleh personel yang berkompeten dalam melakukan analisis deteksi	Hasil deteksi peristiwa siber dianalisis lebih lanjut oleh personel yang berkompeten, namun belum ada prosedur yang standar	- Laporan analisis hasil deteksi peristiwa siber yang menunjukkan bahwa analisis dilakukan secara manual oleh personel berkompeten. - Catatan personel yang melakukan analisis.
3	- Organisasi melakukan deteksi peristiwa siber - Hasil deteksi dianalisis lebih lanjut secara manual oleh personel yang berkompeten dalam melakukan analisis deteksi - Menyusun prosedur pemeriksaan hasil analisis deteksi peristiwa siber	Organisasi telah menyusun prosedur atau panduan resmi untuk memeriksa hasil analisis deteksi peristiwa siber, dan hasil deteksi dianalisis oleh personel berkompeten.	- Prosedur atau panduan pemeriksaan hasil analisis deteksi yang telah disusun. - Laporan hasil deteksi dan analisis manual yang mengikuti prosedur tersebut.
4	- Organisasi melakukan deteksi peristiwa siber - Hasil deteksi dianalisis lebih lanjut secara manual oleh personel yang berkompeten dalam melakukan analisis deteksi - Menyusun prosedur pemeriksaan hasil analisis deteksi peristiwa siber - Melakukan monitoring dan reviu terhadap hasil deteksi, hasil analisis, serta prosedur yang sudah ditetapkan	Organisasi tidak hanya menyusun prosedur, tetapi juga secara rutin melakukan monitoring dan reviu terhadap hasil deteksi, analisis, dan prosedur yang ditetapkan.	- Laporan hasil monitoring dan reviu yang menunjukkan evaluasi terhadap deteksi, analisis, dan prosedur yang ada. - Dokumen reviu dan evaluasi yang dilakukan secara berkala
5	- Organisasi melakukan deteksi peristiwa Siber - peristiwa Siber dianalisis menggunakan sistem terotomisasi - hasil analisis sistem terotomisasi diverifikasi oleh personel yang berkompeten dalam melakukan analisis deteksi	Organisasi telah mengimplementasikan sistem otomatisasi untuk menganalisis peristiwa siber dan hasil analisis tersebut diverifikasi oleh personel yang berkompeten.	- Bukti penggunaan sistem terotomatisasi untuk analisis deteksi peristiwa siber. - Laporan verifikasi hasil analisis otomatis oleh personel berkompeten.

148 Kontrol 4.2.1.b:

Kontrol	Penyelenggara IIV mengumpulkan dan menganalisis laporan peristiwa siber yang diterima baik dari pengguna layanan, maupun sumber eksternal organisasi misalnya laporan dari Tim Tanggap Insiden Siber nasional atau mitra pihak ketiga
Deskripsi Kontrol	Penyelenggara IIV perlu mengumpulkan dan menganalisis laporan peristiwa siber yang diterima dari berbagai sumber, seperti pengguna layanan, Tim Tanggap Insiden Siber nasional, atau mitra pihak ketiga. Langkah ini penting untuk memastikan bahwa organisasi memiliki pemahaman yang mendalam tentang ancaman atau insiden siber yang terjadi, termasuk pola serangan dan potensi dampaknya. Tujuan dari kontrol ini adalah untuk mendukung kemampuan organisasi dalam mendeteksi, merespons, dan memitigasi insiden siber secara efektif serta meningkatkan kesiapsiagaan organisasi terhadap ancaman serupa di masa depan
Deskripsi Bukti Dukung	Berikut beberapa dokumen yang dapat digunakan sebagai bukti dukung untuk kontrol ini: - Laporan insiden dari pengguna layanan. - Dokumen laporan insiden yang diterima dari Tim Tanggap Insiden Siber nasional atau mitra pihak ketiga. - Sistem pencatatan insiden (incident log) atau database yang mendokumentasikan peristiwa siber. - Analisis tren atau pola insiden dari berbagai laporan. - Prosedur standar untuk penerimaan dan analisis laporan peristiwa siber.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

Kriteria Pemenuhan Kontrol 4.2.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi tidak memiliki layanan aduan/pelaporan	Tidak ada sistem atau mekanisme untuk menerima laporan peristiwa siber dari pengguna atau pihak eksternal.	Tidak ada catatan atau dokumentasi mengenai layanan aduan/pelaporan.
1	Organisasi memiliki layanan aduan/pelaporan namun tidak dianalisis	Organisasi memiliki mekanisme untuk menerima laporan peristiwa siber tetapi tidak ada proses analisis terhadap laporan tersebut.	Terdapat saluran aduan/pelaporan, namun tidak ada dokumentasi analisis atau tindak lanjut.
2	Organisasi memiliki layanan aduan/pelaporan, dianalisis, namun belum memiliki prosedurnya	Organisasi mengumpulkan laporan dan menganalisis insiden, namun belum memiliki prosedur atau kebijakan formal untuk pengelolaan laporan tersebut.	Ada analisis terhadap laporan, tetapi tidak ada prosedur atau pedoman standar yang ditetapkan untuk menangani laporan peristiwa siber. Contoh dokumen seperti laporan tanggap insiden; dokumen analisis laporan insiden, namun tidak ada prosedur atau pedoman yang jelas.
3	Organisasi memiliki layanan aduan/pelaporan, dianalisis, dan sudah ditetapkan prosedurnya	Organisasi memiliki prosedur atau pedoman yang jelas untuk menerima menganalisis, dan menindaklanjuti laporan peristiwa siber.	Ada prosedur yang terdokumentasi untuk pengumpulan, analisis, dan respons terhadap laporan peristiwa siber
4	Organisasi memiliki layanan aduan/pelaporan, dianalisis, dan sudah ditetapkan prosedurnya, serta dilakukan monitoring dan reviu berkala	Organisasi secara rutin memonitor dan mereviu proses pengumpulan, analisis, dan penanganan laporan peristiwa siber untuk memastikan efektivitas dan kesesuaian dengan kebutuhan.	Bukti adanya evaluasi atau reviu berkala terhadap efektivitas prosedur yang diterapkan, serta monitoring laporan yang diterima
5	Organisasi memiliki layanan aduan/pelaporan, dianalisis, dan sudah ditetapkan prosedurnya, serta dilakukan monitoring dan reviu berkala, kemudian dilakukan perbaikan jika diperlukan	Organisasi tidak hanya melakukan monitoring dan reviu, tetapi juga melakukan perbaikan berkelanjutan berdasarkan hasil evaluasi dan temuan insiden.	Bukti adanya tindakan perbaikan yang dilakukan berdasarkan hasil reviu, serta penerapan pembaruan prosedur jika diperlukan.

4.2.2. Mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan identifikasi dan analisis poteksi dampak dari insiden siber untuk membantu Penyelenggara IIV memahami dan mengevaluasi sejauh mana dampak yang insiden siber dapat mempengaruhi sistem, layanan, atau data dalam organisasi. Fokusnya adalah mengidentifikasi berbagai jenis dampak, seperti operasional, keuangan, reputasi, hukum, dan keamanan data, serta menganalisis tingkat keparahan (apakah dapat mengancam kerahasiaan, integritas, atau ketersediaan informasi), skala, dan durasi dampak tersebut. Penilaian terhadap kerentanan juga dilakukan untuk mengidentifikasi faktor penyebab insiden, serta menilai dampaknya terhadap pihak eksternal seperti pelanggan atau mitra bisnis. Hasil analisis ini membantu Penyelenggara IIV untuk menyusun prioritas tindak lanjut, menentukan langkah penanggulangan dan pemulihan yang tepat, mengurangi dampak lebih lanjut, meminimalkan kerugian, serta memulihkan layanan dengan cepat.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan penilaian dampak dan analisis potensi risiko.
Dampak	**Tinggi** – Dengan analisis dampak yang tepat, organisasi dapat merencanakan langkah-langkah mitigasi dan pemulihan yang sesuai untuk mengurangi dampak negatif dari insiden siber.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan metodologi yang tepat untuk mengidentifikasi dan menganalisis potensi dampak dari insiden siber.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

149 Kontrol 4.2.2.a:

Kontrol	Penyelenggara IIV harus mengidentifikasi dan menganalisis potensi dampak Insiden Siber pada layanan IIV, termasuk organisasi, dan pihak terkait seperti mitra ketiga berdasarkan laporan lengkap Insiden Siber
Deskripsi Kontrol	Penyelenggara IIV harus mengidentifikasi dan menganalisis potensi dampak dari insiden siber terhadap layanan IIV itu sendiri, organisasi, maupun pihak terkait seperti mitra ketiga. Proses ini dilakukan berdasarkan laporan lengkap insiden siber yang mencakup detail kejadian, sumber, dan area terdampak. Kontrol ini bertujuan agar penyelenggara IIV memahami sejauh mana insiden siber dapat mempengaruhi operasional, keuangan, reputasi, dan keamanan sehingga organisasi dapat mengambil langkah-langkah mitigasi yang tepat, meminimalkan kerugian, dan memulihkan layanan dengan efektif.
Deskripsi Bukti Dukung	Untuk melakukan identifikasi dan analisis potensi dampak insiden siber pada layanan IIV dengan sistematis dan cermat, serta mementukan langkah-langkah yang diperlukan untuk mengurangi dampak negatif dan memulihkan layanan dengan efektif, maka penyelenggara IIV perlu menyediakan bukti dukung terhadap kontrol ini. Bukti dukung tersebut antara lain: - Laporan lengkap insiden siber yang berisi kronologi, penyebab, dan dampak insiden. - Dokumen hasil analisis dampak terhadap layanan IIV, organisasi, dan pihak terkait. - Protokol atau prosedur analisis dampak insiden siber. - Bukti komunikasi dengan mitra ketiga terkait dampak insiden. - Rekaman rapat evaluasi dampak insiden dengan pemangku kepentingan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

Kriteria Pemenuhan Kontrol 4.2.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV, organisasi, dan pihak terkait	Tidak ada proses atau mekanisme identifikasi dan analisis dampak insiden siber terhadap layanan IIV, organisasi, dan pihak terkait.	Tidak ada laporan atau dokumentasi terkait identifikasi dan analisis dampak insiden siber
1	Organisasi sudah melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV, organisasi, dan pihak terkait, namun belum berdasarkan laporan lengkap Insiden Siber (masih bersifat sporadis)	Organisasi telah melakukan identifikasi dan analisis dampak insiden siber, tetapi belum melakukannya berdasarkan laporan lengkap yang komprehensif dan masih dilakukan secara tidak terstruktur.	Terdapat laporan atau catatan identifikasi dan analisis dampak insiden siber, namun tidak lengkap atau sporadis
2	Organisasi sudah melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV, organisasi, dan pihak terkait berdasarkan laporan lengkap Insiden Siber, namun belum memiliki prosedur pelaksanaannya	Organisasi telah melakukan proses identifikasi dan analisis dampak dilakukan berdasarkan laporan lengkap, namun prosedur pelaksanaan atau pedoman yang mendasari proses tersebut belum ada.	Bukti laporan lengkap insiden siber yang dianalisis, namun tidak ada prosedur atau pedoman yang terdokumentasi terkait identifikasi dan analisis dampak
3	Organisasi sudah melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV, organisasi, dan pihak terkait berdasarkan laporan lengkap Insiden Siber, yang mengacu kepada prosedur pelaksanaannya	Prosedur pelaksanaan untuk identifikasi dan analisis dampak insiden siber sudah terdokumentasi dan diikuti, dan dilakukan berdasarkan laporan lengkap insiden siber.	Ada prosedur atau pedoman yang terdokumentasi untuk identifikasi dan analisis dampak, serta laporan yang dihasilkan mengacu pada prosedur tersebut
4	- Organisasi sudah melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV, organisasi, dan pihak terkait berdasarkan laporan lengkap Insiden Siber, yang mengacu kepada prosedur pelaksanaannya - Pelaksanaan identifikasi dan analisis potensi dampak Insiden Siber dimonitor secara berkala - Prosedur pelaksanaan identifikasi dan analisis potensi dampak Insiden Siber direviu secara berkala	Proses identifikasi dan analisis dampak dilakukan dengan mengacu pada prosedur yang sudah terdokumentasi, serta dilaksanakan dan dimonitor secara berkala. Prosedur tersebut juga direviu secara berkala.	Bukti monitoring berkala terhadap pelaksanaan identifikasi dan analisis dampak insiden siber serta laporan reviu prosedur secara berkala.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	- Organisasi sudah melakukan identifikasi dan analisis potensi dampak Insiden Siber pada layanan IIV organisasi, dan pihak terkait berdasarkan laporan lengkap Insiden Siber, yang mengacu kepada prosedur pelaksanaannya - Pelaksanaan identifikasi dan analisis potensi dampak Insiden Siber dimonitor secara berkala - Prosedur pelaksanaan identifikasi dan analisis potensi dampak Insiden Siber direviu secara berkala - Melakukan perbaikan terhadap prosedur dan pelaksanaan identifikasi dan analisis potensi dampak Insiden Siber (jika diperlukan)	Selain monitoring dan reviu, organisasi juga melakukan perbaikan berkelanjutan terhadap prosedur pelaksanaan identifikasi dan analisis dampak, apabila ditemukan celah atau kebutuhan perbaikan.	Bukti adanya perbaikan prosedur dan pelaksanaan analisis dampak yang dilakukan setelah reviu atau monitoring. Adanya laporan perbaikan yang diimplementasikan.

4.2.3. Memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus memastikan setiap insiden siber yang terjadi diklasifikasikan secara konsisten dan akurat berdasarkan kriteria yang telah ditetapkan oleh organisasi. Kategorisasi mencakup tingkat keparahan, jenis insiden, dampak pada layanan IIV dan pihak terkait, prioritas penanganan, serta sumber daya yang diperlukan untuk merespon insiden tersebut. Dengan melakukan kategorisasi insiden siber, Penyelenggara IIV dapat memprioritaskan respon, mengalokasikan sumber daya efektif, memberikan panduan untuk tindakan pemulihan yang lebih efisien dan memastikan penanganan yang sesuai dengan tingkat keparahan. Dengan adanya kategorisasi juga memudahkan pelaporan dan analisis lebih lanjut untuk meningkatkan proses penanganan insiden di masa depan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menetapkan kriteria dan mengkategorikan insiden secara konsisten.
Dampak	**Tinggi** – Dengan kategori yang jelas, organisasi dapat merespons insiden dengan cara yang sesuai dengan tingkat keparahannya, sehingga mengurangi dampak negatif.
Kompleksitas	**Sedang** – Memerlukan metodologi yang tepat untuk menetapkan kriteria dan mengkategorikan insiden siber secara efektif.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

150 Kontrol 4.2.3.a:

Kontrol	Penyelenggara IIV memastikan laporan Insiden Siber dikumpulkan, dikategorisasikan, dan diprioritaskan sesuai dampak risiko terhadap organisasi
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa setiap insiden siber yang terjadi dikumpulkan dengan cermat, kemudian dikategorikan berdasarkan jenis dan karakteristiknya, serta diprioritaskan berdasarkan dampak risiko yang ditimbulkan terhadap organisasi. Kontrol ini bertujuan untuk insiden siber diidentifikasi dari yang paling kritis dan memerlukan penanganan segera, sehingga sumber daya dapat dialokasikan secara efektif. Dengan melakukan kategorisasi dan skala prioritas insiden siber, organisasi dapat merespon ancaman dengan lebih terarah, meminimalkan dampak negatif, memastikan pemulihan layanan yang cepat dan tepat, serta meningkatkan ketahanan siber secara keseluruhan.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - Kebijakan atau prosedur manajemen insiden yang mencakup proses pengumpulan, pengkategorian, dan pemrioritasan insiden. - Laporan insiden siber yang mencakup informasi kategori insiden, tingkat risiko, dan langkah-langkah penanganan. - Log atau catatan kronologi insiden yang terdokumentasi. - Bukti sistem pelaporan insiden, seperti aplikasi tiket insiden atau formulir pelaporan manual. - Laporan evaluasi pasca-insiden yang menunjukkan efektivitas kategori dan prioritas yang diberikan. - Daftar tim atau individu yang bertanggung jawab atas manajemen insiden di organisasi. - Dokumentasi pelatihan personel terkait manajemen dan pelaporan insiden siber.
Ancaman/ Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-08** **NIST CSF 1.1: RS.AN-2** **NIST SP 800-53r5: CP-2, IR-4, RA-3** **SNI ISO/IEC 27001:2022: 5.27**

Kriteria Pemenuhan Kontrol 4.2.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan pengumpulan laporan Insiden Siber	Tidak ada pengumpulan laporan insiden siber	Tidak ada laporan insiden yang dikumpulkan
1	Organisasi sudah mengumpulkan laporan Insiden Siber, namun belum dikategorisasi dan diprioritaskan sesuai dampak risiko terhadap organisasi	Organisasi telah mengumpulkan laporan insiden siber, tetapi belum ada pengkategorian dan pemrioritasan berdasarkan dampak risiko.	Laporan insiden yang dikumpulkan, namun tanpa pengkategorian dan pemprioritasan risiko.
2	Organisasi sudah mengumpulkan, mengkategorisasikan, dan memprioritaskan laporan Insiden Siber sesuai dampak risiko terhadap organisasi, namun belum memiliki prosedur pelaksanaannya	Organisasi telah melakukan pengumpulan, pengkategorian, dan pemrioritasan laporan, namun belum ada prosedur yang terdokumentasi untuk pelaksanaan ini.	Laporan insiden yang mengandung kategori dan prioritas, namun tanpa kebijakan prosedural
3	Organisasi sudah mengumpulkan, mengkategorisasikan, dan memprioritaskan laporan Insiden Siber sesuai dampak risiko terhadap organisasi yang mengacu kepada prosedur pelaksanaannya	Organisasi telah melakukan pengumpulan, pengkategorian, dan pemrioritasan insiden sesuai prosedur yang terdokumentasi	- Prosedur tertulis terkait pengelolaan laporan insiden (misalnya, dokumen SOP) - Laporan insiden siber yang sesuai dengan prosedur
4	- Organisasi sudah mengumpulkan, mengkategorisasikan, dan memprioritaskan laporan Insiden Siber sesuai dampak risiko terhadap organisasi yang mengacu kepada prosedur pelaksanaannya - Pelaksanaan pengumpulan, pengkategorisasian, dan prioritisasi laporan Insiden Siber dimonitor secara berkala - Prosedur pengumpulan, pengkategorisasian, dan prioritisasi laporan Insiden Siber direviu secara berkala	Organisasi tidak hanya mengikuti prosedur, tetapi juga memonitor pelaksanaannya dan mereviu prosedur secara berkala untuk memastikan efektivitas dan kesesuaian.	Monitoring pelaksanaan pengelolaan insiden dan bukti reviu prosedur yang dilakukan secara berkala.
5	- Organisasi sudah mengumpulkan, mengkategorisasikan, dan memprioritaskan laporan Insiden Siber sesuai dampak risiko terhadap organisasi yang mengacu kepada prosedur pelaksanaannya - Pelaksanaan pengumpulan, pengkategorisasian, dan prioritisasi laporan Insiden Siber dimonitor secara berkala - Prosedur pengumpulan, pengkategorisasian, dan prioritisasi laporan Insiden Siber direviu secara berkala - Melakukan perbaikan terhadap prosedur dan pelaksanaan pengumpulan, pengkategorisasian, dan prioritisasi laporan Insiden Siber (jika diperlukan)	Organisasi telah mencapai tingkat kematangan tertinggi dengan tidak hanya memonitor dan mereviu, tetapi juga melakukan perbaikan (improvement) terhadap prosedur dan pelaksanaan pengumpulan, kategorisasi, dan prioritisasi laporan insiden siber berdasarkan temuan reviu.	Bukti monitoring dan reviu, serta dokumen terkait perbaikan prosedur yang diterapkan jika ditemukan ketidaksesuaian.

4.2.4. Memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait

Kriteria	Detail
Deskripsi	Penyelenggara IIV harus memastikan bahwa setiap insiden siber yang terjadi segera dilaporkan kepada pihak-pihak terkait, baik pihak internal maupun pihak ekternal organisasi, sesuai dengan kebijakan dan regulasi yang berlaku. Pihak terkait dapat mencakup tim tanggap insiden organisasi, manajemen senior, regulator, mitra bisnis, atau lembaga pemerintah seperti tim tanggap insiden siber nasional. Pelaporan yang cepat dan tepat waktu penting untuk memastikan tindakan respon yang cepat dan koordinasi yang efektif dalam penanganan insiden, meminimalkan dampak, dan memastikan kepatuhan terhadap regulasi yang berlaku.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem pelaporan yang efektif dan sumber daya untuk melakukan pelaporan secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan pelaporan yang efektif, organisasi dapat memastikan bahwa respons terhadap insiden dilakukan dengan cepat dan tepat oleh pihak yang berwenang.
Kompleksitas	**Sedang** – Memerlukan sistem pelaporan yang tepat dan prosedur untuk menyampaikan informasi insiden secara efektif.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-01, RS.MA-04, RS.CO-02, RS.CO-03, RC.CO-04** **NIST CSF 1.1: RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5** **NIST SP 800-53r5: AU-6, CP-2, IR-4, IR-6, IR-8, PE-6, SI-5, PM-15** **SNI ISO/IEC 27001:2022: 6.8**

151 Kontrol 4.2.4.a:

Kontrol	Penyelenggara IIV memastikan informasi mengenai Insiden Siber dilaporkan kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa setiap insiden siber yang terjadi dilaporkan kepada pihak yang berwenang, baik internal maupun eksternal, sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku. Kontrol ini bertujuan untuk memastikan transparansi, akuntabilitas, dan kepatuhan terhadap regulasi, serta memungkinkan koordiansi yang efektif dengan pihak yang berwenang dalam rangka penanggulangan dan pemulihan insiden siber. Laporan insiden siber yang tepat waktu dan akurat membantu organisasi dalam mitigasi risiko, meminimalkan dampak, mempercepat pemulihan, dan memenuhi kewajiban hukum atau regulasi yang terkait dengan keamanan siber.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - Kebijakan dan prosedur pelaporan insiden siber yang mencakup mekanisme pelaporan kepada pihak internal dan eksternal. - Dokumen daftar pihak berwenang (internal dan eksternal) yang harus menerima laporan insiden. - Formulir atau template pelaporan insiden siber. - Bukti laporan insiden siber yang telah disampaikan ke pihak berwenang. - Log komunikasi terkait pelaporan insiden, seperti email atau surat resmi. - Dokumentasi kriteria insiden yang harus dilaporkan sesuai dengan regulasi. - Bukti pelatihan personel terkait pelaporan insiden siber.
Ancaman/ Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.CO-02, RS.CO-03, RC.CO-04** **NIST CSF 1.1: RS.CO-2, RS.CO-3** **NIST SP 800-53r5: AU-6, CP-2, IR-4, IR-6, IR-8** **SNI ISO/IEC 27001:2022: 6.8**

Kriteria Pemenuhan Kontrol 4.2.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melaporkan informasi mengenai Insiden Siber kepada pihak yang berwenang	Tidak ada pelaporan Insiden Siber yang dilakukan kepada pihak yang berwenang.	Tidak ada bukti dukung yang tersedia
1	Organisasi hanya melaporkan sebagian informasi mengenai Insiden Siber kepada pihak yang berwenang	Pelaporan dilakukan, tetapi informasi yang dilaporkan tidak lengkap atau hanya sebagian.	Laporan insiden yang tidak lengkap atau tidak sesuai dengan ketentuan perundang-undangan.
2	Organisasi sudah melaporkan seluruh informasi mengenai Insiden Siber kepada pihak yang berwenang, namun belum memiliki prosedur pelaksanaannya	Organisasi telah melaporkan seluruh insiden siber, tetapi belum memiliki prosedur tertulis untuk mengatur proses pelaporan.	- Laporan Insiden Siber yang lengkap. - Tidak ada prosedur formal atau dokumentasi prosedur pelaporan yang mengatur pelaporan insiden.
3	Organisasi sudah melaporkan seluruh informasi mengenai Insiden Siber kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku	Organisasi telah memiliki prosedur tertulis untuk pelaporan insiden siber dan melakukannya sesuai dengan kriteria organisasi dan peraturan perundangan yang berlaku.	- Laporan yang disampaikan lengkap dan sesuai dengan regulasi perundang-undangan yang berlaku. - Prosedur pelaporan tertulis yang menggambarkan langkah-langkah pelaporan yang jelas.
4	- Organisasi sudah melaporkan seluruh informasi mengenai Insiden Siber kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku - Pelaksanaan pelaporan Insiden Siber kepada pihak yang berwenang dimonitor secara berkala - Prosedur pelaporan Insiden Siber kepada pihak yang berwenang direviu secara berkala	Organisasi tidak hanya mengikuti prosedur, tetapi juga memonitor pelaksanaannya dan mereviu prosedur secara berkala untuk memastikan efektivitas dan kesesuaian.	- Laporan monitoring pelaksanaan pelaporan insiden siber. - Catatan hasil reviu prosedur. - Dokumen tindak lanjut dari hasil reviu.
5	- Organisasi sudah melaporkan seluruh informasi mengenai Insiden Siber kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku - Pelaksanaan pelaporan Insiden Siber kepada pihak yang berwenang dimonitor secara berkala - Prosedur pelaporan Insiden Siber kepada pihak yang berwenang direviu secara berkala - Melakukan perbaikan terhadap prosedur dan pelaksanaan pelaporan Insiden Siber kepada pihak yang berwenang (jika diperlukan)	Organisasi telah mencapai tingkat kematangan tertinggi dengan tidak hanya memonitor dan mereviu, tetapi juga melakukan perbaikan (improvement) terhadap prosedur dan pelaksanaan pelaporan insiden siber berdasarkan temuan reviu.	- Laporan insiden yang lengkap dan diterima oleh pihak berwenang. - Bukti monitoring pelaksanaan pelaporan yang dilakukan secara berkala. - Dokumen yang menunjukkan adanya reviu dan perbaikan prosedur pelaporan

152 Kontrol 4.2.4.b:

Kontrol	Penyelenggara IIV memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap Insiden Siber (seperti kepada Kementerian atau Lembaga pembina sektor, Tim Tanggap Insiden Siber nasional, atau mitra pihak ketiga)
Deskripsi Kontrol	Penyelenggara IIV perlu memastikan bahwa koordinasi dengan para pemangku kepentingan, termasuk kementerian/lembaga pembina sektor, Tim Tanggap Insiden Siber Nasional, atau mitra pihak ketiga, dilakukan secara efektif sesuai dengan rencana tanggap insiden siber yang telah disusun. Proses ini bertujuan untuk memastikan adanya sinergi dalam menangani insiden siber, meningkatkan efisiensi penanganan, dan meminimalkan dampak terhadap organisasi serta sektor terkait. Tujuan dari kontrol ini adalah untuk menilai kesiapan organisasi dalam melakukan koordinasi yang cepat dan terstruktur dengan pemangku kepentingan yang relevan dalam menghadapi insiden siber.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - Rencana Tanggap Insiden Siber yang mencantumkan mekanisme koordinasi dengan pemangku kepentingan eksternal. - Dokumen MoU atau perjanjian kerja sama dengan pihak terkait (kementerian, lembaga, mitra pihak ketiga). - Log atau catatan komunikasi selama insiden siber yang menunjukkan koordinasi dilakukan sesuai rencana. - Dokumentasi simulasi atau latihan tanggap insiden yang melibatkan pemangku kepentingan eksternal. - Bukti pelaporan insiden ke pihak berwenang, seperti Tim Tanggap Insiden Siber Nasional atau regulator sektor. - Catatan pertemuan atau laporan kolaborasi dengan mitra terkait selama insiden. - Prosedur operasional standar (SOP) yang mencakup langkahlangkah koordinasi tanggap insiden
Ancaman/ Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-01, RS.MA-04, RS.CO-03** **NIST CSF 1.1: RS.CO-4, RS.CO-5** **NIST SP 800-53r5: CP-2, PE-6, IR-4, IR-8, SI-5, PM-15** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.2.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan identifikasi siapa saja para pemangku kepentingan terkait jika terjadi Insiden Siber	Organisasi belum memiliki daftar pemangku kepentingan yang harus diajak berkoordinasi	Tidak ada dokumen identifikasi pemangku kepentingan atau rencana komunikasi
1	Organisasi sudah mengidentifikasi siapa saja para pemangku kepentingan, namun belum melakukan koordinasi kepada para pemangku kepentingan tersebut	Organisasi memiliki daftar pemangku kepentingan namun belum ada tindakan koordinasi yang dilaksanakan	Daftar pemangku kepentingan yang diidentifikasi
2	Organisasi sudah mengidentifikasi siapa saja para pemangku kepentingan dan sudah melakukan koordinasi kepada para pemangku kepentingan tersebut	Organisasi telah melakukan koordinasi awal dengan pemangku kepentingan namun belum ada pengawasan terhadap efektivitas koordinasi	Notulen rapat atau laporan koordinasi dengan pemangku kepentingan
3	Organisasi sudah memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap Insiden Siber	Proses koordinasi dengan pemangku kepentingan dilaksanakan sesuai dengan rencana yang ada	Dokumen rencana tanggap Insiden Siber dan laporan koordinasi yang mencantumkan pelaksanaan sesuai rencana
4	- Organisasi sudah memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap Insiden Siber - elaksanaan koordinasi dengan para pemangku kepentingan dimonitor secara berkala - Rencana tanggap Insiden Siber direviu secara berkala	Melakukan evaluasi rutin terhadap efektivitas koordinasi	Laporan monitoring koordinasi dan reviu rencana tanggap Insiden Siber
5	- Organisasi sudah memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap Insiden Siber - Pelaksanaan koordinasi dengan para pemangku kepentingan dimonitor secara berkala - Rencana tanggap Insiden Siber direviu secara berkala - Melakukan perbaikan terhadap rencana tanggap Insiden Siber dan pelaksanaan koordinasi dengan para pemangku kepentingan (jika diperlukan)	Menerapkan siklus perbaikan berdasarkan hasil evaluasi	Rencana tanggap Insiden Siber direviu secara berkala

4.3. Melaksanakan penanggulangan dan pemulihan Insiden Siber

Pelaksanaan penanggulangan dan pemulihan insiden siber dilakukan secara menyeluruh dengan memastikan insiden segera diisolasi dan dimitigasi sesuai rencana tanggap, serta mengumpulkan dan memelihara bukti dari IIV terdampak. Proses ini dilanjutkan dengan investigasi, eradikasi penyebab, dan koordinasi dengan pihak terkait untuk eskalasi penanganan. Setelah insiden ditangani, keamanan setiap aset informasi diperiksa, sistem dan data dipulihkan melalui prosedur pencadangan, serta retensi hasil cadangan yang tidak terpakai ditetapkan sesuai ketentuan. Untuk menjamin keberhasilan pemulihan, dilakukan pengujian ulang terhadap fungsi vital dan pendukung. Selain itu, organisasi juga memastikan adanya strategi komunikasi publik serta penyampaian informasi penanggulangan dan pemulihan kepada pihak terkait.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber;
b) mengumpulkan dan memelihara bukti Insiden Siber dari IIV terdampak;
c) menginvestigasi dan eradikasi penyebab Insiden Siber;
d) mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber.
e) memastikan setiap aset informasi diperiksa keamanannya setelah penanganan Insiden Siber;
f) melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan;
g) menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan;
h) pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi;
i) memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber; dan
j) penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Melaksanakan penanggulangan dan pemulihan Insiden Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**RS.MI-01, RS.MI-02, RS.AN-03, RS.AN-06, RS.MA-03, RC.CO-03, RC.CO-04**
NIST CSF 1.1	**:**	**RS.MI-1, RS.MI-2, RS.AN-3, RS.AN-4, RC.CO-1, RC.CO-2, RC.CO-3**
NIST SP 800-53r5	**:**	**IR-4, CP-2, IR-5, IR-8, RA-3, AU-7**
SNI ISO/IEC 27001:2022	**:**	**5.25, 5.26, 5.28, 8.7**

4.3.1. Memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara Infrastruktur Informasi Vital (IIV) mengisolasi dan memitigasi insiden siber sesuai rencana tanggap insiden dengan mengumpulkan bukti, menginvestigasi penyebab, serta berkoordinasi dengan pihak terkait. Mereka memastikan keamanan aset informasi, melaksanakan pencadangan dan pemulihan sistem, serta menerapkan retensi data sesuai ketentuan. Pengujian ulang dilakukan untuk menjamin pemulihan optimal, sementara strategi komunikasi publik diterapkan guna menyampaikan informasi insiden, penanggulangan, dan pemulihan kepada pihak berkepentingan.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk mengisolasi dan memitigasi insiden, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan isolasi dan mitigasi yang efektif, organisasi dapat mengurangi kerusakan dan menjaga keamanan sistem serta data.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan koordinasi yang baik untuk mengisolasi dan memitigasi insiden.
Referensi Kontrol	**NIST CSF 2.0: RS.MI-01, RS.MI-02** **NIST CSF 1.1: RS.MI-1, RS.MI-2** **NIST SP 800-53r5: IR-4** **SNI ISO/IEC 27001:2022: 5.26, 8.7**

153 Kontrol 4.3.1.a:

Kontrol	Penyelenggara IIV harus mengambil langkah-langkah yang diperlukan untuk meminimalkan kerusakan terkait keamanan dan mengurangi dampak yang disebabkan oleh Insiden Siber tersebut. Misalnya melakukan isolasi terhadap jaringan yang terdapat Insiden Siber.
Deskripsi Kontrol	Penyelenggara IIV perlu mengambil langkah-langkah yang tepat untukmeminimalkan kerusakan yang timbul akibat insiden siber dan mengurangi dampaknya. Salah satu langkah yang dapat diambil adalah melakukan isolasi jaringan atau sistem yang terinfeksi atau terkena dampak insiden siber untuk mencegah penyebaran lebih lanjut. Tujuan dari kontrol ini adalah untuk mengevaluasi kesiapan organisasi dalam menanggapi insiden siber dengan tindakan yang efektif guna mengurangi dampak pada operasional dan keamanan organisasi.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Laporan tindakan yang diambil selama insiden siber, termasuk isolasi sistem atau jaringan. - Protokol atau SOP yang menjelaskan prosedur isolasi jaringan dalam situasi insiden siber. - Catatan pemantauan atau log yang menunjukkan pemisah anantara jaringan yang terinfeksi dengan bagian lain dari sistem. - Dokumentasi hasil evaluasi dampak dari insiden siber dan langkah mitigasi yang diterapkan. - Bukti pelaporan insiden dan tindak lanjut yang dilakukan kepada pihak terkait (seperti regulator atau pihak ketiga). - Hasil latihan atau simulasi insiden siber yang mencakup langkah-langkah isolasi jaringan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MI-01, RS.MI-02** **NIST CSF 1.1: RS.MI-1, RS.MI-2** **NIST SP 800-53r5: IR-4** **SNI ISO/IEC 27001:2022: 5.26, 8.7**

Kriteria Pemenuhan Kontrol 4.3.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki dan mengetahui prosedur untuk meminimalkan kerusakan keamanan akibat Insiden Siber	Tidak ada kesadaran terhadap perlunya containment.	Tidak ada dokumen atau bukti prosedur penanganan insiden.
1	Organisasi mulai menerapkan Prosedur containment untuk meminimalkan kerusakan keamanan akibat Insiden Siber, Organisasi mulai mengidentifikasi dampak yang dapat ditimbulkan akibat Insiden Siber alternatif: Organisasi sudah menerapkan langkah-langkah containment untuk meminimalkan kerusakan keamanan akibat Insiden Siber, namun belum menyeluruh serta belum memiliki prosedur yang telah di formalkan	Organisasi mulai menyusun dan menerapkan prosedur containment secara terbatas.	Draft awal prosedur containment. Catatan insiden yang telah ditangani secara manual. Dokumen awal terkait identifikasi dampak insiden.
2	Organisasi telah menerapkan Prosedur containment namun belum ditetapkan dan belum dijalankan, Organisasi telah melakukan Identifikasi kerusakan dan dampak dari Insiden Siber Alternatif: Organisasi sudah menerapkan langkah-langkah containment untuk meminimalkan kerusakan keamanan akibat Insiden Siber, secara menyeluruh namun belum memiliki prosedur yang telah di formalkan	Organisasi telah memiliki prosedur containment tetapi belum ditetapkan secara formal dan belum dijalankan secara konsisten.	Dokumen prosedur containment yang belum disahkan. Laporan identifikasi kerusakan dan dampak insiden. Bukti penerapan prosedur dalam beberapa kasus insiden.
3	Organisasi telah menetapkan Prosedur Containment dan mulai dijalankan untuk meminimalkan kerusakan keamanan dan mengurangi dampak insiden	Organisasi telah memiliki prosedur containment yang ditetapkan dan mulai menerapkannya dalam penanganan insiden.	SOP penanganan insiden yang telah disahkan. Bukti penerapan containment dalam beberapa kasus nyata. Laporan awal evaluasi efektivitas containment.
4	Organisasi telah menetapkan secara formal dan menjalankan prosedur containment terhadap Insiden Siber untuk meminimalkan kerusakan dan mengurangi dampak dari Insiden Siber tersebut secara berkelanjutan dan dilakukan monitoring dan reviu	Prosedur containment telah ditetapkan secara formal dan dijalankan secara berkelanjutan.	SOP containment yang telah diperbarui berdasarkan hasil monitoring. Laporan monitoring dan reviu insiden siber. Bukti pelatihan atau simulasi containment bagi personel terkait.
5	Organisasi menjalankan prosedur containment yang telah ditetapkan secara konsisten, dilakukan monitoring, reviu dan perbaikan berkelanjutan serta untuk mengurangi dampak dari Insiden Siber Prosedur containment telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi menjalankan prosedur containment secara konsisten dan berbasis perbaikan berkelanjutan.	SOP containment yang telah mengalami pembaruan berkala. Bukti implementasi containment dalam sistem otomatisasi. Laporan audit keamanan siber. Dokumentasi integrasi containment dalam proses bisnis organisasi.

154 Kontrol 4.3.1.b:

Kontrol	Penyelenggara IIV harus mengidentifikasi hal-hal yang perlu diprioritaskan dan ruang lingkup respons yang perlu diambil.
Deskripsi Kontrol	Penyelenggara IIV harus mengidentifikasi hal-hal yang perlu diprioritaskan dan ruang lingkup respons yang perlu diambil dalam menghadapi insiden siber. Langkah ini penting untuk memastikan bahwa respons yang diambil sesuai dengan tingkat keparahan insiden dan untuk mengalokasikan sumber daya secara efektif. Prioritas ini bisa mencakup identifikasi aset yang paling kritis, pemulihan sistem penting, dan perlindungan data sensitif yang terpengaruh. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang jelas untuk menentukan prioritas dalam menangani insiden siber dan apakah proses pengambilan keputusan dalam respons insiden sudah tepat.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Prosedur penanganan insiden - BIA atau Matriks Insiden (Adanya Prioritas Penanganan Insiden)
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.1.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan identifikasi prioritas yang harus dilakukan dalam menghadapi Insiden Siber	Tidak ada inisiatif atau aktivitas dalam mengidentifikasi prioritas dan ruang lingkup respons Insiden Siber.	Tidak ada dokumentasi terkait identifikasi prioritas dan ruang lingkup respons terhadap Insiden Siber
1	Organisasi sudah menerapkan langkah identifikasi prioritas dan ruang lingkup respons dalam menghadapi Insiden Siber namun belum menyeluruh (sebagian kecil) serta belum memiliki prosedur yang telah di formalkan	Identifikasi prioritas dan ruang lingkup respons telah dimulai tetapi masih terbatas dalam cakupan kecil dan belum memiliki prosedur resmi.	Draft awal atau konsep identifikasi prioritas yang belum diformalkan
2	Organisasi sudah menerapkan langkah identifikasi prioritas dan ruang lingkup respons dalam menghadapi Insiden Siber namun belum menyeluruh (sebagian besar) namun belum memiliki prosedur yang telah di formalkan	Identifikasi prioritas dan ruang lingkup respons telah mencakup sebagian besar aspek yang relevan, tetapi prosedur masih belum formal.	Dokumen identifikasi prioritas yang mencakup sebagian besar aspek yang relevan
3	Organisasi sudah menerapkan langkah identifikasi prioritas dan ruang lingkup respons dalam menghadapi Insiden Siber secara menyeluruh serta sudah memiliki prosedur yang telah di formalkan	Identifikasi prioritas dan ruang lingkup respons telah menyeluruh dan prosedur telah terdokumentasi secara resmi.	Dokumen prosedur identifikasi prioritas dan ruang lingkup respons telah tersedia dan terdokumentasi.
4	Organisasi menjalankan Prosedur identifikasi prioritas dan ruang lingkup respons terhadap Insiden Siber untuk meminimalkan kerusakan dan mengurangi dampak dari Insiden Siber sesuai dengan prosedur yang telah ditetapkan dimonitor dan dilakukan reviu secara berkelanjutan	Prosedur identifikasi prioritas dan ruang lingkup respons sudah diterapkan, dimonitor, dan dievaluasi secara berkala untuk memastikan efektivitasnya.	Hasil pemantauan dan evaluasi berkala terhadap efektivitas prosedur. Laporan reviu dan peningkatan prosedur secara periodik.
5	Organisasi menjalankan Prosedur identifikasi prioritas dan ruang lingkup respons terhadap Insiden Siber untuk meminimalkan kerusakan dan mengurangi dampak dari Insiden Siber sesuai dengan prosedur yang telah ditetapkan dimonitor dan dilakukan reviu secara berkelanjutan Prosedur identifikasi prioritas dan ruang lingkup respons telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Prosedur identifikasi prioritas dan ruang lingkup respons telah terintegrasi dengan proses bisnis atau dalam sistem otomatisasi untuk meningkatkan efektivitas.	Integrasi prosedur identifikasi dan respons Insiden Siber dengan proses bisnis utama organisasi atau sistem otomatisasi. Sistem otomatisasi dalam identifikasi dan respons Insiden Siber. Dokumentasi integrasi dan evaluasi efektivitas otomatisasi.

155 Kontrol 4.3.1.c:

Kontrol	Penyelenggara IIV harus mengambil tindakan yang tepat terhadap perangkat yang terpengaruh oleh Insiden Siber, terutama mengenai fasilitas produksi yang rusak akibat insiden keamanan.
Deskripsi Kontrol	Organisasi harus mengambil tindakan yang tepat terhadap perangkat yang terpengaruh oleh insiden siber, terutama mengenai fasilitas produksi yang rusak akibat insiden keamanan. Tindakan ini mencakup pemulihan atau penggantian perangkat yang terpengaruh, isolasi sistem yang terkena dampak, serta pemulihan data yang mungkin hilang atau rusak. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang jelas dan efektif untuk menangani perangkat yang terpengaruh oleh insiden siber, khususnya yang dapat mempengaruhi kelangsungan operasional, terutama di fasilitas produksi yang kritis.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Prosedur penanganan insiden - SOP Tanggap Darurat - Dokumentasi Tanggap Darurat
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.1.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk melakukan tindakan atau penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber.	Tidak ada kebijakan atau prosedur yang mengatur penanganan perangkat yang terdampak insiden.	Tidak terdapat dokumen kebijakan atau prosedur penanganan insiden.
1	Organisasi telah melakukan tindakan atau penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Penanganan dilakukan pada sebagian kecil perangkat terdampak. Prosedur belum terdokumentasi secara resmi.	Laporan insiden yang menunjukkan adanya tindakan penanganan. Draft Dokumentasi tanggap darurat.
2	Organisasi telah melakukan tindakan atau penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Penanganan dilakukan pada sebagian besar perangkat terdampak. Prosedur masih bersifat tidak formal atau belum terdokumentasi secara resmi.	Laporan insiden yang lebih sistematis. Dokumentasi tanggap darurat. Draft prosedur penanganan insiden.
3	Organisasi telah melakukan tindakan atau penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Semua perangkat terdampak insiden mendapatkan tindakan penanganan. Prosedur formal telah terdokumentasi dengan jelas.	Dokumen Prosedur Penanganan Insiden yang telah disahkan. SOP Tanggap Darurat terkait insiden siber. Laporan insiden yang menunjukkan implementasi prosedur secara menyeluruh.
4	Organisasi telah menjalankan Prosedur penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan, dimonitor dan dilakukan reviu secara berkelanjutan Organisasi telah menjalankan secara menyeluruh dan melakukan reviu terhadap tindakan terhadap perangkat yang terpengaruh oleh Insiden Siber.	Prosedur yang telah diformalkan dijalankan secara menyeluruh. Proses monitoring dan reviu dilakukan secara berkala.	Dokumen SOP Tanggap Darurat yang diperbarui secara berkala. Dokumentasi Tanggap Darurat dari insiden sebelumnya. Catatan monitoring dan reviu berkala atas prosedur penanganan insiden.
5	Organisasi menjalankan Prosedur penanganan terhadap perangkat yang terpengaruh oleh Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Prosedur penanganan telah terintegrasi dengan proses bisnis organisasi atau diotomatisasi. Proses monitoring dan reviu dilakukan secara berkala dan terdokumentasi.	Bukti integrasi prosedur dalam sistem bisnis organisasi atau sistem otomatisasi. Laporan monitoring dan reviu berkala yang menunjukkan perbaikan berkelanjutan. Sistem otomatisasi penanganan insiden yang terdokumentasi.

156 Kontrol 4.3.1.d:

Kontrol	Penyelenggara IIV mendokumentasikan hasil mitigasi Insiden Siber tersebut sebagai bahan pembelajaran berkelanjutan.
Deskripsi Kontrol	Organisasi harus mendokumentasikan hasil mitigasi insiden siber untuk digunakan sebagai bahan pembelajaran berkelanjutan. Dokumentasi ini berfungsi untuk mengidentifikasi langkah-langkah yang efektif dan area yang memerlukan perbaikan dalam proses respons insiden, serta untuk meningkatkan kesiapan organisasi dalam menangani insiden serupa dimasa depan. Tujuan dari kontrol ini adalah untuk memastikan bahwa setiap insiden siber yang terjadi dianalisis secara menyeluruh dan hasil mitigasinya terdokumentasi dengan baik, sebagai dasar untuk meningkatkan kebijakan, prosedur, dan pelatihan yang ada.
Deskripsi Bukti Dukung	Bukti Dukung dapat berupa: - Prosedur penanganan insiden - Laporan Hasil Penanganan Insiden - Daftar Insiden dan Penanganannya
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MI-01, RS.MI-02** **NIST CSF 1.1: RS.MI-1, RS.MI-2** **NIST SP 800-53r5: IR-4** **SNI ISO/IEC 27001:2022: 5.26, 8.7**

Kriteria Pemenuhan Kontrol 4.3.1.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber.	Tidak ada dokumentasi atau prosedur terkait mitigasi insiden siber.	Tidak ditemukan bukti dokumen terkait mitigasi insiden.
1	Organisasi telah melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Dokumentasi mitigasi insiden dilakukan tetapi masih sporadis dan tidak terstruktur.	Laporan hasil penanganan insiden dalam bentuk tidak terstandarisasi.
2	Organisasi telah melakukan melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Dokumentasi mitigasi insiden dilakukan lebih luas tetapi belum mencakup semua insiden. Prosedur belum diformalkan.	Laporan hasil penanganan insiden dalam format yang lebih konsisten, daftar insiden dan penanganannya mulai terdokumentasi.
3	Organisasi telah melakukan melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Semua insiden siber terdokumentasi secara sistematis. Terdapat prosedur resmi yang digunakan.	Prosedur penanganan insiden, daftar insiden dan penanganannya, laporan hasil penanganan insiden sesuai prosedur yang ditetapkan.
4	Organisasi telah menjalankan Prosedur melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Implementasi prosedur dokumentasi mitigasi insiden dilakukan penuh. Proses dimonitor dan direviu secara berkala untuk perbaikan.	Prosedur penanganan insiden yang diterapkan, laporan hasil penanganan insiden dengan catatan monitoring dan reviu berkala.
5	Organisasi menjalankan Prosedur melakukan tindakan pendokumentasian hasil mitigasi Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Dokumentasi mitigasi insiden telah terintegrasi dengan proses bisnis atau sistem otomatisasi. Proses dimonitor, direviu, dan diperbarui secara berkelanjutan.	Prosedur penanganan insiden yang terotomatisasi, sistem manajemen insiden terintegrasi, laporan hasil penanganan insiden dengan analisis tren dan perbaikan berkelanjutan.

4.3.2. Mengumpulkan dan memelihara bukti Insiden Siber dari IIV terdampak

Kriteria	Detail
Deskripsi	Penyelenggara IIV mengumpulkan dan memelihara bukti insiden siber dengan mengkategorikan serta menyimpan informasi insiden yang terdeteksi berdasarkan ukuran dampak keamanan, penyebab insiden, dan faktor relevan lainnya. Proses ini dilakukan secara sistematis untuk memastikan akurasi dan integritas data, sehingga mendukung analisis forensik, evaluasi risiko, serta perbaikan berkelanjutan terhadap sistem keamanan. Dengan dokumentasi yang lengkap dan terstruktur, organisasi dapat meningkatkan kemampuan respons serta memastikan kepatuhan terhadap regulasi dan standar yang berlaku.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk mengumpulkan, menyimpan, dan memelihara bukti secara aman.
Dampak	**Tinggi** – Dengan bukti yang lengkap dan terpelihara dengan baik, organisasi dapat melakukan investigasi yang efektif dan mengambil tindakan yang tepat berdasarkan bukti tersebut.
Kompleksitas	**Sedang** – Memerlukan prosedur yang terstruktur dan sistem penyimpanan yang aman untuk mengumpulkan serta memelihara bukti.
Referensi Kontrol	**NIST CSF 2.0: RS.MA-03** **NIST CSF 1.1: RS.AN-4** **NIST SP 800-53r5: CP-2, IR-4, IR-5, IR-8, RA-3** **SNI ISO/IEC 27001:2022: 5.25**

157 Kontrol 4.3.2.a:

Kontrol	Penyelenggara IIV memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan.
Deskripsi Kontrol	Organisasi harus memastikan bahwa informasi terkait insiden keamanan yang terdeteksi dikategorikan dan disimpan berdasarkan ukuran dampak,penyebab insiden, dan faktor lainnya yang relevan. Tujuan dari kontrol ini adalah untuk memastikan bahwa insiden keamanan yang terdeteksi dikelompokkan secara sistematis agar dapat dianalisis lebih lanjut untuk menemukan pola, menentukan prioritas, dan mengidentifikasi area yang membutuhkan perhatian khusus. Dengan cara ini, organisasi dapat merespons dengan cepat dan tepat dalam menangani insiden serupa di masa depan.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa daftar kategori insiden
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MA-03** **NIST CSF 1.1: RS.AN-4** **NIST SP 800-53r5: CP-2, IR-4, IR-5, IR-8, RA-3** **SNI ISO/IEC 27001:2022: 5.25**

Kriteria Pemenuhan Kontrol 4.3.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan.	Tidak ada kebijakan, prosedur, atau dokumentasi terkait kategorisasi dan penyimpanan insiden keamanan	Tidak ada dokumen atau bukti yang menunjukkan adanya proses kategorisasi dan penyimpanan insiden keamanan.
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Terdapat upaya awal dalam melakukan kategorisasi dan penyimpanan insiden, namun hanya terbatas pada beberapa kasus atau unit tertentu. Belum ada prosedur formal yang disusun.	Draft prosedur atau kebijakan awal. Dokumentasi insiden terbatas.
2	Organisasi telah melakukan langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Kategorisasi dan penyimpanan insiden telah diterapkan di sebagian besar unit atau sistem, tetapi masih belum memiliki prosedur yang ditetapkan secara resmi.	Dokumentasi insiden dengan kategori yang lebih luas. Bukti penerapan di beberapa unit. Laporan insiden yang mencantumkan kategori dan dampak.
3	Organisasi telah melakukan melakukan langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Kategorisasi dan penyimpanan insiden telah diterapkan di seluruh organisasi dengan prosedur yang terdokumentasi secara resmi.	Dokumen prosedur/kebijakan formal. Daftar kategori insiden yang digunakan secara organisasi. Laporan insiden yang terstruktur.
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Implementasi prosedur telah berjalan secara penuh, dilakukan pemantauan, serta adanya evaluasi dan perbaikan berkelanjutan.	Laporan monitoring insiden keamanan. Bukti reviu atau audit periodik. Hasil evaluasi dan perbaikan prosedur.
5	Organisasi menjalankan langkah atau prosedur untuk memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan, dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Prosedur telah menjadi bagian dari proses bisnis organisasi atau terotomatisasi dalam sistem manajemen keamanan siber. Pemantauan dan reviu dilakukan secara berkala dan sistematis.	Sistem otomatis untuk pencatatan dan kategorisasi insiden. Integrasi dengan sistem manajemen keamanan siber. Bukti keterkaitan dengan proses bisnis organisasi.

4.3.3. Menginvestigasi dan eradikasi penyebab Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV menerapkan forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk mengidentifikasi penyebab insiden serta mendukung proses investigasi dan audit. Setiap komponen aset informasi yang terdampak diperiksa secara menyeluruh guna memastikan penghapusan kode berbahaya atau indikasi ancaman lain yang terkait dengan Insiden Siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan tim investigasi dan alat forensik untuk melakukan analisis mendalam serta eradikasi ancaman.
Dampak	**Sangat Tinggi** – Dengan eradikasi yang efektif, organisasi dapat memastikan bahwa ancaman tidak akan muncul kembali, sehingga meningkatkan keamanan jangka panjang.
Kompleksitas	**Tinggi** – Memerlukan kemampuan analitis yang mendalam dan teknologi canggih untuk menginvestigasi serta mengeradikasi ancaman.
Referensi Kontrol	**NIST CSF 2.0: RS.MI-01, RS.MI-02, RS.AN-03, RS.AN-06** **NIST CSF 1.1: RS.MI-1, RS.MI-2, RS.AN-3** **NIST SP 800-53r5: AU-7, IR-4** **SNI ISO/IEC 27001:2022: 5.26, 5.28, 8.7**

158 Kontrol 4.3.3.a:

Kontrol	Untuk keperluan investigasi dan/atau audit, maka Penyelenggara IIV menerapkan forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden.
Deskripsi Kontrol	Organisasi harus menerapkan forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk tujuan investigasi dan audit.Proses ini bertujuan untuk mengidentifikasi penyebab dan dampak insiden, mengumpulkan bukti yang sah, serta mendukung proses pemulihan dan pembelajaran dari insiden tersebut. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi memiliki prosedur yang jelas dan efektif dalam melakukan forensik digital pada insiden keamanan untuk memperoleh pemahaman yang lebih mendalam mengenai penyebab insiden serta sebagai bukti yang sah jika diperlukan dalam proses audit atau penuntutan.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa hasil audit forensik ketika terjadi insiden.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.AN-03, RS.AN-06** **NIST CSF 1.1: RS.AN-3** **NIST SP 800-53r5: AU-7, IR-4** **SNI ISO/IEC 27001:2022: 5.28**

Kriteria Pemenuhan Kontrol 4.3.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit	Tidak ada kebijakan, prosedur, atau mekanisme terkait forensik digital.	Tidak ditemukan dokumen kebijakan atau prosedur forensik digital.
1	Organisasi telah melakukan langkah atau prosedur forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Ada upaya awal dalam melakukan forensik digital tetapi masih bersifat ad-hoc atau terbatas pada beberapa kasus. Belum ada prosedur tertulis yang baku.	Bukti investigasi forensik pada beberapa insiden sebelumnya. Dokumen awal terkait prosedur forensik digital, meskipun belum diformalkan.
2	Organisasi telah melakukan langkah atau prosedur untuk forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Forensik digital telah dilakukan pada sebagian besar insiden keamanan. Sudah ada draf prosedur, tetapi belum diresmikan atau diimplementasikan secara formal.	Laporan investigasi insiden dengan metode forensik digital pada sebagian besar kasus. Draf prosedur forensik digital yang sedang dalam proses pengesahan.
3	Organisasi telah melakukan langkah atau prosedur forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Prosedur forensik digital telah ditetapkan secara resmi. Setiap insiden keamanan ditangani dengan prosedur forensik yang telah ditentukan.	Dokumen kebijakan dan prosedur forensik digital yang telah disahkan. Laporan investigasi forensik yang dilakukan terhadap semua insiden keamanan.
4	Organisasi telah menjalankan langkah atau prosedur forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Prosedur forensik digital dijalankan sesuai dengan kebijakan yang ditetapkan. Forensik digital dilakukan pada semua insiden, dengan monitoring dan evaluasi berkala. Terdapat mekanisme pelaporan dan peningkatan prosedur berdasarkan hasil audit dan evaluasi.	Laporan hasil audit atau reviu berkala terhadap prosedur forensik digital. Bukti monitoring penerapan prosedur forensik digital. Dokumentasi peningkatan atau pembaruan prosedur berdasarkan evaluasi sebelumnya.
5	Organisasi menjalankan langkah atau prosedur forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden, untuk keperluan investigasi dan/atau audit secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Forensik digital telah menjadi bagian dari proses bisnis organisasi. Sistem otomatisasi forensik telah diterapkan untuk mendukung investigasi insiden. Pemantauan dan audit dilakukan secara real-time atau terjadwal, dengan umpan balik untuk perbaikan berkelanjutan.	Bukti integrasi prosedur forensik digital dalam sistem manajemen insiden organisasi. Penggunaan alat atau sistem otomatisasi dalam investigasi forensik. Laporan audit dan monitoring yang menunjukkan efektivitas sistem forensik digital.

159 Kontrol 4.3.3.b:

Kontrol	Penyelenggara IIV harus memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Siber
Deskripsi Kontrol	Organisasi harus memastikan bahwa seluruh aset informasi yang terdampak insiden siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait insiden siber. Hal ini penting untuk memastikan bahwa sistem yang terdampak tidak lagi mengandung ancaman yang dapat membahayakan keamanan data dan operasional organisasi. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang efektif dalam memeriksa dan membersihkan aset informasi yang terdampak dari ancaman yang tersisa setelah insiden siber terjadi.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - SOP Manajemen Insiden. - Daftar Checklist Pemeriksaan Kode berbahaya
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: RS.MI-01, RS.MI-02** **NIST CSF 1.1: RS.MI-1, RS.MI-2** **NIST SP 800-53r5: IR-4** **SNI ISO/IEC 27001:2022: 5.26, 8.7**

Kriteria Pemenuhan Kontrol 4.3.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Siber	Tidak ada prosedur atau langkah yang terdokumentasi terkait pemeriksaan aset informasi pasca insiden siber.	Tidak tersedia SOP Manajemen Insiden.
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi memiliki prosedur atau langkah awal terkait pemeriksaan aset informasi pasca insiden, tetapi masih bersifat ad-hoc atau belum terdokumentasi dengan baik.	Draft atau rancangan prosedur pemeriksaan aset pasca insiden.
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah memiliki prosedur atau langkah pemeriksaan yang lebih terstruktur namun belum terdokumentasi secara resmi. Implementasi pemeriksaan dilakukan pada sebagian besar aset yang terdampak insiden, tetapi belum menyeluruh.	Draft prosedur pemeriksaan aset pasca insiden. Laporan insiden yang mencatat pemeriksaan sebagian besar aset yang terdampak.
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Sibersecara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi memiliki SOP resmi terkait pemeriksaan aset pasca insiden siber. Implementasi pemeriksaan dilakukan pada seluruh aset yang terdampak.	SOP Manajemen Insiden yang telah disahkan. Laporan insiden yang mencatat pemeriksaan menyeluruh terhadap semua aset terdampak.
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait	SOP pemeriksaan aset pasca insiden telah diterapkan secara konsisten. Proses pemeriksaan dilakukan dengan pemantauan dan evaluasi berkala.	SOP Manajemen Insiden yang telah dijalankan dan diperbarui secara berkala. Laporan hasil monitoring dan evaluasi pemeriksaan aset pasca insiden.

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan		
5	Organisasi menjalankan langkah atau prosedur untuk memastikan bahwa seluruh aset informasi yang terdampak Insiden Siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait Insiden Siber secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Proses pemeriksaan aset pasca insiden telah terintegrasi dengan proses bisnis organisasi. Sistem otomatis digunakan untuk mendeteksi dan menghapus ancaman siber pada aset informasi. Reviu dan monitoring dilakukan secara terus-menerus dan hasilnya digunakan untuk peningkatan sistem keamanan.	SOP Manajemen Insiden yang telah terintegrasi dengan proses bisnis organisasi. Laporan otomatisasi pemeriksaan aset pasca insiden. Bukti implementasi sistem monitoring otomatis. Laporan evaluasi dan peningkatan prosedur berdasarkan hasil monitoring.

4.3.4. Mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV memastikan prosedur eskalasi Insiden Siber terlaksana secara efektif dengan menyiapkan dan menjalankan mekanisme pelaporan kepada Tim Tanggap Insiden Siber (TTIS) sektoral dan nasional saat insiden meningkat atau meluas. Dalam proses ini, Penyelenggara IIV mengoordinasikan langkah-langkah strategis dengan pihak terkait serta menyediakan informasi relevan untuk mempercepat respons dan mitigasi dampak insiden.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk koordinasi serta komunikasi dengan pihak terkait.
Dampak	**Tinggi** – Dengan koordinasi yang baik, organisasi dapat merespons insiden dengan cepat dan efektif, serta mengurangi dampak negatif dari insiden tersebut.
Kompleksitas	**Sedang** – Memerlukan prosedur koordinasi yang jelas dan sistem komunikasi yang efektif untuk mengoordinasikan penanggulangan insiden.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

160 Kontrol 4.3.4.a:

Kontrol	Jika insiden meningkat atau meluas, maka Penyelenggara IIV perlu menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut.
Deskripsi Kontrol	Jika insiden meningkat atau meluas, maka organisasi perlu menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut.Langkah ini penting untuk memastikan bahwa insiden yang dapat berdampak lebih luas mendapatkan perhatian yang cepat dan tepat, serta koordinasi dengan pihak yang lebih tinggi atau eksternal dilakukan dengan baik untuk mitigasi yang lebih efektif. Tujuan dari control ini adalah untuk menilai apakah organisasi memiliki prosedur eskalasi yang jelas dan efektif dalam menangani insiden yang semakin parah.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - SOP pelaporan Insiden. - SOP Manajemen Insiden (Hirarki pelaporan insiden ke TTIS)
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas	Tidak ada kebijakan, prosedur, atau dokumentasi yang mengatur eskalasi insiden siber.	Tidak terdapat dokumen terkait eskalasi insiden.
1	Organisasi telah melakukan langkah atau prosedur untuk menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Terdapat inisiatif awal dalam menyusun prosedur eskalasi insiden, tetapi belum diterapkan secara menyeluruh dan belum ada dokumen resmi.	Draft prosedur eskalasi insiden. Catatan diskusi atau rapat terkait eskalasi insiden.
2	Organisasi telah melakukan langkah atau prosedur untuk untuk menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Prosedur telah lebih berkembang dan mulai diterapkan di sebagian besar unit kerja, namun masih bersifat ad-hoc dan belum menjadi kebijakan resmi.	SOP eskalasi insiden dalam bentuk draft. Laporan penerapan prosedur di beberapa unit kerja.
3	Organisasi telah melakukan langkah atau prosedur untuk menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas, secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Prosedur eskalasi insiden telah diterapkan di seluruh organisasi dengan dokumen resmi yang mengatur pelaporan dan eskalasi insiden.	SOP pelaporan insiden yang telah disahkan. SOP Manajemen Insiden (hirarki pelaporan insiden ke TTIS).
4	Organisasi telah menjalankan langkah atau prosedur untuk menyiapkan dan melaksanakan prosedur	Prosedur telah diterapkan secara efektif, dengan mekanisme pemantauan dan	Laporan monitoring dan evaluasi prosedur eskalasi insiden. - Hasil audit kepatuhan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	evaluasi berkala untuk memastikan kepatuhan dan efektivitas.	terhadap SOP eskalasi insiden. Bukti pelaksanaan simulasi insiden siber.
5	Organisasi menjalankan langkah atau prosedur untuk menyiapkan dan melaksanakan prosedur eskalasi Insiden Siber, seperti melaporkan kepada tim tanggap Insiden Siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait Insiden Siber tersebut, jika insiden meningkat atau meluas secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Prosedur eskalasi insiden tidak hanya diterapkan dan dievaluasi secara berkala, tetapi juga telah terintegrasi dengan sistem manajemen insiden secara otomatis dan menjadi bagian dari strategi bisnis organisasi.	Sistem otomatisasi pelaporan dan eskalasi insiden (SIEM, SOAR). Dokumentasi integrasi eskalasi insiden dengan proses bisnis. Laporan hasil evaluasi dan perbaikan prosedur berbasis data otomatisasi.

4.3.5. Memastikan setiap aset informasi diperiksa keamanannya setelah penanganan Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV secara proaktif memeriksa seluruh aset informasi yang berhubungan dengan IIV setelah penanganan insiden siber untuk memastikan tidak ada indikasi ancaman atau sisa serangan yang dapat membahayakan sistem. Pemeriksaan ini mencakup identifikasi, analisis, dan verifikasi terhadap setiap komponen infrastruktur guna memastikan bahwa seluruh sistem dalam kondisi aman sebelum kembali beroperasi secara normal. Dengan langkah ini, Penyelenggara IIV memastikan kesinambungan layanan serta mencegah potensi eskalasi atau serangan berulang di masa mendatang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan pemeriksaan keamanan aset informasi secara menyeluruh.
Dampak	**Tinggi** – Dengan pemeriksaan yang komprehensif, organisasi dapat memastikan bahwa aset informasi aman dan terlindungi dari ancaman yang mungkin masih ada.
Kompleksitas	**Sedang** – Memerlukan prosedur pemeriksaan yang terstruktur dan alat yang tepat untuk memeriksa keamanan aset informasi.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

161 Kontrol 4.3.5.a:

Kontrol	Penyelenggara IIV melakukan pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi
Deskripsi Kontrol	Organisasi melakukan pemeriksaan seluruh aset informasi yang berhubungan dengan Layanan Sistem Elektronik (Infrastruktur Informasi Vital) untuk memastikan bahwa sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi. Pemeriksaan ini penting untuk memastikan bahwa semua sistem yang terkait dengan Layanan Sistem Elektronik tidak terpengaruh oleh ancaman atau serangan yang dapat merusak integritas, kerahasiaan, atau ketersediaan data dan layanan. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang memadai untuk memverifikasi bahwa seluruh aset yang terkait dengan Layanan Sistem Elektronik telah diperiksa dan dibersihkan dari ancaman atau serangan siber.
Deskripsi Bukti Dukung	Bukti dukung dapat berupa: - SOP Manajemen Insiden - Daftar Checklist Pemeriksaan Bersih dari indikasi ancaman
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.5.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi	Tidak ada kebijakan, prosedur, atau aktivitas terkait pemeriksaan aset informasi dari indikasi ancaman atau serangan.	Tidak ada dokumen atau bukti terkait aktivitas pemeriksaan keamanan aset informasi.
1	Organisasi telah melakukan langkah atau prosedur pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Langkah-langkah pemeriksaan telah dilakukan tetapi cakupannya masih terbatas. Belum ada prosedur resmi yang terdokumentasi.	Bukti pelaksanaan pemeriksaan (misalnya, log pemeriksaan aset dalam lingkup terbatas).
2	Organisasi telah melakukan langkah atau prosedur untuk pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Proses pemeriksaan sudah mencakup sebagian besar aset informasi. Masih belum ada prosedur formal yang terdokumentasi.	Bukti pelaksanaan pemeriksaan yang lebih luas (misalnya, laporan hasil pemeriksaan aset informasi).
3	Organisasi telah melakukan langkah atau prosedur pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi, secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Pemeriksaan telah dilakukan terhadap seluruh aset informasi. Prosedur pemeriksaan telah diformalkan dan terdokumentasi.	SOP Manajemen Insiden. Daftar checklist pemeriksaan bersih dari indikasi ancaman. Laporan hasil pemeriksaan aset informasi secara menyeluruh.
4	Organisasi telah menjalankan langkah atau prosedur pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi,secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Pemeriksaan aset informasi dilakukan secara menyeluruh sesuai prosedur. Monitoring dan reviu dilakukan secara berkala.	Log monitoring pemeriksaan aset. Laporan hasil reviu berkala. SOP Monitoring dan Reviu Pemeriksaan Keamanan.
5	Organisasi menjalankan langkah atau prosedur pemeriksaan seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi, secara menyeluruh sesuai dengan prosedur yang telah ditetapkan, dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Pemeriksaan dilakukan menyeluruh dan otomatis. Proses telah terintegrasi dalam bisnis organisasi. Monitoring dan reviu dilakukan secara otomatis dan berkelanjutan.	Log sistem otomatisasi pemeriksaan aset. Integrasi pemeriksaan dalam proses bisnis. Dashboard pemantauan keamanan aset informasi.

4.3.6. Melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan

Kriteria	Detail
Deskripsi	Penyelenggara IIV melakukan serangkaian tindakan yang sudah direncanakan untuk memastikan kelangsungan operasional sistem dan data organisasi jika terjadi insiden siber (seperti peretasan, serangan malware, atau kerusakan sistem).
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan investasi dalam teknologi pencadangan dan sumber daya untuk melakukan pemeliharaan serta pengujian secara berkala.
Dampak	**Tinggi** – Dengan prosedur pencadangan yang efektif, organisasi dapat mengurangi risiko kehilangan data dan memastikan bahwa data dapat dipulihkan dengan cepat dan lengkap jika terjadi insiden.
Kompleksitas	**Sedang** – Memerlukan sistem pencadangan yang tepat dan prosedur pengujian yang terstruktur untuk memastikan bahwa pencadangan data dilakukan dengan benar dan diuji secara berkala.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

162 Kontrol 4.3.6.a:

Kontrol	Penyelenggara IIV melaksanakan prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat.
Deskripsi Kontrol	Penyelenggara IIV melaksanakan prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat. Hal ini bertujuan untuk memastikan bahwa data dan sistem yang kritis dapat dipulihkan dengan cepat dan efisien jika terjadi insiden yang mengganggu operasional normal organisasi. Tujuan dari kontrol ini Adalah untuk menilai apakah penyelenggara IIV memiliki prosedur yang terstruktur dan teruji dalam melakukan pemulihan data dan sistem dari media penyimpanan selama situasi darurat, guna mengurangi dampak terhadap bisnis.
Deskripsi Bukti Dukung	Data dukung berupa prosedur pemulihan sistem/data yang telah disahkan oleh pimpinan organisasi dan dokumentasi bukti penerapan dari prosedur pemulihan sistem/data. Contohnya antara lain: - Dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat - Dokumentasi/laporan pelaksanaan pemulihan sistem/data dari media penyimpanan dalam keadaan darurat (jika pernah terjadi keadaan darurat) - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga)
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat.	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi mengimplementasikan sebagian kecil langkah pemulihan sistem/data dari media penyimpanan	- Rancangan dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat - Dokumen atau laporan bukti implementasi sebagian kecil langkah pemulihan sistem/data dari media penyimpanan. (Jika organisasi pernah dalam keadaa darurat) - Dokumen atau laporan bukti simulasi implementasi sebagian kecil langkah pemulihan sistem/data dari media penyimpanan. - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga)
2	Organisasi telah melakukan langkah atau prosedur untuk pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi mengimplementasikan sebagian besar langkah pemulihan sistem/data dari media penyimpanan	- Rancangan dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat - Dokumen atau laporan bukti implementasi sebagian besar langkah pemulihan sistem/data dari media penyimpanan. (Jika organisasi pernah dalam keadaa darurat) - Dokumen atau laporan bukti simulasi implementasi sebagian besar langkah pemulihan sistem/data dari media penyimpanan. - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga)
3	Organisasi telah melakukan langkah atau prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat. secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi mengimplementasikan seluruh langkah pemulihan sistem/data dari media penyimpanan berdasarkan prosedur yang telah diformalkan	- Dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat yang telah diformalkan - Dokumen atau laporan bukti implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. (Jika organisasi pernah dalam keadaa darurat) - Dokumen atau laporan bukti simulasi implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga)
4	Organisasi telah menjalankan langkah atau prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi	Organisasi mengimplementasikan seluruh langkah pemulihan sistem/data dari media	- Dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat yang telah diformalkan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	keadaan darurat.secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	penyimpanan berdasarkan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Dokumen atau laporan bukti implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. (Jika organisasi pernah dalam keadaa darurat) - Dokumen atau laporan bukti simulasi implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat. secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi mengimplementasikan seluruh langkah pemulihan sistem/data dari media penyimpanan berdasarkan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis atau dilakukan otomatisasi	- Dokumen prosedur pemulihan sistem/data dari media penyimpanan dalam keadaan darurat yang telah diformalkan - Dokumen atau laporan bukti implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. (Jika organisasi pernah dalam keadaa darurat) - Dokumen atau laporan bukti simulasi implementasi seluruh langkah pemulihan sistem/data dari media penyimpanan. - Dokumen kontraktual dengan penyedia layanan pemulihan sistem/data (jika dilimpahkan kepada pihak ketiga) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

163 Kontrol 4.3.6.b:

Kontrol	Penyelenggara IIV melaksanakan simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik.
Deskripsi Kontrol	Penyelenggara IIV melaksanakan simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik. Langkah ini penting untuk memastikan bahwa prosedur pemulihan yang telah ditetapkan dapat diterapkan dengan efektif dalam situasi nyata. Tujuan dari kontrol ini adalah untuk menilai apakah penyelenggara IIV secara rutin menguji kemampuan dan kesiapan prosedur pemulihan data melalui simulasi, yang dapat mencakup pengujian media cadangan untuk memastikan data dapat dipulihkan dengan benar tanpa adanya kerusakan.
Deskripsi Bukti Dukung	Data dukung berupa laporan simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik. Contohnya antara lain: - Jadwal simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Laporan hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi mengimplementasikan sebagian kecil langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan	- Dokumen atau laporan hasil pelaksanaan simulasi sebagian kecil langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang - Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang
2	Organisasi telah melakukan langkah atau prosedur untuk simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi mengimplementasikan sebagian besar langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan	- Dokumen atau laporan hasil pelaksanaan simulasi sebagian besar langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang - Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang
3	Organisasi telah melakukan langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodiksecara menyeluruh, serta sudah	Organisasi mengimplementasikan seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan berdasarkan prosedur simulasi yang telah diformalkan	- Jadwal simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen atau laporan hasil pelaksanaan simulasi seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	memiliki prosedur yang telah di formalkan		- Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik
4	Organisasi telah menjalankan langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodiksecara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi mengimplementasikan seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan berdasarkan prosedur simulasi yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Jadwal simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen atau laporan hasil pelaksanaan simulasi seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi mengimplementasikan seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan berdasarkan prosedur simulasi yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis atau dilakukan otomatisasi	- Jadwal simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen atau laporan hasil pelaksanaan simulasi seluruh langkah/prosedur simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen rekomendasi tindak lanjut dari hasil simulasi terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang secara periodik - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

164 Kontrol 4.3.6.c:

Kontrol	Prosedur rekam cadang (back-up) sedapat mungkin dilakukan secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling.
Deskripsi Kontrol	Prosedur rekam cadang (backup) harus dilakukan secara otomatis jika memungkinkan, untuk memastikan data yang penting tidak hilang atau rusak akibat kejadian tak terduga seperti insiden siber, kegagalan perangkat keras, atau bencana lainnya. Penggunaan perangkat penyimpanan yang memiliki fitur job-scheduling memungkinkan proses backup dilakukan secara terjadwal tanpa campur tangan manual, yang meningkatkan efisiensi dan keandalan. Tujuan dari kontrol ini adalah untuk memastikan bahwa penyelenggara IIV memiliki prosedur backup yang terotomatisasi, mengurangi risiko kehilangan data kritis dan meminimalkan kesalahan manusia.
Deskripsi Bukti Dukung	Data dukung berupa dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling. Contohnya antara lain: - Prosedur otomatisasi rekam cadang - Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan back-up secara otomatis dengan fitur jobscheduling, namun hanya diimplementasikan ke sebagian kecil data penting/kritis yang dimiliki organisasi	- Rancangan prosedur otomatisasi rekam cadang data penting/kritis yang dimiliki organisasi - Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling sebagian kecil data penting/kritis yang dimiliki organisasi - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling sebagian kecil data penting/kritis yang dimiliki organisasi
2	Organisasi telah melakukan langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan back-up secara otomatis dengan fitur job-scheduling, namun hanya diimplementasikan ke sebagian besar data penting/kritis yang dimiliki organisasi	- Rancangan prosedur otomatisasi rekam cadang data penting/kritis yang dimiliki organisasi - Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling sebagian besar data penting/kritis yang dimiliki organisasi - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling sebagian besar data penting/kritis yang dimiliki organisasi
3	Organisasi telah melakukan langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat	Organisasi telah melakukan back-up secara otomatis dengan fitur job-scheduling terhadap seluruh data penting/kritis yang dimiliki organisasi	- Prosedur otomatisasi rekam cadang data penting/kritis yang dimiliki organisasi yang sudah diformalkan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	penyimpanan yang mempunyai fitur job-schedulling secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	sesuai prosedur otomatisasi rekam cadang yang sudah diformalkan	- Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi
4	Organisasi telah menjalankan langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah melakukan back-up secara otomatis dengan fitur job-scheduling terhadap seluruh data penting/kritis yang dimiliki organisasi sesuai prosedur otomatisasi rekam cadang yang sudah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Prosedur otomatisasi rekam cadang data penting/kritis yang dimiliki organisasi yang sudah diformalkan - Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur rekam cadang (back-up) secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur job-schedulling secara menyeluruh sesuai dengan prosedur yang telah ditetapkan,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah melakukan back-up secara otomatis dengan fitur job-scheduling terhadap seluruh data penting/kritis yang dimiliki organisasi sesuai prosedur otomatisasi rekam cadang yang sudah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi	- Prosedur otomatisasi rekam cadang data penting/kritis yang dimiliki organisasi yang sudah diformalkan - Dokumentasi konfigurasi otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi - Dokumentasi hasil pelaksanaan otomatisasi prosedur rekam cadang yang mempunyai fitur job-scheduling seluruh data penting/kritis yang dimiliki organisasi - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi

165 Kontrol 4.3.6.d:

Kontrol	Penyelenggara IIV memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa data yang disimpan pada media penyimpanan rekam cadang (backup) diamankan menggunakan enkripsi untuk mencegah akses tidak sah, pencurian data, atau kebocoran informasi sensitif. Enkripsi pada data backup penting untuk menjaga kerahasiaan dan integritas data meskipun media penyimpanan fisik hilang atau dicuri. Tujuan dari kontrol ini adalah untuk memastikan bahwa data yang disalin ke media penyimpanan cadangan tetap terlindungi dari ancaman keamanan eksternal dan internal yang mungkin mengaksesnya tanpa izin.
Deskripsi Bukti Dukung	Data dukung berupa prosedur dan bukti penerapan enkripsi dalam media penyimpanan rekam cadang yang sesuai dengan standar dan praktik terbaik. Contohnya antara lain: - Kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang - Dokumentasi dan/atau bukti penerapan enkripsi pada media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi - Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi
Ancaman/Risiko yang dimitigasi	TH053 TH071 TH054
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.d Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah menerapkan enkripsi untuk mengamankan data yang disimpan pada media penyimpanan, namun hanya diimplementasikan ke sebagian kecil data yang dimiliki organisasi	- Draft kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang - Dokumentasi dan/atau bukti penerapan enkripsi pada sebagian kecil data yang disimpan di media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi - Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi
2	Organisasi telah melakukan langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah menerapkan enkripsi untuk mengamankan data yang disimpan pada media penyimpanan, namun hanya diimplementasikan ke sebagian kecil data yang dimiliki organisasi	- Draft kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang - Dokumentasi dan/atau bukti penerapan enkripsi pada sebagian besar data yang disimpan di media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi - Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah menerapkan enkripsi untuk mengamankan seluruh data yang disimpan pada media penyimpanan sesuai dengan kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan	- Kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan - Dokumentasi dan/atau bukti penerapan enkripsi pada sebagian besar data yang disimpan di media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah menerapkan enkripsi untuk mengamankan seluruh data yang disimpan pada media penyimpanan sesuai dengan kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan - Dokumentasi dan/atau bukti penerapan enkripsi pada sebagian besar data yang disimpan di media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi - Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur untuk memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi, secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah menerapkan enkripsi untuk mengamankan seluruh data yang disimpan pada media penyimpanan sesuai dengan kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Kebijakan dan/atau prosedur penerapan enkripsi pada media penyimpanan rekam cadang yang telah diformalkan - Dokumentasi dan/atau bukti penerapan enkripsi pada sebagian besar data yang disimpan di media penyimpanan rekam cadang - Dokumentasi dan/atau bukti bahwa penerapan enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai penerapan enkripsi - Dokumentasi dan/atau bukti pengelolaan kunci enkripsi pada media penyimpanan rekam cadang sesuai dengan standar dan/atau praktik terbaik mengenai pengelolaan kunci enkripsi - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

166 Kontrol 4.3.6.e:

Kontrol	Penyelenggara IIV menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi.
Deskripsi Kontrol	Penyelenggara IIV harus menentukan waktu pelaksanaan rekam cadang (backup) terhadap data dengan mempertimbangkan tingkat kritikalitas data dan kebutuhan operasional. Misalnya, data yang sangat kritikal dan sering berubah harus dibackup lebih sering dibandingkan data yang kurang penting. Tujuan dari kontrol ini adalah untuk memastikan bahwa data yang vital untuk kelangsungan operasional selalu tersedia dan dapat dipulihkan dengan cepat jika terjadi insiden yang mengganggu.
Deskripsi Bukti Dukung	Data dukung berupa jadwal pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi. Contohnya antara lain: - Daftar tingkat kritikalitas data organisasi - Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas data organisasi
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.e Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi, namun hanya diimplementasikan ke sebagian kecil data yang dimiliki organisasi	- Daftar tingkat kritikalitas sebagian kecil data organisasi - Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas sebagian kecil data organisasi
2	Organisasi telah melakukan langkah atau prosedur untuk menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi, namun baru diimplementasikan ke sebagian besar data yang dimiliki organisasi	- Daftar tingkat kritikalitas sebagian besar data organisasi - Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas sebagian besar data organisasi
3	Organisasi telah melakukan langkah atau prosedur menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah menentukan waktu pelaksanaan rekam cadang terhadap seluruh data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi dalam bentuk yang telah diformalkan	Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas seluruh data organisasi yang telah diformalkan
4	Organisasi telah menjalankan langkah atau prosedur menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah menentukan waktu pelaksanaan rekam cadang terhadap seluruh data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi dalam bentuk yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas seluruh data organisasi yang telah diformalkan - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi menjalankan langkah atau prosedur menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah menentukan waktu pelaksanaan rekam cadang terhadap seluruh data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi dalam bentuk yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Jadwal pelaksanaan rekam cadang berdasarkan daftar tingkat kritikalitas seluruh data organisasi yang telah diformalkan - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

167 Kontrol 4.3.6.f:

Kontrol	Penyelenggara IIV memastikan hasil pelaksanaan rekam cadang data didokumentasikan.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa setiap hasil pelaksanaan rekam cadang (backup) data didokumentasikan dengan baik. Dokumentasi ini mencakup rincian tentang data yang telah dibackup, waktu pelaksanaan, serta media penyimpanan yang digunakan. Tujuan dari kontrol ini adalah untuk memastikan bahwa semua proses backup tercatat dengan baik untuk keperluan audit, verifikasi, dan pemulihan data yang efisien di masa mendatang.
Deskripsi Bukti Dukung	Data dukung berupa dokumentasi hasil pelaksanaan rekam cadang data. Contohnya dokumentasi seluruh hasil pelaksanaan rekam cadang data yang dilakukan secara periodik sesuai ketentuan yang telah ditetapkan sebagai prosedur di organisasi
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.6.f Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan dokumentasi terhadap sebagian kecil hasil pelaksanaan rekam cadang data	- Draft prosedur dokumentasi hasil pelaksanaan rekam cadang data - Laporan/bukti dokumentasi terhadap sebagian kecil hasil pelaksanaan rekam cadang data
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan dokumentasi terhadap sebagian besar hasil pelaksanaan rekam cadang data	- Draft prosedur dokumentasi hasil pelaksanaan rekam cadang data - Laporan/bukti dokumentasi terhadap sebagian besar hasil pelaksanaan rekam cadang data
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah melakukan dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data sesuai dengan prosedur dokumentasi yang telah diformalkan	- Prosedur dokumentasi hasil pelaksanaan rekam cadang data yang telah diformalkan - Laporan/bukti dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah melakukan dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data sesuai dengan prosedur dokumentasi yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Prosedur dokumentasi hasil pelaksanaan rekam cadang data yang telah diformalkan - Laporan/bukti dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
5	Organisasi menjalankan langkah atau prosedur forensik digital terhadap untuk memastikan hasil pelaksanaan rekam cadang data didokumentasikan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah melakukan dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data sesuai dengan prosedur dokumentasi yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Prosedur dokumentasi hasil pelaksanaan rekam cadang data yang telah diformalkan - Laporan/bukti dokumentasi terhadap seluruh hasil pelaksanaan rekam cadang data - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

4.3.7. Menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan

Kriteria	Detail
Deskripsi	Penyelenggara IIV menetapkan dan menjalankan kebijakan mengenai berapa lama data cadangan (backup) disimpan, serta memastikan bahwa backup yang sudah tidak dibutuhkan lagi dihapus atau dimusnahkan dengan cara yang aman, sesuai dengan standar keamanan dan peraturan yang berlaku.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk mengelola dan menerapkan retensi data yang tepat, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan retensi yang jelas, organisasi dapat mengurangi risiko kebocoran data dan memastikan bahwa data yang tidak lagi diperlukan dimusnahkan dengan aman.
Kompleksitas	**Sedang** – Memerlukan kebijakan retensi yang jelas dan prosedur yang terstruktur untuk menerapkan retensi data secara efektif.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

168 Kontrol 4.3.7.a:

Kontrol	Penyelenggara IIV memastikan media penyimpanan rekam cadang telah disimpan secara aman.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa media penyimpanan rekam cadang (backup) disimpan dengan aman untuk mencegah kehilangan atau kerusakan data yang dapat mempengaruhi keberlanjutan operasi. Penyimpanan yang aman mencakup perlindungan fisik dan logis terhadap media penyimpanan, seperti enkripsi, kontrol akses fisik, dan pengawasan terhadap kondisi fisik media. Tujuan dari kontrol ini adalah untuk memastikan bahwa media penyimpanan backup dilindungi dari ancaman atau gangguan yang dapat merusak data yang disimpan.
Deskripsi Bukti Dukung	Data dukung berupa dokumen kebijakan dan/atau prosedur serta bukti pelaksanaan penyimpanan media rekam cadang secara aman. Contohnya antara lain: - Dokumen kebijakan dan/atau prosedur mengenai pengamanan media penyimpanan rekam cadang - Daftar rincian media penyimpanan rekam cadang yang digunakan yang memuat informasi mengenai nama, jenis, karakteristik, serta dimana tempat disimpannya media penyimpanan yang digunakan - Dokumen yang berisi keterangan mengenai apa saja kontrol yang diterapkan untuk memenuhi unsur keamanan dalam menyimpan media penyimpanan rekam cadang
Ancaman/Risiko yang dimitigasi	TH053 TH071 TH054
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.7.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan media penyimpanan rekam cadang telah disimpan secara aman	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan media penyimpanan rekam cadang telah disimpan secara aman, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah memastikan sebagian kecil media penyimpanan rekam cadang telah disimpan secara aman	- Draft prosedur pengamanan media penyimpanan rekam cadang - Dokumen/bukti pengamanan sebagian kecil media penyimpanan rekam cadang
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan media penyimpanan rekam cadang telah disimpan secara aman, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah memastikan sebagian besar media penyimpanan rekam cadang telah disimpan secara aman	- Draft prosedur pengamanan media penyimpanan rekam cadang - Dokumen/bukti pengamanan sebagian besar media penyimpanan rekam cadang
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan media penyimpanan rekam cadang telah disimpan secara amansecara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah memastikan seluruh media penyimpanan rekam cadang telah disimpan secara aman sesuai dengan prosedur yang telah diformalkan	- Prosedur pengamanan media penyimpanan rekam cadang yang telah diformalkan - Dokumen/bukti pengamanan seluruh media penyimpanan rekam cadang
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan media penyimpanan rekam cadang telah disimpan secara aman secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah memastikan seluruh media penyimpanan rekam cadang telah disimpan secara aman sesuai dengan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Prosedur pengamanan media penyimpanan rekam cadang yang telah diformalkan - Dokumen/bukti pengamanan seluruh media penyimpanan rekam cadang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur untuk memastikan media penyimpanan rekam cadang telah disimpan secara aman secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah memastikan seluruh media penyimpanan rekam cadang telah disimpan secara aman sesuai dengan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Prosedur pengamanan media penyimpanan rekam cadang yang telah diformalkan - Dokumen/bukti pengamanan seluruh media penyimpanan rekam cadang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

169 Kontrol 4.3.7.b:

Kontrol	Pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi.
Deskripsi Kontrol	Pemusnahan data pada media rekam cadang harus dilakukan dengan persetujuan pimpinan penyelenggara IIV untuk memastikan proses tersebut dilakukan secara sah, terkendali, dan sesuai dengan kebijakan yang berlaku. Hal ini penting untuk menghindari penghapusan data yang masih memiliki nilai operasional, hukum, atau bisnis, serta memastikan bahwa tindakan pemusnahan dilakukan dengan metode yang aman dan sesuai standar keamanan. Tujuan dari kontrol ini adalah untuk memastikan bahwa proses pemusnahan data melibatkan otorisasi yang jelas, meminimalkan risiko kehilangan data penting, dan menjaga kepatuhan terhadap regulasi atau kebijakan penyelenggara IIV.
Deskripsi Bukti Dukung	Data dukung berupa dokumen kebijakan dan/atau prosedur yang mensyaratkan bahwa pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi. Contohnya antara lain: - Dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang - Dokumen atau bukti persetujuan pimpinan dalam proses pemusnahan data yang disimpan pada media rekam cadang
Ancaman/Risiko yang dimitigasi	TH053 TH054
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.7.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah memastikan pemusnahan terhadap sebagian kecil data yang disimpan pada media rekam cadang dilaksanakan dengan persetujuan pimpinan organisasi	- Draft dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang - Dokumen atau bukti persetujuan dari pimpinan organisasi terhadap pemusnahan sebagian kecil data yang disimpan pada media rekam cadang
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah memastikan pemusnahan terhadap sebagian besar data yang disimpan pada media rekam cadang dilaksanakan dengan persetujuan pimpinan organisasi	- Draft dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang - Dokumen atau bukti persetujuan dari pimpinan organisasi terhadap pemusnahan sebagian besar data yang disimpan pada media rekam cadang
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah memastikan pemusnahan terhadap seluruh data yang disimpan pada media rekam cadang dilaksanakan dengan persetujuan pimpinan organisasi sesuai dengan kebijakan dan/atau prosedur yang telah diformalkan	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang yang telah diformalkan - Dokumen atau bukti persetujuan dari pimpinan organisasi terhadap pemusnahan seluruh data yang disimpan pada media rekam cadang
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi secara menyeluruh sesuai dengan prosedur yang telah	Organisasi telah memastikan pemusnahan terhadap seluruh data yang disimpan pada media rekam cadang dilaksanakan dengan persetujuan pimpinan organisasi sesuai dengan kebijakan dan/atau prosedur yang telah	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang yang telah diformalkan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Dokumen atau bukti persetujuan dari pimpinan organisasi terhadap pemusnahan seluruh data yang disimpan pada media rekam cadang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur untuk memastikan pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah memastikan pemusnahan terhadap seluruh data yang disimpan pada media rekam cadang dilaksanakan dengan persetujuan pimpinan organisasi sesuai dengan kebijakan dan/atau prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan persetujuan pimpinan organisasi dalam proses pemusnahan data yang disimpan pada media rekam cadang yang telah diformalkan - Dokumen atau bukti persetujuan dari pimpinan organisasi terhadap pemusnahan seluruh data yang disimpan pada media rekam cadang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

170 Kontrol 4.3.7.c:

Kontrol	Pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi.
Deskripsi Kontrol	Pemusnahan data pada media rekam cadang dengan metode format ulang dan memastikan data tidak dapat diakses lagi bertujuan untuk menghilangkan jejak data dari media penyimpanan. Hal ini dilakukan untuk melindungi kerahasiaan dan integritas data, terutama yang bersifat sensitif atau kritis. Format ulang media penyimpanan harus dilengkapi dengan langkah-langkah tambahan, seperti penghapusan data secara menyeluruh (secure erase) atau penggunaan perangkat lunak khusus untuk memastikan data tidak dapat dipulihkan. Tujuan dari kontrol ini adalah untuk memastikan data yang tidak lagi diperlukan benar-benar dihapus secara aman untuk mencegah penyalahgunaan atau kebocoran data.
Deskripsi Bukti Dukung	Data dukung berupa dokumen kebijakan dan/atau prosedur yang mensyaratkan bahwa pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi. Contohnya antara lain: - Dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data - Dokumen bukti atau sejenis berita acara pemusnahan data yang dilakukan dengan mekanisme format ulang terhadap media penyimpanan data
Ancaman/Risiko yang dimitigasi	TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.7.c Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi.	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan pemusnahan sebagian kecil data pada media rekam cadang dengan metode format ulang	- Draft dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data - Dokumen bukti atau sejenis berita acara pemusnahan sebagian kecil data pada media rekam cadang dengan metode format ulang
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan pemusnahan sebagian besar data pada media rekam cadang dengan metode format ulang	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data yang telah diformalkan - Dokumen bukti atau sejenis berita acara pemusnahan seluruh data pada media rekam cadang dengan metode format ulang
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi. secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah melakukan pemusnahan seluruh data pada media rekam cadang dengan metode format ulang sesuai dengan kebijakan dan/atau prosedur yang telah diformalkan	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data yang telah diformalkan - Dokumen bukti atau sejenis berita acara pemusnahan seluruh data pada media rekam cadang dengan metode format ulang
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi.t secara menyeluruh sesuai dengan prosedur yang telah	Organisasi telah melakukan pemusnahan seluruh data pada media rekam cadang dengan metode format ulang sesuai dengan kebijakan dan/atau prosedur yang telah diformalkan. Di samping itu juga melakukan	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data yang telah diformalkan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Dokumen bukti atau sejenis berita acara pemusnahan seluruh data pada media rekam cadang dengan metode format ulang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur untuk memastikan pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi. secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah melakukan pemusnahan seluruh data pada media rekam cadang dengan metode format ulang sesuai dengan kebijakan dan/atau prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Dokumen kebijakan dan/atau prosedur yang mensyaratkan harus dilakukannya format ulang atas media rekam cadang ketika pemusnahan data yang telah diformalkan - Dokumen bukti atau sejenis berita acara pemusnahan seluruh data pada media rekam cadang dengan metode format ulang - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

4.3.8. Pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi

Kriteria	Detail
Deskripsi	Penyelenggara IIV memeriksa dan/atau melakukan verifikasi ulang terhadap sistem, layanan, atau proses yang sebelumnya terdampak insiden siber, untuk memastikan bahwa semuanya sudah dipulihkan dengan benar, sudah kembali berfungsi seperti semula, dan tidak ada kerusakan tersembunyi atau celah keamanan yang tersisa.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk melakukan pengujian ulang secara menyeluruh terhadap semua fungsi vital dan pendukung.
Dampak	**Tinggi** – Dengan pengujian ulang yang menyeluruh, organisasi dapat memastikan bahwa semua sistem kembali berfungsi normal dan tidak ada kerentanan yang tersisa setelah pemulihan.
Kompleksitas	**Sedang** – Memerlukan prosedur pengujian yang terstruktur dan alat yang tepat untuk memastikan bahwa semua fungsi diuji secara efektif.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

171 Kontrol 4.3.8.a:

Kontrol	Penyelenggara IIV harus menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber
Deskripsi Kontrol	Penyelenggara IIV harus menyusun dan menerapkan prosedur untuk memastikan seluruh fungsi layanan IIV kembali beroperasi normal setelah Insiden Siber. Prosedur ini bertujuan untuk memastikan proses pemulihan dilakukan secara terencana, terstruktur, dan efisien guna meminimalkan dampak operasional dan bisnis. Selain itu, hal ini penting untuk mengidentifikasi dan menyelesaikan masalah yang mungkin timbul pasca-insiden, memastikan kelangsungan layanan, serta menjaga kepercayaan pemangku kepentingan
Deskripsi Bukti Dukung	Dokumen data dukung dapat berupa: - Dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber - Dokumentasi/bukti yang menunjukkan bahwa seluruh fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber)
Ancaman/Risiko yang dimitigasi	TH050 TH054 TH071 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.8.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum di formalkan	Organisasi telah menerapkan prosedur pemeriksaan ulang terhadap sebagian kecil fungsi pada layanan IIV (Jika pernah terjadi Insiden Siber)	- Draft dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber - Dokumentasi/bukti yang menunjukkan bahwa sebagian kecil fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber)
2	Organisasi telah menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum di formalkan	Organisasi telah menerapkan prosedur pemeriksaan ulang terhadap sebagian besar fungsi pada layanan IIV (Jika pernah terjadi Insiden Siber)	- Draft dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber - Dokumentasi/bukti yang menunjukkan bahwa sebagian besar fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber)
3	Organisasi telah menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber secara menyeluruh, serta telah di formalkan	Organisasi telah melakukan pemeriksaan ulang terhadap seluruh fungsi pada layanan IIV (Jika pernah terjadi Insiden Siber) sesuai dengan prosedur yang telah diformalka	- Dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber yang telah diformalkan - Dokumentasi/bukti yang menunjukkan bahwa seluruh fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber)
4	Organisasi telah menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber secara menyeluruh, telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah melakukan pemeriksaan ulang terhadap seluruh fungsi pada layanan IIV (Jika pernah terjadi Insiden Siber) sesuai dengan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi (Jika pernah terjadi Insiden Siber) dan kebijakan secara berkelanjutan	- Dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber yang telah diformalkan - Dokumentasi/bukti yang menunjukkan bahwa seluruh fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi (Jika pernah terjadi Insiden Siber) dan kebijakan secara

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca Insiden Siber, telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi	Organisasi telah melakukan pemeriksaan ulang terhadap seluruh fungsi pada layanan IIV (Jika pernah terjadi Insiden Siber) sesuai dengan prosedur yang telah diformalkan. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi (Jika pernah terjadi Insiden Siber) dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Dokumen prosedur pemeriksaan seluruh fungsi layanan IIV pasca terjadi Insiden Siber yang telah diformalkan - Dokumentasi/bukti yang menunjukkan bahwa seluruh fungsi layanan IIV sudah kembali beroperasi normal setelah Insiden Siber (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi (Jika pernah terjadi Insiden Siber) dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

4.3.9. Memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber

Kriteria	Detail
Deskripsi	Penyelenggara IIV memiliki upaya sistematis untuk menyiapkan, melaksanakan, dan mengevaluasi cara berkomunikasi secara terbuka, tepat waktu, dan bertanggung jawab kepada publik dan pemangku kepentingan selama dan setelah terjadinya insiden siber, guna menjaga kepercayaan, reputasi, serta mematuhi regulasi
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan waktu dan sumber daya untuk menyusun serta mengimplementasikan strategi komunikasi publik, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan strategi komunikasi yang efektif, organisasi dapat menjaga kepercayaan publik dan meminimalkan dampak reputasional dari insiden siber.
Kompleksitas	**Sedang** – Memerlukan kebijakan komunikasi yang jelas dan prosedur untuk mengelola informasi publik dengan efektif.
Referensi Kontrol	**NIST CSF 2.0: RC.CO-03, RC.CO-04** **NIST CSF 1.1: RC.CO-1, RC.CO-2, RC.CO-3** **NIST SP 800-53r5: IR-4, CP-2** **SNI ISO/IEC 27001:2022: -**

172 Kontrol 4.3.9.a:

Kontrol	Penyelenggara IIV perlu menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber.
Deskripsi Kontrol	Penyelenggara IIV perlu menyusun dan menerapkan strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan terkait Insiden Siber. Strategi ini bertujuan untuk memastikan bahwa komunikasi dilakukan secara transparan, akurat, dan terkoordinasi, sehingga dapat menjaga kepercayaan publik, meminimalkan dampak reputasi, serta memastikan bahwa informasi yang disampaikan tidak memperburuk situasi atau membuka celah lebih lanjut bagi ancaman keamanan.
Deskripsi Bukti Dukung	Dokumen data dukung dapat berupa: - Dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber - Dokumentasi/laporan simulasi penerapan strategi komunikasi terkait insiden siber yang diikuti oleh seluruh pihak terkait sesuai peran masing-masing - Dokumentasi atau laporan penerapan strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber)Siber (Jika pernah terjadi Insiden Siber)
Ancaman/Risiko yang dimitigasi	TH053 TH065 TH077 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: RC.CO-03, RC.CO-04** **NIST CSF 1.1: RC.CO-1, RC.CO-2, RC.CO-3** **NIST SP 800-53r5: IR-4, CP-2** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.9.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber.	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum di formalkan	Organisasi telah melakukan simulasi penerapan strategi komunikasi terkait insiden siber untuk menerapkan sebagian kecil strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber	- Draft dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber - Dokumentasi atau laporan simulasi penerapan sebagian kecil strategi komunikasi yang telah dilakukan - Dokumentasi atau laporan penerapan sebagian kecil strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber)
2	Organisasi telah menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum di formalkan	Organisasi telah melakukan simulasi penerapan strategi komunikasi terkait insiden siber untuk menerapkan sebagian besar strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber	- Draft dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber - Dokumentasi atau laporan simulasi penerapan sebagian besar strategi komunikasi yang telah dilakukan - Dokumentasi atau laporan penerapan sebagian besar strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber)
3	Organisasi telah menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber secara menyeluruh, serta telah di formalkan	Organisasi telah melakukan simulasi penerapan strategi komunikasi terkait insiden siber untuk menerapkan seluruh strategi komunikasi publik yang telah diformalkan dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber	- Dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber yang telah diformalkan - Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi yang telah dilakukan - Dokumentasi atau laporan penerapan seluruh strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber)
4	Organisasi telah menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu	Organisasi telah melakukan simulasi penerapan strategi komunikasi terkait insiden siber untuk menerapkan sebagian	- Dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber yang telah diformalkan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	disampaikan terkait Insiden Siber secara menyeluruh, telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	besar strategi komunikasi publik yang telah diformalkan dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi yang telah dilakukan - Dokumentasi atau laporan penerapan seluruh strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber, telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi	Organisasi telah melakukan simulasi penerapan strategi komunikasi terkait insiden siber untuk menerapkan sebagian besar strategi komunikasi publik yang telah diformalkan dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Dokumen strategi komunikasi publik untuk mengelola informasi yang perlu disampaikan baik selama maupun setelah terjadi Insiden Siber yang telah diformalkan - Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi yang telah dilakukan - Dokumentasi atau laporan penerapan seluruh strategi komunikasi yang telah dilakukan berdasarkan dokumen strategi komunikasi yang telah disusun (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi - Sudah dilakukan Integrasi ke proses bisnis organisasi atau dilakukan otomatisasi (Jika memungkinkan)

173 Kontrol 4.3.9.b:

Kontrol	Penyelenggara IIV memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan.
Deskripsi Kontrol	Penyelenggara IIV harus memastikan bahwa proses penanganan dan pemulihan insiden siber dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundang-undangan yang berlaku. Hal ini penting untuk menjaga transparansi, memastikan kepatuhan terhadap regulasi yang berlaku, dan memberikan informasi yang tepat waktu kepada pemangku kepentingan yang relevan, seperti pihak berwenang, mitra bisnis, pelanggan, atau pihak ketiga terkait. Tujuan dari kontrol ini adalah untuk mengevaluasi sejauh mana penyelenggara IIV mengelola komunikasi yang berkaitan dengan penanganan dan pemulihan insiden siber, serta memastikannya sesuai dengan kewajiban hukum dan peraturan yang berlaku.
Deskripsi Bukti Dukung	Dokumen data dukung dapat berupa: - Dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumentasi atau laporan yang membuktikan bahwa proses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan pihak yang berkepentingan (Jika pernah terjadi Insiden Siber)
Ancaman/Risiko yang dimitigasi	TH053 TH065 TH077 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: RC.CO-03, RC.CO-04** **NIST CSF 1.1: RC.CO-1, RC.CO-2, RC.CO-3** **NIST SP 800-53r5: IR-4, CP-2** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.9.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum memiliki langkah atau prosedur untuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan	Tidak ada kriteria	Tidak ada bukti dukung
1	Organisasi telah melakukan langkah atau prosedur untuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan, namun belum diimplementasikan secara menyeluruh (sebagian kecil), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan sebagian kecil langkah untuk mengomunikasikan insiden siber kepada pihak yang berkepentingan sesuai peraturan perundangan dan/atau ruang lingkup yang telah disepakati	- Draft dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan sebagian kecil strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumentasi atau laporan yang membuktikan bahwa proses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan sebagian kecil pihak yang berkepentingan (Jika pernah terjadi Insiden Siber)
2	Organisasi telah melakukan langkah atau prosedur untuk untuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan, namun belum diimplementasikan secara menyeluruh (sebagian besar), serta belum memiliki prosedur yang telah di formalkan	Organisasi telah melakukan sebagian besar langkah untuk mengomunikasikan insiden siber kepada pihak yang berkepentingan sesuai peraturan perundangan dan/atau ruang lingkup yang telah disepakati	- Draft dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan sebagian besar strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan (Jika pernah terjadi Insiden Siber) - Dokumentasi atau laporan yang membuktikan bahwa proses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan sebagian besar pihak yang berkepentingan (Jika pernah terjadi Insiden Siber)
3	Organisasi telah melakukan langkah atau prosedur untuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan secara menyeluruh, serta sudah memiliki prosedur yang telah di formalkan	Organisasi telah melakukan seluruh langkah untuk mengomunikasikan insiden siber kepada pihak yang berkepentingan sesuai dokumen strategi komunikasi yang telah diformalkan serta peraturan perundangan dan/atau ruang lingkup yang telah disepakati	- Dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan yang telah diformalkan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
			- Dokumentasi atau laporan yang membuktikan bahwaproses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan seluruh pihak yang berkepentingan (Jika pernah terjadi Insiden Siber)
4	Organisasi telah menjalankan langkah atau prosedur untuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan	Organisasi telah melakukan seluruh langkah untuk mengomunikasikan insiden siber kepada pihak yang berkepentingan sesuai dokumen strategi komunikasi yang telah diformalkan serta peraturan perundangan dan/atau ruang lingkup yang telah disepakati. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan	- Dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan yang telah diformalkan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumentasi atau laporan yang membuktikan bahwa proses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan seluruh pihak yang berkepentingan (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi
5	Organisasi menjalankan langkah atau prosedur funtuk memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan secara menyeluruh sesuai dengan prosedur yang telah ditetapkan ,dimonitor dan dilakukan reviu secara berkelanjutan, serta telah terintegrasi dengan proses bisnis Organisasi atau dalam sistem terotomatisasi	Organisasi telah melakukan seluruh langkah untuk mengomunikasikan insiden siber kepada pihak yang berkepentingan sesuai dokumen strategi komunikasi yang telah diformalkan serta peraturan perundangan dan/atau ruang lingkup yang telah disepakati. Di samping itu juga melakukan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan. Dari hasil monitoring dan reviu mungkin saja menghasilkan peningkatan seperti integrasi ke proses bisnis organisasi atau dilakukan otomatisasi	- Dokumen strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan yang telah diformalkan - Dokumen daftar pihak yang berkepentingan beserta ruang lingkup kepentingannya terhadap proses penanganan dan pemulihan Insiden Siber - Dokumentasi atau laporan simulasi penerapan seluruh strategi komunikasi penanganan dan pemulihan Insiden Siber dengan pihak yang berkepentingan sesuai dengan peraturan perundangan - Dokumentasi atau laporan yang membuktikan bahwa proses penanganan dan pemulihan Insiden Siber sudah dikomunikasikan dengan seluruh pihak yang berkepentingan (Jika pernah terjadi Insiden Siber) - Dokumen atau laporan monitoring dan reviu terhadap implementasi dan kebijakan secara berkelanjutan sesuai dengan kebijakan organisasi

4.3.10. Penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait

Kriteria	Detail
Deskripsi	Penyelenggara IIV menyampaikan data, laporan, atau pemberitahuan mengenai suatu insiden siber (seperti serangan siber, kebocoran data, atau gangguan sistem) kepada semua pihak yang memiliki peran atau kepentingan dalam menangani insiden tersebut. Hal ini merupakan bagian penting dari manajemen insiden siber untuk memastikan respon yang cepat, efektif, dan terkoordinasi. Tujuannya dari penyampaian informasi ini yaitu menginformasikan pihak terkait bahwa insiden telah terjadi, melakukan koordinasi dalam proses penanggulangan dan pemulihan, mengurangi dampak insiden melalui tindakan cepat dari berbagai pihak, dan memenuhi kewajiban hukum atau regulasi, jika pelaporan insiden diwajibkan
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sistem pelaporan yang efektif dan sumber daya untuk melakukan pelaporan secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan pelaporan yang efektif, organisasi dapat memastikan bahwa respons terhadap insiden dilakukan dengan cepat dan tepat oleh pihak yang berwenang.
Kompleksitas	**Sedang** – Memerlukan sistem pelaporan yang tepat dan prosedur untuk menyampaikan informasi penanggulangan dan pemulihan secara efektif.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

174 Kontrol 4.3.10.a:

Kontrol	Penyelenggara IIV menyusun laporan hasil penanganan Insiden Siber dan menyampaikannya kepada Kementerian atau Lembaga di masing-masing sektor.
Deskripsi Kontrol	Penyelenggara IIV harus menyusun laporan hasil penanganan Insiden Siber untuk mendokumentasikan tindakan yang telah diambil, hasil yang dicapai, dan evaluasi dari insiden tersebut. Laporan ini bertujuan untuk memberikan pemahaman yang jelas mengenai respons insiden, serta langkah-langkah mitigasi dan pemulihan yang telah diterapkan. Selain itu, laporan ini perlu disampaikan kepada Kementerian atau Lembaga di masing- masing sektor untuk memenuhi kewajiban pelaporan yang diatur oleh peraturan atau untuk mendukung koordinasi lebih lanjut dalam menanggapi ancaman atau insiden serupa di masa depan.
Deskripsi Bukti Dukung	Dokumen data dukung dapat berupa: - Dokumen atau laporan hasil penanganan Insiden Siber (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber) - Dokumen evaluasi pasca terjadinya insiden siber berisi pembelajaran yang dapat diambil dari terjadinya insiden serta hal apa saja yang harus dilakukan setelahnya sebagai upaya pencegahan agar tidak terjadi insiden serupa (Jika pernah terjadi insiden siber)
Ancaman/Risiko yang dimitigasi	TH053 TH065 TH077 TH054 TH071
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.3.10.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum pernah menyusun laporan hasil penanganan Insiden Siber	Tidak ada kriteria	Tidak ada bukti dukung
1	- Organisasi telah menyusun draft laporan hasil penanganan Insiden Siber - isi draft laporan belum mencakup 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi.	Organisasi telah menyusun draft laporan hasil penanganan insiden namun belum mencakup 4 kriteria yaitu jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, dan rekomendasi mitigasi	- Draft laporan hasil penanganan insiden siber namun belum mencakup 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber)
2	- Organisasi telah menyusun draft laporan hasil penanganan Insiden Siber - isi draft laporan belum komprehensif namun sudah mencakup minimal salah satu dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi.	Organisasi telah menyusun draft laporan hasil penanganan insiden namun sudah mencakup minimal salah satu dari 4 kriteria yaitu jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, dan rekomendasi mitigasi	- Draft laporan hasil penanganan insiden siber namun sudah mencakup salah satu dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber)
3	- Organisasi sudah menyusun laporan hasil penanganan Insiden Siber dan telah disahkan oleh pimpinan Organisasi - isi laporan belum komprehensif namun sudah mencakup minimal 2 dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi. - Laporan hasil penanganan Insiden Siber sudah disampaikan kepada Kementerian atau Lembaga di masing-masing sektor	Organisasi telah menyusun laporan hasil penanganan insiden yang telah disahkan namun sudah mencakup minimal 2 dari 4 kriteria yaitu jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, dan rekomendasi mitigasi	- Laporan hasil penanganan insiden siber yang sudah disahkan namun sudah mencakup minimal 2 dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber)
4	- Organisasi sudah menyusun laporan hasil penanganan Insiden Siber dan telah disahkan oleh pimpinan Organisasi	Organisasi telah menyusun laporan hasil penanganan insiden yang telah disahkan namun sudah mencakup	- Laporan hasil penanganan insiden siber yang sudah disahkan namun sudah mencakup minimal 3 dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- isi laporan belum komprehensif namun sudah mencakup minimal 3 dari 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi. - Laporan hasil penanganan Insiden Siber sudah disampaikan kepada Kementerian atau Lembaga di masing-masing sektor	minimal 3 dari 4 kriteria yaitu jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, dan rekomendasi mitigasi	distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber)
5	- Organisasi sudah menyusun laporan hasil penanganan Insiden Siber dan telah disahkan oleh pimpinan Organisasi - isi laporan telah komprehensif mencakup minimal 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi. - Laporan hasil penanganan Insiden Siber sudah disampaikan kepada Kementerian atau Lembaga di masing-masing sektor	Organisasi telah menyusun laporan hasil penanganan insiden yang telah disahkan namun sudah mencakup minimal 4 kriteria yaitu jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, dan rekomendasi mitigasi	- Laporan hasil penanganan insiden siber yang sudah disahkan namun sudah mencakup minimal 4 kriteria antara lain: jenis indikasi Insiden Siber, kode distribusi informasi, sistem dan/atau aset terdampak, rekomendasi mitigasi (Jika pernah terjadi insiden siber) - Bukti penyampaian laporan insiden siber kepada pihak berwenang sesuai kewajiban berdasarkan peraturan perundangan (Jika pernah terjadi insiden siber)

4.4. Meningkatkan keamanan setelah terjadinya Insiden Siber

Setelah terjadinya insiden siber, peningkatan keamanan menjadi langkah krusial untuk mencegah kejadian serupa di masa depan. Langkah ini mencakup peninjauan ulang terhadap efektivitas kontrol keamanan yang telah diterapkan, guna memastikan bahwa perlindungan yang ada mampu menghadapi ancaman yang terus berkembang. Selain itu, organisasi perlu secara berkala mereviu dan memperbarui dokumen rencana tanggap insiden siber serta rencana keberlangsungan kegiatan, agar tetap relevan dan responsif terhadap kondisi terkini. Pengumpulan dan pemeliharaan hasil forensik digital juga menjadi bagian penting, sebagai dasar analisis dan pembelajaran dari insiden yang terjadi. Tak kalah penting, efektivitas kinerja tim tanggap insiden siber harus dievaluasi secara rutin, untuk memastikan kesiapan dan respons yang optimal dalam menghadapi potensi ancaman di masa mendatang.

Kategori ini terdiri atas sub kategori kegiatan, antara lain:

a) meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan;
b) mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala;
c) mengumpulkan dan memelihara bukti hasil forensik digital; dan
d) meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala.

Kontrol-kontrol yang dapat dijadikan acuan/referensi untuk menerapkan Kategori Kegiatan “Meningkatkan keamanan setelah terjadinya Insiden Siber” secara efektif antara lain:

NIST CSF 2.0	**:**	**ID.IM-03, ID.IM-04, ID.RA-06**
NIST CSF 1.1	**:**	**RS.IM-1, RS.IM-2, RS.MI-3, RC.IM-1, RC.IM-2**
NIST SP 800-53r5	**:**	**CA-2, CA-7, CP-2, IR-4, IR-8, RA-3, RA-5, RA-7**
SNI ISO/IEC 27001:2022	**:**	**5.27, 8.8**

4.4.1. Meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan

Kriteria	Detail
Deskripsi	Meninjau kembali efektivitas kontrol keamanan yang telah diterapkan merupakan langkah penting untuk memastikan bahwa mekanisme perlindungan tetap relevan terhadap dinamika ancaman siber yang terus berkembang. Penyelenggara IIV perlu secara berkala mengevaluasi apakah kontrol yang ada masih memadai dalam menghadapi spektrum ancaman terkini, sekaligus mengidentifikasi area yang membutuhkan perbaikan maupun penambahan kontrol baru. Proses ini tidak hanya menjaga keberlanjutan keamanan, tetapi juga memastikan bahwa organisasi selalu adaptif dan responsif terhadap perubahan risiko yang dapat memengaruhi kelancaran operasional maupun perlindungan aset informasi.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan peninjauan secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan peninjauan yang rutin, organisasi dapat memastikan bahwa kontrol keamanan tetap efektif dan dapat diadaptasi sesuai dengan ancaman yang berkembang.
Kompleksitas	**Sedang** – Memerlukan prosedur peninjauan yang terstruktur dan sistem dokumentasi yang tepat untuk menilai efektivitas kontrol keamanan.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

175 Kontrol 4.4.1.a:

Kontrol	Penyelenggara IIV mengevaluasi kontrol keamanan yang diterapkan apakah masih relevan terhadap spektrum ancaman yang ada atau perlu ada perbaikan dan penambahan.
Deskripsi Kontrol	Organisasi harus melakukan evaluasi terhadap kontrol keamanan yang diterapkan untuk memastikan bahwa kontrol tersebut tetap efektif dan relevan dengan ancaman yang terus berkembang. Evaluasi ini melibatkan peninjauan terhadap kontrol yang ada, seperti kebijakan, prosedur, alat,dan sistem keamanan yang digunakan, serta membandingkannya dengan perubahan dalam spektrum ancaman (misalnya ancaman siber baru, kebijakan, atau peraturan yang berlaku). Jika ditemukan ketidaksesuaian atau kelemahan, organisasi harus memperbaiki dan menambah kontrol yang diperlukan untuk meningkatkan ketahanan terhadap ancaman yang ada dan yang potensial. Tujuan dari kontrol ini adalah untuk mengevaluasi apakah organisasi secara proaktif menyesuaikan kontrolkeamanannya dengan ancaman yang ada, serta melakukan perbaikan atau penambahan apabila diperlukan.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Laporan hasil evaluasi kontrol keamanan yang mencakup analisis terhadap kontrol yang ada dan identifikasi area yang memerlukan peningkatan. - Dokumen perubahan atau pembaruan kebijakan dan prosedur keamanan. - Catatan audit atau penilaian keamanan yang menunjukkan apakah kontrol masih efektif terhadap ancaman yang berkembang. - Hasil uji penetrasi atau vulnerability assessment yang mencerminkan kelemahan dalam kontrol yang ada. - Dokumen perencanaan atau peta jalan untuk perbaikan dan pengembangan kontrol keamanan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.4.1.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menerapkan kontrol keamanan	Organisasi belum memiliki mekanisme evaluasi maupun penerapan kontrol keamanan, sehingga efektivitas pengamanan belum dapat diukur.	Tidak terdapat laporan evaluasi, kebijakan, atau dokumen pendukung terkait penerapan kontrol keamanan.
1	Organisasi telah mengevaluasi sebagian besar aspek kontrol keamanan namun belum ditetapkan menjadi kebijakan	Organisasi mulai melakukan evaluasi terhadap sebagian aspek kontrol keamanan, namun hasilnya belum diformalkan dalam kebijakan atau prosedur resmi.	Dokumentasi internal berupa catatan evaluasi parsial, draft laporan, atau notulen rapat yang menunjukkan upaya peninjauan kontrol keamanan.
2	- Organisasi mengevaluasi kontrol keamanan yang diterapkan secara menyeluruh dan sudah ditetapkan melalui sebuah kebijakan - hasil evaluasi kontrol keamanan disusun dalam bentuk laporan hasil evaluasi yang berisi kontrol-kontrol yang masih relevan dan yang sudah tidak relevan terhadap spektrum ancaman yang ada - merekomendasikan perbaikan dan penambahan terhadap kontrol yang sudah tidak relevan terhadap spektrum ancaman yang ada.	Evaluasi kontrol keamanan dilakukan secara menyeluruh dan hasilnya dituangkan dalam kebijakan organisasi untuk memastikan kesesuaian dengan ancaman yang ada.	Laporan hasil evaluasi kontrol keamanan, rekomendasi perbaikan, serta dokumen kebijakan resmi yang mendukung penerapannya.
3	- Organisasi mengevaluasi kontrol keamanan yang diterapkan secara menyeluruh dan sudah ditetapkan melalui sebuah kebijakan - hasil evaluasi kontrol keamanan disusun dalam bentuk laporan hasil evaluasi yang berisi kontrol-kontrol yang masih relevan dan yang sudah tidak relevan terhadap spektrum ancaman yang ada - melakukan perbandingan kontrol keamanan dengan standar-standar nasional dan internasional yang berkaitan - melakukan perbaikan dan penambahan terhadap kontrol yang sudah tidak relevan terhadap spektrum ancaman yang ada.	Organisasi secara rutin mengevaluasi kontrol keamanan secara menyeluruh, membandingkannya dengan standar nasional maupun internasional, serta memperbarui kebijakan berdasarkan hasil evaluasi.	Laporan evaluasi kontrol, dokumen kebijakan terbaru, catatan audit, serta hasil uji penetrasi atau vulnerability assessment yang digunakan sebagai dasar perbaikan.
4	- Organisasi mengevaluasi kontrol keamanan yang diterapkan secara menyeluruh dan sudah ditetapkan melalui sebuah kebijakan	Evaluasi kontrol keamanan dilakukan menyeluruh dengan benchmarking pada standar global, dan hasil evaluasi digunakan	Laporan hasil evaluasi, dokumen perbandingan dengan standar, catatan

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
	- hasil evaluasi kontrol keamanan disusun dalam bentuk laporan hasil evaluasi yang berisi kontrol-kontrol yang masih relevan dan yang sudah tidak relevan terhadap spektrum ancaman yang ada - melakukan perbandingan kontrol keamanan dengan standar-standar nasional dan internasional yang berkaitan - melakukan perbaikan dan penambahan terhadap kontrol yang sudah tidak relevan terhadap spektrum ancaman yang ada.	untuk menyusun roadmap perbaikan berkelanjutan.	audit keamanan, serta peta jalan perbaikan kontrol keamanan.
5	- Organisasi mengevaluasi kontrol keamanan yang diterapkan secara menyeluruh dan sudah ditetapkan melalui sebuah kebijakan - hasil evaluasi kontrol keamanan disusun dalam bentuk laporan hasil evaluasi yang berisi kontrol-kontrol yang masih relevan dan yang sudah tidak relevan terhadap spektrum ancaman yang ada - melakukan perbandingan kontrol keamanan dengan standar-standar nasional dan internasional yang berkaitan - melakukan perbaikan dan penambahan terhadap kontrol yang sudah tidak relevan terhadap spektrum ancaman yang ada	Organisasi menerapkan evaluasi kontrol keamanan berkelanjutan, terintegrasi dengan manajemen risiko, serta didukung oleh pembaruan kebijakan dan rencana strategis jangka panjang.	Dokumen hasil evaluasi berkala, laporan audit, hasil vulnerability assessment, dokumen perubahan kebijakan, serta roadmap pengembangan kontrol keamanan jangka panjang.

4.4.2. Mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala

Kriteria	Detail
Deskripsi	Mereviu dan memperbarui dokumen rencana tanggap Insiden Siber serta rencana keberlangsungan kegiatan secara berkala merupakan upaya penting untuk menjaga kesiapan organisasi dalam menghadapi potensi gangguan. Penyelenggara IIV melakukan peninjauan dan pembaruan dokumen tersebut setiap kali terdapat temuan baru atau pengalaman insiden yang dapat menjadi bahan pembelajaran berkelanjutan. Selain itu, setiap kerentanan, ancaman, maupun risiko baru yang teridentifikasi didokumentasikan beserta rencana mitigasinya dalam dokumen pengelolaan risiko, sehingga organisasi senantiasa adaptif dan mampu meningkatkan ketahanan terhadap ancaman siber.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan reviu dan pembaruan dokumen secara berkala.
Dampak	**Tinggi** – Dengan dokumen yang selalu diperbarui, organisasi dapat memastikan bahwa rencana tanggap dan keberlangsungan selalu siap digunakan dalam situasi krisis.
Kompleksitas	**Sedang** – Memerlukan prosedur reviu yang terstruktur dan sistem dokumentasi yang tepat untuk memperbarui dokumen secara berkala
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03, ID.IM-04, ID.RA-06** **NIST CSF 1.1: RS.IM-1, RS.MI-3, RC.IM-1** **NIST SP 800-53r5: CA-2, CA-7, CP-2, IR-4, IR-8, RA-3, RA-5, RA-7** **SNI ISO/IEC 27001:2022: 5.27, 8.8**

176 Kontrol 4.4.2.a:

Kontrol	Penyelenggara IIV melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap Insiden Siber dan pemulihan jika terdapat hal-hal yang dapat dijadikan pembelajaran berkelanjutan bagi organisasi.
Deskripsi Kontrol	Organisasi harus melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap insiden siber dan pemulihan untuk memastikan bahwa rencana tersebut selalu sesuai dengan kondisi terkini dan dapat mengakomodasi perubahan dalam ancaman, kebijakan, atau teknologi. Reviu ini dilakukan dengan tujuan untuk menyertakan pembelajaran dari insiden yang telah terjadi, memperbaiki prosedur yang ada, serta memastikan kesiapan organisasi dalam menghadapi insiden yang akan datang. Pembaharuan ini harus dilakukan secara berkala dan setelah setiap insiden besar untuk memastikan bahwa langkah-langkah pemulihan dan tanggap insiden yang ada tetap efektif dan relevan.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Laporan hasil reviu dan pembaharuan rencana tanggap insiden siber. - Dokumentasi yang menunjukkan perubahan atau penyesuaian terhadap prosedur dalam rencana tanggap insiden. - Catatan hasil evaluasi insiden sebelumnya dan langkah-langkah yang diambil berdasarkan pembelajaran dari insiden tersebut. - Notulen rapat yang membahas pembaruan atau perbaikan terhadap rencana pemulihan. - Salinan dokumen rencana tanggap insiden siber terbaru yang mencakup pembaruan dan perbaikan yang telah diterapkan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03, ID.IM-04, ID.RA-06** **NIST CSF 1.1: RS.IM-1, RS.MI-3, RC.IM-1** **NIST SP 800-53r5: CA-2, CA-7, CP-2, IR-4, IR-8, RA-3, RA-5, RA-7** **SNI ISO/IEC 27001:2022: 5.27, 8.8**

Kriteria Pemenuhan Kontrol 4.4.2.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum menyusun dokumen rencana tanggap Insiden Siber dan pemulihan	Organisasi tidak memiliki dokumen rencana tanggap Insiden Siber maupun rencana pemulihan sehingga belum ada acuan dalam menghadapi insiden.	Tidak terdapat dokumen rencana tanggap Insiden Siber, dokumen pemulihan, maupun bukti pendukung lainnya.
1	- Organisasi telah melakukan sebagian kecil reviu dan pembaharuan dokumen rencana tanggap Insiden Siber dan pemulihan, namun belum ditetapkan menjadi kebijakan - Reviu terhadap isi dari dokumen Rencana tanggap Insiden Siber minimal terdapat 1 dari 6 kriteria antara lain: tahapan penanganan Insiden Siber; jenis Insiden Siber yang ditangani; daftar peran dan tanggung jawab anggota TTIS; daftar perangkat, teknologi, dan sumber daya yang diperlukan; daftar proses pemulihan jaringan dan data yang penting/kritikal; dan daftar pihak internal dan eksternal yang perlu dihubungi.	Reviu hanya mencakup sebagian kecil aspek dari rencana tanggap Insiden Siber dan pemulihan, sehingga dokumen belum komprehensif dan belum diformalkan.	Draft atau catatan reviu awal, notulen rapat, atau dokumen parsial yang memuat minimal 1 dari 6 kriteria utama isi rencana tanggap Insiden Siber.
2	- Organisasi telah melakukan sebagian besar reviu dan pembaharuan dokumen rencana tanggap Insiden Siber dan pemulihan, namun belum ditetapkan menjadi kebijakan - Reviu terhadap isi dari dokumen Rencana tanggap Insiden Siber minimal terdapat 3 dari 6 kriteria antara lain: tahapan penanganan Insiden Siber; jenis Insiden Siber yang ditangani; daftar peran dan tanggung jawab anggota TTIS; daftar perangkat, teknologi, dan sumber daya yang diperlukan; daftar proses pemulihan jaringan dan data yang penting/kritikal; dan daftar pihak internal dan eksternal yang perlu dihubungi.	Reviu telah mencakup sebagian besar aspek penting dalam rencana tanggap Insiden Siber, namun dokumen belum disahkan secara formal sebagai kebijakan.	Laporan reviu yang mencakup minimal 3 dari 6 kriteria utama rencana tanggap Insiden Siber, beserta catatan evaluasi insiden sebelumnya.
3	Organisasi melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap Insiden Siber dan telah disahkan oleh pimpinan Organisasi	Reviu dan pembaruan dokumen dilakukan secara menyeluruh berdasarkan pengalaman insiden sebelumnya dan sudah mendapatkan pengesahan pimpinan.	Laporan hasil reviu, dokumen rencana tanggap Insiden Siber terbaru yang sudah diperbarui, dan dokumen pengesahan dari pimpinan.
4	Organisasi melakukan reviu dan pembaharuan secara berkala terhadap dokumen rencana tanggap Insiden Siber dan telah disahkan oleh pimpinan Organisasi	Reviu dan pembaruan dilakukan secara teratur dan berkala untuk memastikan kesesuaian dokumen dengan kondisi terbaru serta disahkan oleh pimpinan.	Laporan hasil reviu berkala, notulen rapat pembahasan pembaruan, serta salinan dokumen tanggap Insiden Siber terbaru.
5	- Organisasi melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap Insiden Siber dan telah disahkan oleh pimpinan Organisasi - reviu terhadap dokumen rencana tanggap Insiden Siber dilakukan secara berkala sesuai kebutuhan - pembaruan terhadap dokumen rencana tanggap Insiden Siber telah disahkan oleh pimpinan Organisasi	Reviu dilakukan secara berkesinambungan dengan menambahkan pembelajaran dari insiden terdahulu, mendokumentasikan kerentanan/ancaman baru, serta mengintegrasikan rencana mitigasi ke dalam dokumen pengelolaan risiko.	Laporan reviu berkala, dokumentasi pembaruan prosedur, catatan evaluasi insiden dan pembelajaran, notulen rapat pembahasan perbaikan, serta salinan dokumen rencana tanggap Insiden Siber terbaru berikut peta jalan perbaikan.

177 Kontrol 4.4.2.b:

Kontrol	Penyelenggara IIV mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko
Deskripsi Kontrol	Organisasi mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko. Hal ini penting untuk memastikan bahwa semua potensi risiko yang baru diketahui dapat segera diidentifikasi, dianalisis, dan ditanggulangi dengan rencana mitigasi yang jelas. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki proses yang sistematis dalam mencatat dan mengelola risiko yang baru teridentifikasi agar dapat mengurangi dampak negatif terhadap operasional dan keamanan informasi.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Dokumen pengelolaan risiko yang mencatat kerentanan dan ancaman yang baru ditemukan. - Rencana mitigasi risiko untuk setiap kerentanan atau ancaman yang teridentifikasi. - Laporan hasil pemindaian atau penilaian risiko yang menunjukkan kerentanan yang ditemukan. - Protokol atau prosedur pengelolaan risiko yang menyebutkan langkah-langkah mitigasi dan penanggulangan risiko. - Notulen atau laporan rapat tim keamanan yang membahas identifikasi dan mitigasi risiko baru. - Alat atau perangkat yang digunakan untuk pemantauan dan pencatatan risiko (misalnya perangkat manajemen risiko).
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03, ID.IM-04, ID.RA-06** **NIST CSF 1.1: RS.IM-1, RS.MI-3, RC.IM-1** **NIST SP 800-53r5: CA-2, CA-7, CP-2, IR-4, IR-8, RA-3, RA-5, RA-7** **SNI ISO/IEC 27001:2022: 5.27, 8.8**

Kriteria Pemenuhan Kontrol 4.4.2.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi telah menyusun draft dokumen pengelolaan risiko, namun belum mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam draft dokumen tersebut	Organisasi berada pada tahap awal, hanya memiliki draft dokumen pengelolaan risiko tanpa pencatatan kerentanan atau ancaman baru maupun langkah mitigasinya.	Tidak terdapat catatan risiko baru; tidak ada rencana mitigasi yang terdokumentasi; draft dokumen masih bersifat umum tanpa rincian terbaru.
1	Organisasi telah menyusun draft dokumen pengelolaan risiko dan sudah melakukan Pengumpulan data/analisis terhadap kerentanan, ancaman, atau risiko yang baru ditemukan, namun belum mendokumentasikan ke dalam draft dokumen tersebut	Organisasi sudah mulai melakukan analisis risiko dan mengidentifikasi kerentanan baru, tetapi hasilnya belum dituangkan secara formal dalam dokumen pengelolaan risiko.	Laporan hasil pemindaian atau penilaian risiko; catatan analisis awal; notulen rapat pembahasan identifikasi risiko baru.
2	- Organisasi telah menyusun dokumen pengelolaan risiko dan telah disahkan oleh pimpinan Organisasi - Organisasi telah mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan ke dalam dokumen pengelolaan risiko - pembaruan terhadap dokumen pengelolaan risiko telah disahkan oleh pimpinan Organisasi	Organisasi sudah memiliki dokumen pengelolaan risiko yang formal dan sah, serta mulai mencatat kerentanan/ancaman baru yang ditemukan.	Salinan dokumen pengelolaan risiko terbaru; laporan hasil penilaian risiko yang menyertakan kerentanan baru; dokumen pengesahan pimpinan.
3	- Organisasi telah menyusun dokumen pengelolaan risiko dan telah disahkan oleh pimpinan Organisasi - Organisasi telah mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko - pembaruan terhadap dokumen pengelolaan risiko telah disahkan oleh pimpinan Organisasi	Dokumen pengelolaan risiko mencakup pencatatan kerentanan, ancaman, serta langkah mitigasi yang sesuai, dengan pembaruan yang disahkan pimpinan.	Dokumen pengelolaan risiko yang memuat daftar kerentanan dan ancaman baru; rencana mitigasi risiko; protokol pengelolaan risiko yang diperbarui; laporan hasil rapat evaluasi.
4	- Organisasi telah menyusun dokumen pengelolaan risiko dan telah disahkan oleh pimpinan Organisasi - Organisasi telah mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko - pembaruan terhadap dokumen pengelolaan risiko telah disahkan oleh pimpinan Organisasi	Organisasi melakukan pengelolaan risiko secara terstruktur, dengan pencatatan dan pembaruan rencana mitigasi setiap kali ditemukan kerentanan atau ancaman baru.	Laporan pemindaian risiko; catatan perubahan pada dokumen risiko; notulen rapat tim keamanan; dokumen mitigasi risiko terbaru.
5	- Organisasi telah menyusun dokumen pengelolaan risiko dan telah disahkan oleh pimpinan Organisasi - Organisasi telah mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko - pendokumentasian terhadap kerentanan, ancaman,atau risiko dilakukan secara berkala sesuai kebutuhan - pembaruan terhadap dokumen pengelolaan risiko telah disahkan oleh pimpinan Organisasi	Organisasi memiliki mekanisme berkelanjutan untuk mendokumentasikan risiko, menyusun mitigasi, serta memperbarui dokumen secara berkala dan berkesinambungan.	Dokumen pengelolaan risiko terbaru dengan catatan berkala; laporan hasil vulnerability assessment; rencana mitigasi risiko jangka panjang; protokol/prosedur pengelolaan risiko; bukti penggunaan perangkat manajemen risiko.

4.4.3. Mengumpulkan dan memelihara hasil forensik digital

Kriteria	Detail
Deskripsi	Mengumpulkan dan memelihara hasil forensik digital merupakan langkah penting dalam memastikan bukti insiden siber terdokumentasi dengan baik dan dapat digunakan secara sah. Laporan hasil forensik digital tidak hanya mencatat temuan teknis, tetapi juga memuat informasi relevan yang mendukung proses analisis lebih lanjut. Dokumen ini dipelihara secara aman untuk menjaga integritas dan keabsahannya, serta dapat disampaikan kepada pihak berwajib sebagai dasar investigasi maupun penegakan hukum sesuai ketentuan yang berlaku.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan alat forensik dan sumber daya untuk mengumpulkan serta menyimpan bukti secara aman.
Dampak	**Tinggi** – Dengan bukti yang lengkap dan terpelihara dengan baik, organisasi dapat melakukan investigasi yang efektif dan mengambil tindakan yang tepat berdasarkan bukti tersebut.
Kompleksitas	**Sedang** – Memerlukan prosedur pengumpulan yang terstruktur dan sistem penyimpanan yang aman untuk memelihara bukti digital.
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

178 Kontrol 4.4.3.a:

Kontrol	Laporan hasil pelaksanaan forensik digital dikumpulkan dan dipelihara meliputi juga informasi-informasi yang relevan terhadapnya.
Deskripsi Kontrol	Laporan hasil pelaksanaan forensik digital dikumpulkan dan dipelihara meliputi juga informasi-informasi yang relevan terhadapnya. Hal ini penting untuk memastikan bahwa hasil forensik digital dapat digunakan sebagai bukti yang sah dan valid dalam investigasi insiden keamanan, serta dapat diakses dengan mudah jika diperlukan untuk audit atau analisis lebih lanjut. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang sistematis untuk mendokumentasikan dan menyimpan hasil forensik secara lengkap dan terorganisir.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Laporan forensik digital yang memuat analisis dan temuan terkait insiden. - Catatan atau dokumentasi terkait dengan proses pengumpulan bukti digital. - Laporan pengujian atau audit hasil forensik. - Dokumen yang menunjukkan keterkaitan bukti dengan aset yang terdampak insiden. - Prosedur atau kebijakan penyimpanan data forensik untuk memastikan keamanannya. - Catatan tentang siapa yang bertanggung jawab atas pemeliharaan laporan dan bukti forensik. - Alat atau sistem yang digunakan untuk menyimpan dan mengelola hasil forensik (misalnya sistem manajemen bukti atau arsip digital).
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.4.3.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Kegiatan forensik digital belum dilaksanakan	Kegiatan forensik digital belum pernah dilakukan, tidak ada dokumentasi atau laporan terkait insiden siber.	Tidak tersedia bukti atau dokumen pendukung.
1	Kegiatan forensik digital sudah dilaksanakan namun laporan hasil pelaksanaan forensik digital belum pernah disusun/diformalkan	Kegiatan forensik digital sudah dilakukan namun belum menghasilkan laporan formal.	- Catatan informal atau dokumentasi internal mengenai proses pengumpulan bukti. - Bukti aktivitas awal investigasi tanpa format laporan standar.
2	Kegiatan forensik digital sudah dilaksanakan sesuai dengan praktik terbaik namun laporan hasil pelaksanaan forensik digital belum pernah disusun/diformalkan	Kegiatan forensik digital dilakukan sesuai praktik terbaik, tetapi laporan hasil belum pernah diformalkan.	- Catatan teknis atau dokumentasi proses analisis forensik. - Bukti keterkaitan antara insiden dan aset terdampak.
3	Kegiatan forensik digital sudah dilaksanakan sesuai dengan praktik terbaik dan laporan hasil pelaksanaan forensik digital sudah disusun/diformalkan berikut juga pengumpulan dan pemeliharaan informasi-informasi yang relevan terhadapnya	Kegiatan forensik digital dilakukan sesuai praktik terbaik, laporan hasil telah diformalkan, serta informasi relevan dikumpulkan dan dipelihara.	- Laporan forensik digital yang memuat analisis dan temuan insiden. - Dokumentasi pengumpulan bukti digital. - Dokumen keterkaitan bukti dengan aset terdampak. - Catatan penanggung jawab pemeliharaan laporan dan bukti.
4	- Kegiatan forensik digital sudah dilaksanakan sesuai dengan praktik terbaik dan laporan hasil pelaksanaan forensik digital sudah disusun/diformalkan berikut juga pengumpulan dan pemeliharaan informasi-informasi yang relevan terhadapnya - Kebijakan pelaporan pelaksanaan forensik digital berikut juga pengumpulan dan pemeliharaan informasi-informasi yang relevan terhadapnya telah dilakukan reviu berkala berdasarkan pelaksanaan forensik digital	Selain pelaksanaan dan pelaporan forensik digital sesuai praktik terbaik, kebijakan pelaporan serta pemeliharaan informasi relevan telah dilakukan reviu secara berkala.	- Laporan forensik digital formal. - Prosedur/kebijakan penyimpanan data forensik. - Catatan reviu berkala kebijakan dan prosedur. - Laporan audit atau pengujian hasil forensik.
5	- Kebijakan pelaksanaan forensik digital telah ditetapkan, pelaksanaan forensik digital sudah dilakukan sesuai prosedur yang lengkap sesuai prosedur yang ditetapkan - Kebijakan pelaporan pelaksanaan forensik digital berikut juga pengumpulan dan pemeliharaan informasi-informasi yang relevan terhadapnya telah dilakukan reviu berkala berdasarkan pelaksanaan forensik digital dan dilakukan perbaikan	Kebijakan pelaksanaan forensik digital telah ditetapkan, prosedur lengkap diterapkan, dan kegiatan dilaksanakan sesuai prosedur. Reviu berkala dilakukan dengan perbaikan berkelanjutan.	- Kebijakan resmi pelaksanaan forensik digital. - Laporan forensik digital formal. - Prosedur standar penyimpanan dan pengelolaan bukti. - Catatan reviu dan perbaikan kebijakan/prosedur. - Alat atau sistem manajemen bukti digital (arsip digital/EBMS).

179 Kontrol 4.4.3.b:

Kontrol	Laporan hasil pelaksanaan forensik digital dapat disampaikan kepada pihak berwajib untuk proses investigasi dan penegakkan hukum sesuai ketentuan yang berlaku
Deskripsi Kontrol	Laporan hasil pelaksanaan forensik digital dapat disampaikan kepada pihak berwajib untuk proses investigasi dan penegakan hukum sesuai ketentuan yang berlaku. Hal ini memastikan bahwa hasil forensik dapat digunakan secara sah dalam prosedur hukum, serta mendukung pihak berwajib dalam proses penegakan hukum dan penyelesaian insiden. Tujuan dari kontrol ini adalah untuk menilai apakah organisasi memiliki prosedur yang jelas dan aman dalam menyampaikan hasil forensik digital kepada pihak yang berwenang, sesuai dengan peraturan yang berlaku.
Deskripsi Bukti Dukung	Data dukung berupa: - Salinan laporan forensik digital yang mencantumkan bukti yang relevan dengan insiden. - Dokumen resmi yang menunjukkan komunikasi atau permintaan dari pihak berwajib untuk mendapatkan laporan. - Protokol atau prosedur pengiriman laporan forensik ke pihak berwajib. - Surat atau dokumen yang menyatakan bahwa laporan telah diterima oleh pihak berwajib. - Catatan tentang pihak yang bertanggung jawab dalam mengirimkan laporan kepada pihak berwajib. - Kebijakan atau pedoman internal mengenai penyerahan laporan forensik digital untuk keperluan hukum.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: -** **NIST CSF 1.1: -** **NIST SP 800-53r5: -** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.4.3.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Kegiatan forensik digital belum pernah dilaksanakan	Kegiatan forensik digital belum pernah dilakukan, tidak ada laporan atau bukti pelaksanaan.	Tidak tersedia dokumen atau catatan pendukung.
1	Kegiatan forensik digital pernah dilaksanakan namun laporan hasil pelaksanaan forensik digital belum pernah disusun.	Kegiatan forensik digital pernah dilakukan, tetapi laporan hasil pelaksanaan belum pernah disusun secara formal.	- Catatan internal atau dokumentasi awal insiden. - Bukti aktivitas forensik tanpa laporan resmi.
2	Laporan hasil pelaksanaan forensik digital telah disusun namun masih berupa draft yang belum ditandatangani oleh Tim Forensik Digital	Laporan hasil forensik digital telah disusun, tetapi masih berupa draft dan belum ditandatangani tim forensik digital.	- Draft laporan forensik digital. - Catatan proses penyusunan laporan.
3	Laporan hasil pelaksanaan forensik digital telah ditandatangani oleh Tim Forensik Digital namun baru dilaporkan kepada Pimpinan Organisasi dan/atau Ketua TTIS	Laporan hasil forensik digital telah ditandatangani tim forensik digital, tetapi baru disampaikan kepada pimpinan organisasi atau Ketua TTIS.	- Salinan laporan forensik digital yang ditandatangani. - Dokumen internal pengesahan atau distribusi terbatas di lingkup organisasi.
4	- Laporan forensik digital telah ditandatangani oleh tim forensik digital dan disahkan oleh pimpinan Organisasi atau Ketua TTIS - Laporan hasil pelaksanaan forensik digital telah disampaikan kepada pihak berwajib untuk proses investigasi dan penegakkan hukum sesuai ketentuan yang berlaku	Laporan forensik digital telah ditandatangani oleh tim forensik digital dan disahkan pimpinan organisasi/ketua TTIS, serta disampaikan ke pihak berwajib untuk investigasi dan penegakan hukum.	- Salinan laporan forensik digital yang relevan dengan insiden. - Dokumen resmi komunikasi atau permintaan laporan dari pihak berwajib. - Protokol/prosedur pengiriman laporan ke pihak berwajib. - Surat atau dokumen tanda terima laporan dari pihak berwajib. - Catatan penanggung jawab pengiriman laporan.
5	- Laporan forensik digital telah ditandatangani oleh tim forensik digital dan disahkan oleh pimpinan Organisasi atau Ketua TTIS - Laporan hasil pelaksanaan forensik digital telah disampaikan kepada pihak berwajib untuk proses investigasi dan penegakkan hukum sesuai ketentuan yang berlaku - Penyampaian Laporan telah mempertimbangkan Klasifikasi Informasi dan/atau Kode Distribusi Informasi	Selain telah ditandatangani dan disahkan, laporan forensik digital yang disampaikan ke pihak berwajib sudah mempertimbangkan klasifikasi informasi/kode distribusi informasi sesuai ketentuan hukum dan kebijakan internal.	- Kebijakan/pedoman internal mengenai penyerahan laporan forensik digital. - Salinan laporan forensik digital yang disampaikan dengan klasifikasi informasi. - Dokumen tanda terima dari pihak berwajib. - Catatan penanggung jawab distribusi dan penyampaian laporan. - Bukti reviu kepatuhan terhadap klasifikasi informasi/kode distribusi.

4.4.4. Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala

Kriteria	Detail
Deskripsi	Peninjauan efektivitas kinerja penanganan insiden oleh Tim Tanggap Insiden Siber dilakukan secara berkala untuk memastikan setiap langkah yang ditempuh berjalan optimal. Penyelenggara IIV secara aktif mengevaluasi hasil penanganan insiden, kemudian melakukan perbaikan yang diperlukan baik dari sisi teknologi, tata kelola, maupun peningkatan kapasitas sumber daya manusia. Upaya ini bertujuan agar proses penanganan insiden siber semakin responsif, terukur, dan berkesinambungan dalam menghadapi ancaman yang terus berkembang.
Biaya	Untuk menerapkan kontrol ini, terdapat potensi kebutuhan biaya, karena memerlukan sumber daya untuk melakukan peninjauan secara berkala, tetapi tidak selalu membutuhkan teknologi tambahan.
Dampak	**Tinggi** – Dengan peninjauan yang rutin, organisasi dapat memastikan bahwa tim tanggap insiden tetap siap dan mampu merespons insiden dengan cara yang efektif.
Kompleksitas	**Sedang** – Memerlukan prosedur peninjauan yang terstruktur dan sistem evaluasi kinerja yang tepat untuk menilai efektivitas tim tanggap insiden.
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: RS.IM-2, RC.IM-2** **NIST SP 800-53r5: CP-2, IR-4, IR-8** **SNI ISO/IEC 27001:2022: -**

180 Kontrol 4.4.4.a:

Kontrol	Penyelenggara IIV melakukan peninjauan terhadap efektifitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala.
Deskripsi Kontrol	Organisasi melakukan peninjauan terhadap efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala. Peninjauan ini bertujuan untuk mengevaluasi sejauh mana respons terhadap insiden telah dilaksanakan sesuai prosedur yang ditetapkan, mengidentifikasi kekuatan dan kelemahan dalam proses penanganan, serta memastikan bahwa tindakan perbaikan atau peningkatan dapat diimplementasikan untuk mengoptimalkan respons di masa depan. Tujuan dari kontrol ini adalah untuk memastikan bahwa tim tanggap insiden selalu siap, kompeten, dan mampu menangani insiden dengan efisien, serta untuk meningkatkan kesiapan organisasi menghadapi ancaman siber di masa mendatang.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Laporan hasil peninjauan efektivitas kinerja tim tanggap insiden. - Prosedur peninjauan berkala terhadap penanganan insiden. - Catatan rapat evaluasi pasca-penanganan insiden (post-incident reviu). - Checklist atau kriteria evaluasi yang digunakan dalam peninjauan. - Dokumentasi rekomendasi perbaikan dan tindak lanjut hasil peninjauan. - Laporan pelatihan atau simulasi yang relevan dengan penanganan insiden. - Daftar insiden sebelumnya beserta evaluasi kinerja yang dilakukan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: RS.IM-2, RC.IM-2** **NIST SP 800-53r5: CP-2, IR-4, IR-8** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.4.4.a Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan peninjauan terhadap efektifitas kinerja penanganan insiden	Tidak tersedia kriteria	Tidak tersedia dokumen pendukung atau catatan evaluasi.
1	- TTIS sudah menangani Insiden Siber namun belum pernah dilakukan evaluasi terhadap efektifitas kinerja penanganan Insiden secara mandiri - Organisasi belum pernah melakukan peninjauan terhadap efektifitas kinerja penanganan Insiden yang dilakukan oleh TTIS	Tim Tanggap Insiden Siber (TTIS) sudah menangani insiden siber namun belum dilakukan evaluasi efektivitas kinerja baik secara mandiri maupun oleh organisasi.	Catatan insiden yang pernah ditangani tanpa evaluasi pasca-insiden.
2	- TTIS sudah pernah melakukan evaluasi terhadap efektifitas kinerja penanganan insiden secara mandiri namun belum dilakukan peninjauan oleh organisasi	TTIS sudah melakukan evaluasi efektivitas kinerja penanganan insiden secara mandiri, tetapi organisasi belum melakukan peninjauan.	- Laporan hasil evaluasi mandiri TTIS. - Checklist atau kriteria evaluasi yang digunakan.
3	- TTIS sudah pernah melakukan evaluasi terhadap efektifitas kinerja penanganan Insiden secara mandiri - Organisasi telah melakukan peninjauan terhadap efektifitas kinerja penanganan Insiden yang dilakukan oleh tim tanggap Insiden Siber	TTIS sudah melakukan evaluasi efektivitas kinerja penanganan insiden secara mandiri dan organisasi telah melakukan peninjauan.	- Laporan hasil peninjauan efektivitas kinerja tim tanggap insiden. - Catatan rapat evaluasi pasca-penanganan insiden (post-incident reviu). - Dokumentasi rekomendasi perbaikan dan tindak lanjut.
4	- TTIS sudah pernah melakukan evaluasi terhadap efektifitas kinerja penanganan Insiden secara mandiri - Organisasi telah melakukan peninjauan terhadap efektifitas kinerja penanganan Insiden yang dilakukan oleh tim tanggap Insiden Siber - Kebijakan/pedoman/prosedur peninjauan terhadap efektifitas kinerja penanganan Insiden Siber oleh TTIS sudah ditetapkan/diformalkan	Selain evaluasi mandiri TTIS dan peninjauan oleh organisasi, kebijakan/pedoman/prosedur peninjauan efektivitas kinerja penanganan insiden sudah ditetapkan secara formal.	- Prosedur peninjauan berkala terhadap penanganan insiden. - Kebijakan internal terkait evaluasi insiden. - Dokumentasi rekomendasi dan tindak lanjut hasil peninjauan. - Laporan pelatihan atau simulasi penanganan insiden.
5	- TTIS sudah pernah melakukan evaluasi terhadap efektifitas kinerja penanganan Insiden secara mandiri - Organisasi telah melakukan peninjauan terhadap efektifitas kinerja penanganan Insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala minimal satu kali dalam satu tahun - Kebijakan/pedoman/prosedur peninjauan terhadap efektifitas kinerja penanganan Insiden Siber oleh TTIS sudah ditetapkan/diformalkan dan sudah dilakukan reviu secara berkala dan dilakukan perbaikan.	Evaluasi mandiri TTIS dan peninjauan organisasi dilakukan secara berkala (minimal sekali dalam setahun). Kebijakan, pedoman, dan prosedur peninjauan telah ditetapkan, direviu, serta diperbaiki sesuai kebutuhan.	- Laporan peninjauan efektivitas kinerja secara berkala. - Prosedur peninjauan yang telah direviu dan diperbarui. - Dokumentasi rekomendasi perbaikan yang sudah ditindaklanjuti. - Daftar insiden sebelumnya beserta hasil evaluasi. - Laporan pelatihan/simulasi untuk peningkatan kapasitas SDM.

181 Kontrol 4.4.4.b:

Kontrol	Melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.
Deskripsi Kontrol	Organisasi perlu melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber untuk memastikan peningkatan kemampuan dalam menghadapi insiden serupa di masa depan. Langkah-langkah ini dapat mencakup evaluasi teknologi yang digunakan, revisi tata kelola insiden, atau pelatihan dan pengembangan kapasitas SDM. Tujuan dari kontrol ini adalah untuk memastikan bahwa organisasi belajar dari insiden yang terjadi dan terus memperkuat strategi responsnya untuk mengurangi risiko dan dampak serupa di masa mendatang.
Deskripsi Bukti Dukung	Data dukung dapat berupa: - Laporan evaluasi pasca-insiden yang mencakup identifikasi kelemahan teknologi, tata kelola, dan kapasitas SDM. - Rencana tindakan perbaikan untuk teknologi, seperti pembaruan perangkat lunak, implementasi solusi keamanan baru, atau peningkatan infrastruktur. - Revisi kebijakan dan prosedur tata kelola insiden siber. - Program pelatihan atau peningkatan kapasitas SDM yang relevan. - Dokumentasi hasil pelatihan, termasuk sertifikasi atau laporan kehadiran. - Laporan audit internal atau eksternal terkait langkah perbaikan. - Bukti implementasi perbaikan, seperti notulen rapat, bukti pembelian perangkat, atau konfigurasi baru yang diterapkan.
Ancaman/Risiko yang dimitigasi	TH036 TH039 TH043 TH050 TH054 TH071 TH038 TH040 TH044 TH053 TH065 TH077
Referensi Kontrol	**NIST CSF 2.0: ID.IM-03** **NIST CSF 1.1: RS.IM-2, RC.IM-2** **NIST SP 800-53r5: CP-2, IR-4, IR-8** **SNI ISO/IEC 27001:2022: -**

Kriteria Pemenuhan Kontrol 4.4.4.b Berdasarkan Indeks:

Indeks	Kriteria Indeks	Deskripsi Kriteria Indeks	Kriteria Bukti Dukung
0	Organisasi belum melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.	Organisasi belum melakukan langkah-langkah perbaikan terhadap pelaksanaan penanganan insiden siber dari segi teknologi, tata kelola, maupun peningkatan kapasitas SDM.	Tidak tersedia dokumen atau bukti pelaksanaan perbaikan.
1	Organisasi belum pernah melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber oleh TTIS	Organisasi belum pernah melakukan langkah-langkah perbaikan terhadap pelaksanaan penanganan insiden siber oleh TTIS.	Catatan insiden tanpa dokumentasi perbaikan.
2	Organisasi telah melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber oleh TTIS namun belum secara komprehensif meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.	Organisasi telah melakukan perbaikan namun belum komprehensif, hanya mencakup sebagian aspek (teknologi, tata kelola, atau kapasitas SDM).	- Laporan evaluasi pasca-insiden dengan identifikasi kelemahan tertentu. - Rencana tindakan perbaikan sebagian (misalnya teknologi saja).
3	TTIS telah melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.	TTIS telah melakukan langkah-langkah perbaikan mencakup teknologi, tata kelola, dan peningkatan kapasitas SDM.	- Laporan evaluasi pasca-insiden mencakup kelemahan di semua aspek. - Rencana perbaikan teknologi (pembaruan perangkat lunak, solusi keamanan baru, peningkatan infrastruktur). - Revisi kebijakan/prosedur tata kelola insiden. - Program pelatihan peningkatan kapasitas SDM.
4	Organisasi bersama dengan TTIS telah melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.	Organisasi bersama TTIS telah melaksanakan perbaikan secara menyeluruh mencakup aspek teknologi, tata kelola, dan kapasitas SDM.	- Dokumentasi hasil pelatihan, termasuk sertifikat/laporan kehadiran. - Bukti implementasi perbaikan (notulen rapat, pembelian perangkat, konfigurasi baru). - Laporan audit internal atau eksternal terkait langkah perbaikan.
5	- Organisasi bersama dengan TTIS telah melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan Insiden Siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM. - langkah-langkah perbaikan tersebut dievaluasi dan diperbarui secara berkala sesuai kebutuhan.	Organisasi bersama TTIS melakukan perbaikan secara komprehensif dan mengevaluasi serta memperbaruinya secara berkala sesuai kebutuhan.	- Laporan perbaikan yang diperbarui secara berkala. - Revisi kebijakan/prosedur setelah evaluasi. - Bukti tindak lanjut hasil audit atau reviu. - Dokumentasi pembaruan teknologi, tata kelola, dan peningkatan SDM yang berkesinambungan.

PENUTUP

Demikianlah Panduan Pemenuhan Kontrol Kematangan Keamanan Siber ini disusun dengan harapan dapat memberikan pemahaman yang lebih jelas mengenai penerapan dan pentingnya keamanan siber di berbagai sektor. Panduan ini diharapkan dapat menjadi acuan yang berguna bagi semua pemangku kepentingan dalam mengidentifikasi serta meningkatkan kematangan keamanan siber organisasi melalui Instrumen Penilaian Kematangan Keamanan Siber (IKAS).

Seiring dengan berkembangnya teknologi dan dinamika ancaman siber yang terus berubah, panduan ini akan terus diperbarui dan disesuaikan dengan kebutuhan dan perkembangan terkini. Oleh karena itu, panduan ini bersifat *living document* yang akan terus berkembang seiring waktu untuk memastikan bahwa penerapan keamanan siber tetap relevan dan efektif.

Kami mengharapkan partisipasi aktif dan komitmen dari semua pihak dalam implementasi dan pemenuhan kontrol kematangan keamanan siber demi terciptanya lingkungan digital yang lebih aman dan terlindungi.

TAKSONOMI ANCAMAN

Ancaman memiliki potensi untuk merusak aset seperti informasi, proses, dan sistem, dan organisasi. Ancaman dapat berasal dari manusia, teknologi atau alam, dan dapat bersifat tidak sengaja atau disengaja. Daftar Taksonomi Ancaman di bawah ini dapat digunakan sebagai acuan dalam menentukan ancaman/risiko yang dapat dimitigasi dengan penerapan kontrol kematangan keamanan siber.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
Ancaman Fisik	TH001	Api	Kebakaran di ruang server akibat kesalahan listrik merusak infrastruktur dan mengakibatkan hilangnya data
	TH002	Air	Kebocoran pada ruang server yang menyebabkan rusaknya perangkat dan terganggunya ketersediaan layanan.
	TH003	Polusi, radiasi berbahaya	Tumpahan bahan kimia dari pabrik terdekat mencemari lingkungan kantor, mengganggu operasi.
	TH004	Kecelakaan besar	Keruntuhan struktur di dalam fasilitas merusak departemen IT dan menyebabkan hilangnya data kritis
	TH005	Ledakan	Ledakan merusak jendela bangunan dan peralatan IT
	TH006	Debu, korosi, pembekuan	Debu dan korosi pada perangkat keras menyebabkan kegagalan sistem; suhu beku menyebabkan kegagalan sistem pendingin dan overheating.
Ancaman Alam	TH007	Fenomena iklim	Suhu ekstrem menyebabkan server terlalu panas dan potensi kegagalan sistem, sehingga membahayakan integritas data dan ketersediaan jaringan.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH008	Fenomena seismik	Kerusakan pusat data akibat gempa bumi dapat membahayakan keamanan fisik dan jaringan, meningkatkan risiko kehilangan data dan akses tidak sah selama pemulihan
	TH009	Fenomena vulkanik	Abu vulkanik dapat mengganggu sistem pendingin di pusat data, meningkatkan risiko kegagalan peralatan dan pelanggaran keamanan berikutnya
	TH010	Fenomena meteorologi	Badai parah dapat mematikan infrastruktur listrik dan komunikasi, melemahkan keamanan jaringan sementara dan mengekspos sistem terhadap ancaman siber.
	TH011	Banjir	Banjir dapat merusak infrastruktur TI, menyebabkan kegagalan perangkat keras dan pelanggaran data karena kegagalan langkah-langkah keamanan fisik.
	TH012	Pandemi/epidemi	Kekurangan staf akibat pandemi memunculkan kebutuhan pada pengaturan kerja jarak jauh (remote work) yang berpotensi tidak aman, meningkatkan kerentanan terhadap serangan cyber.
Kegagalan Infrastruktur	TH013	Kegagalan/gangguan pada supply chain	Kegagalan pada supply chain dapat mengganggu sistem elektronik, menyebabkan sistem tidak tersedia dan potensi pelanggaran keamanan karena tidak adanya redundansi/ redundansi terganggu.
	TH014	Kegagalan/gangguan pada sistem pendingin atau ventilasi	Kenaikan suhu server dan perangkat jaringan akibat kegagalan sistem pendingin dapat mengakibatkan kerusakan perangkat keras dan potensi kehilangan atau kerusakan data
	TH015	Kehilangan pasokan listrik	Pemadaman listrik mendadak dapat menyebabkan sistem mati mendadak, membahayakan integritas data dan membuka peluang untuk serangan siber selama fase pemulihan

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH016	Kegagalan jaringan telekomunikasi	Gangguan jaringan telekomunikasi dapat mengisolasi segmen jaringan, mengganggu kemampuan pemantauan dan respons keamanan, dan berpotensi membuat sistem rentan terhadap intrusi yang tidak terdeteksi
	TH017	Kegagalan peralatan telekomunikasi	Kerusakan atau kegagalan peralatan telekomunikasi dapat mengganggu transmisi data, meningkatkan risiko penyadapan data dan akses tidak sah
	TH018	Radiasi elektromagnetik	Gangguan elektromagnetik dapat membahayakan integritas transmisi data, berpotensi menyebabkan kerusakan data atau kebocoran data yang tidak sah
	TH019	Radiasi termal	Paparan radiasi termal berlebihan dapat merusak peralatan sensitif, berpotensi mengubah konfigurasi keamanan dan melemahkan pertahanan sistem
	TH020	Ledakan singkat energi elektromagnetik (Electromagnetic pulses/EMP)	Ledakan Elektromagnetik (EMP) dapat menyebabkan gangguan elektronik yang tiba-tiba dan meluas, secara kritis memengaruhi kemampuan penyimpanan dan pemrosesan data, serta menonaktifkan keamanan sistem.
	TH021	Cacat Perangkat Lunak	Kesalahan pengembang saat menulis kode sumber atau merancang sistem. Sistem yang kompleks meningkatkan kemungkinan adanya bug atau kesalahan
	TH022	Cacat Perangkat Keras	Cacat yang muncul akibat kesalahan dalam pembuatan atau perakitan komponen dan kualitas material/komponen yang rendah
Kegagalan Teknis	TH023	Kegagalan perangkat atau sistem	Kegagalan perangkat keras server dapat berdampak ke database sistem yang mungkin mengekspos data ke sistem yang lebih kurang aman selama proses failover
	TH024	Jenuh sistem informasi	Beban berlebihan pada sistem dapat mengurangi efektivitas firewall, meningkatkan kerentanan terhadap serangan siber.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH025	Pelanggaran pemeliharaan sistem informasi	Perubahan konfigurasi jaringan yang tidak sah dapat membuka port eksternal, memfasilitasi serangan ransomware.
Tindakan Manusia	TH026	Teror, serangan, sabotase	Perusakan pada perangkat keras (contoh: server) dapat mengganggu operasi, menyebabkan kehilangan data yang signifikan
	TH027	Rekayasa social (Social Engineering)	Phishing dapat menipu karyawan untuk mengungkapkan kredensial sensitif, menyebabkan pelanggaran data.
	TH028	Pencegatan radiasi perangkat	Data sensitif dapat terkompromi melalui emisi elektromagnetik dari perangkat
	TH029	Mata-mata jarak jauh (Remote spying)	Alat akses jarak jauh yang tidak sah dapat digunakan untuk memantau dan mencuri informasi rahasia.
	TH030	Pencegatan (Eavesdropping)	Komunikasi pribadi dapat dicuri selama transmisi, mengekspos data sensitif.
	TH031	Pencurian media atau dokumen	Pencurian fisik media penyimpanan dapat mengakibatkan hilangnya data kepemilikan.
	TH032	Pencurian peralatan	Kehilangan perangkat dapat menyebabkan akses data yang tidak sah dan potensi kerentanan jaringan.
	TH033	Pencurian identitas digital atau kredensial	Kredensial yang berhasil dicuri dapat digunakan untuk memfasilitasi serangan yang lebih mendalam/ lebih parah dalam jaringan.
	TH034	Pengambilan Kembali media yang telah di daur ulang atau dibuang	Pembuangan media yang tidak tepat dapat menyebabkan kebocoran data.
	TH035	Pengungkapan informasi	Database atau penyimpanan yang dikonfigurasi secara salah dapat mengekspos data sensitif
	TH036	Data input dari sumber yang tidak dapat dipercaya	Malware pada sistem dapat menyebabkan kerusakan.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH037	Memodfikasi tanpa izin pada perangkat keras (Tampering with hardware)	Modifikasi perangkat keras yang tidak sah dapat membuka akses backdoor pada jaringan
	TH038	Memodfikasi tanpa izin pada Mengutak-atik perangkat lunak (Tampering with software)	Modifikasi perangkat lunak sistem dapat melemahkan kontrol keamanan, memungkinkan manipulasi data
	TH039	unduhan drive-by (Drive-by-exploits) menggunakan komunikasi berbasis web	Pengguna dapat secara tidak sengaja mengunduh malware dari situs web yang terkompromi
	TH040	Replay attack, serangan man-in-the-middle	Data yang sedang ditransmisikan (data-in-transit) dapat dicegat dan dimanipulasi, membahayakan integritas transaksi.
	TH041	Pengolahan data pribadi yang tidak sah	Pengolahan data pribadi tanpa persetujuan dapat melanggar peraturan atau undang undang terkait privasi
	TH042	Masuk ke fasilitas tanpa izin	Penyusup dapat memperoleh akses dan memungkinkan pencurian atau perusakan sistem elektronik
	TH043	Penggunaan perangkat tanpa izin	Penggunaan perangkat perusahaan untuk aktivitas yang tidak sah dapat mengekspos jaringan terhadap risiko
	TH044	Penggunaan perangkat yang tidak benar	Mis konfigurasi perangkat dapat menyebabkan kerentanan keamanan
	TH045	Merusak perangkat atau media	Kerusakan media penyimpanan dapat menyebabkan hilangnya data dan biaya pemulihan
	TH046	Pembajakan perangkat lunak	Perangkat lunak ilegal dapat menyebabkan kerentanan pada sistem elektronik dan kemungkinan pelanggaran hukum.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH047	Penggunaan perangkat lunak palsu atau bajakan	Perangkat lunak palsu dengan malware yang terinstal dapat membahayakan keamanan sistem
	TH048	Kerusakan data (Corruption of data)	Kerusakan data dapat memengaruhi pengambilan keputusan dan operasi
	TH049	Pengolahan data ilegal	Pengolahan data yang tidak sah dapat menyebabkan denda karna melanggar hukum dan merusak reputasi organisasi
	TH050	Mengirim atau menyebarkan malware	Malware dapat menyebar melalui jaringan melalui komunikasi, menyebabkan infeksi yang luas ke banyak sistem elektronik pada organisasi
	TH051	Pendeteksian posisi	Lokasi perangkat yang terdeteksi secara tidak sah dapat digunakan untuk serangan terarah atau pengawasan.
Gangguan Fungsi atau Layanan	TH052	Kesalahan penggunaan	Penonaktifan firewall yang tidak disengaja dapat menyebabkan akses yang tidak terfilter dan potensi akses tidak sah pada jaringan.
	TH053	Penyalahgunaan hak atau izin	Penyalahgunaan akses "administrator" pada sistem elektronik dapat digunakan untuk mencuri dokumen rahasia, membahayakan integritas sistem elektronik dan melanggar kepatuhan pada peraturan yang berlaku.
	TH054	Pemalsuan hak atau izin / Akses tidak sah	Serangan phishing dapat digunakan untuk memperoleh kredensial admin, kemudian mengubah kontrol akses untuk menyebarkan malware secara internal.
	TH055	Penolakan tindakan	Pembaruan keamanan yang tidak sengaja diblokir secara otomatis oleh sistem dapat membuat sistem rentan terhadap eksploitasi
Ancaman Organisasi	TH056	Kekurangan staf	Kekurangan personel keamanan siber dapat menyebabkan sistem elektronik tidak dimonitor, sehingga pelanggaran atau serangan pada sistem elektornik tidak terdeteksi.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
	TH057	Kekurangan sumber daya	Alokasi anggaran keamanan siber yang tidak cukup dapat mengakibatkan sistem keamanan yang ketinggalan zaman, meningkatkan kerentanan terhadap malware baru dan serangan siber.
	TH058	Kegagalan penyedia layanan	Gangguan layanan cloud dapat mengganggu akses ke data dan layanan penting bagi banyak klien
	TH059	Pelanggaran hukum atau peraturan	Ketidakpatuhan terhadap regulasi yang dapat menyebabkan sanksi hukum dan hilangnya kepercayaan pelanggan.
	TH060	Kurangnya kesiapan	Organisasi yang tidak melakukan penilaian keamanan siber tidak akan memahami postur keamanan mereka sendiri (misalnya, tidak terimplementasinya kontrol yang cukup untuk mengurangi risiko).
Ancaman siber pada supply chain			
Pemalsuan	TH061	Barang palsu disisipkan ke dalam rantai pasokan	Perangkat keras palsu yang ditemukan pada sistem elektronik dapat menyebabkan potensi kebocoran data.
Malicious Insiders	TH062	Pencurian Kekayaan Intelektual (Intellectual Property)	Karyawan yang tidak bertanggung jawab dapat memanfaatkan aksesnya ke database untuk mencuri informasi dan menjualnya ke pesaing, mengakibatkan kerugian finansial dan hilangnya *competitive advantage* yang signifikan.
Intelijen Asing	TH063	Penyisipan Perangkat Lunak Jahat	Malicious code yang tertanam dalam sistem elektronik dapat membahayakan sistem operasional di perusahaan utilitas.
Industrial Espionage/Cyber Criminals	TH064	Pengintaian Industri (Industrial Espionage) atau Kehilangan Kekayaan Intelektual	Informasi sensitif yang bocor secara online mungkin terjadi dikarenakan serangan phishing yang menargetkan level eksekutif organisasi.
Organize Cyber Criminals	TH065	Ransomware menyebabkan gangguan proses Produksi kritis	Serangan ransomware dapat mengganggu sistem kontrol dan akses data di organisasi, menghentikan operasi dan berisiko menyebabkan gangguan luas.

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
Legal/Regulatory	TH066	Komplikasi Hukum atau Peraturan berdampak pada ketersediaan produk atau layanan yang disediakan oleh Key Supplier	Ketidakpatuhan terhadap peraturan perlindungan data yang baru dapat mengakibatkan denda besar.
Resiko Ekonomi	TH067	Kegagalan bisnis key supplier menyebabkan gangguan rantai pasokan	Kegagalan vendor pada sistem penting dapat menyebabkan gangguan dalam operasional.
Gangguan Pasokan	TH068	Kekurangan bahan baku	Kekurangan bahan baku logam dapat memperlambat produksi dan berdampak pada jadwal pengiriman.
Bencana	TH069	Geopolitik atau bencana alam menyebabkan gangguan rantai pasokan	Gempa bumi yang parah dapat merusak pusat data, menyebabkan gangguan layanan yang signifikan.
Kegagalan Perangkat Keras	TH070	Perencanaan kapasitas yang tidak memadai menyebabkan pemadaman di platform cloud	Gangguan pada cloud dapat mengganggu layanan dan operasional.
Negligent Insiders	TH071	Kesalahan konfigurasi menyebabkan paparan data	Database yang dikonfigurasi salah dapat mengekspos data pelanggan, menyebabkan pelanggaran undang-undang privasi.
Ancaman Keamanan sistem OT			
Gangguan atas kontrol (Interferensi Kontrol)	TH072	Penolakan kendali (Denial of control)	Sistem yang beroperasi tanpa kendali dapat menyebabkan insiden keselamatan, penghentian produksi, atau kerusakan peralatan.
	TH073	Manipulasi kendali (Manipulation of control)	Kegagalan peralatan, insiden lingkungan, atau penghentian operasional akibat perubahan kontrol yang tidak sah dapat mengganggu operasi

Jenis Ancaman	ID Ancaman	Peristiwa Ancaman	Peristiwa Risiko
Penipuan dan Kesalahan Informasi	TH074	Pesan palsu (Spoofed reporting message)	Tanggapan yang tertunda atau salah terhadap masalah sistem dapat menyebabkan operasi yang tidak efisien atau berhentinya operasional pada sistem.
Pelanggaran dan Pencurian Data	TH075	Pencurian informasi operasional	Eksposur data operasional sensitif dapat menyebabkan spionase, kerugian kompetitif, atau serangan siber di masa depan.
Penonaktifan Keamanan	TH076	Kehilangan keamanan	Peningkatan risiko kecelakaan atau bahaya akibat mekanisme keselamatan yang hilang/ terganggu dapat mengakibatkan hilangnya nyawa.
Kehilangan Integritas dan Ketersediaan Sistem	TH077	Kehilangan ketersediaan	downtime pada sistem, penundaan produksi, atau kehilangan data dapat menyebabkan kerugian finansial dan gangguan operasional.

BADAN SIBER
DAN SANDI
NEGARA

DIREKTORAT KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI

DEPUTI BIDANG STRATEGI DAN KEBIJAKAN KEAMANAN SIBER DAN SANDI

Jln. Raya Muchtar No. 70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok, 16518
Telepon (021) 77973360, Faximile (021) 78844104 Website: https://www.bssn.go.id
E-mail: humas@bssn.go.id