



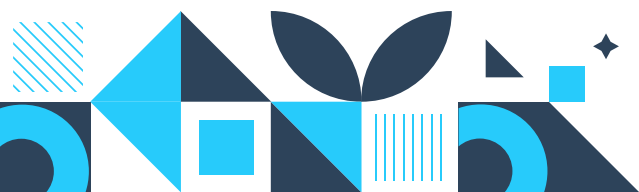
**BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA**

GARDA

GUARDING AWARENESS AND RESILIENCE IN DIGITAL ARCHIPELAGO



INDEKS KEMATANGAN BUDAYA KEAMANAN SIBER 2025



**DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI
DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI**



**BADAN SIBER
DAN SANDI NEGARA**

INDEKS KEMATANGAN BUDAYA KEAMANAN SIBER INDONESIA 2025



TIM PENYUSUN



INDEKS KEMATANGAN
BUDAYA KEAMANAN SIBER
INDONESIA **TAHUN 2025**

PENGARAH

Deputi Bidang Operasi Keamanan Siber dan Sandi

Mayjen TNI Bondan Widiawan, S.Kom., M.Si.

PENANGGUNG JAWAB

Direktur Operasi Keamanan dan Pengendalian Informasi

Satryo Suryantoro, S.Sos.

KOORDINATOR

Nurul Sugiarti, S.E., M.M.

PENULIS

Indy Rahmadhona, S.ST., M.M.

Dhea Septi Kurnia Dati, S.Tr.Kom.

Muhammad Syihaab Al-Faaruuq, S.Tr.Kom.

Shalihati Mutiara Rejki, S.Tr.Kom.

Assoc. Prof. Dr. Hendra Kaprisma, S.Hum.

Assoc. Prof. Dr. Devie Rahmawati, CICS

Dr. Nurita Andayani, M.Si.

DESAINER GRAFIK, SAMPUL, DAN TATA LETAK

Muhammad Syihaab Al-Faaruuq, S.Tr.Kom.

PENERBIT

DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI

DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI

BADAN SIBER DAN SANDI NEGARA

Jl. Harsono RM 70 Ragunan, Pasar Minggu, Jakarta Selatan, 12550

Telp. +62 21 780 5814

Fax. +62 21 7884 4104

UKURAN :

E-ISBN :

ISBN :

CETAKAN PERTAMA: JANUARI 2026

Hak Penerbitan ©2026 Badan Siber dan Sandi Negara

Dilarang mengutip dan memperbanyak tanpa izin tertulis dari penerbit, sebagian atau seluruhnya dalam bentuk apa pun, baik cetak, *photoprint*, *microfilm*, dan sebagainya.



KATA PENGANTAR

Puji dan syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya Buku Laporan Indeks Kematangan Budaya Keamanan Siber Indonesia Tahun 2025 dapat disusun dan diterbitkan. Buku ini merupakan wujud komitmen Badan Siber dan Sandi Negara dalam menyediakan rujukan berbasis data dan analisis yang komprehensif mengenai kondisi budaya keamanan siber masyarakat Indonesia.

Perkembangan teknologi digital yang semakin pesat telah menjadikan ruang siber sebagai bagian yang tidak terpisahkan dari kehidupan sosial, ekonomi, dan pemerintahan. Seiring dengan meningkatnya pemanfaatan teknologi digital, tantangan keamanan siber juga mengalami perkembangan yang signifikan, baik dari sisi teknis maupun non-teknis. Berbagai peristiwa dan dinamika di ruang siber menunjukkan bahwa aspek perilaku, kesadaran, dan kebiasaan pengguna memegang peranan penting dalam menentukan tingkat keamanan siber secara keseluruhan.

Buku ini disusun untuk memberikan gambaran yang utuh mengenai tingkat kematangan budaya keamanan siber masyarakat Indonesia, yang diukur melalui Indeks Kematangan Budaya Keamanan Siber. Indeks ini dirancang sebagai ukuran komposit yang mengintegrasikan beberapa dimensi pengukuran, mencakup pengetahuan, sikap, perilaku, serta praktik keamanan siber yang diterapkan dalam aktivitas digital sehari-hari. Melalui pendekatan tersebut, buku ini tidak hanya menyajikan angka indeks, tetapi juga menjelaskan makna, konteks, dan implikasi dari hasil pengukuran yang diperoleh.

Penyusunan buku Indeks Kematangan Budaya Keamanan Siber ini dimaksudkan sebagai sarana dokumentasi dan diseminasi hasil pengukuran nasional, sekaligus sebagai referensi bagi para pemangku kepentingan dalam memahami kondisi aktual budaya keamanan siber di Indonesia. Informasi dan analisis yang disajikan diharapkan dapat mendukung proses perumusan kebijakan, perencanaan program literasi dan edukasi, serta penyusunan intervensi keamanan siber yang lebih terarah, terukur, dan berkelanjutan.

KATA PENGANTAR

Selain itu, buku ini juga diharapkan dapat menjadi media pembelajaran bersama bagi masyarakat luas mengenai pentingnya membangun budaya keamanan siber yang kuat. Dengan meningkatnya pemahaman dan kesadaran kolektif, upaya penguatan keamanan siber nasional diharapkan dapat berjalan secara lebih efektif dan partisipatif.

Akhir kata, saya menyampaikan apresiasi dan terima kasih kepada seluruh pihak yang telah berkontribusi dalam penyusunan Buku Indeks Kematangan Budaya Keamanan Siber Indonesia Tahun 2025. Semoga buku ini dapat memberikan manfaat nyata sebagai rujukan strategis, serta menjadi landasan dalam upaya membangun ruang siber Indonesia yang aman, inklusif, dan berkelanjutan.



LETJEN TNI DRS. NUGROHO SULISTYO BUDI, M.M.
KEPALA BADAN SIBER DAN SANDI NEGARA



DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	iii
DAFTAR TABEL	iv
DAFTAR GAMBAR	v
BAB I PENDAHULUAN	1
BAB II KERANGKA KONSEPTUAL	6
BAB III METODOLOGI	17
BAB IV ANALISIS DAN DISKUSI	41
BAB V PEMBAHASAN STRATEGI NASIONAL	85
BAB VI REKOMENDASI	90
DAFTAR PUSTAKA	94

**DAFTAR TABEL**

Tabel 3.1 Pembobotan Dimensi IKBKS _____	19
Tabel 3.2 Normalisasi Kesadaran Keamanan Siber _____	19
Tabel 3.3 Normalisasi Peta Perilaku Pengguna Ruang Siber _____	27
Tabel 3.4 Perhitungan Peta Perilaku Pengguna Ruang Siber _____	38
Tabel 3.5 Perhitungan Indeks Kesadaran Keamanan Siber _____	38
Tabel 3.6 Perhitungan Tingkat Keberhasilan Literasi Keamanan Siber _____	39
Tabel 4.1 Peringkat Indeks dan Predikat IKBKS _____	42
Tabel 4.2 Skor Dimensi Per Provinsi _____	44
Tabel 4.3 Nilai IKBKS Provinsi Aceh _____	47
Tabel 4.4 Nilai IKBKS Provinsi Bali _____	48
Tabel 4.5 Nilai IKBKS Provinsi Banten _____	49
Tabel 4.6 Nilai IKBKS Provinsi Bengkulu _____	50
Tabel 4.7 Nilai IKBKS Provinsi Daerah Istimewa Yogyakarta _____	51
Tabel 4.8 Nilai IKBKS Provinsi DKI Jakarta _____	52
Tabel 4.9 Nilai IKBKS Provinsi Gorontalo _____	53
Tabel 4.10 Nilai IKBKS Provinsi Jambi _____	54

**DAFTAR TABEL**

Tabel 4.11 Nilai IKBKS Provinsi Jawa Barat	55
Tabel 4.12 Nilai IKBKS Provinsi Jawa Tengah	56
Tabel 4.13 Nilai IKBKS Provinsi Jawa Timur	57
Tabel 4.14 Nilai IKBKS Provinsi Kalimantan Barat	58
Tabel 4.15 Nilai IKBKS Provinsi Kalimantan Selatan	59
Tabel 4.16 Nilai IKBKS Provinsi Kalimantan Tengah	60
Tabel 4.17 Nilai IKBKS Provinsi Kalimantan Timur	61
Tabel 4.18 Nilai IKBKS Provinsi Kalimantan Utara	62
Tabel 4.19 Nilai IKBKS Provinsi Kepulauan Bangka Belitung	63
Tabel 4.20 Nilai IKBKS Provinsi Kepulauan Riau	64
Tabel 4.21 Nilai IKBKS Provinsi Lampung	65
Tabel 4.22 Nilai IKBKS Provinsi Maluku	66
Tabel 4.23 Nilai IKBKS Provinsi Maluku Utara	67
Tabel 4.24 Nilai IKBKS Provinsi Nusa Tenggara Barat	68
Tabel 4.25 Nilai IKBKS Provinsi Nusa Tenggara Timur	69
Tabel 4.26 Nilai IKBKS Provinsi Papua	70

**DAFTAR TABEL**

Tabel 4.27 Nilai IKBKS Provinsi Papua Barat	71
Tabel 4.28 Nilai IKBKS Provinsi Papua Barat Daya	72
Tabel 4.29 Nilai IKBKS Provinsi Papua Pegunungan	73
Tabel 4.30 Nilai IKBKS Provinsi Papua Selatan	74
Tabel 4.31 Nilai IKBKS Provinsi Papua Tengah	75
Tabel 4.32 Nilai IKBKS Provinsi Riau	76
Tabel 4.33 Nilai IKBKS Provinsi Sulawesi Barat	77
Tabel 4.34 Nilai IKBKS Provinsi Sulawesi Selatan	78
Tabel 4.35 Nilai IKBKS Provinsi Sulawesi Tengah	79
Tabel 4.36 Nilai IKBKS Provinsi Sulawesi Tenggara	80
Tabel 4.37 Nilai IKBKS Provinsi Sulawesi Utara	81
Tabel 4.38 Nilai IKBKS Provinsi Sumatra Barat	82
Tabel 4.23 Nilai IKBKS Provinsi Sumatra Selatan	83
Tabel 4.24 Nilai IKBKS Provinsi Sumatra Utara	84



DAFTAR GAMBAR

Gambar 3.1 Tingkat Kematangan Budaya Keamanan Siber

40



BAB I

PENDAHULUAN

AWARENESS

kesadaran adalah awal dari kematangan

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah mendorong terjadinya transformasi digital secara luas dalam berbagai aspek kehidupan masyarakat. Ruang siber tidak hanya menjadi medium pendukung aktivitas, tetapi telah bertransformasi menjadi ruang utama bagi interaksi sosial, ekonomi, pendidikan, dan penyelenggaraan pemerintahan. Seiring dengan peningkatan intensitas pemanfaatan ruang digital tersebut, risiko keamanan siber juga mengalami eskalasi, baik dari sisi kompleksitas maupun dampaknya terhadap individu, organisasi, dan negara (International Telecommunication Union, 2021; Internet Society, 2019).

Berbagai studi dan praktik menunjukkan bahwa sebagian besar insiden keamanan siber tidak semata-mata disebabkan oleh kelemahan teknologi, melainkan dipicu oleh perilaku pengguna yang tidak aman, rendahnya kesadaran terhadap risiko digital, serta lemahnya kepatuhan terhadap prinsip-prinsip dasar keamanan siber. Fenomena seperti penggunaan kata sandi yang lemah, ketidakpedulian terhadap perlindungan data pribadi, serta mudahnya pengguna terpengaruh oleh manipulasi informasi menjadi indikasi bahwa faktor manusia (*human factor*) merupakan elemen paling krusial sekaligus paling rentan dalam ekosistem keamanan siber (Bulgurcu et al., 2010; Parsons et al., 2014; KnowBe4, 2023).

Dalam konteks tersebut, keamanan siber perlu dipahami sebagai suatu konstruksi sosial dan budaya, bukan sekadar persoalan teknis. Budaya keamanan siber mencerminkan seperangkat nilai, sikap, pengetahuan, dan praktik yang membentuk cara individu dan kelompok berperilaku di ruang digital. Tanpa budaya keamanan siber yang memadai, penguatan infrastruktur dan sistem pengamanan teknologi tidak akan memberikan perlindungan yang optimal, karena perilaku pengguna yang berisiko dapat mengabaikan atau bahkan meniadakan efektivitas kontrol teknis yang telah diterapkan (Da Veiga & Martins, 2015a; Da Veiga & Martins, 2015b; Alshaikh, 2020).

Urgensi pengukuran budaya keamanan siber semakin mengemuka dalam konteks perumusan kebijakan nasional yang berbasis data (*data-based policy*). Hingga saat ini, upaya peningkatan keamanan siber sering kali berfokus pada aspek teknologi dan regulasi, sementara kondisi empiris terkait tingkat kesadaran dan perilaku masyarakat di ruang siber belum sepenuhnya terpetakan secara sistematis. Ketiadaan data yang terukur mengenai budaya keamanan siber berpotensi menyebabkan kebijakan peningkatan budaya keamanan siber bersifat parsial, tidak tepat sasaran, serta sulit dievaluasi efektivitasnya (Fertig & Schütz, 2020; Rizal & Setiawan, 2024; Rohan et al., 2023).

Sebagai lembaga yang memiliki tugas pemerintahan dalam penyelenggaraan keamanan siber nasional, Badan Siber dan Sandi Negara memandang pengukuran budaya keamanan siber

sebagai langkah fundamental untuk memperoleh gambaran objektif mengenai tingkat kematangan kesadaran dan perilaku masyarakat dalam menghadapi ancaman siber. Pengukuran ini berfungsi sebagai instrumen untuk mengidentifikasi pola perilaku berisiko, kelompok masyarakat yang rentan, serta kesenjangan antara pengetahuan, sikap, dan praktik keamanan siber. Pendekatan pengukuran ini sejalan dengan arah kebijakan nasional keamanan siber serta kerangka penguatan ketahanan siber nasional yang tertuang dalam rencana strategis dan rencana aksi nasional BSSN (BSSN, 2020; BSSN, 2024; BSSN, 2025).

Lebih lanjut, hasil pengukuran budaya keamanan siber memiliki peran strategis dalam mendukung pendekatan berbasis risiko (risk-based approach) dan berorientasi manusia (human-centric cybersecurity). Data empiris yang dihasilkan dapat digunakan untuk mengidentifikasi pola perilaku berisiko, kelompok masyarakat yang rentan, serta kesenjangan antara pengetahuan, sikap, dan praktik keamanan siber. Pendekatan ini sejalan dengan teori perilaku terencana yang menekankan keterkaitan antara sikap, norma subjektif, dan kontrol perilaku dalam membentuk tindakan individu (Ajzen, 1991; National Cyber Security Centre, 2025).

Dengan demikian, pengukuran budaya keamanan siber tidak hanya berfungsi sebagai alat evaluasi, tetapi juga sebagai fondasi konseptual dan empiris dalam pembangunan keamanan siber nasional (Prümmer et al., 2024; Yunita & Nurdeni, 2023). Melalui pengukuran yang terstandar, berkelanjutan, dan berbasis metodologi, diharapkan dapat terwujud pemahaman yang komprehensif mengenai dinamika perilaku masyarakat di ruang siber, sekaligus menjadi dasar yang kuat bagi pengambilan kebijakan dan perencanaan program peningkatan budaya keamanan siber secara nasional.

1.2 Maksud dan Tujuan

1.2.1 Maksud

Maksud pengukuran budaya keamanan siber adalah sebagai berikut.

- a. Memperoleh gambaran empiris dan komprehensif mengenai tingkat kesadaran, sikap, dan perilaku masyarakat dalam memanfaatkan ruang siber secara aman dan bertanggung jawab.
- b. Menjadi instrumen strategis dalam mendukung penyusunan kebijakan keamanan siber yang berbasis data dan risiko sehingga intervensi yang dirancang tidak hanya berfokus pada aspek teknis, tetapi juga mempertimbangkan dimensi sosial dan budaya dalam pemanfaatan ruang siber.

1.2.2 Tujuan

Tujuan pengukuran budaya keamanan siber adalah sebagai berikut.

- a. Menyediakan ukuran untuk menilai tingkat perkembangan, pengetahuan, sikap, perilaku, serta praktik keamanan siber yang diterapkan masyarakat Indonesia.
- b. Menyediakan gambaran pola perilaku masyarakat Indonesia di ruang siber berupa data mengenai media penyebaran konten, jenis konten, dan tindakan pengguna saat menemukan konten.
- c. Menyediakan ukuran kondisi keamanan siber teknis dan keamanan siber sosial yang telah menjadi bagian dari perilaku dan kebiasaan sehari-hari masyarakat Indonesia.
- d. Menyediakan nilai yang menggambarkan keberhasilan dan efektivitas intervensi organisasi melalui kampanye dan literasi keamanan siber yang diberikan kepada masyarakat Indonesia.

1.3 Ruang Lingkup

Ruang lingkup pengukuran Indeks Kematangan Budaya Keamanan Siber mencakup batasan wilayah, subjek, dan aspek pengukuran yang dirancang untuk memberikan gambaran komprehensif mengenai kondisi budaya keamanan siber masyarakat Indonesia secara nasional. Adapun ruang lingkup pengukuran ini meliputi hal berikut ini.

- a. Cakupan Wilayah
Pengukuran dilaksanakan secara nasional dengan menjangkau seluruh 38 provinsi di Indonesia pada tahun 2025, guna memastikan representativitas kondisi budaya keamanan siber di berbagai karakteristik wilayah, baik perkotaan maupun perdesaan.
- b. Subjek Pengukuran
Subjek pengukuran adalah masyarakat Indonesia sebagai pengguna ruang siber, tanpa membedakan latar belakang demografis tertentu, sehingga hasil pengukuran mencerminkan kondisi umum budaya keamanan siber masyarakat secara agregat.
- c. Objek Pengukuran
Objek pengukuran difokuskan pada tingkat kematangan budaya keamanan siber, yang mencerminkan perkembangan pengetahuan, sikap, perilaku, serta praktik keamanan siber yang diterapkan oleh masyarakat dalam aktivitas digital sehari-hari.

d. Dimensi Pengukuran

Pengukuran dilakukan menggunakan tiga dimensi pengukuran yang digunakan untuk menilai tingkat perkembangan, pengetahuan, sikap, perilaku, serta praktik keamanan siber yang diterapkan masyarakat Indonesia.

e. Waktu Pelaksanaan

Pengukuran dilaksanakan pada tahun 2025 sebagai baseline nasional gambaran kondisi budaya keamanan siber masyarakat Indonesia serta sebagai dasar perbandingan pada pengukuran periode selanjutnya.

f. Dasar Hukum

- 1) UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP);
- 2) Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber dan Manajemen Krisis Siber (SKSN);
- 3) Perpres No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV);
- 4) Perpres No. 132 Tahun 2022 tentang Arsitektur SPBE Nasional;
- 5) Perpres No. 95 Tahun 2018 tentang SPBE;
- 6) Permen PANRB No. 95 Tahun 2020 tentang Penerapan SPBE;
- 7) Permen Kominfo No. 4 Tahun 2016 tentang SMPI bagi PSTE;
- 8) Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber 2024-2028;
- 9) Peraturan BSSN Nomor 3 Tahun 2021 tentang Penyelenggaraan Literasi Media dan Literasi Keamanan Siber;
- 10) Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
- 11) Peraturan Kepala BSSN Nomor 4 Tahun 2025 tentang Pengukuran Kematangan Budaya Keamanan Siber; dan
- 12) Rencana Strategis Direktorat Operasi Keamanan dan Pengendalian Informasi Tahun 2025 s.d. 2029.

BAB II

KERANGKA KONSEPTUAL

UNDERSTANDING
mulai memahami struktur dan pola

2.1 Transformasi Ruang Siber dan Urgensi Keamanan Digital Publik

Transformasi digital dalam pelayanan publik telah mengubah ruang siber mengambil peran sebagai infrastruktur sosial yang sama pentingnya dengan jalan raya atau jaringan listrik. Administrasi kependudukan, jaminan kesehatan, jaminan sosial, pendidikan, perpajakan, bantuan sosial, hingga berbagai layanan kepolisian semakin banyak bergantung pada aplikasi daring, pusat data nasional, dan ekosistem identitas digital. Laporan Global Cybersecurity Index (GCI) dari International Telecommunication Union menunjukkan bahwa hampir semua negara sedang memperluas layanan publik digital, tetapi kapasitas tata kelola dan perlindungan keamanannya berkembang tidak secepat laju digitalisasi tersebut (International Telecommunication Union, 2021). Studi mengenai posisi Indonesia dalam GCI menegaskan bahwa ancaman terhadap layanan publik tidak hanya bersifat teknis, melainkan juga berkaitan dengan koordinasi antaraktor, kapasitas SDM, dan budaya keamanan di lembaga-lembaga negara (Cloramidine & Badaruddin, 2023).

Berbagai insiden global, seperti contohnya serangan ransomware WannaCry pada tahun 2017 yang melumpuhkan layanan kesehatan di Inggris hingga gangguan pada jaringan pipa bahan bakar di Amerika Serikat. Kejadian ini memperlihatkan bahwa gangguan keamanan siber dapat segera berubah menjadi krisis layanan publik. Dalam konteks Indonesia, kebocoran data identitas, data kesehatan, dan gangguan pada infrastruktur pusat data menunjukkan pola risiko yang serupa: ketika sistem digital terganggu, hak warga atas pelayanan menjadi terancam dan kepercayaan publik pada negara ikut terkikis. Pendekatan keamanan yang hanya menekankan aspek teknologi jelas tidak memadai untuk menjawab kompleksitas risiko ini. Identity breach adalah serangan peniruan identitas berbasis identitas di mana peretas mengeksploitasi kerentanan untuk memperoleh informasi identitas pribadi (PII), informasi kontak, nomor kartu kredit, dan kredensial penting seperti kata sandi dan nama pengguna untuk melakukan pencurian identitas, penipuan identitas, atau kejahatan siber lainnya tanpa sepengetahuan korban UpGuard. Pelanggaran data terjadi ketika organisasi mengalami kebocoran atau kehilangan informasi pribadi pelanggan yang tidak sah (Goldsmith & Hutchings, 2025).

Sejumlah studi empiris dan laporan industri menggambarkan bahwa faktor manusia tetap menjadi titik lemah utama di balik banyak insiden tersebut. Laporan “Oh, Behave!” yang menganalisis sikap dan perilaku keamanan siber publik di Inggris dan Amerika Serikat menemukan adanya kesenjangan konsisten antara pengetahuan dan praktik aman sehari-hari —misalnya dalam pengelolaan kata sandi, pemutakhiran perangkat, dan kewaspadaan terhadap phishing (National Cyber Security Alliance & CybSafe, 2021). Laporan KnowBe4 menunjukkan bahwa lebih dari sepertiga pegawai yang belum pernah mengikuti pelatihan keamanan gagal mengenali email phishing, sementara pelatihan yang sistematis dapat menurunkan tingkat kegagalan ini secara drastis dalam satu tahun (KnowBe4, 2023).

Temuan-temuan ini menegaskan bahwa keamanan digital publik tidak dapat dipahami semata-mata sebagai persoalan teknologi, melainkan sebagai persoalan perilaku dan budaya organisasi.

Dimensi lain yang tidak kalah penting adalah krisis kepercayaan (*trust deficit*) terhadap tata kelola data dan ruang digital. Sejumlah kajian menunjukkan adanya penurunan kepercayaan publik terhadap institusi, media, dan platform digital, yang berdampak pada tingkat penerimaan masyarakat terhadap kebijakan berbasis data dan inisiatif keamanan siber (Flew, 2021; Internet Society, 2019). Studi tentang sikap publik terhadap pemanfaatan data administratif menegaskan bahwa dukungan warga sangat bergantung pada persepsi manfaat publik, perlindungan privasi, dan transparansi penggunaan data (Waind, 2020). Di sisi lain, literatur tentang surveilans digital menunjukkan bahwa praktik pengawasan yang tidak akuntabel, baik oleh negara maupun korporasi, dapat melahirkan rasa ketidakbebasan digital dan memperkuat kecurigaan bahwa kebijakan keamanan siber adalah alasan untuk memperluas kontrol atau pengawasan (Lyon, 2017; Małagocka, 2024).

Dalam lanskap seperti ini, masyarakat mudah curiga bahwa survei atau pemetaan keamanan siber justru akan menambah lapisan pengawasan, terutama bila tujuan dan tata kelola datanya tidak dikomunikasikan dengan jelas. Karena itu, kerangka keamanan digital publik yang berorientasi pada hak, sebagaimana didorong dalam agenda rights-oriented digital transformation, menekankan perlunya menempatkan perlindungan data pribadi, akuntabilitas, dan partisipasi publik sebagai prinsip inti (OECD, 2024).

Dari perspektif kebijakan, implikasinya jelas yaitu untuk menjamin keberlanjutan layanan publik digital, negara membutuhkan instrumen yang tidak hanya memetakan kesiapan teknis dan kelembagaan, tetapi juga mengukur sejauh mana budaya keamanan siber sudah terinternalisasi di kalangan aparatur dan warga untuk mendapatkan kembali trust atau keyakinan publik di dunia digital. Di sinilah kebutuhan akan sebuah Indeks kematangan Budaya Keamanan Siber (IKBKS) yang secara spesifik berfokus pada dimensi manusia dalam keamanan digital publik menjadi relevan dan aktual.

2.2 Budaya Keamanan Siber: Dari Kepatuhan Teknis ke Orientasi Manusia

Literatur keamanan informasi generasi awal banyak berfokus pada kontrol teknis, seperti enkripsi, firewall, dan prosedur akses. Ada juga kerangka manajemen risiko berbasis standar, misalnya ISO/IEC 27001. Namun, sejak lebih dari satu dekade terakhir, muncul kesadaran luas bahwa aturan dan teknologi tidak akan efektif bila tidak didukung oleh nilai, norma, dan kebiasaan kerja sehari-hari yang konsisten di dalam organisasi. Perhatian inilah yang melahirkan konsep budaya keamanan siber (*cyber security culture*).

Da Veiga dan Martins mendefinisikan budaya keamanan informasi sebagai seperangkat nilai, asumsi, dan pola perilaku bersama yang membentuk bagaimana anggota organisasi memandang dan mempraktikkan keamanan informasi dalam pekerjaan mereka (Da Veiga & Martins, 2015a; 2015b). Sedangkan Alshaikh (2020) mendefinisikannya sebagai perilaku manusia dalam konteks organisasi untuk melindungi informasi yang diproses oleh organisasi melalui kepatuhan terhadap kebijakan keamanan informasi dan pemahaman tentang cara mengimplementasikan persyaratan dengan cara yang hati-hati dan penuh perhatian, tertanam melalui komunikasi rutin, kesadaran, pelatihan, dan inisiatif pendidikan. Dalam kerangka ini, kepatuhan terhadap kebijakan bukan hanya hasil dari pengawasan atau sanksi, tetapi juga dari keyakinan bersama bahwa keamanan adalah bagian dari profesionalisme dan tanggung jawab moral terhadap pemangku kepentingan. Studi mereka menunjukkan bahwa budaya dapat diukur secara sistematis dan ditingkatkan melalui kombinasi pemantauan, umpan balik, dan tindakan perbaikan yang berkelanjutan (Da Veiga & Martins, 2015a).

National Cyber Security Centre (NCSC) di Inggris mengembangkan prinsip-prinsip budaya keamanan siber yang menekankan bahwa keamanan harus dipahami sebagai enabler, bukan penghambat organisasi, bahwa orang perlu merasa aman secara psikologis untuk melaporkan insiden, serta bahwa aturan harus realistis dan selaras dengan cara orang benar-benar bekerja (National Cyber Security Centre, 2025). Prinsip-prinsip ini berangkat dari temuan empiris bahwa apabila kebijakan keamanan terasa terlalu rumit atau menghambat kerja, pegawai cenderung mencari jalan pintas yang justru melemahkan keamanan. Maka dalam pemahaman konteks buku ini, Budaya keamanan siber menjadi cara pandang yang lebih makro, yaitu untuk sebuah negara.

Ketika konsep budaya keamanan siber dibawa ke konteks negara seperti Indonesia, yang majemuk secara etnis, agama, dan memiliki tradisi moral yang kuat, muncul tantangan sosiokultural yang tidak boleh diabaikan. Sebagian wacana keamanan digital, termasuk dalam praktik kebijakan di berbagai negara, cenderung menyandingkan kategori ancaman yang memiliki dasar hukum jelas, seperti eksploitasi seksual anak, penipuan, ujaran kebencian berbasis SARA, atau penyebaran data pribadi tanpa izin, dengan kategori yang lebih bersifat moral dan identitas, misalnya pergeseran nilai, ajaran sesat, atau ekspresi orientasi seksual dan keyakinan tertentu.

Penelitian di tingkat global menunjukkan bahwa kebijakan dan regulasi keamanan siber yang tidak berbasis HAM dapat dengan mudah bergeser menjadi instrumen kontrol sosial terhadap kelompok rentan. Penelitian dari Brown dan Pytlak (2020) serta Millar et al. (2021) menunjukkan bagaimana kerangka keamanan siber yang mengklaim netralitas justru abai terhadap risiko spesifik yang dialami perempuan dan kelompok marginal, termasuk kekerasan berbasis gender daring. Laporan Global Partners Digital dan ARTICLE 19 (2024) mendokumentasikan kasus-kasus di Afrika, Timur Tengah, dan Turki di mana undang-undang

kejahatan siber dipakai untuk membungkam oposisi dan kelompok minoritas. Human Rights Watch (2024a) dan Electronic Frontier Foundation (2023) memperlihatkan pola serupa: regulasi dunia maya, termasuk pasal kejahatan siber dan norma kesusilaan, digunakan untuk mengkriminalisasi kelompok LGBT dan pembela HAM di berbagai negara.

Dalam perspektif ini, menyusun instrumen pengukuran budaya keamanan siber—termasuk IKBKS, tanpa sensitivitas HAM berisiko memperkuat bias normatif tertentu. Jika butir-butir survei menyimbolkan kelompok atau ekspresi tertentu (misalnya identitas gender, orientasi seksual, atau keyakinan agama minoritas) sebagai “ancaman”, indeks dapat secara tidak sengaja melegitimasi pandangan diskriminatif. Selain itu, fokus yang terlalu besar pada kategori moral yang kontroversial dapat mengalihkan perhatian dari ancaman digital yang secara langsung menimbulkan kerugian nyata, seperti penipuan, eksploitasi anak, kebocoran data, dan kekerasan berbasis gender daring.

Bagi IKBKS, implikasinya dua lapis. Pertama, dimensi budaya keamanan perlu dirumuskan secara rights-oriented, dengan menjadikan perlindungan martabat dan keselamatan warga, bukan terkait penyeragaman moral, tapi sebagai titik tolak pemahaman. Hal ini sejalan dengan dorongan untuk mengintegrasikan prinsip HAM ke dalam seluruh siklus kebijakan keamanan siber, sebagaimana diusulkan oleh Pavlova (2025) dalam analisisnya terhadap Konvensi Kejahatan Siber PBB. Kedua, proses penyusunan dan revisi instrumen perlu melibatkan pemangku kepentingan yang beragam: lembaga HAM, komunitas digital, perwakilan kelompok rentan, serta komunitas keagamaan dan adat, sehingga dimensi budaya yang diukur tidak hanya mencerminkan perspektif arus utama.

Berbagai studi kasus menunjukkan bahwa organisasi yang berhasil membangun budaya keamanan yang positif memiliki beberapa ciri: pimpinan secara aktif memberi teladan perilaku aman; pelatihan keamanan terintegrasi dalam siklus kerja, bukan sekadar kegiatan tahunan; mekanisme pelaporan insiden dibuat sederhana dan tanpa menyalahkan korban; dan penghargaan diberikan kepada perilaku yang proaktif melindungi data (Da Veiga & Martins, 2015a; National Cyber Security Centre, 2025).

Dalam konteks layanan publik, konsep budaya keamanan siber menjadi semakin penting karena aparatur negara tidak hanya mengelola aset digital organisasi, tetapi juga data warga dan infrastruktur layanan esensial. Budaya keamanan yang lemah di lembaga publik dapat berujung pada kebocoran data berskala masif, disinformasi, atau lumpuhnya layanan vital. Oleh karena itu, IKBKS dirancang untuk menangkap dimensi budaya ini secara lebih sistematis—sehingga pemerintah dapat mengidentifikasi area yang sudah kuat ataupun celah yang perlu diperbaiki.

2.3 Indeks dan Model Kematangan Keamanan Siber di Sektor Publik

Pengukuran keamanan siber pada level negara ataupun organisasi kerap dilakukan melalui indeks dan model kematangan. Pendekatan ini memungkinkan pengambil kebijakan untuk memperoleh gambaran menyeluruh, membandingkan kinerja antarunit atau antarnegara, serta memantau kemajuan dari waktu ke waktu. Dalam tradisi manajemen, model kematangan, mulai dari Capability Maturity Model (CMM) hingga berbagai cybersecurity maturity model, pada dasarnya menggambarkan perkembangan kapasitas dari tahap yang tidak terstruktur (ad hoc) menuju tahap yang terdokumentasi, terukur, dan terus diperbaiki (optimized).

Di tingkat global, Global Cybersecurity Index (GCI) yang dikembangkan International Telecommunication Union menilai kapasitas keamanan siber negara berdasarkan lima pilar antara lain kebijakan, kerangka hukum, kapasitas teknis, organisasi dan kerja sama, serta pembangunan kapasitas (International Telecommunication Union, 2021). Skor komposit GCI sering digunakan sebagai indikator kesiapan nasional, sekaligus bahan evaluasi perbandingan antarnegara dan rujukan bagi lembaga internasional. Analisis terhadap posisi Indonesia dalam GCI menunjukkan bahwa pilar kerja sama internasional dan penguatan kerangka regulasi relatif berkembang, namun tantangan besar masih terdapat pada aspek kapasitas sumber daya manusia, koordinasi antar lembaga, dan internalisasi praktik keamanan di berbagai sektor (Cloramidine & Badaruddin, 2023). Temuan ini mengimplikasikan bahwa peningkatan skor indeks global tidak otomatis berarti budaya keamanan yang kuat di level operasional, misalnya di unit layanan publik garis depan atau di kalangan warga pengguna layanan.

Di tingkat nasional, Badan Siber dan Sandi Negara mengembangkan Indeks Keamanan Informasi (Indeks KAMI) sebagai alat evaluasi untuk mengukur kesiapan penerapan SNI ISO/IEC 27001 di instansi pemerintah (Badan Siber dan Sandi Negara, 2020). Indeks ini menilai beberapa area, antara lain tata kelola, kerangka kebijakan, pengelolaan risiko, pengamanan teknologi, serta aspek pemulihan insiden. Versi terbaru pedoman pengisian Indeks KAMI menegaskan bahwa instrumen ini dimaksudkan sebagai evaluasi mandiri guna membantu organisasi memahami tingkat kematangan program keamanan informasinya dan merencanakan perbaikan berkelanjutan (Badan Siber dan Sandi Negara, 2025). Di sejumlah pemerintah daerah, hasil Indeks KAMI menunjukkan rentang capaian yang lebar: ada yang sudah mencapai kategori “baik”, namun tidak sedikit yang masih berada pada kategori “rendah” dan “belum layak”, terutama pada aspek kebijakan, penerapan teknis, dan pengelolaan sumber daya.

Meskipun penting, baik GCI maupun Indeks KAMI relatif lebih menekankan dimensi struktural dan teknis—misalnya keberadaan regulasi, prosedur, unit kerja, dan teknologi—dibanding dimensi budaya dan perilaku. Literatur keamanan siber menunjukkan bahwa kegagalan pada tataran perilaku pengguna tetap menjadi penyebab mayoritas insiden, seperti kebocoran kredensial, keberhasilan phishing, dan penyalahgunaan hak akses (National Cyber Security Alliance & CybSafe, 2021; KnowBe4, 2023; Rohan et al., 2023).

Dari perspektif ini, model kematangan yang hanya menginventarisasi kebijakan dan kontrol teknis berisiko memberikan gambaran “semu”, dimana secara dokumen tampak sudah baik, tetapi dalam praktik sehari-hari perilaku aman belum menjadi kebiasaan.

Selain itu, indeks dan model kematangan tidak pernah sepenuhnya netral secara politis. Cara sebuah indeks dirancang, apa yang dihitung, apa yang diabaikan, dan bagaimana bobot diberikan, akan memengaruhi bagaimana suatu organisasi, wilayah, atau negara dipersepsikan. Berbagai kajian menunjukkan bahwa instrumen hukum dan kebijakan di ranah kejahatan siber dan keamanan digital kerap dimanfaatkan untuk memperluas kontrol sosial, membungkam oposisi, atau menstigma kelompok tertentu ketika tidak berlandaskan prinsip hak asasi manusia yang kuat (Global Partners Digital & ARTICLE 19 West Africa, 2024; Pavlova, 2025). Di beberapa negara, indikator-indikator seperti ketertiban dan stabilitas bahkan dipakai untuk membenarkan pembatasan ekspresi sah di ruang digital, sementara kekerasan berbasis gender daring, peretasan terhadap pembela HAM, dan kebocoran data warga kurang mendapat perhatian (Brown & Pytlak, 2020; Human Rights Watch, 2024a).

Dalam konteks ini, IKBKS hadir sebagai instrumen yang secara eksplisit ingin memetakan kematangan budaya keamanan siber. Indeks ini bukan sekadar hadir sebagai kontrol teknis, dengan fokus pada sektor publik dan warga negara sebagai pengguna layanan digital.

Tetapi IKBKS diposisikan sebagai pelengkap GCI dan Indeks KAMI, bukan untuk menggantikan pengukuran yang sudah ada, melainkan untuk mengisi celah pada dimensi manusia dan budaya. Di satu sisi, indeks ini mengoperasionalkan dimensi kesadaran, perilaku, dan literasi/program ke dalam indikator yang terukur; di sisi lain, IKBKS perlu disadari sebagai instrumen kebijakan yang membawa konsekuensi politis: ia dapat dipakai untuk mengarahkan dukungan dan sumber daya ke wilayah yang paling rentan, tetapi juga berpotensi disalahgunakan untuk memberi label negatif pada provinsi atau kelompok tertentu jika dirancang dan dikomunikasikan tanpa kehati-hatian.

Oleh karena itu, terdapat kebutuhan untuk mengembangkan instrumen pelengkap yang secara khusus memetakan tingkat kematangan budaya keamanan siber, khususnya di sektor publik yang mengelola data dan layanan warga. IKBKS diposisikan bukan untuk menggantikan indeks yang sudah ada, melainkan mengisi celah pada dimensi manusia—bagaimana pengetahuan, sikap, dan perilaku aparaturnya dan warga terkait keamanan digital publik membentuk ekosistem keamanan secara keseluruhan.

2.4 Pengukuran Literasi dan Kesadaran Keamanan Siber

Konsep literasi dan kesadaran keamanan informasi (information security awareness, ISA) berkembang sebagai upaya untuk memahami sejauh mana individu mengenali risiko keamanan, memahami kebijakan, dan bertindak secara aman ketika berinteraksi dengan sistem digital. Lebih dalam, Bulgurcu et al. (2010) mendefinisikannya sebagai pengetahuan umum pegawai tentang keamanan informasi dan kesadarannya terhadap kebijakan keamanan informasi organisasinya, yang mengacu pada pengetahuan dan pemahaman keseluruhan karyawan tentang isu-isu potensial terkait keamanan informasi Emerald Insight. Banyak definisi modern memposisikan ISA sebagai kombinasi pengetahuan, sikap, dan perilaku (knowledge–attitude–behaviour, KAB) yang saling berkaitan (Parsons et al., 2014; Yunita & Nurdeni, 2023). Dalam model KAB, peningkatan pengetahuan diharapkan memengaruhi sikap dan pada akhirnya tercermin dalam perilaku, meskipun penelitian empiris menunjukkan bahwa hubungan ini tidak selalu linier.

Parsons et al. (2014) mengembangkan instrumen Human Aspects of Information Security Questionnaire (HAIS-Q) yang secara eksplisit mengukur tiga komponen tersebut di beberapa domain, seperti pengelolaan kata sandi, penggunaan email, aktivitas internet, dan penanganan informasi fisik. Instrumen ini menunjukkan bahwa individu dapat memiliki pengetahuan yang cukup tetapi tetap berperilaku tidak aman karena sikap yang permisif atau tekanan konteks kerja. Studi validasi menunjukkan bahwa skor HAIS-Q berkorelasi dengan kerentanan terhadap simulasi phishing dan perilaku dalam eksperimen laboratorium, menegaskan bahwa dimensi manusia dapat diukur secara sistematis dan dikaitkan dengan risiko keamanan yang nyata (Parsons et al., 2017). Temuan utama dari riset ini adalah bahwa individu dapat memiliki pengetahuan yang memadai tetapi tetap menunjukkan perilaku tidak aman ketika sikapnya permisif atau ketika tekanan konteks kerja mendorong munculnya jalan pintas.

Serangkaian tinjauan sistematis terbaru memperlihatkan bahwa mayoritas instrumen ISA yang digunakan di berbagai negara mengadopsi kerangka KAB dan mengukur kombinasi dari pengetahuan objektif, persepsi risiko, serta perilaku yang dilaporkan sendiri (self-reported behaviour). Fertig dan Schütz memetakan puluhan instrumen ISA dan menyoroti variasi yang cukup besar dalam definisi dan indikator, sehingga menyulitkan perbandingan lintas studi (Fertig & Schütz, 2020). Rohan dan kolega secara khusus menelaah skala-skala siber yang mengukur ISA dan menemukan bahwa banyak skala belum melalui uji validitas psikometrik yang memadai, terutama terkait reliabilitas jangka panjang dan validitas lintas budaya (Rohan et al., 2023).

Di tingkat Asia dan Indonesia, muncul beberapa studi yang mencoba menyesuaikan instrumen ISA dengan konteks lokal. Rizal dan Setiawan mengulas instrumen-instrumen ISA yang ada dan mengusulkan area pengukuran yang lebih terfokus, seperti dimensi kebijakan, teknologi mobile, media sosial, dan privasi (Rizal & Setiawan, 2024).

Yunita dan Nurdeni (2023) melakukan systematic literature review (SLR) dan menyimpulkan bahwa hampir semua model ISA yang kuat kembali ke tiga komponen KAB, tetapi menekankan pentingnya memasukkan konteks praktik sehari-hari pengguna media sosial dan platform publik, bukan hanya lingkungan kerja formal.

Pada ranah empiris, beberapa penelitian di Indonesia mulai mengukur ISA pegawai dan pelajar dengan memodifikasi instrumen yang ada. Permadi dan Ramli (2024) menganalisis pengukuran ISA pegawai di sebuah institusi pengelola data aparatur sipil negara dengan menggabungkan kuesioner dan simulasi phishing, dan mendapati bahwa meski pemahaman terhadap aturan formal cukup tinggi, kerentanan terhadap serangan rekayasa sosial masih signifikan. Perkasa (2024) mengukur tingkat ISA siswa SMA pascapandemi COVID-19 dan menemukan bahwa penggunaan intensif media sosial dan online learning tidak otomatis berbanding lurus dengan perilaku aman; banyak siswa masih menggunakan kata sandi lemah dan mengabaikan pengaturan privasi, meski mereka mengaku tahu risikonya. Temuan-temuan ini menguatkan argumentasi bahwa pengukuran ISA tidak cukup berhenti pada tes pengetahuan, tetapi perlu mengintegrasikan indikator perilaku dan, sejauh mungkin, data objektif.

Di luar aspek teknis pengukuran, literatur menyoroti adanya dimensi etis dan sosiokultural dalam penyusunan instrumen ISA. Yunita dan Nurdeni (2023) mengingatkan bahwa butir kuesioner yang dirancang tanpa mempertimbangkan keragaman konteks dapat mengandung nilai normatif tertentu dan berpotensi menstigma kelompok pengguna tertentu. Di tingkat global, analisis atas kebijakan kejahatan siber menunjukkan bahwa kategori “konten berbahaya” dapat diperluas secara problematik untuk memasukkan ekspresi politik, identitas gender, atau orientasi seksual yang sebenarnya dilindungi HAM (Global Partners Digital & ARTICLE 19 West Africa, 2024; Pavlova, 2025). Oleh karena itu, dalam merancang Survei Kesadaran Keamanan Siber (SKKS) sebagai bagian dari IKBKS, penting untuk memastikan bahwa kategori ancaman dan perilaku berisiko yang diukur berlandaskan kerangka hukum dan prinsip HAM yang jelas, misalnya perlindungan data pribadi, pencegahan eksploitasi anak, penipuan, dan kekerasan berbasis gender daring, serta membedakannya secara tegas dari perbedaan nilai moral dan ekspresi identitas.

Secara keseluruhan, literatur ISA memberikan beberapa pelajaran penting bagi pengembangan IKBKS. Pertama, instrumen perlu membedakan secara jelas antara pengetahuan, sikap, dan perilaku, sekaligus melihat keterkaitannya. Kedua, skala harus diuji secara psikometrik untuk konteks budaya Indonesia dan berbagai jenis organisasi publik.

Ketiga, pengukuran ISA idealnya dihubungkan dengan indikator perilaku nyata dan insiden, seperti hasil simulasi phishing atau data pelaporan insiden, agar tidak hanya menangkap persepsi, tetapi juga risiko riil yang dihadapi warga dan aparatur. Keempat, proses penyusunan butir perlu peka terhadap keragaman sosial, agama, dan identitas, sehingga IKBKS benar-benar menjadi alat untuk melindungi, bukan menstigma, warga negara di ruang digital.

2.5 Perilaku Keamanan Digital, *Cyber Hygiene*, dan Budaya Sehari-hari

Jika ISA berbicara tentang apa yang diketahui dan diyakini orang tentang keamanan, maka perilaku keamanan digital sehari-hari, atau sering disebut sebagai *cyber hygiene*. Perilaku ini menunjukkan sejauh mana pengetahuan dan sikap tersebut diwujudkan dalam praktik konkret. *Cyber hygiene* merujuk pada seperangkat kebiasaan rutin, seperti menggunakan autentikasi multifaktor, memperbarui perangkat lunak, mengelola kata sandi dengan aman, berhati-hati terhadap tautan dan lampiran mencurigakan, serta membatasi berbagi data pribadi secara berlebihan (Armoogum et al., 2025). Tinjauan komprehensif Armoogum dan kolega (2025) menegaskan bahwa konsistensi praktik *cyber hygiene* sering kali lebih menentukan tingkat risiko organisasi dibandingkan keberadaan teknologi keamanan canggih; teknologi tanpa perilaku aman hanyalah “kunci” yang dibiarkan menggantung di pintu.

Berbagai temuan global menguatkan pandangan ini. Laporan “Oh, Behave!” menemukan bahwa banyak individu memandang keamanan siber sebagai tanggung jawab utama organisasi atau pemerintah, bukan tanggung jawab pribadi, sehingga mengabaikan langkah-langkah dasar seperti memeriksa keaslian situs, meninjau pengaturan privasi, atau mengaktifkan proteksi tambahan (National Cyber Security Alliance & CybSafe, 2021). Laporan benchmarking KnowBe4 (2023) mengungkapkan bahwa tanpa pelatihan, sekitar sepertiga pegawai cenderung gagal dalam simulasi phishing. Setelah program pelatihan dan edukasi berkelanjutan selama 12 bulan, angka ini dapat turun hingga di bawah 10%. Pola serupa ditemukan di berbagai studi organisasi, seperti intervensi yang menggabungkan edukasi, simulasi insiden, dan umpan balik individual lebih efektif mengubah perilaku daripada pelatihan satu arah berbasis ceramah (Prümmer et al., 2024).

Prümmer dan kolega (2024), melalui systematic review terkait metode pelatihan keamanan siber, menyimpulkan bahwa pendekatan yang paling efektif biasanya menggabungkan: (1) materi yang relevan dengan tugas kerja, (2) simulasi insiden seperti phishing, (3) umpan balik individual, dan (4) nudges perilaku dan pengingat visual di tempat kerja. Pendekatan yang hanya mengandalkan modul pasif atau pelatihan satu kali cenderung menciptakan peningkatan pengetahuan jangka pendek tetapi tidak mengubah kebiasaan. Temuan ini sejalan dengan kerangka Theory of Planned Behavior (TPB) dan COM-B, yang menempatkan perilaku sebagai hasil kombinasi kemampuan (*capability*), kesempatan (*opportunity*), dan motivasi (*motivation*) (Ajzen, 1991; Michie et al., 2011). Dengan kata lain, pengguna baru akan konsisten berperilaku aman bila mereka memahami apa yang harus dilakukan, memiliki lingkungan dan alat yang memudahkan tindakan aman, dan merasakan dorongan (normatif ataupun pribadi) untuk melakukannya.

Nuansa konteks kolektif Indonesia menambah kompleksitas ini. Berbagai studi budaya menunjukkan bahwa masyarakat Indonesia secara umum lebih kolektif dan memiliki jarak kuasa yang tinggi: identitas kelompok, harmoni sosial, dan kepatuhan pada otoritas memiliki pengaruh besar terhadap perilaku sehari-hari (Hofstede et al., 2010; Artina et al., 2020; Setyaningrum et al., 2022).

Dalam praktik digital, hal ini tercermin dalam kebiasaan berbagi perangkat dan akun dalam keluarga, penggunaan satu nomor telepon atau akun untuk berbagai layanan oleh banyak anggota rumah tangga, serta kuatnya pengaruh tokoh agama, adat, dan pimpinan organisasi dalam menentukan sikap terhadap teknologi dan privasi.

Denganacamata TPB, faktor norma subjektif, yaitu keyakinan bahwa orang-orang penting mengharapkan atau tidak mengharapkan suatu perilaku—sangat menonjol. Keputusan untuk, misalnya, menolak permintaan data pribadi yang tidak jelas, melaporkan insiden keamanan, atau menegur rekan kerja yang membagikan kata sandi sering kali tidak hanya ditentukan oleh pengetahuan teknis, tetapi juga oleh pertimbangan “apakah ini akan menyinggung atasan”, “apakah keluarga akan menganggap saya berlebihan”, atau “apakah tokoh yang saya hormati menganggap ini wajar”. Di banyak situasi, tekanan untuk menjaga harmoni dan loyalitas kelompok dapat membuat individu enggan melakukan tindakan yang secara teknis benar tetapi secara sosial dianggap tidak nyaman (Ajzen, 1991; Hofstede et al., 2010).

Agar sensitif terhadap realitas ini, dimensi perilaku dalam IKBKS tidak cukup hanya mengukur “apa yang Anda lakukan” sebagai individu. Instrumen perlu memasukkan indikator tentang norma digital kolektif, misalnya sejauh mana keluarga, lingkungan kerja, dan komunitas menegur atau memberi contoh terkait perilaku digital berisiko. Bagaimana peran tokoh agama, adat, dan pemimpin lokal dalam mendorong atau justru menghambat praktik cyber hygiene, serta bagaimana berbagi perangkat dan akun dipraktikkan dan dinormalkan. Dengan mengintegrasikan dimensi ini, IKBKS dapat mengidentifikasi apakah rendahnya perilaku aman lebih disebabkan oleh kurangnya pengetahuan, ketiadaan fasilitas, atau oleh norma sosial yang mentolerir perilaku berisiko.

Bagi keamanan digital publik, implikasinya jelas. Keberhasilan melindungi data warga dan layanan publik sangat bergantung pada seberapa jauh prinsip-prinsip cyber hygiene dan budaya keamanan melekat dalam keseharian aparatur ataupun warga. Karena itu, IKBKS tidak hanya menilai apakah kebijakan dan pelatihan sudah tersedia, tetapi juga mengukur sejauh mana perilaku aman benar-benar dipraktikkan, seperti misalnya kebiasaan memverifikasi permintaan data pribadi, menghindari berbagi kredensial antarpegawai, menggunakan kanal resmi untuk pelaporan insiden, dan mendiskusikan risiko digital dalam keluarga dan komunitas. Dengan demikian, indeks ini berupaya menjembatani kesenjangan antara desain kebijakan keamanan dan realitas perilaku di lapangan, dalam konteks masyarakat Indonesia yang majemuk dan kolektifis.

BAB III

METODOLOGI

DISCIPLINE
kematangan tumbuh dari kebiasaan

3.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian deskriptif dan desain survei yang bertujuan untuk mengukur tingkat kematangan budaya keamanan siber masyarakat Indonesia secara objektif, sistematis, dan terstandar. Pendekatan kuantitatif dipilih karena memungkinkan fenomena sosial yang bersifat abstrak, seperti tingkat perkembangan pengetahuan, sikap, perilaku, serta praktik keamanan siber masyarakat Indonesia. Fenomena ini dioperasionalisasikan ke dalam variabel dan indikator terukur sehingga dapat dianalisis secara statistik dan dibandingkan secara kuantitatif.

3.2 Desain Penelitian

Jumlah penduduk Indonesia dengan usia produktif pada tahun 2025 diperkirakan mencapai 214,9 Juta Jiwa [5]. Angka ini menjadi dasar estimasi populasi dalam pengukuran Indeks Kematangan Budaya Keamanan Siber Indonesia. Metode pemilihan sampel dari populasi yang telah ditentukan menggunakan pendekatan stratified random sampling. Stratified random sampling merupakan metode pengambilan sampel acak berlapis berdasarkan kelompok demografis yang mewakili variasi populasi pengguna ruang siber di Indonesia. Stratifikasi dalam penentuan sampel pengukuran Indeks Kematangan Budaya Keamanan Siber Indonesia dilakukan dengan mempertimbangkan kelompok usia, jenis kelamin, tingkat pendidikan, dan jenis pekerjaan.

Penentuan jumlah sampel minimum menggunakan pendekatan kuantitatif berbasis rumus Slovin, dengan mempertimbangkan ukuran populasi, dan tingkat kesalahan yang dapat diterima (margin of error) sebesar 5%. Rumus Slovin dinyatakan sebagai berikut.

$$n = \frac{N}{1 + N(e)^2}$$

dengan:

n = ukuran sampel minimum

N = ukuran populasi

e = tingkat kesalahan (*margin of error*)

Populasi dalam pengukuran Indeks Kematangan Budaya Keamanan Siber Indonesia adalah 214.944.100 orang dengan menggunakan margin of error sebesar 5%, diperoleh perhitungan minimal jumlah sampel adalah 5.101 responden. Jumlah sampel per-provinsi sebesar 200 responden, sehingga jumlah sampel total di 38 provinsi adalah 7.600 responden. Perolehan jumlah sampel total di 38 provinsi melebihi target minimal yaitu sebesar 9.488 responden.

3.3 Analisis Data

3.3.1 Pembobotan

Pembobotan dilakukan untuk memberikan tingkat kepentingan yang berbeda pada setiap dimensi atau indikator. Setiap unsur diberi bobot sesuai perannya terhadap budaya keamanan siber.

Tabel 3.1 Pembobotan Dimensi IKBKS

Dimensi	Kode	Bobot Indikator
Kesadaran Keamanan Siber	W1	1.00–4.00
Perilaku Pengguna Siber	W2	1.00–4.00
Literasi Keamanan Siber	W3	1.00–4.00

3.3.2 Normalisasi

Normalisasi digunakan untuk menyamakan skala antarvariabel agar seluruh indikator memiliki rentang nilai yang setara.

a. Kesadaran Keamanan Siber

Tabel 3.2 Normalisasi Kesadaran Keamanan Siber

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
U1	Apakah anda telah membaca dengan teliti mengenai syarat dan ketentuan aplikasi sebelum anda menginstalnya?	Saya tidak membacanya	1
		Saya hanya membaca pada poin penting	2
		Saya membacanya sekilas	3
		Saya membacanya dengan teliti	4
U2	Dengan menyetujui syarat dan ketentuan sebelum instalasi, apakah anda memberikan izin kepada aplikasi untuk dapat mengakses data pribadi milik anda?	Saya mengizinkannya walaupun tidak memahami risikonya	1
		Saya tidak mengizinkannya karena tidak memahami risikonya	2
		Saya tidak mengizinkannya karena ragu terhadap keamanan risikonya	3
		Saya mengizinkannya dengan memahami risikonya	4
U3	Apakah anda menggunakan <i>password</i> dengan kombinasi tersebut?	Saya mengabaikannya	1
		Saya menggunakan salah satu kombinasi	2
		Saya menggunakan beberapa kombinasi	3
		Saya menggunakan seluruh kombinasi	4



Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
U4	Apakah anda membagikan <i>password</i> kepada orang lain?	Saya membagikan <i>password</i> seluruh akun yang saya miliki	1
		Saya membagikan <i>password</i> hanya kepada orang yang saya percayai	2
		Saya membagikannya ketika hanya ada urgensi	3
		Saya tidak pernah membagikan <i>password</i> akun kepada siapapun	4
U5	Apakah anda mengganti <i>password</i> secara rutin?	Tidak sama sekali	1
		Jika saya ingat saja	2
		Ya, setiap setahun sekali	3
		Ya, setiap tiga bulan sekali	4
U6	Apakah anda menyimpan <i>password</i> dengan aplikasi penyimpan <i>password</i> (<i>password manager</i>) yang tepercaya?	Saya tidak menyimpan <i>password</i> saya	1
		Saya tidak menyimpannya pada aplikasi penyimpan <i>password</i>	2
		Saya menyimpannya pada aplikasi penyimpan <i>password</i> meskipun tidak tepercaya	3
		Saya menyimpannya pada aplikasi yang tepercaya	4
U7	Apakah anda menggunakan <i>password</i> yang berbeda untuk setiap akun digital yang anda miliki?	Setiap akun digital saya memiliki <i>password</i> yang sama	1
		Beberapa akun digital saya memiliki <i>password</i> yang sama	2
		Satu sampai dua akun digital saya memiliki <i>password</i> yang sama	3
		Setiap akun digital saya memiliki <i>password</i> yang berbeda-beda	4
U8	Apakah anda mengaktifkan fitur 2FA (<i>Two Factor Authentication</i>) pada aplikasi yang anda gunakan?	Saya tidak mengetahuinya	1
		Saya tidak mengaktifkannya	2
		Saya mengaktifkannya jika tidak mengunduh aplikasi tambahan	3
		Saya mengaktifkannya walaupun harus menggunakan aplikasi tambahan	4
U9	Apakah anda menyadari risiko saat membuka lampiran atau mengeklik tautan dari sumber yang tidak dikenal?	Saya tidak menyadari risikonya	1
		Saya menyadari risikonya tetapi tetap mengekliknya	2



Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
		Saya menyadari risikonya dan mengabaikan tautannya	3
		Saya menyadari risikonya dan mengecek validitas sumbernya	4
U10	Apakah anda menyadari bahwa aktivitas <i>online</i> yang anda lakukan dapat terekam dan diawasi oleh orang yang tidak berkepentingan?	Saya tidak menyadari risikonya sama sekali	1
		Saya tidak terlalu menyadari risikonya	2
		Saya menyadari risikonya tetapi saya tidak peduli	3
		Saya sangat menyadari risikonya dan selalu waspada	4
U11	Apakah anda menghindari kunjungan ke situs yang mencurigakan?	Saya sering mengunjungi situs yang mencurigakan	1
		Saya kadang-kadang mengunjungi situs yang mencurigakan	2
		Saya jarang mengunjungi situs yang mencurigakan secara tidak sengaja	3
		Saya tidak pernah mengunjungi situs yang mencurigakan	4
U12	Apakah anda menggunakan koneksi internet yang aman dan menghindari penggunaan jaringan publik untuk transaksi keuangan?	Saya selalu menggunakan jaringan publik	1
		Saya sering menggunakan jaringan publik	2
		Saya kadang-kadang menggunakan jaringan publik	3
		Saya tidak pernah menggunakan jaringan publik	4
U13	Apakah anda selalu memastikan untuk terhubung ke jaringan WiFi yang dilindungi kata sandi?	Saya tidak pernah memastikannya	1
		Saya kadang-kadang memastikannya	2
		Saya sering memastikannya	3
		Saya selalu memastikannya	4
U14	Apakah anda melakukan <i>update software</i> pada perangkat digital yang anda miliki secara rutin?	Saya tidak pernah melakukan <i>update software</i>	1
		Saya jarang melakukan <i>update software</i>	2
		Saya melakukan <i>update</i> secara berkala terutama saat menerima pemberitahuan	3
		Saya selalu melakukan <i>update software</i> secara rutin	4

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
U15	Apakah anda memasang antivirus pada perangkat digital yang anda miliki?	Saya tidak pernah memasang antivirus pada perangkat digital	1
		Saya mengandalkan perlindungan bawaan dari sistem operasi	2
		Saya hanya memasang antivirus pada beberapa perangkat digital saya tergantung kebutuhan dan aktivitas <i>online</i> saya	3
		Saya selalu memasang antivirus pada semua perangkat digital saya	4
U16	Apakah anda hanya mengunduh aplikasi dari penyedia aplikasi resmi?	Saya selalu mengunduh aplikasi dari penyedia yang tidak resmi	1
		Saya terkadang mengunduh aplikasi dari sumber yang tidak resmi ketika aplikasi tersebut tidak tersedia dari penyedia resmi	2
		Saya beberapa kali mengunduh aplikasi dari penyedia aplikasi resmi	3
		Saya hanya mengunduh aplikasi dari penyedia aplikasi resmi seperti <i>Google Play Store</i> atau <i>Apple Store</i>	4
U17	Apakah anda melakukan <i>update</i> antivirus secara berkala?	Saya tidak pernah melakukan <i>update</i> antivirus	1
		Saya jarang melakukan <i>update</i> antivirus	2
		Saya melakukan <i>update</i> secara berkala terutama saat menerima pemberitahuan	3
		Saya selalu melakukan <i>update</i> antivirus secara rutin	4
U18	Apakah anda menonaktifkan posisi geografis perangkat digital ketika tidak digunakan?	Saya tidak mengetahui mengenai pengaturan penonaktifkan posisi geografis	1
		Saya mengaktifkan posisi geografis perangkat digital	2
		Saya menonaktifkan posisi geografis perangkat saya dalam situasi tertentu	3
		Saya selalu menonaktifkan posisi geografis perangkat saya ketika tidak digunakan	4
U19	Apakah anda melakukan <i>backup data</i> dari perangkat digital yang anda miliki secara berkala?	Saya tidak pernah melakukan <i>backup data</i>	1
		Saya jarang melakukan <i>backup data</i>	2
		Saya melakukan <i>backup data</i> secara berkala terutama saat menerima pemberitahuan	3
		Saya selalu melakukan <i>backup data</i> secara rutin	4

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
U20	Apakah anda mengetahui pihak berwenang yang dapat dihubungi ketika mengalami peretasan?	Saya tidak mengetahui sama sekali pihak berwenang dalam penanganan insiden siber	1
		Saya hanya mengetahui beberapa pihak berwenang dalam penanganan insiden siber	2
		Saya mengetahui semua pihak berwenang dalam penanganan insiden siber, namun tidak tahu cara menghubunginya	3
		Saya mengetahui semua pihak berwenang dalam penanganan insiden siber dan tahu cara menghubunginya	4
U21	Apakah anda melaporkan kepada pihak berwenang apabila terjadi kasus peretasan pada akun anda?	Saya tidak melaporkannya kepada pihak berwenang	1
		Saya ragu untuk melaporkannya kepada pihak berwenang karena tidak yakin akan ditindak	2
		Saya menunda melaporkannya kepada pihak berwenang karena mencoba menyelesaikannya sendiri	3
		Saya langsung melaporkannya kepada pihak berwenang	4
U22	Apakah anda mengetahui bahwa BSSN berwenang mengatasi peretasan akun?	Saya tidak mengetahui BSSN memiliki layanan aduan siber	1
		Saya pernah mendengar BSSN memiliki layanan aduan siber	2
		Saya mengetahui namun tidak paham mekanisme pelaporan layanan aduan siber BSSN	3
		Saya mengetahui dan paham mekanisme pelaporan layanan aduan siber BSSN	4
U23	Apakah anda mengetahui negara memiliki aturan tentang pelarangan meretas infrastruktur teknologi publik?	Saya tidak tahu pemerintah memiliki aturan tersebut	1
		Saya pernah mendengar pemerintah memiliki aturan tersebut	2
		Saya tidak tahu secara detail	3
		Saya tahu secara detail	4
U24	Apakah anda pernah mencoba atau melakukan peretasan terhadap infrastruktur publik?	Saya pernah melakukannya walaupun tahu jika itu dilarang	1
		Saya pernah melakukan karena tidak mengetahui jika itu dilarang	2



Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
		Saya tidak pernah melakukannya namun tidak tahu jika itu dilarang	3
		Saya tidak pernah melakukan karena saya tahu itu dilarang	4
U25	Apakah anda menyadari bahwa terdapat praktik oleh pihak yang tidak bertanggung jawab yang mencoba memanipulasi identitas orang lain untuk tujuan penipuan <i>online</i> ?	Saya tidak menyadari dan tidak mengetahui adanya penipuan <i>online</i>	1
		Saya tidak menyadari adanya praktik tersebut namun mengetahui adanya penipuan <i>online</i>	2
		Saya sadar tapi kurang berhati-hati dalam berinteraksi <i>online</i>	3
		Saya sadar dan selalu berhati-hati dalam berinteraksi <i>online</i>	4
U26	Apakah anda pernah memberikan informasi pribadi atau kredensial <i>login</i> kepada orang lain melalui media apapun?	Saya selalu berbagi informasi pribadi	1
		Saya sering berbagi informasi pribadi	2
		Saya jarang membagikan informasi pribadi	3
		Saya tidak pernah membagikan informasi pribadi	4
U27	Apakah anda mengerti bahwa menjaga keamanan akun <i>online</i> penting untuk mencegah manipulasi data?	Saya tidak mengerti dan tidak peduli	1
		Saya tidak mengerti hal tersebut penting bagi data saya	2
		Saya mengerti hal tersebut penting tapi tidak tahu manfaatnya	3
		Saya mengerti hal tersebut penting demi mencegah manipulasi data	4
U28	Seberapa sering anda melakukan pengecekan situs atau informasi saat menerima tawaran atau promosi <i>online</i> yang mencurigakan?	Saya tidak pernah melakukan pengecekan	1
		Saya jarang melakukan pengecekan	2
		Saya sering melakukan pengecekan	3
		Saya selalu melakukan pengecekan	4
U29	Apakah anda berupaya untuk meningkatkan literasi keamanan siber guna melindungi diri dari manipulasi <i>online</i> ?	Saya tidak minat dengan keamanan siber	1
		Saya tidak minat namun mengetahui ancamannya	2
		Saya berupaya namun tidak selalu meningkatkan literasi keamanan siber	3
		Saya berupaya dan selalu meningkatkan literasi keamanan siber	4

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
U30	Apakah anda mengetahui bahwa segala bentuk rekayasa sosial dapat dilakukan melalui media email, pesan singkat, telepon maupun video?	Saya tidak mengetahui definisinya maupun bentuk praktik rekayasa sosial	1
		Saya hanya mengetahui definisinya namun tidak mengetahui bentuk praktik rekayasa sosial	2
		Saya mengetahui bentuk praktik rekayasa sosial hanya pada beberapa media	3
		Saya mengetahui bentuk praktik rekayasa sosial pada media apapun	4
U31	Apakah anda menyebarkan konten negatif di <i>platform</i> media sosial yang anda miliki?	Saya selalu menyebarkannya	1
		Saya sering menyebarkannya	2
		Saya jarang menyebarkannya	3
		Saya tidak pernah menyebarkannya	4
U32	Apakah anda memastikan kebenaran informasi sebelum meneruskannya kepada orang lain?	Saya langsung percaya dan langsung meneruskannya kebenaran informasi tersebut	1
		Saya tidak langsung percaya dan tidak memastikan kebenaran informasi tersebut	2
		Saya tidak langsung percaya dan memastikan kebenaran informasi tersebut	3
		Saya tidak langsung percaya, memastikannya dan meneruskan kebenaran informasi tersebut	4
U33	Apakah anda menyebarkan informasi untuk menyerang seorang/kelompok tertentu pada media <i>online</i> ?	Saya selalu menyebarkannya	1
		Saya sering menyebarkannya	2
		Saya jarang menyebarkannya	3
		Saya tidak pernah menyebarkannya	4
U34	Apakah anda mengaktifkan pengaturan privasi di media sosial?	Saya tidak mengetahui mengenai pengaturan privasi pada media sosial	1
		Saya tidak mengaktifkan pengaturan privasi pada media sosial	2
		Saya mengaktifkan pengaturan privasi pada media sosial saya dalam situasi tertentu	3
		Saya selalu mengaktifkan pengaturan privasi pada media sosial saya	4
U35	Apakah anda membagikan detail pribadi secara <i>real time</i> di media sosial?	Saya selalu membagikannya	1
		Saya sering membagikannya	2

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
		Saya jarang membagikannya	3
		Saya tidak pernah membagikannya	4
U36	Saya berusaha menjaga sikap positif dan tidak membagikan konten yang dapat merugikan diri sendiri atau orang lain.	Saya tidak peduli	1
		Saya merasa perlu namun belum melakukannya sepenuhnya	2
		Saya sudah melakukannya	3
		Saya sudah melakukannya dan mengingatkan orang lain untuk bersikap positif	4
U37	Apakah anda mengetahui bahwa penggunaan media sosial yang berlebihan dapat berdampak pada kesehatan mental dan produktivitas?	Saya tidak menyadari dampak negatifnya dan berlebihan menggunakan media sosial	1
		Saya tidak menyadari dampak negatifnya dan banyak menggunakan media sosial	2
		Saya menyadari dampak negatifnya namun banyak menggunakan media sosial	3
		Saya menyadari dampak negatifnya dan menggunakan media sosial dengan bijak	4
U38	Apakah anda merespons positif dan menghormati pandangan orang lain di media online?	Saya merasa tidak perlu melakukannya	1
		Saya merasa perlu namun belum melakukannya	2
		Saya sudah melakukannya namun hanya kepada orang yang saya kenal	3
		Saya sudah melakukannya	4
U39	Apakah anda mengetahui pihak berwenang yang dapat dihubungi ketika menemukan konten negatif?	Saya tidak mengetahui sama sekali pihak berwenang dalam penanganan konten negatif	1
		Saya hanya mengetahui beberapa pihak berwenang dalam penanganan konten negatif	2
		Saya mengetahui semua pihak berwenang dalam penanganan konten negatif, namun tidak tahu cara menghubunginya	3
		Saya mengetahui semua pihak berwenang dalam penanganan konten negatif dan tahu cara menghubunginya	4
U40	Apakah anda melaporkan adanya konten negatif kepada pihak berwenang apabila menemukannya di media sosial?	Saya tidak pernah melaporkannya	1
		Saya jarang melaporkannya	2
		Saya sering melaporkannya	3

Kode	Unsur (Pernyataan)	Jawaban Unsur	Normalisasi
		Saya selalu melaporkannya	4
U41	Apakah anda mengetahui adanya pelayanan lapor konten yang disediakan oleh BSSN?	Saya tidak mengetahui BSSN memiliki layanan Lapor Konten	1
		Saya pernah mendengar BSSN memiliki layanan Lapor Konten	2
		Saya mengetahui namun tidak paham mekanisme layanan Lapor Konten BSSN	3
		Saya mengetahui dan paham mekanisme layanan Lapor Konten BSSN	4
U42	Apakah anda mengetahui pemerintah memiliki aturan tentang larangan penyebaran konten negatif di media sosial?	Saya tidak tahu pemerintah memiliki aturan tersebut	1
		Saya pernah mendengar pemerintah memiliki aturan tersebut	2
		Saya tidak tahu secara detail	3
		Saya tahu secara detail	4
U43	Apakah anda percaya konsekuensi hukum bagi pelaku penyebar konten negatif akan ditindak oleh pemerintah?	Saya tidak peduli dengan hal tersebut	1
		Saya tidak percaya pihak berwenang akan menegakkan aturan tersebut	2
		Saya hanya mempercayai sebagian pihak berwenang akan menegakkan aturan tersebut	3
		Saya percaya seluruh pihak berwenang akan menegakkan aturan tersebut	4

b. Peta Perilaku Pengguna Ruang Siber

Tabel 3.3 Normalisasi Peta Perilaku Pengguna Ruang Siber

Kode	Unsur	Jawaban Unsur	Pembobotan
U1	Durasi (<i>screentime</i>) penggunaan internet dalam sehari	Kurang dari 2 jam	4
		2-4 jam	3
		5-8 jam	2
		Lebih dari 8 jam	1
U2	Durasi (<i>screentime</i>) penggunaan media sosial dalam sehari	Kurang dari 2 jam	4
		2-4 jam	3
		5-8 jam	2
		Lebih dari 8 jam	1

Kode	Unsur	Jawaban Unsur	Pembobotan
U3	Jenis perangkat yang paling sering Anda gunakan untuk mengakses internet	Handphone	1
		Laptop	1
		Tablet	3
		Komputer/PC	2
		Game Console	4
		Lainnya	3
U4	Jenis media sosial yang paling sering Anda gunakan	Tidak ada media sosial yang saya miliki	0
		Instagram	2
		Facebook	1
		Tiktok	1
		X (Twitter)	1
		YouTube	2
		Pinterest	3
		LinkedIn	4
		Threads	3
U5	Jenis aplikasi pesan singkat yang paling sering Anda gunakan	Tidak ada aplikasi pesan singkat yang saya miliki	0
		WhatsApp	2
		Telegram	1
		Line	4
		Facebook Messenger	3
		Discord	2
		WeChat	4
		Signal	4
		MiChat	1
		Microsoft Teams	3
U6	Tujuan utama penggunaan internet	Kebutuhan Tugas Sekolah/Pembelajaran Jarak Jauh	4
		Bekerja/Bisnis: membaca berita, streaming video, live streaming, trading/investasi online, jualan online	3

Kode	Unsur	Jawaban Unsur	Pembobotan
		Hiburan: membaca berita, melihat sosmed, streaming video, live streaming, game online, belanja	1
U7	Jenis konten media daring atau media sosial yang paling Anda sukai	Online Shop/Marketplace	2
		Lifestyle	2
		Film	3
		Politik	2
		Kesehatan	3
		Game	1
		Tranding/Investasi Online	1
		Edukasi	4
		Agama	2
		Lainnya	2
U8	Jenis koneksi internet yang sering Anda gunakan	Paket Data/Kuota	4
		Pakai Internet Rumah	4
		Koneksi Internet Rumah Teman/Tetangga/Saudara	2
		Koneksi Internet di Sekolah/Kampus	3
		Koneksi Internet di Kantor	4
		Wifi di Ruang Publik	1
		Koneksi Internet di Warnet	1
U9	Apakah Anda pernah melihat konten <i>Violent Extremism</i> ?	Tidak	4
		Ya	1
U9.2	Apakah Anda pernah melihat konten <i>Violent Extremism</i> ?	Tidak pernah melihat konten violent extremism	4
		Instagram	3
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	2
		WhatsApp	1



Kode	Unsur	Jawaban Unsur	Pembobotan
		YouTube	2
		Facebook Messenger	3
		Pinterest	4
		LinkedIn	4
		Threads	3
U9.3	Jenis Konten yang Paling Sering Ditemukan	Tidak pernah melihat konten violent extremism	4
		Terorisme	2
		Konflik Bersenjata	2
		Kekerasan terhadap etnis: suku, agama, dan ras	1
		Kekerasan berbasis gender	1
		Kekerasan terhadap kelompok minoritas	3
U9.4	Apa yang Anda lakukan ketika melihat konten <i>Violent Extremism</i> ?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U9.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan <i>Violent Extremism</i> di media online?	Ya	1
		Tidak	4
U10.1	Apakah Anda pernah melihat konten Penyalahgunaan <i>Artificial Intelligence</i> ?	Tidak	4
		Ya	1
U10.2	Pada platform mana Anda pernah melihat konten Penyalahgunaan <i>Artificial Intelligence</i> ?	Tidak pernah melihat konten Penyalagunaan Artificial Intelligence	4
		Instagram	3
		Facebook	2
		TikTok	1
		Telegram	1
		X (Twitter)	1
		WhatsApp	2
		YouTube	2
		Facebook Messenger	3

Kode	Unsur	Jawaban Unsur	Pembobotan
		Pinterest	4
		LinkedIn	4
		Threads	3
U10.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten Penyalagunaan Artificial Intelligence	4
		Hoaks/Disinformasi	2
		Deepfake	1
U10.4	Apa yang Anda lakukan ketika melihat konten Penyalahgunaan Artificial Intelligence?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U10.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan Artificial Intelligence di media online?	Ya	1
		Tidak	4
U11.1	Apakah Anda pernah melihat konten Narkotika, Psikotropika dan Zat Adiktif (NAPZA)?	Tidak	4
		Ya	1
U11.2	Pada platform mana Anda pernah melihat konten Narkotika, Psikotropika dan Zat Adiktif (NAPZA)?	Tidak pernah melihat konten NAPZA	4
		Instagram	2
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	2
		WhatsApp	1
		YouTube	2
		Facebook Messenger	3
		Pinterest	3
		LinkedIn	4
		Threads	4
U11.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten NAPZA	4
		Penyalahgunaan narkotika	2
		Peredaran gelap narkotika	1

Kode	Unsur	Jawaban Unsur	Pembobotan
		Kasus overdosis narkoba	3
		Kasus kecanduan narkoba	3
		Penyakit yang diakibatkan narkoba	4
U11.4	Apa yang Anda lakukan ketika melihat konten Narkoba, Psikotropika dan Zat Adiktif (NAPZA)?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U11.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan Narkoba, Psikotropika dan Zat Adiktif (NAPZA) di media <i>online</i> ?	Ya	1
		Tidak	4
U12.1	Apakah Anda pernah melihat konten Penyimpangan Perilaku Sosial?	Tidak	4
		Ya	1
U12.2	Pada <i>platform</i> mana Anda pernah melihat konten penyimpangan perilaku sosial?	Tidak pernah melihat konten penyimpangan perilaku sosial	4
		Instagram	2
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	1
		WhatsApp	3
		YouTube	3
		Facebook Messenger	3
		Pinterest	4
		LinkedIn	4
		Threads	4
U12.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten penyimpangan perilaku sosial	4
		LGBT	4
		Cyberbullying	3
		Hate speech	2
		Fan war	4
		Hoaks/Disinformasi	3



Kode	Unsur	Jawaban Unsur	Pembobotan
		Penyebaran ideologi ekstrimis	2
		Pencurian Identitas	1
		Doxxing	1
		Ajaran sesat	2
U12.4	Apa yang Anda lakukan ketika melihat konten penyimpangan perilaku sosial?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U12.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan penyimpangan perilaku sosial di media <i>online</i> ?	Ya	1
		Tidak	4
U13.1	Apakah Anda pernah melihat konten Ancaman Digital terhadap Anak?	Tidak	4
		Ya	1
U13.2	Pada platform mana Anda pernah melihat konten Ancaman Digital terhadap Anak berupa <i>Cyberbullying</i> (menjadi korban atau pelaku), <i>Sexting</i> atau berbagi foto/video sensitif, Menyebarkan ujaran kebencian atau diskriminasi, Berpartisipasi dalam tantangan viral	Tidak pernah melihat konten Ancaman Digital terhadap Anak	4
		TikTok	1
		YouTube	3
		Platform Game Online	2
U13.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten Ancaman Digital terhadap Anak	4
		Child grooming	1
		Pedofilia	1
		Cyberbullying	3
		Pelecehan seksual online	2
		Eksplorasi anak	2
		Perdagangan anak	1
		Kekerasan terhadap anak	3
		Pergeseran nilai moral. Contoh: tawuran, balap liar	3
U13.4	Apa yang Anda lakukan ketika melihat konten Ancaman Digital terhadap Anak?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4



Kode	Unsur	Jawaban Unsur	Pembobotan
U13.5	Apakah Anda pernah diajak/mengajak/membuat yang berkaitan dengan Ancaman Digital terhadap Anak di media <i>online</i> ?	Ya	1
		Tidak	4
U13.6	Apakah saat ini anda berperan sebagai orangtua/wali?	Tidak	4
		Ya	4
U13.7	Apa yang akan Anda lakukan jika anak Anda memberitahu/bertanya tentang konten bermuatan negatif?	Membiarkan saja	4
		Memberikan penjelasan terkait konten yang ditemukan	4
		Membatasi penggunaan gadget	4
		Membatasi akses terhadap konten melalui fitur parenting control	4
		Mencari Pertolongan kepada Profesional	4
U14.1	Apakah Anda pernah melihat konten Pornografi?	Tidak	4
		Ya	1
U14.2	Pada <i>platform</i> mana Anda pernah melihat konten Pornografi?	Tidak pernah melihat konten Pornografi	4
		Instagram	3
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	1
		WhatsApp	2
		YouTube	3
		Facebook Messenger	3
		Pinterest	4
		LinkedIn	4
		Threads	3
		Platform Game Online	2
		Aplikasi Kencan	1
U14.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten Pornografi	4
		Jual beli foto/video vulgar	2
		Penyebaran konten pornografi	2

Kode	Unsur	Jawaban Unsur	Pembobotan
		Prostitusi online	1
		Grup aktivitas seksual	1
U14.4	Apa yang Anda lakukan ketika melihat konten Pornografi?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U14.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan Ponografi di media online?	Ya	1
		Tidak	4
U15.1	Apakah Anda pernah melihat konten <i>Financial Crime</i> ?	Tidak	4
		Ya	1
U15.2	Pada platform mana Anda pernah melihat konten <i>Financial Crime</i> ?	Tidak pernah melihat konten <i>Financial Crime</i>	4
		Instagram	3
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	2
		WhatsApp	1
		YouTube	2
		Facebook Messenger	3
		Pinterest	4
		LinkedIn	4
		Threads	3
U15.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten <i>Financial Crime</i>	4
		<i>Phising/vishing</i>	2
		<i>Online shopping scam</i>	3
		<i>Investment scam</i>	2
		<i>Love scam</i>	3
		<i>Rental scam</i>	3
		<i>Job scam</i>	3
		Judi online	1

Kode	Unsur	Jawaban Unsur	Pembobotan
		Pinjaman <i>online</i> ilegal	2
U15.4	Apa yang Anda lakukan ketika melihat konten <i>Financial Crime</i> ?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U15.5	Apakah Anda pernah diajak/mengajak yang berkaitan dengan <i>Financial Crime</i> di media <i>online</i> ?	Ya	1
		Tidak	4
U16.1	Apakah Anda pernah melihat konten Negatif tentang Politik?	Tidak	4
		Ya	1
U16.2	Pada <i>platform</i> mana Anda pernah melihat konten negatif yang berkaitan dengan politik?	Tidak pernah melihat konten negatif tentang politik	4
		Instagram	3
		Facebook	2
		TikTok	2
		Telegram	1
		X (Twitter)	2
		WhatsApp	1
		YouTube	3
		Facebook Messenger	1
		Pinterest	4
		LinkedIn	4
		Threads	3
U16.3	Jenis konten apa yang paling sering Anda temukan?	Tidak pernah melihat konten negatif tentang politik	4
		Netralitas ASN	4
		Polarisasi politik	2
		Kerusuhan dan kekerasan politik	1
		Diskriminasi politik	3
		Pelanggaran pemilu	3
		Pelanggaran hak politik	4
		Politik uang	1

Kode	Unsur	Jawaban Unsur	Pembobotan
		Black campaign	2
		KKN (Korupsi, Kolusi, dan Nepotisme)	1
		Penyalahgunaan kekuasaan	1
U16.4	Apa yang Anda lakukan ketika melihat konten negatif yang berkaitan dengan politik?	Mengabaikan saja	1
		Membaca untuk informasi pribadi	2
		Membaca dan melaporkan ke orangtua/guru/pihak berwenang	4
U16.5	Apakah Anda pernah diajak/mengajak/membuat yang berkait dengan konten negatif yang berkaitan dengan Politik di media <i>online</i> ?	Ya	1
		Tidak	4

3.3.3 Perhitungan Indeks

Perhitungan indeks dalam penelitian ini dilakukan untuk mendapatkan satu nilai ringkas yang dapat menggambarkan seberapa tinggi tingkat kesadaran keamanan siber, bagaimana pola perilaku pengguna di ruang digital, serta seberapa efektif literasi keamanan siber yang mereka miliki. Indeks tersebut diperoleh dengan mengolah skor dari setiap dimensi, yang sebelumnya dikumpulkan melalui jawaban responden pada kuesioner penelitian. Dengan cara ini, seluruh informasi dari berbagai indikator dapat dirangkum menjadi satu ukuran yang lebih mudah dipahami dan dianalisis.

a. Dimensi Peta Perilaku Pengguna Ruang Siber

Dimensi Peta Perilaku Pengguna Ruang Siber (P3RS) digunakan untuk gambaran pola perilaku masyarakat Indonesia di ruang siber berupa data mengenai media penyebaran konten, jenis konten, dan tindakan pengguna saat menemukan konten.

$$P3RS = \frac{\sum_{i=1}^n \sum_{j=1}^o NP}{n \times o}$$

dengan:

$$\sum_{i=1}^n \sum_{j=1}^m NK = \text{Total Nilai Peta Perilaku Pengguna Ruang Siber}$$

n = Jumlah Responden

o = Jumlah Pertanyaan P3RS

Tabel 3.4 Perhitungan Peta Perilaku Pengguna Ruang Siber

Rentang P3RS	Predikat	Interprestasi
1,00 - 1,74	Buruk	Pengguna memiliki perilaku tindakan berisiko tinggi terhadap praktik keamanan siber
1,75 - 2,49	Kurang Baik	Pengguna memiliki perilaku tindakan berisiko sedang terhadap praktik keamanan siber
2,50 - 3,24	Baik	Pengguna memiliki perilaku tindakan berisiko rendah terhadap praktik keamanan siber
3,25 - 4,00	Sangat Baik	Pengguna memiliki perilaku tindakan konsisten dan proaktif terhadap praktik keamanan siber

b. Dimensi Kesadaran Keamanan Siber

Nilai Kesadaran Keamanan Siber merupakan ukuran kondisi keamanan siber teknis dan keamanan siber sosial yang telah menjadi bagian dari perilaku dan kebiasaan sehari-hari masyarakat Indonesia. Rumus indeks kesadaran keamanan siber suatu kelompok dijabarkan sebagai berikut.

$$KKS = \frac{\sum_{i=1}^n \sum_{j=1}^m NK}{n \times m}$$

dengan:

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^m NK &= \text{Total Nilai Kesadaran Keamanan Siber} \\ n &= \text{Jumlah Responden} \\ m &= \text{Jumlah Pertanyaan IKKS} \end{aligned}$$

Nilai Kesadaran Keamanan Siber yang diperoleh melalui Survei Kesadaran Keamanan Siber (SKKS) disajikan dalam bentuk indeks dengan rentang nilai 1,00 hingga 4,00.

Tabel 3.5 Perhitungan Indeks Kesadaran Keamanan Siber

Rentang IKKS	Predikat	Interprestasi
1,00 - 1,74	Buruk	Pengguna memiliki kesadaran yang rendah terhadap praktik keamanan siber
1,75 - 2,49	Kurang Baik	Pengguna memiliki kesadaran yang sedang terhadap praktik keamanan siber
2,50 - 3,24	Baik	Pengguna memiliki kesadaran yang tinggi terhadap praktik keamanan siber
3,25 - 4,00	Sangat Baik	Pengguna memiliki kesadaran yang konsisten dan proaktif terhadap praktik keamanan siber

c. Dimensi Tingkat Keberhasilan Literasi Keamanan Siber

Dimensi Tingkat Keberhasilan Literasi Keamanan Siber (TLKS) merupakan nilai yang menggambarkan keberhasilan dan efektivitas intervensi organisasi melalui kampanye dan literasi keamanan siber yang diberikan kepada masyarakat Indonesia. Indikator ini dihitung dengan rumus sebagai berikut.

$$TLKS = \frac{(MR \times 4) + (N - MR)}{N}$$

dengan:

TLKS = Tingkat Keberhasilan Literasi Keamanan Siber

MR = Jumlah Masyarakat yang Teredukasi

N = Jumlah Populasi Masyarakat Nasional

Masyarakat yang teredukasi merupakan responden yang telah memperoleh literasi keamanan siber yang diselenggarakan oleh BSSN, mencakup berbagai bentuk sosialisasi, pelatihan, seminar, kampanye, dan kegiatan edukatif lainnya yang bertujuan untuk meningkatkan pemahaman masyarakat terhadap ancaman dan praktik keamanan di ruang siber. Dimensi ini mencerminkan sejauh mana upaya peningkatan kapasitas masyarakat melalui literasi siber dijalankan secara efektif dan konsisten sesuai perencanaan.

Tabel 3.6 Perhitungan Tingkat Keberhasilan Literasi Keamanan Siber

Rentang TLKS	Predikat	Interprestasi
1,00 - 1,74	Buruk	Program literasi keamanan siber menghasilkan perubahan peningkatan pengetahuan yang rendah
1,75 - 2,49	Kurang Baik	Program literasi keamanan siber menghasilkan perubahan peningkatan pengetahuan yang sedang
2,50 - 3,24	Baik	Program literasi keamanan siber menghasilkan perubahan peningkatan pengetahuan yang tinggi
3,25 - 4,00	Sangat Baik	Program literasi keamanan siber menghasilkan perubahan peningkatan pengetahuan yang optimal dan berkelanjutan

3.3.5 Model Tingkat Kematangan

Rumus Umum IKBKS adalah sebagai berikut

$$IKBKS = P3RS + KKS + TLKS$$

dengan:

P3RS = Skor Pemetaan Perilaku Pengguna Ruang Siber

KKS = Skor Indeks Kesadaran Keamanan Siber

TLKS = Skor Literasi Keamanan Siber

Rumus Umum IKBKS adalah sebagai berikut:

$$IKBKS = P3RS + KKS + TLKS$$

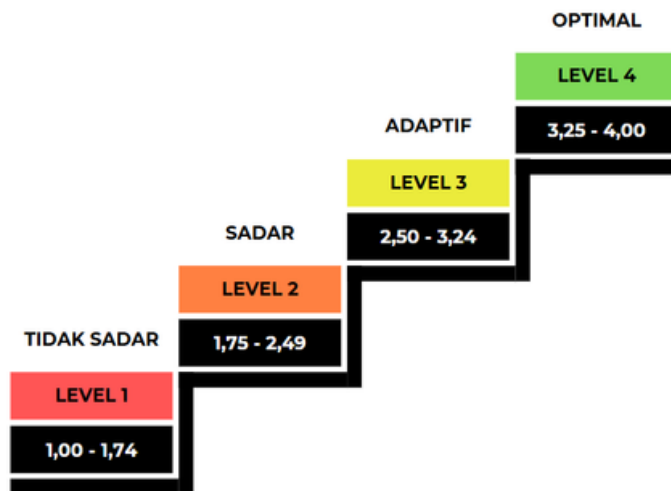
dengan:

P3RS = Skor Pemetaan Perilaku Pengguna Ruang Siber

KKS = Skor Indeks Kesadaran Keamanan Siber

TLKS = Skor Literasi Keamanan Siber

Leveling IKBKS dibagi menjadi empat level, yang masing-masing mencerminkan tingkat kematangan budaya keamanan siber.



Gambar 3.1 Tingkat Kematangan Budaya Keamanan Siber

1. Tidak Sadar
Masyarakat masih memiliki kesadaran keamanan siber yang rendah, dengan perilaku negatif di ruang digital dan literasi keamanan siber yang masih minim.
2. Sadar
Masyarakat mulai sadar dan budaya keamanan siber mulai tumbuh, tetapi belum merata.
3. Adaptif
Masyarakat mulai aktif menerapkan perilaku aman di ruang digital dan budaya keamanan siber mengalami peningkatan signifikan.
4. Optimal
Masyarakat mampu menyesuaikan diri dengan perubahan ancaman digital dan menunjukkan perilaku positif di ruang siber.

BAB IV

ANALISIS DAN DISKUSI

INTEGRATION

manusia dan sistem bekerja sebagai satu budaya

4.1 Gambaran Umum Hasil 2025

Indeks Kematangan Budaya Keamanan Siber (IKBKS) merupakan instrumen yang digunakan untuk mengukur tingkat kematangan masyarakat dalam memahami, menyikapi, dan merespons risiko serta ancaman di ruang siber. Indeks ini memiliki rentang nilai 1–4, dengan klasifikasi: nilai 1 menunjukkan tingkat Tidak Sadar, 2 menunjukkan Sadar, 3 menunjukkan Adaptif/Baik, dan 4 menunjukkan Optimal/Sangat Baik. Semakin tinggi nilai indeks, semakin matang pula budaya keamanan siber masyarakat di wilayah tersebut.

Hasil pengukuran IKBKS Tahun 2025 menunjukkan bahwa secara nasional Indonesia berada pada nilai 2,32 dengan predikat “Sadar”. Capaian ini mengindikasikan bahwa kesadaran terhadap pentingnya keamanan siber telah terbentuk di tingkat masyarakat dan pemerintah daerah. Namun demikian, kesadaran tersebut belum sepenuhnya terinternalisasi sebagai budaya yang konsisten dalam perilaku digital sehari-hari. Kondisi ini menegaskan bahwa Indonesia masih berada pada fase transisi dari peningkatan kesadaran menuju pembudayaan keamanan siber, sehingga diperlukan upaya strategis yang lebih terarah dan berkelanjutan untuk meningkatkan tingkat kematangan nasional.

Tabel 4.1 Peringkat Indeks dan Predikat IKBKS

PROVINSI	INDEKS IKBKS	PREDIKAT IKBKS
Nasional	2.32	SADAR
Jawa Tengah	2.49	SADAR
Aceh	2.46	SADAR
Bali	2.43	SADAR
DKI Jakarta	2.38	SADAR
Sulawesi Tenggara	2.37	SADAR
Riau	2.35	SADAR
Jawa Timur	2.34	SADAR
Sumatra Barat	2.33	SADAR
Lampung	2.32	SADAR
Kepulauan Bangka Belitung	2.32	SADAR
Sumatra Utara	2.31	SADAR
Kalimantan Barat	2.31	SADAR
Daerah Istimewa Yogyakarta	2.31	SADAR
Kalimantan Timur	2.31	SADAR
Jambi	2.30	SADAR
Banten	2.30	SADAR
Sulawesi Barat	2.29	SADAR
Kepulauan Riau	2.29	SADAR
Jawa Barat	2.29	SADAR
Bengkulu	2.28	SADAR
Nusa Tenggara Barat	2.28	SADAR



PROVINSI	INDEKS IKBKS	PREDIKAT IKBKS
Sumatra Selatan	2.28	SADAR
Sulawesi Selatan	2.27	SADAR
Papua Barat	2.27	SADAR
Gorontalo	2.26	SADAR
Kalimantan Utara	2.25	SADAR
Kalimantan Selatan	2.25	SADAR
Maluku Utara	2.24	SADAR
Kalimantan Tengah	2.24	SADAR
Papua Tengah	2.23	SADAR
Sulawesi Utara	2.22	SADAR
Sulawesi Tengah	2.22	SADAR
Papua Selatan	2.22	SADAR
Maluku	2.20	SADAR
Nusa Tenggara Timur	2.20	SADAR
Papua Pegunungan	2.19	SADAR
Papua	2.16	SADAR
Papua Barat Daya	2.16	SADAR

Pada tingkat provinsi, hasil pengukuran menunjukkan adanya variasi capaian yang cukup signifikan. Provinsi Bali (3,35), Sulawesi Tenggara (3,28), dan Jawa Tengah (3,26) menempati posisi tertinggi dengan predikat “Sangat Baik”. Capaian ini mencerminkan tingkat kesadaran, perilaku, serta penerapan prinsip keamanan siber yang relatif matang dan konsisten. Keberhasilan ketiga provinsi tersebut dapat dikaitkan dengan tingkat literasi digital yang lebih baik, intensitas pemanfaatan teknologi yang tinggi, serta dukungan kebijakan daerah dan program literasi keamanan digital yang berjalan secara berkelanjutan.

Secara nasional, terdapat delapan provinsi yang memiliki nilai IKBKS di atas indeks nasional, yaitu Jawa Tengah, Aceh, Bali, DKI Jakarta, Sulawesi Tenggara, Riau, Jawa Timur, dan Sumatra Barat. Provinsi-provinsi ini menunjukkan kemampuan yang relatif lebih baik dalam mengintegrasikan kesadaran keamanan siber ke dalam perilaku dan praktik digital masyarakatnya.

Sebagian besar provinsi lainnya berada pada kategori “Baik”, dengan rentang nilai indeks antara 2,69 hingga 3,15. Kondisi ini menunjukkan bahwa secara umum budaya keamanan siber di Indonesia telah berkembang ke arah yang positif. Meskipun demikian, masih terdapat kesenjangan antarwilayah, terutama antara wilayah dengan tingkat pembangunan digital yang lebih maju dan wilayah yang masih menghadapi keterbatasan infrastruktur serta kapasitas sumber daya manusia. Beberapa provinsi di kawasan timur Indonesia cenderung memiliki skor yang relatif lebih rendah, yang mengindikasikan perlunya intervensi kebijakan yang lebih kontekstual dan berbasis karakteristik wilayah.

Kesenjangan capaian IKBKS antarprovinsi tersebut memiliki keterkaitan yang kuat dengan profil kesiapan digital wilayah, khususnya jika dikaitkan dengan Indeks Masyarakat Digital Indonesia (IMDI). Provinsi dengan skor IMDI yang lebih tinggi umumnya menunjukkan tingkat kematangan budaya keamanan siber yang lebih baik. Hal ini disebabkan oleh akses internet yang lebih merata, tingkat pemanfaatan teknologi digital yang lebih aktif, serta pemahaman masyarakat yang lebih baik terhadap manfaat dan risiko ruang digital. Sebaliknya, wilayah dengan skor IMDI yang lebih rendah cenderung memiliki nilai IKBKS yang lebih rendah akibat keterbatasan infrastruktur digital, rendahnya literasi digital, serta minimnya edukasi mengenai keamanan siber.

Dengan demikian, peningkatan budaya keamanan siber tidak dapat dipisahkan dari upaya pemerataan pembangunan digital di seluruh wilayah Indonesia. Semakin tinggi kesiapan digital suatu daerah, semakin besar pula peluang terbentuknya kesadaran dan perilaku masyarakat yang aman dan bertanggung jawab di ruang siber. Temuan ini menegaskan bahwa penguatan budaya keamanan siber memerlukan pendekatan yang terintegrasi antara pembangunan infrastruktur digital, peningkatan literasi, dan kebijakan keamanan siber yang adaptif terhadap karakteristik wilayah.

4.2 Skor Per Dimensi

Pengukuran Indeks Kematangan Budaya Keamanan Siber (IKBKS) dilakukan melalui beberapa dimensi utama, yaitu Indeks Sikap dan Perilaku Ruang Siber (SPRS), Indeks Keamanan dan Kesadaran Siber (IKKS), serta Indeks Keberhasilan Literasi Keamanan Siber. Ketiga dimensi ini digunakan untuk menangkap gambaran yang lebih rinci mengenai aspek perilaku, kesadaran, dan efektivitas intervensi literasi keamanan siber di tingkat nasional maupun provinsi.

Hasil pengukuran tahun 2025 menunjukkan bahwa secara nasional Indeks SPRS mencapai nilai 2,98 dengan predikat “Baik”, sementara Indeks IKKS berada pada nilai 2,94 dengan predikat yang sama. Temuan ini mengindikasikan bahwa secara umum aspek sikap dan perilaku masyarakat dalam menggunakan ruang siber relatif lebih kuat dibandingkan aspek kesadaran dan pemahaman teknis terhadap risiko serta mekanisme keamanan siber.

Tabel 4.2 Skor Dimensi Per Provinsi

PROVINSI	INDEKS P3RS	PREDIKAT P3RS	INDEKS KKS	PREDIKAT IKKS	INDEKS TLKS
Nasional	2.98	Baik	2.94	Baik	1.03
Aceh	3.15	Baik	3.21	Baik	1.03
Bali	3.35	Sangat Baik	2.92	Baik	1.03
Banten	3.05	Baik	2.82	Baik	1.03
Bengkulu	2.88	Baik	2.93	Baik	1.03
Daerah Istimewa Yogyakarta	2.93	Baik	2.97	Baik	1.03



PROVINSI	INDEKS P3RS	PREDIKAT P3RS	INDEKS KKS	PREDIKAT IKKS	INDEKS TLKS
DKI Jakarta	2.93	Baik	3.19	Baik	1.03
Gorontalo	2.96	Baik	2.80	Baik	1.03
Jambi	2.96	Baik	2.92	Baik	1.03
Jawa Barat	3.01	Baik	2.83	Baik	1.03
Jawa Tengah	3.26	Sangat Baik	3.16	Baik	1.03
Jawa Timur	2.89	Baik	3.10	Baik	1.03
Kalimantan Barat	3.01	Baik	2.90	Baik	1.03
Kalimantan Selatan	2.83	Baik	2.88	Baik	1.03
Kalimantan Tengah	2.76	Baik	2.94	Baik	1.03
Kalimantan Timur	2.74	Baik	3.14	Baik	1.03
Kalimantan Utara	2.90	Baik	2.82	Baik	1.03
Kepulauan Bangka Belitung	2.97	Baik	2.95	Baik	1.03
Kepulauan Riau	2.88	Baik	2.97	Baik	1.03
Lampung	3.01	Baik	2.93	Baik	1.03
Maluku	2.71	Baik	2.87	Baik	1.03
Maluku Utara	3.01	Baik	2.69	Baik	1.03
Nusa Tenggara Barat	2.96	Baik	2.84	Baik	1.03
Nusa Tenggara Timur	2.82	Baik	2.75	Baik	1.03
Papua	2.76	Baik	2.70	Baik	1.03
Papua Barat	2.92	Baik	2.85	Baik	1.03
Papua Barat Daya	2.69	Baik	2.77	Baik	1.03
Papua Pegunungan	2.85	Baik	2.68	Baik	1.03
Papua Selatan	2.85	Baik	2.77	Baik	1.03
Papua Tengah	2.90	Baik	2.75	Baik	1.03
Riau	3.08	Baik	2.95	Baik	1.03
Sulawesi Barat	3.13	Baik	2.72	Baik	1.03
Sulawesi Selatan	2.87	Baik	2.92	Baik	1.03
Sulawesi Tengah	2.82	Baik	2.80	Baik	1.03
Sulawesi Tenggara	3.28	Sangat Baik	2.81	Baik	1.03
Sulawesi Utara	2.79	Baik	2.85	Baik	1.03
Sumatra Barat	2.97	Baik	2.99	Baik	1.03
Sumatra Selatan	2.94	Baik	2.86	Baik	1.03
Sumatra Utara	3.06	Baik	2.85	Baik	1.03

Pada tingkat provinsi, pola capaian kedua indeks tersebut relatif konsisten. Sebagian besar provinsi menunjukkan nilai SPRS yang sedikit lebih tinggi dibandingkan IKKS. Kondisi ini menandakan bahwa masyarakat di berbagai daerah telah mulai menerapkan perilaku digital yang cukup berhati-hati—seperti kewaspadaan dalam berbagi informasi dan penggunaan aplikasi digital—meskipun pemahaman yang lebih mendalam mengenai ancaman siber, risiko kebocoran data, serta langkah-langkah perlindungan teknis masih perlu diperkuat.

Secara konseptual, Indeks SPRS mengukur tingkat kehati-hatian dan tanggung jawab

Secara konseptual, Indeks SPRS mengukur tingkat kehati-hatian dan tanggung jawab masyarakat dalam beraktivitas di ruang siber. Semakin tinggi nilai SPRS, semakin aman pola penggunaan aplikasi dan layanan digital oleh masyarakat. Sebaliknya, nilai SPRS yang lebih rendah menunjukkan kerentanan yang lebih besar terhadap risiko kejahatan siber, baik sebagai korban maupun sebagai pelaku. Sementara itu, Indeks IKKS merefleksikan tingkat kesadaran dan pemahaman masyarakat terhadap bahaya siber serta pentingnya mekanisme perlindungan. Nilai IKKS yang lebih rendah menunjukkan keterbatasan pemahaman terhadap risiko dan ancaman siber, sehingga meningkatkan potensi paparan terhadap insiden keamanan siber.

Temuan penting lainnya adalah Indeks Keberhasilan Literasi Keamanan Siber yang tercatat seragam pada angka 1,03 di seluruh provinsi. Keceragaman ini menunjukkan bahwa program literasi keamanan siber telah dilaksanakan secara nasional dengan pendekatan yang relatif sama. Namun demikian, capaian indeks yang masih rendah mengindikasikan bahwa efektivitas literasi tersebut belum sepenuhnya menghasilkan peningkatan yang signifikan dalam pembentukan budaya keamanan siber. Hal ini juga dipengaruhi oleh karakter kegiatan literasi yang bersifat nasional dan belum tersebar merata di seluruh provinsi, meskipun melibatkan perwakilan dari beberapa daerah.

Berdasarkan hasil tersebut, dapat disimpulkan bahwa upaya literasi keamanan siber ke depan perlu bergeser dari pendekatan yang dominan bersifat informatif menuju pendekatan yang lebih aplikatif, kontekstual, dan berorientasi pada perubahan perilaku. Transformasi ini penting agar peningkatan pengetahuan dan kesadaran dapat benar-benar terinternalisasi dalam praktik digital masyarakat sehari-hari, sehingga mendorong peningkatan kematangan budaya keamanan siber secara berkelanjutan di seluruh wilayah Indonesia.

4.3 Pemetaan Persebaran Indeks Kematangan Budaya Keamanan Siber Per Provinsi

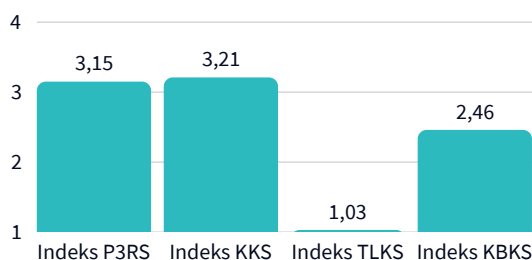
Hasil analisis Indeks Kematangan Budaya Keamanan Siber pada setiap provinsi menjadi representatif tingkat kesiapan dan kesadaran bagi sumber daya manusia di provinsi tersebut dalam mengelola risiko serta ancaman siber. Pengukuran indeks dilakukan dengan mengidentifikasi beberapa variabel yaitu Indeks SPRS, Indeks IKKS, dan Indeks Keberhasilan Literasi Keamanan Siber. Hasil analisis ini dapat dijadikan dasar untuk membuat program atau kebijakan terkait keamanan siber berikutnya khususnya bagi beberapa daerah yang memiliki tingkat IKBKS rendah.

Beberapa indeks yang digunakan dalam perhitungan dapat dijadikan acuan strategis untuk meningkatkan indeks yang memiliki nilai rendah. Peningkatan salah satu indeks berpotensi memberikan dampak yang signifikan terhadap kenaikan nilai indeks lainnya. Dengan demikian, Pemerintah Daerah dapat memanfaatkan hasil analisis ini untuk penentuan prioritas kebijakan terhadap indeks yang memiliki nilai rendah.

4.3.1 Aceh

Tabel 4.3 Nilai IKBKS Provinsi Aceh

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Aceh	3,15	3,21	1,03	2,46



Gambar 4.1 Grafik IKBKS Provinsi Aceh

Provinsi Aceh menunjukkan tingkat kematangan budaya keamanan siber dengan predikat Sadar, yang menandakan bahwa masyarakat dan pemangku kepentingan di wilayah ini telah memiliki kesadaran cukup baik terhadap pentingnya perlindungan data dan keamanan digital dalam aktivitas sehari-hari. Nilai Indeks SPRS Aceh sebesar 3,15 memperlihatkan bahwa strategi, program, regulasi, dan standar keamanan siber telah mulai diimplementasikan secara lebih terstruktur, meskipun masih memerlukan penguatan pada aspek konsistensi penerapan kebijakan.

Selanjutnya, Indeks IKKS yang mencapai 3,21 menunjukkan bahwa upaya-upaya teknis dalam penerapan keamanan siber di Aceh sudah berada pada tahap yang cukup baik, baik dari sisi teknologi, sistem perlindungan informasi, maupun penerapan praktik keamanan pada instansi pemerintah dan layanan publik. Hal ini menjadi indikator adanya komitmen pemerintah daerah dalam memperkuat kesiapan menghadapi potensi ancaman siber.

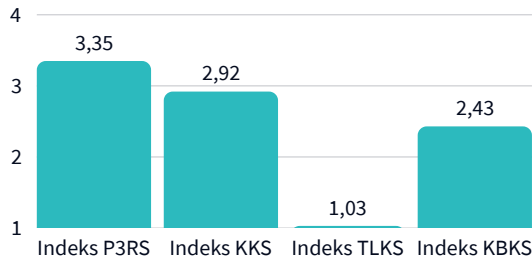
Namun demikian, capaian pada Indeks Keberhasilan Literasi yang bernilai 1,03 menegaskan masih adanya tantangan dalam meningkatkan kesadaran dan perilaku aman masyarakat ketika menggunakan teknologi digital. Literasi keamanan digital masih perlu diperluas melalui pendekatan edukatif yang menasar masyarakat umum, pelajar, pelaku UMKM, serta pengguna aktif media sosial yang berpotensi menjadi target serangan siber.

Dari keseluruhan indikator tersebut, nilai IKBKS Aceh sebesar 2,46 menempatkan provinsi ini pada kondisi yang cukup kuat dalam memulai budaya keamanan siber yang lebih matang. Dengan meningkatkan aspek literasi publik dan memperluas kolaborasi lintas sektor, Aceh memiliki peluang besar untuk mencapai kategori Sangat Sadar di masa mendatang, serta menjadi salah satu daerah yang mampu menerapkan transformasi digital secara aman, inklusif, dan berkelanjutan

4.3.2 Bali

Tabel 4.4 Nilai IKBKS Provinsi Bali

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Bali	3,35	2,92	1,03	2,43



Gambar 4.2 Grafik IKBKS Provinsi Bali

Provinsi Bali memperoleh nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,43, yang menempatkannya pada kategori Sadar. Kondisi ini mencerminkan bahwa masyarakat dan institusi di Bali telah menunjukkan tingkat kesadaran yang cukup terhadap pentingnya keamanan informasi dalam aktivitas digital, terutama dalam mendukung sektor-sektor strategis seperti pariwisata, ekonomi kreatif, dan pelayanan publik berbasis teknologi.

Nilai Indeks SPRS sebesar 3,35 menunjukkan bahwa perumusan strategi, program, regulasi, serta standar keamanan siber di Bali telah berjalan cukup baik dan terarah. Pemerintah daerah dinilai telah menunjukkan komitmen dalam merespons kebutuhan keamanan digital, terutama karena Bali merupakan salah satu tujuan internasional yang memiliki kerentanan lebih tinggi terhadap berbagai ancaman siber.

Sementara itu, Indeks IKKS yang berada pada angka 2,92 menggambarkan bahwa penerapan dan implementasi keamanan siber di berbagai sektor masih memerlukan peningkatan kapasitas, khususnya dalam proteksi data dan peningkatan infrastruktur keamanan pada layanan publik, lembaga swasta, hingga pelaku usaha yang bergantung pada sistem digital.

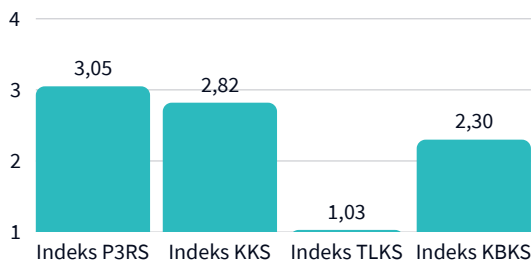
Di sisi lain, nilai Indeks Keberhasilan Literasi sebesar 1,03 menunjukkan bahwa pemahaman dan perilaku aman dalam dunia digital di tingkat masyarakat umum masih relatif rendah. Hal ini menjadi perhatian penting mengingat tingginya intensitas aktivitas digital yang dilakukan warga lokal maupun wisatawan yang berinteraksi dengan berbagai layanan digital di Bali.

Secara keseluruhan, Bali memiliki potensi besar untuk mengembangkan budaya keamanan siber yang lebih matang. Dengan meningkatkan literasi keamanan digital dan memperluas kerja sama lintas sektor, Bali diharapkan mampu memperkuat pertahanan siber untuk menjaga kepercayaan publik, stabilitas layanan pariwisata digital, serta keamanan data seluruh pengguna layanan teknologi di daerah tersebut.

4.3.3 Banten

Tabel 4.5 Nilai IKBKS Provinsi Banten

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Banten	3,05	2,82	1,03	2,30



Gambar 4.3 Grafik IKBKS Provinsi Banten

Provinsi Banten mencatatkan nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,30 dengan kategori Sadar. Hal ini mengindikasikan bahwa kesadaran mengenai pentingnya keamanan data dan perlindungan informasi dalam penggunaan teknologi digital telah mulai berkembang di masyarakat maupun lembaga pemerintahan di wilayah ini.

Nilai Indeks SPRS sebesar 3,05 menunjukkan bahwa strategi, program, regulasi, dan standar keamanan siber di Banten sudah mulai diterapkan secara menyeluruh, meskipun masih memerlukan peningkatan konsistensi dan pemantauan berkala untuk memastikan implementasinya berjalan efektif. Perkembangan ini juga berkaitan dengan posisi Banten sebagai daerah penyangga ibu kota yang memiliki intensitas kegiatan digital tinggi.

Pada aspek Indeks IKKS, Banten memperoleh nilai 2,82, yang menggambarkan bahwa upaya teknis dalam penerapan keamanan siber telah berjalan namun belum optimal. Masih diperlukan peningkatan pada sistem perlindungan data, terutama di sektor layanan publik dan industri yang mengelola informasi sensitif masyarakat.

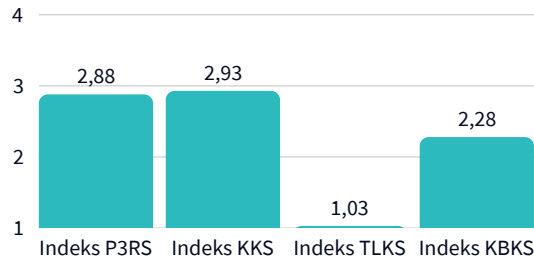
Sementara itu, Indeks Keberhasilan Literasi yang berada pada angka 1,03 menunjukkan bahwa kemampuan masyarakat dalam menerapkan perilaku aman saat menggunakan gawai, platform digital, maupun layanan internet masih harus terus ditingkatkan. Tantangan ini menjadi penting mengingat tingginya tingkat penetrasi internet dan aktivitas perdagangan digital di wilayah Banten.

Secara keseluruhan, kondisi ini menegaskan perlunya penguatan edukasi keamanan digital dan peningkatan kapasitas teknis untuk mengurangi potensi risiko siber yang semakin beragam. Dengan dukungan berbagai pihak, Banten berpeluang untuk meningkatkan kematangan budaya keamanan siber menuju kategori yang lebih tinggi di masa mendatang.

4.3.4 Bengkulu

Tabel 4.6 Nilai IKBKS Provinsi Bengkulu

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Bengkulu	2,88	2,93	1,03	2,28



Gambar 4.4 Grafik IKBKS Provinsi Bengkulu

Provinsi Bengkulu mencatatkan nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,28 dengan predikat Sadar. Hal ini menunjukkan bahwa masyarakat dan instansi di Bengkulu telah memiliki tingkat kesadaran yang cukup baik terhadap pentingnya keamanan siber dalam aktivitas digital, meskipun penerapannya masih perlu diperkuat secara lebih merata.

Nilai Indeks SPRS sebesar 2,88 mengindikasikan bahwa upaya penyusunan strategi, program, regulasi, serta standar keamanan siber di Bengkulu telah berjalan, namun masih dalam tahap pengembangan dan membutuhkan peningkatan kapasitas perencanaan serta pengawasan implementasinya.

Kemudian, Indeks IKKS dengan nilai 2,93 menunjukkan bahwa penerapan keamanan siber, khususnya pada sektor pemerintahan dan layanan digital publik, telah berlangsung cukup baik. Namun, penguatan infrastruktur dan kompetensi SDM keamanan siber tetap diperlukan untuk meningkatkan efektivitas proteksi terhadap potensi insiden digital.

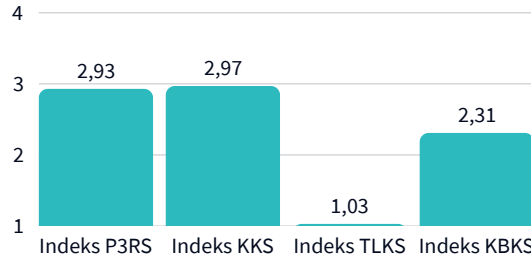
Sementara itu, Indeks Keberhasilan Literasi yang berada pada angka 1,03 menegaskan bahwa masyarakat masih membutuhkan edukasi lebih luas terkait praktik keamanan digital sehari-hari, seperti perlindungan data pribadi, penggunaan sandi yang aman, hingga kewaspadaan terhadap penipuan siber.

Dengan status saat ini, Bengkulu memiliki peluang besar untuk mencapai tingkat kematangan yang lebih tinggi melalui penguatan literasi keamanan siber serta kolaborasi lintas sektor dalam menciptakan ekosistem digital yang aman, adaptif, dan inklusif bagi seluruh masyarakat.

4.3.5 Daerah Istimewa Yogyakarta

Tabel 4.7 Nilai IKBKS Provinsi Daerah Istimewa Yogyakarta

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Daerah Istimewa Yogyakarta	2,93	2,97	1,03	2,31



Gambar 4.5 Grafik IKBKS Provinsi Daerah Istimewa Yogyakarta

Provinsi Daerah Istimewa Yogyakarta mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,31, yang termasuk kategori Sadar. Hal ini menandakan bahwa kesadaran masyarakat dan lembaga pemerintahan mengenai pentingnya keamanan digital sudah mulai terbentuk, meskipun praktik pengamanan data dan penggunaan layanan daring secara aman masih memerlukan penguatan di berbagai lapisan masyarakat.

Dari sisi kebijakan, Indeks SPRS sebesar 2,93 menunjukkan bahwa arah strategi dan regulasi keamanan siber telah dirumuskan dan mulai diterapkan. Provinsi ini menunjukkan komitmen untuk membangun tata kelola keamanan digital yang sistematis, khususnya pada sektor pendidikan, pemerintahan, dan layanan publik.

Indeks IKKS sebesar 2,97 mengindikasikan bahwa kemampuan teknis dalam menjaga keamanan sistem informasi relatif baik. Infrastruktur dan kontrol keamanan mulai diterapkan secara konsisten, meskipun peningkatan kapasitas SDM serta kesiapan menghadapi insiden siber tetap menjadi fokus utama agar sistem lebih tangguh dan adaptif.

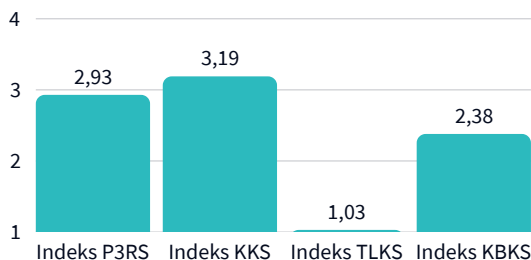
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menunjukkan bahwa literasi masyarakat terkait risiko digital masih terbatas. Program edukasi dan sosialisasi lebih luas diperlukan agar warga dapat mengenali ancaman siber, melindungi data pribadi, dan memanfaatkan layanan digital secara aman.

Secara keseluruhan, Daerah Istimewa Yogyakarta memiliki peluang besar untuk memperkuat budaya keamanan siber melalui pengembangan literasi masyarakat, optimalisasi kapasitas teknis, dan penguatan tata kelola keamanan informasi. Langkah-langkah ini akan mendukung terciptanya ekosistem digital yang aman, adaptif, dan berkelanjutan bagi seluruh masyarakat provinsi ini.

4.3.6 DKI Jakarta

Tabel 4.8 Nilai IKBKS Provinsi DKI Jakarta

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
DKI Jakarta	2,93	3,19	1,03	2,38



Gambar 4.6 Grafik IKBKS Provinsi DKI Jakarta

Provinsi DKI Jakarta mencatatkan nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,38 dengan predikat Sadar. Sebagai pusat pemerintahan dan ekonomi nasional, tingkat aktivitas digital masyarakat Jakarta sangat tinggi, sehingga kesadaran terhadap keamanan informasi sudah mulai tumbuh kuat, baik di kalangan pemerintah, swasta, maupun pengguna individu.

Nilai Indeks SPRS sebesar 2,93 menunjukkan bahwa upaya penyusunan strategi, program, regulasi, serta standar keamanan siber telah dilakukan secara cukup matang. Pemerintah provinsi bersama berbagai lembaga dan sektor swasta aktif dalam mendukung tata kelola keamanan siber, sejalan dengan kebutuhan layanan publik yang semakin terintegrasi secara digital.

Sementara itu, Indeks IKKS yang mencapai 3,19 mengindikasikan bahwa penerapan teknis keamanan siber di Jakarta berada pada level yang cukup baik. Sistem perlindungan data, pusat komando keamanan siber, hingga infrastruktur teknologi memiliki kesiapan yang relatif lebih tinggi dibandingkan banyak provinsi lainnya di Indonesia.

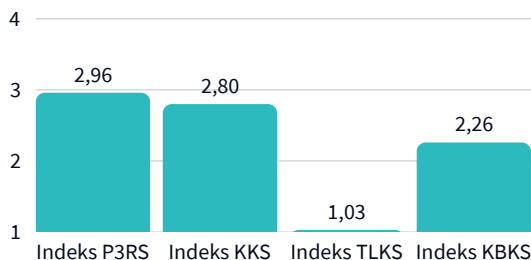
Namun demikian, Indeks Keberhasilan Literasi yang masih berada pada angka 1,03 menunjukkan bahwa peningkatan literasi keamanan digital di masyarakat tetap menjadi kebutuhan mendesak. Tingginya aktivitas digital dan penggunaan layanan berbasis internet menjadikan pengguna Jakarta rentan terhadap kejahatan siber apabila kesadaran dan praktik keamanan sibernya tidak diperkuat.

Secara keseluruhan, DKI Jakarta memiliki potensi besar untuk menjadi salah satu provinsi dengan tingkat kematangan keamanan siber tertinggi di Indonesia. Dengan memperluas jangkauan edukasi keamanan digital kepada seluruh lapisan masyarakat dan memperkuat kolaborasi lintas sektor, Jakarta dapat lebih siap menghadapi dinamika ancaman siber di tengah percepatan transformasi digital nasional.

4.3.7 Gorontalo

Tabel 4.9 Nilai IKBKS Provinsi Gorontalo

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Gorontalo	2,96	2,80	1,03	2,26



Gambar 4.7 Grafik IKBKS Provinsi Gorontalo

Provinsi Gorontalo memperoleh nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,26 dengan predikat Sadar. Hal ini menandakan bahwa kesadaran masyarakat dan institusi di Gorontalo mengenai pentingnya keamanan informasi dalam penggunaan teknologi sudah mulai terbangun, meskipun penguatan pada berbagai aspek masih sangat diperlukan guna mencapai kematangan yang lebih optimal.

Nilai Indeks SPRS sebesar 2,96 menunjukkan bahwa strategi, program, regulasi, serta standar keamanan siber telah mulai diformulasikan dan diimplementasikan secara bertahap di wilayah ini. Dukungan pemerintah daerah dalam membangun tata kelola keamanan digital menjadi modal penting bagi penguatan lingkungan siber yang aman dan tepercaya.

Adapun Indeks IKKS dengan nilai 2,80 mengindikasikan bahwa penerapan teknis keamanan siber di berbagai sektor sudah berjalan, namun masih menghadapi tantangan pada aspek infrastruktur dan efektivitas perlindungan data. Penyempurnaan mekanisme pengamanan serta peningkatan kapasitas SDM perlu terus diupayakan, khususnya pada layanan publik berbasis digital.

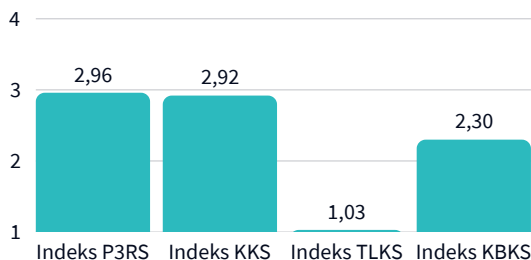
Sementara itu, Indeks Keberhasilan Literasi yang bernilai 1,03 menunjukkan bahwa upaya literasi keamanan digital bagi masyarakat masih harus ditingkatkan. Masyarakat perlu mendapatkan pemahaman yang lebih luas mengenai risiko kejahatan siber dan cara menjaga keamanan akun serta data pribadi dalam aktivitas online.

Secara keseluruhan, Gorontalo berada dalam posisi yang memiliki potensi besar untuk meningkatkan kematangan budaya keamanan siber ke kategori yang lebih tinggi. Dengan penguatan sinergi antara pemerintah daerah, lembaga pendidikan, serta pelaku industri digital, transformasi digital di Gorontalo dapat berlangsung lebih aman, adaptif, dan berkelanjutan.

4.3.8 Jambi

Tabel 4.10 Nilai IKBKS Provinsi Jambi

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Jambi	2,96	2,92	1,03	2,30



Gambar 4.8 Grafik IKBKS Provinsi Jambi

Provinsi Jambi meraih nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,30 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran terhadap pentingnya keamanan informasi dalam penggunaan teknologi digital sudah mulai terbentuk pada masyarakat dan instansi pemerintah di daerah ini, meskipun implementasinya masih perlu diperkuat secara lebih merata.

Nilai Indeks SPRS sebesar 2,96 menggambarkan bahwa Jambi telah berupaya mengembangkan strategi, program, regulasi, serta standar keamanan siber yang dibutuhkan dalam menghadapi dinamika transformasi digital. Dukungan kebijakan dan komitmen pemerintah daerah menjadi salah satu faktor pendorong terciptanya tata kelola keamanan informasi yang lebih terarah.

Pada Indeks IKKS, Jambi mencatatkan nilai 2,92 yang menunjukkan bahwa implementasi keamanan siber pada berbagai sektor—baik pemerintahan maupun layanan publik digital—telah berjalan cukup baik. Meski begitu, masih diperlukan peningkatan pada aspek keamanan teknis dan tata kelola data untuk meminimalkan risiko pencurian informasi dan serangan siber.

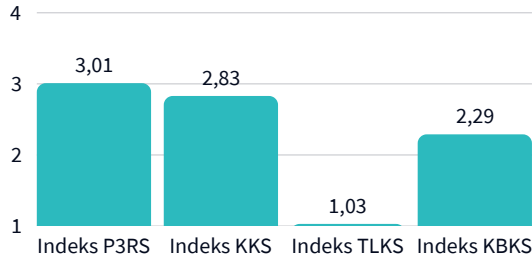
Sementara itu, Indeks Keberhasilan Literasi yang berada pada angka 1,03 menandakan bahwa edukasi mengenai perilaku aman dalam bermedia digital masih harus terus diperkuat. Literasi keamanan digital yang rendah dapat menimbulkan kerentanan terhadap penipuan online, kebocoran data pribadi, serta ancaman siber lainnya.

Dengan kondisi saat ini, Jambi memiliki potensi besar untuk meningkatkan kematangan budaya keamanan siber ke tingkat yang lebih tinggi melalui penguatan kapasitas SDM, kolaborasi lintas sektor, dan program literasi yang lebih menyentuh seluruh lapisan masyarakat. Langkah tersebut dapat mendorong terciptanya ekosistem digital yang aman, adaptif, dan berkelanjutan.

4.3.9 Jawa Barat

Tabel 4.11 Nilai IKBKS Provinsi Jawa Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Jawa Barat	3,01	2,83	1,03	2,29



Gambar 4.9 Grafik IKBKS Provinsi Jawa Barat

Provinsi Jawa Barat memperoleh nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,29 dengan predikat Sadar. Capaian ini menunjukkan bahwa kesadaran masyarakat Jawa Barat terhadap pentingnya keamanan siber dalam penggunaan teknologi digital sudah mulai cukup kuat, mengingat wilayah ini merupakan salah satu provinsi dengan populasi terbesar dan aktivitas digital yang sangat tinggi di Indonesia.

Nilai Indeks SPRS sebesar 3,01 memperlihatkan bahwa strategi, program, regulasi, dan standar keamanan siber telah disusun dan mulai diterapkan secara sistematis di tingkat pemerintahan daerah. Hal ini sejalan dengan meningkatnya kebutuhan layanan publik berbasis digital dan perkembangan ekonomi kreatif yang signifikan di wilayah Jawa Barat.

Untuk Indeks IKKS, Jawa Barat mencatatkan nilai 2,83 yang menunjukkan bahwa penerapan keamanan siber pada berbagai sektor sudah berjalan, namun masih memerlukan peningkatan infrastruktur dan tata kelola sistem keamanan yang lebih kuat, terutama untuk menangani volume aktivitas digital masyarakat yang sangat besar.

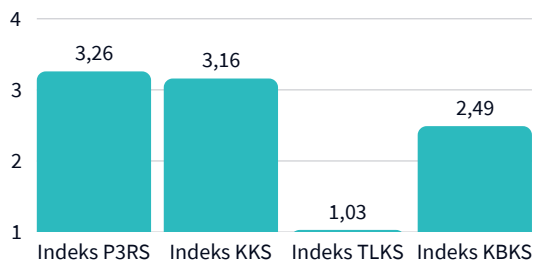
Sementara itu, Indeks Keberhasilan Literasi sebesar 1,03 menunjukkan bahwa literasi keamanan digital masyarakat masih harus terus ditingkatkan. Rendahnya pemahaman masyarakat terhadap risiko kejahatan siber seperti phishing, penipuan digital, dan kebocoran data menjadi tantangan utama dalam mewujudkan lingkungan digital yang aman.

Dengan potensi teknologi dan sumber daya manusia yang tinggi, Jawa Barat memiliki peluang besar untuk meningkatkan kematangan budaya keamanan siber. Penguatan edukasi keamanan informasi, pemanfaatan inovasi digital secara aman, serta peningkatan kolaborasi lintas sektor akan menjadi kunci penting dalam menghadapi berkembangnya ancaman siber di masa depan.

4.3.10 Jawa Tengah

Tabel 4.12 Nilai IKBKS Provinsi Jawa Tengah

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Jawa Tengah	3,26	3,16	1,03	2,49



Gambar 4.10 Grafik IKBKS Provinsi Jawa Tengah

Provinsi Jawa Tengah memperoleh nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,49 dengan predikat Sadar. Hal ini menunjukkan bahwa masyarakat dan pemangku kepentingan di Jawa Tengah telah memiliki tingkat kesadaran yang cukup baik terhadap pentingnya keamanan informasi dalam aktivitas digital, terlebih dengan semakin berkembangnya layanan publik dan sektor ekonomi berbasis teknologi di wilayah ini.

Nilai Indeks SPRS yang mencapai 3,26 memperlihatkan bahwa strategi, program, regulasi, dan standar keamanan siber telah dirancang dengan baik dan mulai diimplementasikan secara luas. Pemerintah daerah menunjukkan komitmen dalam membangun tata kelola keamanan digital yang selaras dengan kebutuhan transformasi digital di berbagai sektor.

Selanjutnya, Indeks IKKS sebesar 3,16 menunjukkan bahwa implementasi keamanan siber pada sistem layanan publik, pemerintahan, dan sektor komersial berjalan pada tingkat yang cukup efektif. Penerapan kontrol keamanan dan infrastruktur pendukung relatif kuat, sehingga membantu meminimalkan risiko serangan siber yang dapat mengganggu pelayanan masyarakat.

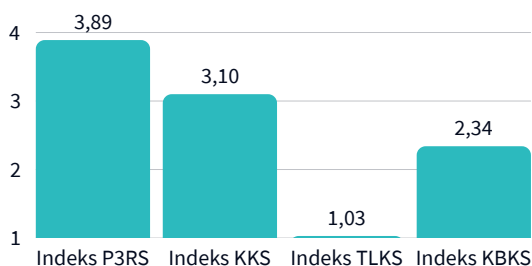
Meskipun demikian, Indeks Keberhasilan Literasi yang masih berada pada angka 1,03 menegaskan bahwa edukasi terkait literasi keamanan digital pada masyarakat umum perlu terus diperluas. Tantangan ini menjadi perhatian penting mengingat tingginya penetrasi internet dan keterlibatan warga dalam aktivitas ekonomi digital, pendidikan daring, serta interaksi melalui media sosial.

Dengan potensi sumber daya manusia serta dukungan kebijakan yang kuat, Provinsi Jawa Tengah memiliki peluang besar untuk meningkatkan kematangan budaya keamanan siber menuju kategori yang lebih tinggi. Penguatan literasi keamanan digital dan kolaborasi antar lembaga menjadi langkah strategis dalam mewujudkan ekosistem digital yang aman, adaptif, dan inklusif bagi seluruh masyarakat.

4.3.11 Jawa Timur

Tabel 4.13 Nilai IKBKS Provinsi Jawa Timur

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Jawa Timur	3,89	3,10	1,03	2,34



Gambar 4.11 Grafik IKBKS Provinsi Jawa Timur

Provinsi Jawa Timur mencatatkan nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,34 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran mengenai pentingnya keamanan informasi dalam aktivitas digital sudah mulai tertanam baik pada masyarakat maupun lembaga pemerintahan di wilayah ini. Sebagai salah satu provinsi dengan populasi besar dan aktivitas ekonomi digital yang meningkat, perhatian terhadap keamanan siber menjadi kebutuhan yang semakin relevan.

Nilai Indeks SPRS sebesar 2,89 menunjukkan bahwa strategi, program, dan regulasi keamanan siber telah dirancang dan dijalankan, namun masih perlu diperkuat untuk meningkatkan efektivitas tata kelola keamanan informasi, terutama pada sektor yang memiliki risiko tinggi kebocoran data.

Sementara itu, Indeks IKKS dengan nilai 3,10 mengindikasikan bahwa penerapan teknis keamanan siber pada layanan publik dan pemerintahan di Jawa Timur berada pada tingkat yang cukup baik. Infrastruktur keamanan siber yang sudah mulai terbangun menjadi modal penting dalam mencegah, mendeteksi, dan menanggulangi potensi serangan siber.

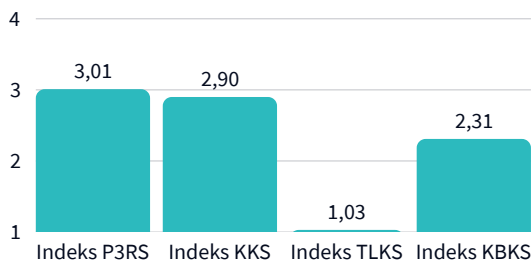
Namun, Indeks Keberhasilan Literasi sebesar 1,03 menunjukkan bahwa literasi keamanan digital masyarakat masih membutuhkan perhatian serius. Di tengah tingginya penggunaan layanan online, e-commerce, dan media sosial, pemahaman masyarakat tentang risiko digital perlu terus ditingkatkan agar tidak mudah terjebak dalam berbagai bentuk kejahatan siber.

Secara keseluruhan, dengan besarnya potensi ekonomi digital dan inovasi teknologi di Jawa Timur, peningkatan kapasitas SDM dan perluasan program literasi keamanan siber akan menjadi langkah krusial dalam memperkuat ekosistem digital yang aman, tangguh, dan berkelanjutan di masa mendatang.

4.3.12 Kalimantan Barat

Tabel 4.14 Nilai IKBKS Provinsi Kalimantan Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kalimantan Barat	3,01	2,90	1,03	2,31



Gambar 4.12 Grafik IKBKS Provinsi Kalimantan Barat

Provinsi Kalimantan Barat mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,31 dengan predikat Sadar. Artinya, tingkat kesadaran masyarakat dan institusi mengenai pentingnya keamanan digital sudah mulai tumbuh, meskipun penerapannya masih belum merata. Pemanfaatan teknologi dalam pelayanan publik dan aktivitas ekonomi menuntut penguatan pemahaman tentang risiko siber yang dapat mengancam data dan privasi.

Indeks SPRS sebesar 3,01 menunjukkan bahwa strategi, program, dan regulasi keamanan siber di Kalimantan Barat sudah dirancang dengan cukup baik dan mulai diimplementasikan pada berbagai sektor layanan digital. Namun, evaluasi dan peningkatan berkelanjutan tetap diperlukan agar pelaksanaannya lebih efektif dan menjangkau seluruh lapisan.

Kemudian, Indeks IKKS dengan nilai 2,90 memperlihatkan bahwa infrastruktur teknis keamanan informasi sudah tersedia dan diterapkan, namun masih belum sepenuhnya optimal dalam melindungi layanan publik, terutama pada daerah dengan kemampuan teknologi yang masih berkembang.

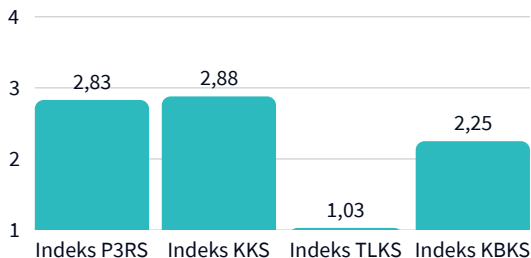
Di sisi lain, Indeks Keberhasilan Literasi hanya sebesar 1,03, mengindikasikan bahwa literasi keamanan digital di tingkat masyarakat masih lemah. Minimnya pemahaman mengenai ancaman siber dapat meningkatkan risiko terhadap phishing, penipuan digital, maupun kebocoran data pribadi, terutama seiring meningkatnya transaksi online dan penggunaan media sosial.

Secara keseluruhan, Kalimantan Barat memiliki fondasi yang cukup baik dalam strategi dan infrastruktur keamanan siber, namun peningkatan kapasitas sumber daya manusia dan edukasi literasi digital perlu menjadi fokus utama. Jika kedua aspek ini diperkuat, provinsi ini akan mampu membangun ekosistem digital yang lebih aman, adaptif, dan mampu menjawab tantangan siber di masa mendatang.

4.3.13 Kalimantan Selatan

Tabel 4.15 Nilai IKBKS Provinsi Kalimantan Selatan

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kalimantan Selatan	2,83	2,88	1,03	2,25



Gambar 4.13 Grafik IKBKS Provinsi Kalimantan Selatan

Provinsi Kalimantan Selatan mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,25 dengan predikat Sadar. Pencapaian ini menunjukkan bahwa pemahaman terhadap pentingnya keamanan informasi di ruang digital sudah mulai terbentuk, baik di kalangan masyarakat maupun institusi pemerintahan. Namun, budaya perlindungan data dan kewaspadaan terhadap ancaman siber masih perlu diperkuat secara konsisten.

Nilai Indeks SPRS sebesar 2,83 mengindikasikan bahwa strategi, program, dan regulasi keamanan siber telah tersedia, meskipun implementasinya belum optimal. Perlu ada peningkatan dalam pengawasan, evaluasi, serta penyempurnaan mekanisme tata kelola keamanan siber, terutama pada sektor yang memiliki risiko paparan data yang lebih besar.

Dari sisi teknis, Indeks IKKS yang mencapai 2,88 menggambarkan bahwa kesiapan infrastruktur dan penerapan kontrol keamanan pada layanan publik telah berjalan cukup baik. Meski begitu, peningkatan kemampuan deteksi dan respons terhadap insiden digital masih menjadi tantangan yang harus segera diperhatikan.

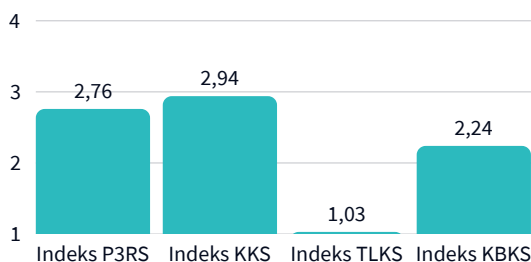
Sementara itu, Indeks Keberhasilan Literasi yang masih berada pada angka 1,03 mengonfirmasi bahwa tingkat literasi keamanan digital masyarakat berada pada kategori rendah. Di tengah meningkatnya pemanfaatan layanan digital dalam berbagai aktivitas, masyarakat harus diberikan edukasi yang lebih luas mengenai cara berinternet yang aman dan bertanggung jawab untuk meminimalkan potensi ancaman yang dapat merugikan diri sendiri maupun lingkungan sekitar.

Secara keseluruhan, Kalimantan Selatan memiliki potensi yang baik dalam penguatan ekosistem keamanan siber. Dengan peningkatan implementasi kebijakan, pembinaan SDM, serta program literasi keamanan digital yang berkelanjutan, provinsi ini dapat mencapai tingkat kematangan budaya keamanan siber yang lebih unggul dan adaptif terhadap perkembangan teknologi di masa mendatang.

4.3.14 Kalimantan Tengah

Tabel 4.16 Nilai IKBKS Provinsi Kalimantan Tengah

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kalimantan Tengah	2,76	2,94	1,03	2,24



Gambar 4.14 Grafik IKBKS Provinsi Kalimantan Tengah

Provinsi Kalimantan Tengah mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,24 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran mengenai pentingnya perlindungan data dan keamanan aktivitas digital telah mulai berkembang, meskipun belum menyeluruh dan masih memerlukan penguatan di berbagai lapisan masyarakat dan institusi pemerintahan.

Dengan Indeks SPRS yang berada pada angka 2,76, dapat dilihat bahwa perencanaan strategi, program, dan regulasi keamanan siber sudah dirumuskan, tetapi implementasinya masih menghadapi sejumlah tantangan. Penguatan kebijakan dan peningkatan efektivitas pelaksanaan kebijakan sangat dibutuhkan untuk meminimalkan risiko yang dapat mengganggu stabilitas keamanan informasi.

Sementara itu, Indeks IKKS dengan nilai 2,94 menunjukkan bahwa kesiapan teknis keamanan siber pada layanan publik sudah cukup baik. Infrastruktur pendukung keamanan digital telah tersedia dan digunakan, meskipun peningkatan pada kemampuan respons terhadap potensi insiden siber masih menjadi prioritas.

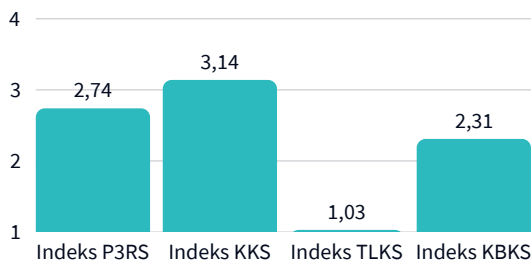
Namun, Indeks Keberhasilan Literasi sebesar 1,03 mencerminkan bahwa tingkat literasi keamanan siber masyarakat masih rendah. Dalam konteks pemanfaatan teknologi digital yang semakin meluas, masyarakat perlu dibekali pemahaman lebih mendalam mengenai ancaman siber serta cara untuk menjaga keamanan data pribadi, agar tidak mudah terjebak dalam aksi kriminal digital.

Secara keseluruhan, Kalimantan Tengah memiliki posisi yang cukup baik untuk melakukan akselerasi dalam pembangunan budaya keamanan siber. Melalui peningkatan kapasitas SDM, edukasi publik yang lebih terarah, dan penguatan regulasi secara bertahap, provinsi ini berpotensi untuk mencapai tingkat kematangan keamanan siber yang lebih adaptif dan berkelanjutan di masa mendatang.

4.3.15 Kalimantan Timur

Tabel 4.17 Nilai IKBKS Provinsi Kalimantan Timur

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kalimantan Timur	2,74	3,14	1,03	2,31



Gambar 4.15 Grafik IKBKS Provinsi Kalimantan Timur

Provinsi Kalimantan Timur mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,31 dengan predikat Sadar. Capaian ini menunjukkan bahwa kesadaran terhadap keamanan aktivitas digital sudah mulai berkembang baik di lingkup masyarakat maupun lembaga pemerintahan. Sebagai wilayah yang ditunjuk sebagai lokasi Ibu Kota Negara (IKN) Nusantara, perhatian terhadap keamanan informasi menjadi semakin penting seiring meningkatnya pembangunan infrastruktur digital dan mobilitas data.

Nilai Indeks SPRS sebesar 2,74 menandakan bahwa strategi, program, serta regulasi keamanan siber telah dirumuskan, namun masih memerlukan penguatan dalam pelaksanaan dan koordinasi lintas sektor. Upaya ini perlu dilakukan terutama untuk memastikan perlindungan data pada layanan publik yang terus bertransformasi secara digital.

Dari sisi penerapan teknis, Indeks KKS sebesar 3,14 menunjukkan bahwa infrastruktur keamanan siber di Kalimantan Timur sudah cukup memadai. Layanan publik dan sistem pemerintahan telah menerapkan berbagai kontrol keamanan sebagai upaya dalam mendeteksi serta merespons potensi serangan siber. Hal ini menjadi fondasi penting untuk menciptakan sistem digital yang tangguh dan berketahanan.

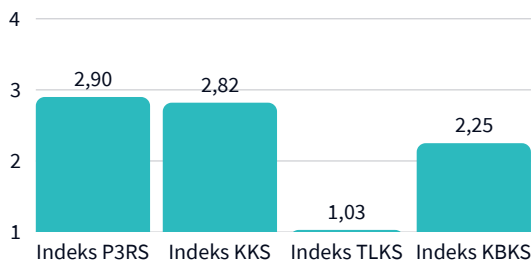
Di sisi lain, Indeks Keberhasilan Literasi yang berada pada angka 1,03 menggambarkan bahwa tingkat literasi keamanan digital masyarakat masih memerlukan perhatian lebih. Dengan meningkatnya penggunaan internet, e-commerce, serta layanan berbasis aplikasi, edukasi keamanan siber menjadi aspek krusial untuk menghindarkan masyarakat dari risiko seperti phishing, penipuan digital, maupun penyalahgunaan data pribadi.

Secara keseluruhan, Kalimantan Timur memiliki potensi besar untuk menghadirkan ekosistem digital yang aman, terlebih dengan kehadiran IKN Nusantara yang menuntut standar keamanan informasi yang lebih tinggi. Percepatan peningkatan kapasitas SDM, kesadaran publik, serta penguatan strategi keamanan siber akan menjadi kunci dalam mewujudkan budaya keamanan siber yang adaptif dan berkelanjutan di provinsi ini.

4.3.16 Kalimantan Utara

Tabel 4.18 Nilai IKBKS Provinsi Kalimantan Utara

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kalimantan Utara	2,90	2,82	1,03	2,25



Gambar 4.16 Grafik IKBKS Provinsi Kalimantan Utara

Provinsi Kalimantan Utara mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,25 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran masyarakat dan instansi pemerintahan mengenai pentingnya keamanan informasi dalam aktivitas digital telah mulai tumbuh, meskipun masih perlu diperkuat secara lebih luas dan sistematis.

Nilai Indeks SPRS sebesar 2,90 mencerminkan bahwa strategi, program, dan regulasi keamanan siber telah disusun dan mulai dijalankan. Namun, efektivitas implementasi kebijakan tersebut masih perlu ditingkatkan, terutama dalam penguatan tata kelola keamanan informasi pada sektor-sektor layanan publik yang bersinggungan langsung dengan data masyarakat.

Dari sisi penerapan kontrol keamanan, Indeks IKKS yang berada pada angka 2,82 menunjukkan bahwa kesiapan teknis dalam menjalankan keamanan siber dinilai cukup. Infrastruktur dasar telah tersedia, tetapi peningkatan kemampuan deteksi ancaman dan kecepatan respons terhadap insiden digital masih menjadi tantangan yang harus terus dioptimalkan.

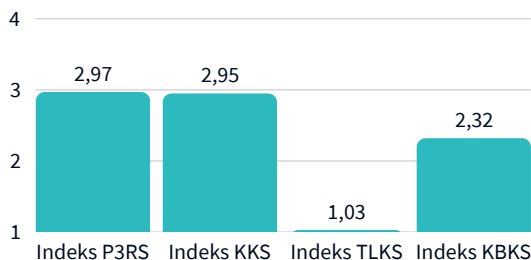
Sementara itu, Indeks Keberhasilan Literasi sebesar 1,03 mengisyaratkan bahwa tingkat literasi keamanan digital masyarakat masih rendah. Dengan bertambahnya pemanfaatan internet, layanan berbasis aplikasi, serta aktivitas ekonomi digital, dibutuhkan edukasi yang lebih intensif untuk mencegah masyarakat terpapar risiko kejahatan siber seperti penipuan online dan penyalahgunaan data pribadi.

Secara keseluruhan, Kalimantan Utara memiliki peluang besar dalam memperkuat budaya keamanan siber seiring pertumbuhan aktivitas digital di wilayahnya. Melalui peningkatan kapasitas sumber daya manusia, kolaborasi lintas sektor, serta program literasi keamanan siber yang lebih masif dan terarah, provinsi ini berpotensi mencapai tingkat kematangan keamanan siber yang lebih tangguh dan adaptif di masa mendatang.

4.3.17 Kepulauan Bangka Belitung

Tabel 4.19 Nilai IKBKS Provinsi Kepulauan Bangka Belitung

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kepulauan Bangka Belitung	2,97	2,95	1,03	2,32



Gambar 4.17 Grafik IKBKS Provinsi Kepulauan Bangka Belitung

Provinsi Kepulauan Bangka Belitung memperoleh Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,32 dengan predikat Sadar. Capaian ini menunjukkan bahwa pemahaman mengenai pentingnya keamanan siber telah mulai tumbuh di tengah masyarakat dan lembaga pemerintahan, meskipun upaya peningkatan budaya kewaspadaan digital masih perlu dilanjutkan secara berkelanjutan.

Dengan Indeks SPRS sebesar 2,97, dapat disimpulkan bahwa strategi, program, serta regulasi keamanan siber telah disusun dan mulai diimplementasikan, namun masih memerlukan penguatan untuk lebih memberikan dampak nyata, khususnya dalam melindungi data publik dan layanan pemerintahan yang semakin terdigitalisasi.

Sementara itu, Indeks IKKS yang mencapai 2,95 mengindikasikan bahwa kesiapan teknis keamanan informasi di provinsi ini cukup baik. Infrastruktur dan kontrol keamanan pada sistem layanan digital sudah mulai diterapkan untuk mencegah dan menanggulangi ancaman siber yang dapat mengganggu pelayanan publik.

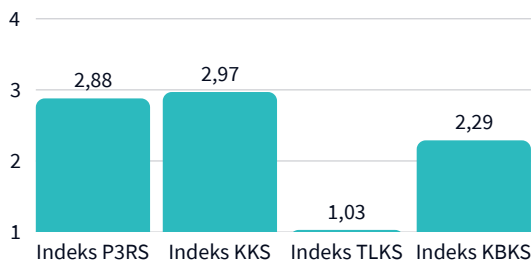
Namun, Indeks Keberhasilan Literasi sebesar 1,03 menegaskan bahwa pengetahuan dan keterampilan masyarakat terkait keamanan digital masih berada pada tingkat rendah. Edukasi dan kampanye literasi siber perlu ditingkatkan agar masyarakat mampu mengidentifikasi, menghindari, serta melaporkan potensi kejahatan siber yang mereka hadapi dalam aktivitas digital sehari-hari.

Secara keseluruhan, Kepulauan Bangka Belitung berada pada jalur yang tepat dalam meningkatkan ekosistem keamanan siber. Dengan memperkuat kolaborasi lintas sektor, meningkatkan kapasitas sumber daya manusia, serta memperluas cakupan literasi keamanan digital, provinsi ini berpotensi mencapai tingkat kematangan budaya keamanan siber yang lebih baik dan berkelanjutan dalam menghadapi perkembangan teknologi di masa mendatang.

4.3.18 Kepulauan Riau

Tabel 4.20 Nilai IKBKS Provinsi Kepulauan Riau

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Kepulauan Riau	2,88	2,97	1,03	2,29



Gambar 4.18 Grafik IKBKS Provinsi Kepulauan Riau

Provinsi Kepulauan Riau mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,29 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran terhadap keamanan informasi dalam aktivitas digital telah mulai berkembang pada masyarakat dan lembaga pemerintahan, terutama di wilayah yang menjadi pusat aktivitas industri dan perdagangan internasional ini.

Dengan Indeks SPRS sebesar 2,88, terlihat bahwa strategi dan regulasi terkait keamanan siber sudah disusun serta mulai diterapkan. Meski demikian, upaya penguatan tata kelola keamanan siber masih diperlukan untuk memastikan perlindungan data berjalan lebih efektif, mengingat tingginya pergerakan data lintas batas di wilayah ini.

Sementara itu, Indeks IKKS sebesar 2,97 menggambarkan bahwa kesiapan teknis serta penerapan kontrol keamanan pada layanan digital pemerintahan cukup baik. Infrastruktur keamanan siber telah mendukung penyelenggaraan sistem informasi yang lebih aman, meskipun perlu peningkatan kemampuan respons terhadap insiden siber yang mungkin terjadi.

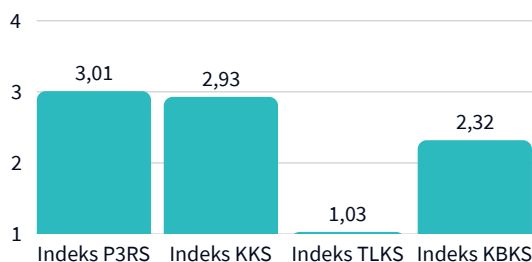
Namun, Indeks Keberhasilan Literasi yang masih berada pada nilai 1,03 menunjukkan bahwa masyarakat perlu diberikan pemahaman yang lebih kuat mengenai keamanan digital. Dengan tingginya penggunaan teknologi dalam aktivitas ekonomi, interaksi sosial, hingga layanan pemerintahan, literasi siber menjadi faktor kunci dalam mencegah kerugian akibat kejahatan digital.

Secara keseluruhan, Kepulauan Riau memiliki potensi besar untuk terus memperkuat budaya keamanan siber. Dengan penguatan edukasi publik, peningkatan kompetensi SDM, serta implementasi strategi keamanan informasi yang lebih adaptif, provinsi ini dapat mencapai ekosistem digital yang aman, berdaya saing, dan mendukung pertumbuhan ekonomi yang berkelanjutan.

4.3.19 Lampung

Tabel 4.21 Nilai IKBKS Provinsi Lampung

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Lampung	3,01	2,93	1,03	2,32



Gambar 4.19 Grafik IKBKS Provinsi Lampung

Provinsi Lampung mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,32 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran akan pentingnya keamanan informasi mulai tertanam dalam aktivitas digital masyarakat maupun institusi pemerintahan. Namun, upaya peningkatan budaya kewaspadaan siber masih perlu dilakukan secara konsisten untuk menghadapi dinamika ancaman digital yang semakin kompleks.

Dengan Indeks SPRS sebesar 3,01, dapat terlihat bahwa strategi, program, dan regulasi keamanan siber sudah direncanakan dan diimplementasikan dengan cukup baik. Meskipun demikian, efektivitas pelaksanaan kebijakan tetap perlu diperkuat agar mampu memberikan perlindungan yang optimal terhadap data dan layanan publik yang semakin terdigitalisasi.

Pada aspek teknis, Indeks IKKS mencapai 2,93, mengindikasikan bahwa infrastruktur serta penerapan kontrol keamanan siber di sektor pemerintahan telah berjalan cukup baik. Hal ini menjadi modal penting dalam menjaga keberlangsungan operasional digital sekaligus meningkatkan kepercayaan masyarakat terhadap layanan publik berbasis teknologi.

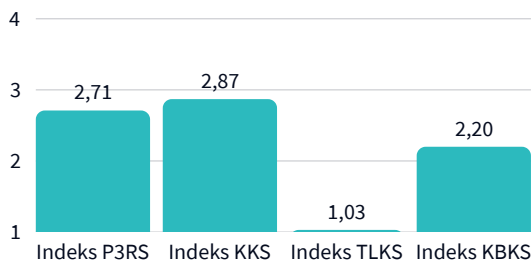
Sementara itu, Indeks Keberhasilan Literasi yang masih di angka 1,03 menunjukkan bahwa literasi keamanan siber masyarakat masih berada pada tingkat rendah. Dengan meningkatnya penggunaan internet dan layanan berbasis aplikasi dalam kehidupan sehari-hari, peningkatan pemahaman masyarakat mengenai ancaman siber perlu menjadi perhatian utama agar mereka dapat melindungi data dan identitas digitalnya secara mandiri.

Secara keseluruhan, Lampung memiliki potensi yang baik untuk memperkuat ekosistem keamanan siber di wilayahnya. Melalui penguatan regulasi, peningkatan kapasitas SDM, serta edukasi keamanan digital yang merata, provinsi ini dapat meningkatkan tingkat kematangan budaya keamanan siber menuju kategori yang lebih adaptif dan tangguh di masa depan.

4.3.20 Maluku

Tabel 4.22 Nilai IKBKS Provinsi Maluku

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Maluku	2,71	2,87	1,03	2,20



Gambar 4.20 Grafik IKBKS Provinsi Maluku

Provinsi Maluku mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,20 dengan predikat Sadar. Meskipun berada pada tingkat kesadaran awal, hal ini menunjukkan bahwa upaya perlindungan data dan keamanan informasi di ruang digital sudah mulai mendapat perhatian di lingkungan masyarakat maupun pemerintah daerah, meskipun masih perlu diperluas secara signifikan.

Dengan Indeks SPRS sebesar 2,71, terlihat bahwa strategi dan program keamanan siber telah mulai dirumuskan dan diimplementasikan. Namun, efektivitas tata kelola keamanan digital masih perlu diperkuat terutama di sektor-sektor layanan publik yang memanfaatkan sistem berbasis teknologi dalam operasionalnya.

Sementara itu, Indeks IKKS mencapai angka 2,87, yang mengindikasikan bahwa infrastruktur dan penerapan teknis keamanan siber sudah berjalan cukup baik. Kontrol keamanan pada sistem informasi telah tersedia sebagai bentuk upaya mencegah dan mengatasi potensi serangan siber yang dapat mengganggu pelaksanaan layanan pemerintahan.

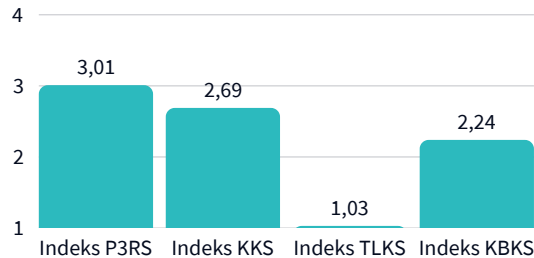
Namun, Indeks Keberhasilan Literasi yang masih bernilai 1,03 menandakan bahwa literasi keamanan digital masyarakat berada pada tingkat rendah. Di tengah peningkatan penggunaan internet untuk kegiatan sosial, pendidikan, maupun ekonomi, edukasi mengenai risiko digital dan langkah pencegahannya harus menjadi prioritas penting demi terciptanya masyarakat yang lebih terlindungi di dunia maya.

Secara keseluruhan, Provinsi Maluku memiliki tantangan sekaligus peluang besar dalam memperkuat budaya keamanan siber. Dengan meningkatkan kualitas sumber daya manusia, memperluas akses edukasi keamanan digital, serta memperkuat kebijakan keamanan informasi, Maluku dapat membangun ekosistem digital yang lebih aman, inklusif, dan berkelanjutan di masa mendatang.

4.3.21 Maluku Utara

Tabel 4.23 Nilai IKBKS Provinsi Maluku Utara

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Maluku Utara	3,01	2,69	1,03	2,24



Gambar 4.21 Grafik IKBKS Provinsi Maluku Utara

Provinsi Maluku Utara mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,24 dengan predikat Sadar. Hal ini menunjukkan bahwa kesadaran akan pentingnya keamanan informasi dalam aktivitas digital sudah mulai berkembang, meskipun budaya kewaspadaan terhadap ancaman siber masih perlu diperkuat secara lebih menyeluruh pada berbagai lapisan masyarakat dan institusi.

Dari sisi kebijakan dan perencanaan, Indeks SPRS sebesar 3,01 mengindikasikan bahwa strategi, program, serta regulasi terkait keamanan siber telah disusun dengan baik dan mulai diterapkan. Langkah ini menjadi fondasi penting dalam memperkuat keamanan data pada layanan publik dan sistem pemerintahan yang semakin terdigitalisasi.

Namun, Indeks IKKS yang berada pada angka 2,69 menunjukkan bahwa kesiapan teknis keamanan siber masih memerlukan peningkatan. Penguatan infrastruktur digital, kemampuan deteksi dini serangan, serta respons cepat terhadap insiden siber menjadi tantangan yang harus dioptimalkan untuk mencegah gangguan layanan digital.

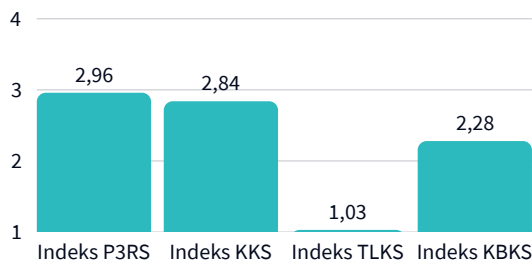
Sementara itu, Indeks Keberhasilan Literasi sebesar 1,03 mencerminkan bahwa pemahaman masyarakat terkait keamanan digital masih rendah. Edukasi dan sosialisasi mengenai ancaman siber perlu diperluas agar masyarakat dapat menjaga privasi dan keamanan data pribadi saat menggunakan layanan online dalam kehidupan sehari-hari.

Secara keseluruhan, Maluku Utara memiliki peluang besar untuk mengembangkan ekosistem keamanan siber yang lebih tangguh. Penguatan tata kelola, peningkatan kapasitas SDM, serta kampanye literasi keamanan siber yang lebih masif akan menjadi kunci dalam membangun budaya digital yang aman, adaptif, dan berkelanjutan di masa depan.

4.3.22 Nusa Tenggara Barat

Tabel 4.24 Nilai IKBKS Provinsi Nusa Tenggara Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Nusa Tenggara Barat	2,96	2,84	1,03	2,28



Gambar 4.22 Grafik IKBKS Provinsi Nusa Tenggara Barat

Provinsi Nusa Tenggara Barat (NTB) mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,28 dengan predikat Sadar. Kondisi ini menggambarkan bahwa masyarakat dan instansi pemerintah di NTB mulai mengenali pentingnya keamanan informasi, terutama seiring meningkatnya pemanfaatan teknologi digital dalam sektor pariwisata, UMKM, dan layanan publik.

Dengan Indeks SPRS senilai 2,96, NTB menunjukkan komitmen dalam penyusunan kerangka strategi dan kebijakan keamanan siber. Meskipun demikian, efektivitas implementasi kebijakan tersebut masih perlu diperkuat agar mampu menjawab tantangan keamanan digital di wilayah yang semakin berkembang pesat secara ekonomi ini.

Di sisi lain, Indeks IKKS sebesar 2,84 menandakan bahwa infrastruktur teknis keamanan informasi telah tersedia dan mulai dimanfaatkan dalam penyelenggaraan layanan berbasis digital. Namun, peningkatan kapabilitas teknis—terutama di sektor pemerintahan daerah dan pendidikan—masih menjadi tantangan yang perlu dijawab untuk menciptakan sistem keamanan yang lebih responsif terhadap ancaman siber.

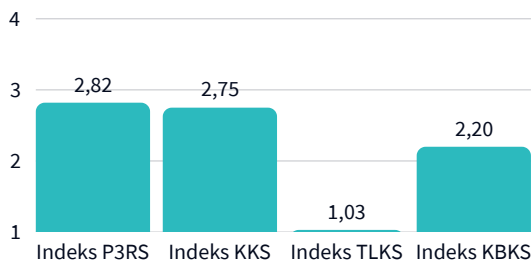
Sementara Indeks Keberhasilan Literasi berada pada skor 1,03, yang menunjukkan bahwa mayoritas masyarakat masih membutuhkan pemahaman lebih baik tentang risiko digital yang dapat terjadi kapan saja. Mengingat NTB adalah daerah dengan pertumbuhan ekosistem UMKM digital yang cukup besar, peningkatan literasi keamanan siber menjadi sangat penting agar pelaku usaha mampu mengamankan transaksi dan data pelanggan dengan lebih baik.

Ke depan, NTB memiliki peluang besar untuk memperkuat budaya keamanan siber melalui pengembangan SDM lokal, pelatihan keamanan digital yang menjangkau masyarakat luas, serta kolaborasi pemerintah dengan komunitas digital dan sektor swasta. Upaya tersebut akan menjadi pondasi penting dalam mendorong transformasi digital yang aman, andal, dan berkelanjutan di wilayah ini.

4.3.23 Nusa Tenggara Timur

Tabel 4.25 Nilai IKBKS Provinsi Nusa Tenggara Timur

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Nusa Tenggara Timur	2,82	2,75	1,03	2,20



Gambar 4.23 Grafik IKBKS Provinsi Nusa Tenggara Timur

Provinsi Nusa Tenggara Timur (NTT) memperoleh Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,20, yang menempatkannya pada predikat Sadar. Hasil ini menunjukkan bahwa perhatian terhadap aspek keamanan informasi sudah mulai tumbuh, walaupun pemahaman dan perilaku aman dalam memanfaatkan layanan digital masih belum merata di seluruh lapisan masyarakat.

Dari sisi kebijakan dan perencanaan, Indeks SPRS sebesar 2,82 mencerminkan bahwa arah strategi dan program keamanan siber telah ditetapkan, namun pelaksanaannya masih menghadapi tantangan, terutama terkait keterjangkauan infrastruktur dan pemerataan layanan digital di wilayah kepulauan yang luas.

Indeks IKKS sebesar 2,75 memperlihatkan bahwa kemampuan teknis dalam menjaga keamanan sistem informasi sudah berada dalam tahap yang cukup memadai. Namun, kapasitas penanganan insiden, ketersediaan tenaga ahli, serta dukungan teknologi canggih masih perlu diperkuat agar lebih adaptif terhadap dinamika ancaman siber yang terus berkembang.

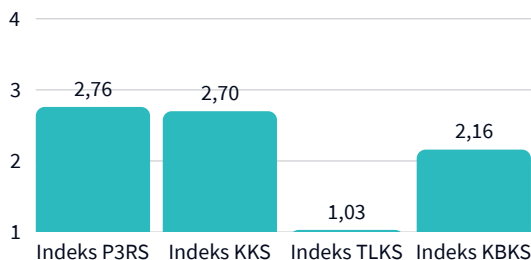
Sementara itu, Indeks Keberhasilan Literasi yang masih bertahan di angka 1,03 menunjukkan adanya kebutuhan mendesak untuk meningkatkan edukasi keamanan digital bagi masyarakat. Keterbatasan akses informasi serta pemanfaatan teknologi yang belum merata membuat sebagian warga masih rentan terhadap berbagai bentuk penipuan online dan pelanggaran data pribadi.

Dengan potensi pertumbuhan digital di sektor layanan publik, ekonomi kreatif, hingga pariwisata, NTT memiliki peluang besar untuk mengejar ketertinggalan. Penguatan kapasitas SDM, dukungan regulasi yang lebih inklusif, serta program literasi siber yang menysasar komunitas hingga wilayah pelosok dapat menjadi strategi kunci dalam mewujudkan budaya keamanan siber yang lebih komprehensif dan berkelanjutan.

4.3.24 Papua

Tabel 4.26 Nilai IKBKS Provinsi Papua

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua	2,76	2,70	1,03	2,16



Gambar 4.24 Grafik IKBKS Provinsi Papua

Provinsi Papua mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,16, yang menempatkannya pada kategori Sadar. Artinya, kesadaran akan pentingnya keamanan informasi mulai terbentuk di masyarakat, meskipun praktik perlindungan data pribadi dan sikap waspada dalam bermedia digital masih perlu terus ditingkatkan di berbagai wilayah.

Dari sisi tata kelola dan perencanaan, Indeks SPRS sebesar 2,76 menunjukkan bahwa upaya penyusunan strategi keamanan siber sudah dilakukan, namun implementasinya masih menghadapi hambatan. Tantangan geografis yang terdiri dari wilayah pegunungan hingga daerah terpencil membuat pemerataan infrastruktur digital membutuhkan perhatian lebih besar.

Kemampuan teknis keamanan sistem informasi di Papua tercermin dari Indeks IKKS sebesar 2,70, yang menandakan bahwa sumber daya dan teknologi pendukung keamanan siber mulai tersedia. Meski begitu, peningkatan kualitas dan jumlah tenaga ahli keamanan digital tetap menjadi kebutuhan mendesak, terutama dalam memperkuat respons terhadap ancaman siber yang semakin kompleks.

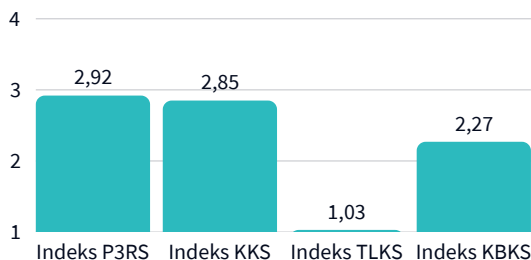
Adapun Indeks Keberhasilan Literasi yang masih berada di angka 1,03 menegaskan bahwa literasi digital masyarakat masih dalam tahap awal perkembangan. Hal ini menunjukkan pentingnya perluasan akses edukasi dan sosialisasi keamanan siber, agar masyarakat lebih mampu mengenali modus penipuan online, penyalahgunaan data pribadi, hingga hoaks yang sering beredar.

Dengan perkembangan teknologi yang kian merambah ke sektor layanan publik, pendidikan, hingga aktivitas ekonomi lokal, Papua memiliki peluang besar untuk meningkatkan ketahanan digitalnya. Investasi dalam infrastruktur konektivitas, pemberdayaan talenta lokal, serta program literasi siber berbasis komunitas dapat menjadi langkah strategis untuk menumbuhkan budaya keamanan siber yang lebih kuat dan berkelanjutan.

4.3.25 Papua Barat

Tabel 4.27 Nilai IKBKS Provinsi Papua Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua Barat	2,92	2,85	1,03	2,27



Gambar 4.25 Grafik IKBKS Provinsi Papua Barat

Provinsi Papua Barat memiliki Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,27, yang termasuk dalam kategori Sadar. Hal ini menunjukkan bahwa pemahaman masyarakat terhadap risiko ancaman digital sudah mulai terbentuk, meskipun praktik pengamanan data dan perilaku aman dalam bermedia digital perlu terus diperkuat agar lebih merata di seluruh wilayah.

Dari sisi kebijakan dan perencanaan, Indeks SPRS yang mencapai 2,92 mencerminkan adanya komitmen pemerintah daerah dalam menyusun dan mengarahkan strategi keamanan siber. Namun, keberhasilan implementasinya masih dipengaruhi oleh tantangan geografis serta keterjangkauan layanan internet bagi masyarakat di wilayah pesisir maupun pedalaman.

Kemampuan teknis dalam mempertahankan keamanan sistem informasi, yang tercermin dari Indeks IKKS sebesar 2,85, menunjukkan bahwa Papua Barat memiliki modal yang cukup baik dalam menjaga keandalan dan keamanan infrastruktur digitalnya. Meski demikian, peningkatan kapasitas SDM, ketersediaan tenaga profesional keamanan siber, serta dukungan teknologi mutakhir masih diperlukan untuk menghadapi ancaman yang terus berkembang.

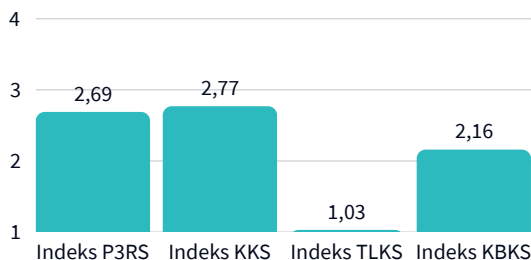
Sementara itu, Indeks Keberhasilan Literasi yang masih berada pada angka 1,03 menandakan bahwa upaya peningkatan literasi keamanan digital perlu lebih diperluas dan diperdalam. Masyarakat perlu dibekali dengan pemahaman mengenai risiko penipuan online, penyebaran konten berbahaya, hingga perlindungan data pribadi, sehingga mereka dapat lebih aman dalam memanfaatkan teknologi.

Dengan perluasan infrastruktur digital dan meningkatnya pemanfaatan layanan daring di sektor pemerintahan hingga ekonomi lokal, Papua Barat memiliki peluang besar untuk memperkuat ketahanan sibernya. Pendekatan inklusif melalui pelatihan berbasis komunitas, penguatan regulasi daerah, dan kolaborasi lintas sektor dapat menjadi langkah penting dalam mewujudkan budaya keamanan siber yang lebih matang dan berkelanjutan.

4.3.26 Papua Barat Daya

Tabel 4.28 Nilai IKBKS Provinsi Papua Barat Daya

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua Barat Daya	2,69	2,77	1,03	2,16



Gambar 4.26 Grafik IKBKS Provinsi Papua Barat Daya

Provinsi Papua Barat Daya mencatatkan nilai Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,16 dengan kategori Sadar. Angka ini menjadi cerminan bahwa kesadaran terhadap pentingnya menjaga keamanan data dan aktivitas digital sudah mulai tumbuh, meskipun masih berada pada tahap awal penerapan yang konsisten di masyarakat maupun instansi pemerintahan.

Pada aspek kebijakan, Indeks SPRS dengan skor 2,69 menunjukkan bahwa kerangka strategis mengenai keamanan siber telah dirumuskan, namun masih memerlukan dorongan lebih kuat dalam eksekusi serta pemerataan akses digital di seluruh wilayah. Sebagai daerah dengan karakter geografis yang tersebar, distribusi infrastruktur menjadi salah satu tantangan utama dalam menjaga ketangguhan keamanan siber.

Dari sisi teknis, Papua Barat Daya meraih Indeks IKKS sebesar 2,77. Hal ini mengindikasikan bahwa perangkat, sistem, dan dukungan keamanan digital sudah mulai diterapkan untuk melindungi layanan pemerintahan serta data publik. Meski demikian, peningkatan kompetensi tenaga profesional dan adopsi teknologi pertahanan siber yang lebih adaptif masih menjadi kebutuhan yang perlu dipenuhi.

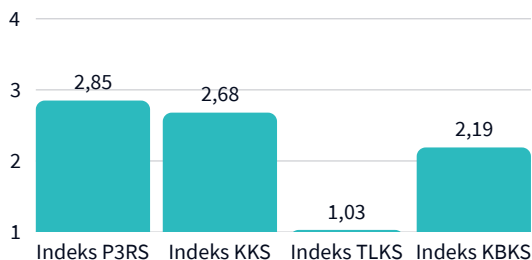
Sementara itu, Indeks Keberhasilan Literasi yang bertahan pada angka 1,03 menunjukkan bahwa edukasi masyarakat terkait ancaman siber dan cara berinternet dengan aman harus diperluas. Di tengah peningkatan aktivitas digital untuk komunikasi, layanan publik, maupun ekonomi lokal, pemahaman yang kurang dapat membuka peluang terjadinya penipuan online dan kebocoran data pribadi.

Ke depan, Papua Barat Daya memiliki kesempatan strategis untuk membangun pondasi keamanan digital yang kuat sejak dini. Kolaborasi pemerintah daerah, komunitas digital, serta dukungan nasional akan berperan penting dalam menumbuhkan budaya keamanan siber yang inklusif dan adaptif, sehingga kemajuan teknologi dapat dinikmati tanpa mengabaikan aspek perlindungan informasi.

4.3.27 Papua Pegunungan

Tabel 4.29 Nilai IKBKS Provinsi Papua Pegunungan

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua Pegunungan	2,85	2,68	1,03	2,19



Gambar 4.27 Grafik IKBKS Provinsi Papua Pegunungan

Provinsi Papua Pegunungan memperoleh Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,19, yang menempatkannya dalam kategori Sadar. Capaian ini menggambarkan bahwa kesadaran awal mengenai keamanan informasi sudah mulai tumbuh, namun masih diperlukan penguatan yang lebih menyeluruh, terutama pada wilayah pedalaman dan komunitas yang akses teknologinya terbatas.

Dari sisi perumusan kebijakan, Indeks SPRS berada pada angka 2,85, mencerminkan bahwa arah strategis dan dukungan regulatif untuk keamanan siber telah tersedia. Meski begitu, implementasi masih menghadapi tantangan geografis serta keterbatasan infrastruktur digital yang berpengaruh pada efektivitas tata kelola keamanan siber di daerah ini.

Indeks IKKS sebesar 2,68 menunjukkan bahwa dukungan teknis dan sistem keamanan digital yang ada masih dalam tahap berkembang. Kemampuan untuk mendeteksi dan merespons ancaman siber memerlukan peningkatan, baik melalui penyediaan sarana pendukung maupun penguatan kapasitas SDM di pemerintahan daerah.

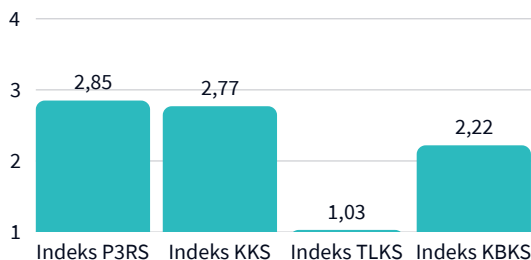
Adapun Indeks Keberhasilan Literasi yang berada pada angka 1,03 menjadi sinyal bahwa upaya edukasi kepada masyarakat mengenai penggunaan internet yang aman masih sangat diperlukan. Minimnya pengetahuan digital membuat pengguna rentan terhadap penyalahgunaan data dan penipuan daring.

Potensi pemanfaatan teknologi untuk layanan publik, pendidikan, hingga peningkatan ekonomi lokal di Papua Pegunungan sangat besar. Oleh karena itu, peningkatan literasi keamanan siber, penetrasi infrastruktur internet, serta kolaborasi lintas sektor akan menjadi langkah strategis untuk mempercepat kematangan budaya keamanan siber yang lebih inklusif dan berkelanjutan di masa mendatang.

4.3.28 Papua Selatan

Tabel 4.30 Nilai IKBKS Provinsi Papua Selatan

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua Selatan	2,85	2,77	1,03	2,22



Gambar 4.28 Grafik IKBKS Provinsi Papua Selatan

Provinsi Papua Selatan mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,22, yang termasuk kategori Sadar. Hal ini menunjukkan bahwa kesadaran masyarakat dan institusi pemerintah mengenai perlindungan data dan keamanan aktivitas digital sudah mulai terbentuk, meski praktiknya masih perlu diperluas dan diperkuat di berbagai lapisan masyarakat.

Dari sisi kebijakan, Indeks SPRS sebesar 2,85 menandakan bahwa strategi dan program keamanan siber telah dirancang, namun implementasinya masih menghadapi tantangan, terutama terkait distribusi layanan digital di wilayah yang luas dan berbatasan dengan daerah terpencil. Penguatan regulasi dan koordinasi lintas sektor tetap menjadi aspek penting untuk meningkatkan efektivitas pengelolaan keamanan siber.

Kemampuan teknis tercermin dari Indeks IKKS sebesar 2,77, yang menunjukkan bahwa infrastruktur dan sistem keamanan digital di provinsi ini sudah mulai memadai. Meskipun demikian, peningkatan kapasitas SDM dan kesiapan menghadapi insiden siber secara cepat masih perlu dilakukan agar proteksi terhadap data dan layanan publik lebih optimal.

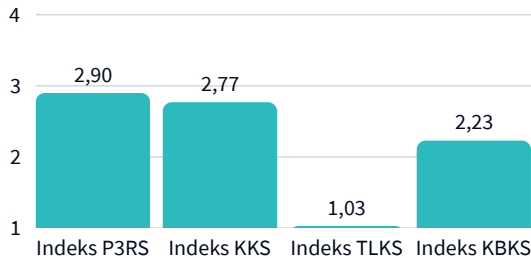
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menegaskan bahwa edukasi masyarakat tentang keamanan digital masih rendah. Untuk menjangkau seluruh masyarakat, khususnya yang berada di daerah terpencil, diperlukan program literasi digital yang lebih luas agar warga dapat mengenali dan menghindari risiko penipuan, kebocoran data, atau serangan siber lainnya.

Secara keseluruhan, Papua Selatan memiliki peluang untuk membangun ekosistem digital yang aman dan berkelanjutan. Investasi pada literasi masyarakat, peningkatan kualitas infrastruktur, dan penguatan tata kelola keamanan siber dapat menjadi langkah strategis untuk mempercepat kematangan budaya keamanan digital di provinsi ini.

4.3.29 Papua Tengah

Tabel 4.31 Nilai IKBKS Provinsi Papua Tengah

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Papua Tengah	2,90	2,75	1,03	2,23



Gambar 4.29 Grafik IKBKS Provinsi Papua Tengah

Provinsi Papua Tengah mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,23, yang menempatkannya pada kategori Sadar. Capaian ini menunjukkan bahwa kesadaran awal mengenai pentingnya keamanan informasi mulai tertanam, meskipun praktik perlindungan data dan penggunaan layanan digital yang aman masih perlu diperluas di berbagai wilayah.

Dari sisi strategi dan regulasi, Indeks SPRS sebesar 2,90 menunjukkan bahwa perencanaan dan kebijakan keamanan siber telah ada dan mulai diterapkan. Namun, tantangan geografis dan keterbatasan infrastruktur digital di beberapa daerah pedalaman memengaruhi efektivitas implementasinya, sehingga penguatan koordinasi dan pengawasan menjadi hal yang penting.

Kemampuan teknis dalam menjaga keamanan sistem informasi tercermin dari Indeks IKKS sebesar 2,75, yang menunjukkan kesiapan dasar sudah tersedia. Meski begitu, peningkatan kapasitas teknis, ketersediaan tenaga profesional keamanan siber, serta pemantauan ancaman secara berkelanjutan masih menjadi kebutuhan utama agar sistem lebih tangguh.

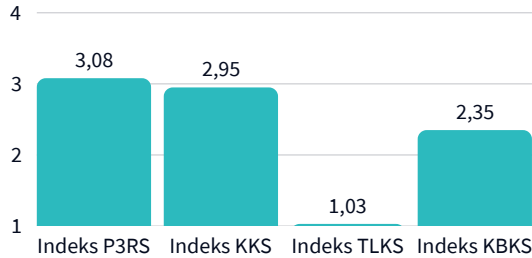
Sementara itu, Indeks Keberhasilan Literasi tetap di angka 1,03, mengindikasikan bahwa masyarakat membutuhkan edukasi lebih luas terkait risiko siber dan perilaku aman dalam penggunaan layanan digital. Literasi yang rendah dapat meningkatkan kerentanan terhadap penipuan online, kebocoran data, dan ancaman siber lainnya.

Secara keseluruhan, Papua Tengah memiliki peluang untuk menguatkan budaya keamanan siber melalui peningkatan literasi digital masyarakat, penguatan kapasitas SDM, serta pengembangan infrastruktur yang merata. Langkah-langkah ini penting untuk membangun ekosistem digital yang aman, adaptif, dan berkelanjutan di provinsi ini.

4.3.30 Riau

Tabel 4.32 Nilai IKBKS Provinsi Riau

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Riau	3,08	2,95	1,03	2,35



Gambar 4.30 Grafik IKBKS Provinsi Riau

Provinsi Riau mencatatkan Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,35, yang menempatkannya pada kategori Sadar. Hasil ini menunjukkan bahwa kesadaran masyarakat dan lembaga pemerintahan mengenai keamanan digital telah terbentuk, meskipun masih perlu diperkuat agar praktik perlindungan data dan penggunaan teknologi aman menjadi lebih konsisten.

Dari sisi kebijakan dan perencanaan, Indeks SPRS sebesar 3,08 menandakan bahwa strategi dan regulasi keamanan siber telah dirumuskan dan diimplementasikan dengan cukup baik. Provinsi ini telah menunjukkan komitmen yang kuat untuk membangun kerangka tata kelola keamanan digital yang lebih sistematis, khususnya pada sektor pemerintahan dan layanan publik.

Indeks IKKS sebesar 2,95 mengindikasikan bahwa kemampuan teknis untuk melindungi sistem informasi sudah memadai. Infrastruktur dan kontrol keamanan mulai diterapkan secara konsisten, meskipun peningkatan kapasitas SDM dan respons terhadap insiden siber tetap menjadi hal yang perlu diperkuat agar lebih adaptif terhadap ancaman yang terus berkembang.

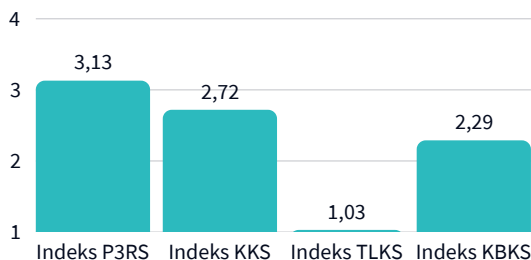
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menegaskan bahwa literasi keamanan digital masyarakat masih rendah. Edukasi terkait risiko siber dan perilaku aman dalam penggunaan internet perlu diperluas, terutama di tengah tingginya aktivitas digital di sektor ekonomi, pendidikan, dan layanan publik.

Secara keseluruhan, Riau memiliki potensi besar untuk memperkuat budaya keamanan siber melalui peningkatan literasi masyarakat, optimalisasi kapasitas teknis, dan penerapan kebijakan yang lebih efektif. Upaya ini akan menjadi fondasi penting untuk menciptakan ekosistem digital yang aman, tangguh, dan berkelanjutan di masa depan.

4.3.31 Sulawesi Barat

Tabel 4.33 Nilai IKBKS Provinsi Sulawesi Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sulawesi Barat	3,13	2,72	1,03	2,29



Gambar 4.31 Grafik IKBKS Provinsi Sulawesi Barat

Provinsi Sulawesi Barat mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,29, yang menempatkannya pada kategori Sadar. Hal ini menunjukkan bahwa kesadaran masyarakat dan lembaga pemerintahan terhadap pentingnya keamanan digital mulai terbentuk, meskipun praktik perlindungan data dan penerapan tata kelola siber masih perlu diperkuat di berbagai sektor.

Dari sisi kebijakan, Indeks SPRS sebesar 3,13 memperlihatkan bahwa strategi, program, dan regulasi keamanan siber telah disusun dengan baik dan mulai diterapkan. Provinsi ini menunjukkan komitmen yang cukup tinggi dalam membangun kerangka kerja yang mendukung tata kelola keamanan informasi yang sistematis.

Indeks IKKS sebesar 2,72 mengindikasikan bahwa kemampuan teknis dalam menjaga keamanan sistem informasi sudah mulai memadai, meskipun peningkatan infrastruktur, tenaga ahli, serta kemampuan respons terhadap ancaman siber tetap menjadi prioritas untuk memastikan sistem lebih tangguh.

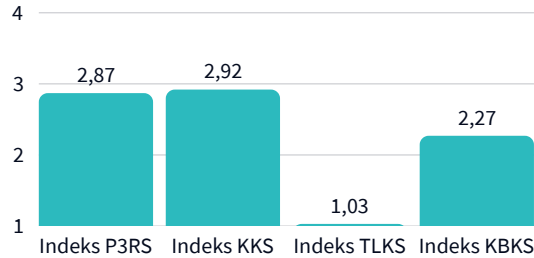
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menunjukkan bahwa masyarakat masih memerlukan edukasi lebih luas mengenai keamanan digital. Literasi yang rendah berpotensi membuat pengguna rentan terhadap penipuan online, kebocoran data, dan ancaman siber lainnya.

Secara keseluruhan, Sulawesi Barat memiliki peluang untuk memperkuat ekosistem keamanan siber melalui pengembangan literasi digital masyarakat, peningkatan kapasitas SDM, dan optimalisasi tata kelola keamanan informasi. Langkah-langkah ini akan menjadi fondasi penting untuk menciptakan ekosistem digital yang aman, tangguh, dan berkelanjutan di provinsi ini.

4.3.32 Sulawesi Selatan

Tabel 4.34 Nilai IKBKS Provinsi Sulawesi Selatan

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sulawesi Selatan	2,87	2,92	1,03	2,27



Gambar 4.32 Grafik IKBKS Provinsi Sulawesi Selatan

Provinsi Sulawesi Selatan mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,27, yang menempatkannya dalam kategori Sadar. Hal ini menunjukkan bahwa kesadaran masyarakat dan institusi pemerintah terhadap perlindungan data serta praktik keamanan digital mulai terbentuk, meskipun masih terdapat ruang untuk penguatan di berbagai sektor.

Dari sisi kebijakan, Indeks SPRS sebesar 2,87 menunjukkan bahwa strategi dan regulasi keamanan siber telah dirancang dan mulai diimplementasikan. Provinsi ini telah menunjukkan komitmen untuk membangun tata kelola keamanan digital, namun efektivitas pelaksanaan kebijakan masih memerlukan pemantauan dan peningkatan kapasitas secara berkelanjutan.

Indeks IKKS sebesar 2,92 mengindikasikan bahwa infrastruktur dan penerapan teknis keamanan sistem informasi berada pada tingkat yang cukup baik. Peningkatan kapasitas teknis, kemampuan respons terhadap insiden siber, dan penguatan SDM tetap menjadi prioritas agar keamanan digital di provinsi ini semakin tangguh.

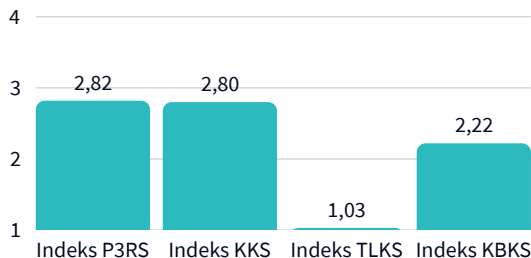
Sementara itu, Indeks Keberhasilan Literasi yang masih di angka 1,03 menandakan bahwa masyarakat memerlukan edukasi lebih lanjut terkait keamanan digital dan perilaku aman dalam penggunaan layanan online. Literasi yang lebih baik akan membantu masyarakat melindungi data pribadi serta mengurangi risiko penipuan dan penyalahgunaan informasi.

Secara keseluruhan, Sulawesi Selatan memiliki potensi besar untuk memperkuat budaya keamanan siber. Pengembangan literasi masyarakat, peningkatan kapasitas teknis, dan optimalisasi tata kelola keamanan informasi akan menjadi kunci dalam membangun ekosistem digital yang aman, adaptif, dan berkelanjutan di provinsi ini.

4.3.33 Sulawesi Tengah

Tabel 4.35 Nilai IKBKS Provinsi Sulawesi Tengah

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sulawesi Tengah	2,82	2,80	1,03	2,22



Gambar 4.33 Grafik IKBKS Provinsi Sulawesi Tengah

Provinsi Sulawesi Tengah meraih Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,22, yang berada pada kategori Sadar. Angka ini menunjukkan bahwa kesadaran masyarakat dan instansi pemerintahan terhadap pentingnya keamanan digital telah mulai terbentuk, meskipun penerapan praktik aman dalam aktivitas daring masih belum merata di seluruh wilayah.

Dari sisi perencanaan dan kebijakan, Indeks SPRS sebesar 2,82 mengindikasikan bahwa strategi dan regulasi keamanan siber sudah dirancang dan diterapkan, namun efektivitasnya masih terbatas karena tantangan geografis serta disparitas akses digital di daerah pedalaman. Penguatan koordinasi antarinstansi dan pemantauan implementasi menjadi kunci agar kebijakan dapat berjalan lebih optimal.

Dalam aspek teknis, Indeks IKKS sebesar 2,80 menunjukkan bahwa infrastruktur dan sistem keamanan digital telah tersedia dan digunakan, meskipun peningkatan kapasitas SDM, kesiapan penanganan insiden siber, serta pemanfaatan teknologi modern masih sangat diperlukan agar proteksi lebih kuat dan responsif terhadap ancaman.

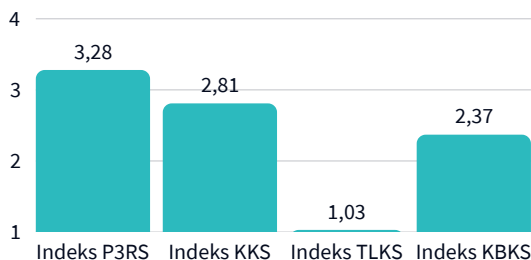
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menegaskan perlunya edukasi lebih luas bagi masyarakat mengenai risiko digital. Tingkat literasi yang rendah dapat membuat warga rentan terhadap penipuan online, penyalahgunaan data, dan ancaman siber lainnya, sehingga program sosialisasi dan pelatihan menjadi sangat penting.

Secara keseluruhan, Sulawesi Tengah memiliki peluang strategis untuk memperkuat ekosistem keamanan siber melalui literasi masyarakat, pengembangan kapasitas teknis, dan penerapan kebijakan yang lebih adaptif. Langkah-langkah ini akan mendukung terciptanya lingkungan digital yang lebih aman, inklusif, dan berkelanjutan bagi seluruh masyarakat provinsi ini.

4.3.34 Sulawesi Tenggara

Tabel 4.36 Nilai IKBKS Provinsi Sulawesi Tenggara

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sulawesi Tenggara	3,28	2,81	1,03	2,37



Gambar 4.34 Grafik IKBKS Provinsi Sulawesi Tenggara

Provinsi Sulawesi Tenggara mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,37, yang termasuk dalam kategori Sadar. Hasil ini menunjukkan bahwa kesadaran masyarakat dan lembaga pemerintahan mengenai keamanan digital sudah mulai terbentuk, meskipun praktik perlindungan data dan keamanan layanan daring masih perlu diperkuat agar lebih merata.

Dari sisi kebijakan, Indeks SPRS yang mencapai 3,28 menegaskan bahwa strategi, program, dan regulasi keamanan siber telah disusun dengan matang dan mulai diimplementasikan. Provinsi ini menunjukkan komitmen yang cukup tinggi dalam membangun kerangka kerja yang mendukung tata kelola keamanan informasi, khususnya untuk layanan publik dan sektor pemerintahan.

Indeks IKKS sebesar 2,81 menunjukkan bahwa kemampuan teknis dalam mengelola keamanan sistem informasi sudah berada pada tingkat yang memadai. Peningkatan kapasitas SDM, kesiapan menghadapi insiden siber, serta pemanfaatan teknologi pendukung tetap menjadi fokus penting agar sistem lebih tangguh dan adaptif terhadap ancaman digital.

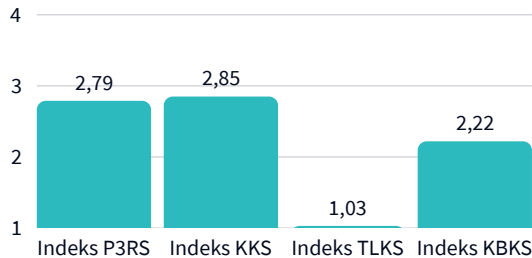
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menunjukkan bahwa literasi masyarakat terkait keamanan digital masih terbatas. Edukasi yang lebih luas sangat diperlukan agar warga mampu mengenali risiko siber, melindungi data pribadi, dan menggunakan layanan digital secara aman.

Secara keseluruhan, Sulawesi Tenggara memiliki peluang besar untuk memperkuat budaya keamanan siber melalui pengembangan literasi masyarakat, optimalisasi kapasitas teknis, dan implementasi kebijakan yang lebih efektif. Upaya ini menjadi langkah strategis untuk menciptakan ekosistem digital yang aman, adaptif, dan berkelanjutan bagi seluruh warga provinsi.

4.3.35 Sulawesi Utara

Tabel 4.37 Nilai IKBKS Provinsi Sulawesi Utara

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sulawesi Utara	2,79	2,85	1,03	2,22



Gambar 4.35 Grafik IKBKS Provinsi Sulawesi Utara

Provinsi Sulawesi Utara mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,22, yang menempatkannya pada kategori Sadar. Angka ini menunjukkan bahwa kesadaran masyarakat dan instansi pemerintah terhadap pentingnya keamanan digital mulai terbentuk, meskipun praktik perlindungan data dan penggunaan layanan daring yang aman masih perlu diperkuat di beberapa wilayah.

Dari sisi kebijakan dan strategi, Indeks SPRS sebesar 2,79 mengindikasikan bahwa perencanaan dan regulasi keamanan siber telah ada dan mulai dijalankan. Namun, tantangan geografis serta penyebaran layanan digital yang belum merata memengaruhi efektivitas implementasi kebijakan ini, sehingga penguatan koordinasi dan pemantauan menjadi hal penting.

Indeks IKKS sebesar 2,85 memperlihatkan bahwa dukungan teknis dan infrastruktur keamanan sistem informasi sudah cukup memadai. Meski demikian, peningkatan kapasitas SDM, kesiapan menghadapi insiden siber, dan pemanfaatan teknologi mutakhir tetap menjadi kebutuhan agar keamanan digital lebih tangguh dan adaptif.

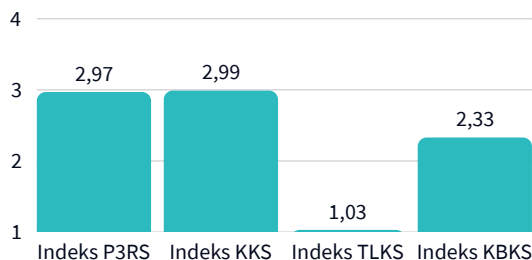
Sementara itu, Indeks Keberhasilan Literasi yang tetap berada di angka 1,03 menunjukkan bahwa literasi digital masyarakat masih rendah. Edukasi lebih luas sangat diperlukan agar warga dapat mengenali risiko siber, melindungi data pribadi, dan menggunakan layanan digital secara aman dan bertanggung jawab.

Secara keseluruhan, Sulawesi Utara memiliki peluang strategis untuk memperkuat budaya keamanan siber melalui pengembangan literasi masyarakat, optimalisasi kapasitas teknis, dan penerapan kebijakan yang lebih efektif. Upaya ini akan menjadi fondasi penting dalam menciptakan ekosistem digital yang aman, adaptif, dan berkelanjutan di provinsi ini.

4.3.36 Sumatra Barat

Tabel 4.38 Nilai IKBKS Provinsi Sumatra Barat

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sumatra Barat	2,97	2,99	1,03	2,33



Gambar 4.36 Grafik IKBKS Provinsi Sumatra Barat

Provinsi Sumatra Barat mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,33, yang termasuk dalam kategori Sadar. Hal ini menandakan bahwa kesadaran masyarakat dan lembaga pemerintahan mengenai pentingnya keamanan digital telah mulai terbentuk, meskipun penerapan praktik perlindungan data dan penggunaan layanan daring secara aman masih perlu diperluas.

Dari sisi kebijakan, Indeks SPRS sebesar 2,97 menunjukkan bahwa strategi, program, dan regulasi keamanan siber telah disusun dan mulai diterapkan. Provinsi ini menunjukkan komitmen untuk membangun tata kelola keamanan digital yang sistematis, terutama dalam mendukung layanan publik dan sektor pemerintahan.

Indeks IKKS sebesar 2,99 memperlihatkan bahwa kemampuan teknis dalam menjaga keamanan sistem informasi cukup baik. Infrastruktur dan kontrol keamanan telah mulai diterapkan secara konsisten, meski peningkatan kapasitas SDM serta kesiapan menghadapi insiden siber masih menjadi fokus penting agar sistem lebih adaptif.

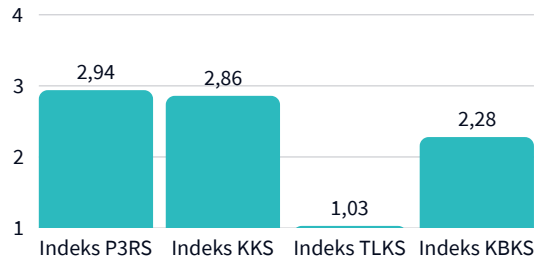
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menunjukkan bahwa literasi masyarakat terkait keamanan digital masih rendah. Upaya edukasi dan sosialisasi lebih luas sangat diperlukan agar masyarakat mampu mengenali risiko siber, menjaga data pribadi, dan menggunakan layanan digital secara aman.

Secara keseluruhan, Sumatra Barat memiliki peluang besar untuk memperkuat budaya keamanan siber melalui pengembangan literasi digital, optimalisasi kapasitas teknis, dan implementasi kebijakan yang lebih efektif. Langkah-langkah ini akan mendukung terciptanya ekosistem digital yang aman, tangguh, dan berkelanjutan bagi seluruh warga provinsi.

4.3.37 Sumatra Selatan

Tabel 4.39 Nilai IKBKS Provinsi Sumatra Selatan

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sumatra Selatan	2,94	2,86	1,03	2,28



Gambar 4.37 Grafik IKBKS Provinsi Sumatra Selatan

Provinsi Sumatra Selatan mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,28, yang menempatkannya dalam kategori Sadar. Hal ini menunjukkan bahwa kesadaran masyarakat dan instansi pemerintah terhadap perlindungan data serta praktik aman dalam layanan digital mulai terbentuk, meski implementasinya belum merata di seluruh wilayah.

Dari sisi perencanaan dan regulasi, Indeks SPRS sebesar 2,94 memperlihatkan bahwa arah strategi dan kebijakan keamanan siber telah ditetapkan dan mulai dijalankan. Tantangan utama masih terkait pemerataan akses infrastruktur digital dan koordinasi lintas sektor agar penerapan kebijakan lebih efektif dan tepat sasaran.

Di ranah teknis, Indeks IKKS sebesar 2,86 menandakan bahwa sistem dan prosedur keamanan informasi telah diterapkan, namun penguatan kapasitas SDM, kesiapan menghadapi insiden siber, serta pemanfaatan teknologi canggih tetap menjadi prioritas agar proteksi lebih tangguh.

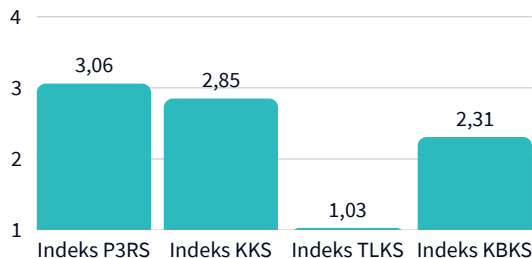
Sementara itu, Indeks Keberhasilan Literasi yang tetap di angka 1,03 menunjukkan bahwa pemahaman masyarakat terhadap risiko digital masih rendah. Edukasi dan sosialisasi yang lebih luas sangat diperlukan agar warga mampu mengenali ancaman siber, melindungi data pribadi, dan menggunakan layanan daring dengan lebih aman.

Secara keseluruhan, Sumatra Selatan memiliki peluang besar untuk membangun ekosistem keamanan siber yang kuat. Peningkatan literasi digital, optimalisasi kapasitas teknis, dan penguatan tata kelola akan menjadi langkah strategis dalam menciptakan lingkungan digital yang aman, adaptif, dan berkelanjutan di provinsi ini.

4.3.38 Sumatra Utara

Tabel 4.40 Nilai IKBKS Provinsi Sumatra Utara

PROVINSI	INDEKS P3RS	INDEKS KKS	INDEKS TLKS	INDEKS KBKS
Sumatra Utara	3,06	2,85	1,03	2,31



Gambar 4.38 Grafik IKBKS Provinsi Sumatra Utara

Provinsi Sumatra Utara mencatat Indeks Kematangan Budaya Keamanan Siber (IKBKS) sebesar 2,31, yang termasuk dalam kategori Sadar. Angka ini menunjukkan bahwa kesadaran masyarakat dan lembaga pemerintahan mengenai keamanan digital telah mulai terbentuk, meski praktik perlindungan data dan tata kelola siber masih perlu diperluas agar lebih konsisten di berbagai sektor.

Dari sisi kebijakan dan strategi, Indeks SPRS sebesar 3,06 menandakan bahwa arah perencanaan dan regulasi keamanan siber telah dirumuskan dengan baik dan mulai diterapkan. Provinsi ini menunjukkan komitmen yang cukup tinggi dalam membangun kerangka tata kelola keamanan digital, khususnya untuk layanan publik dan sektor pemerintahan.

Di aspek teknis, Indeks IKKS sebesar 2,85 menunjukkan bahwa kemampuan menjaga keamanan sistem informasi sudah mulai memadai. Namun, penguatan kapasitas SDM, kesiapan menghadapi insiden siber, serta adopsi teknologi pendukung masih diperlukan agar proteksi sistem lebih tangguh dan adaptif terhadap ancaman digital.

Sementara itu, Indeks Keberhasilan Literasi yang masih berada di angka 1,03 mengindikasikan bahwa literasi digital masyarakat masih rendah. Edukasi lebih luas sangat diperlukan agar warga mampu mengenali risiko siber, menjaga data pribadi, dan menggunakan layanan daring secara aman dan bertanggung jawab.

Secara keseluruhan, Sumatra Utara memiliki peluang strategis untuk memperkuat budaya keamanan siber melalui literasi masyarakat, pengembangan kapasitas teknis, dan penerapan kebijakan yang lebih efektif. Upaya ini akan menjadi fondasi penting dalam menciptakan ekosistem digital yang aman, adaptif, dan berkelanjutan di provinsi ini

BAB V

PEMBASAHAN STRATEGI NASIONAL

RESILIENCE

kematangan diuji saat sistem terganggu

5.1 Analisis Risiko Budaya Keamanan Siber

Hasil pengukuran Indeks Kematangan Budaya Keamanan Siber (IKBKS) menunjukkan bahwa secara nasional Indonesia masih berada pada fase transisi dari kesadaran menuju pembudayaan keamanan siber. Kondisi ini menimbulkan sejumlah risiko strategis apabila tidak direspons secara sistematis dan berkelanjutan. Risiko utama yang muncul adalah ketidakseimbangan antara kemajuan teknologi dan kesiapan budaya pengguna ruang siber. Peningkatan penetrasi internet, adopsi layanan digital pemerintah (SPBE), serta transformasi ekonomi digital yang masif belum sepenuhnya diiringi oleh perilaku aman digital yang konsisten di tingkat individu maupun institusi. Hal ini membuka celah terjadinya insiden siber yang bersumber dari faktor manusia (*human factor vulnerability*), seperti kesalahan konfigurasi, kelalaian pengguna, dan rendahnya kepatuhan terhadap prosedur keamanan.

Dalam konteks mandat BSSN, risiko budaya keamanan siber ini berimplikasi langsung terhadap perlindungan Infrastruktur Informasi Vital (IIV) sebagaimana diamanatkan dalam Perpres Nomor 82 Tahun 2022. Budaya keamanan siber yang belum matang dapat melemahkan efektivitas kebijakan teknis dan operasional, karena teknologi pengamanan yang canggih sekalipun akan kehilangan daya guna apabila tidak didukung oleh perilaku pengguna yang aman dan bertanggung jawab. Selain itu, hasil indeks yang menunjukkan dominasi tingkat Sadar dan Baik mengindikasikan adanya risiko ketergantungan pada pendekatan reaktif, di mana tindakan pengamanan baru dilakukan setelah insiden terjadi. Pola ini bertentangan dengan arah kebijakan BSSN dalam Renstra 2025–2029 yang menekankan pendekatan preventif, manajemen risiko, dan ketahanan siber nasional.

Dengan demikian, risiko budaya keamanan siber tidak hanya berdampak pada individu atau organisasi tertentu, tetapi berpotensi mengganggu stabilitas layanan publik, kepercayaan masyarakat, serta ketahanan nasional di ruang siber. Gangguan terhadap layanan publik berbasis digital, seperti sistem administrasi pemerintahan, layanan kesehatan, pendidikan, dan keuangan, dapat menimbulkan efek berantai yang melemahkan kinerja negara dan menurunkan kualitas pelayanan kepada masyarakat. Dalam jangka panjang, kondisi tersebut berpotensi mengikis tingkat kepercayaan publik terhadap transformasi digital yang sedang dibangun oleh pemerintah.

Lebih jauh lagi, rendahnya budaya keamanan siber dapat meningkatkan kerentanan terhadap serangan siber yang bersifat sistemik, termasuk kebocoran data berskala besar, disrupsi layanan esensial, serta penyalahgunaan informasi yang berdampak pada stabilitas sosial dan ekonomi. Dalam konteks ketahanan nasional, ruang siber telah menjadi domain strategis yang setara dengan darat, laut, dan udara. Oleh karena itu, lemahnya budaya keamanan siber masyarakat dan aparatur negara dapat dimanfaatkan oleh aktor jahat untuk melemahkan ketahanan nasional secara tidak langsung namun berkelanjutan.

Atas dasar tersebut, penguatan budaya keamanan siber perlu dipandang sebagai investasi strategis jangka panjang, bukan sekadar program literasi sesaat. Pembangunan budaya keamanan siber yang matang akan berkontribusi pada terbentuknya masyarakat digital yang tangguh, adaptif, dan berdaya tahan terhadap ancaman siber, sekaligus memperkuat posisi Indonesia dalam menjaga kedaulatan dan ketahanan nasional di ruang siber.

5.2 Kesenjangan Budaya Keamanan Siber Antarprovinsi

Analisis persebaran IKBKS memperlihatkan adanya kesenjangan budaya keamanan siber antarprovinsi yang cukup signifikan. Provinsi dengan tingkat urbanisasi tinggi, infrastruktur digital yang lebih matang, serta dukungan kebijakan daerah yang kuat cenderung menunjukkan indeks kematangan yang lebih tinggi. Wilayah-wilayah ini umumnya memiliki akses TIK yang lebih baik, ekosistem digital yang aktif, serta intensitas program literasi dan pembinaan keamanan siber yang relatif konsisten. Sebaliknya, sejumlah provinsi di wilayah tertinggal, terdepan, dan kepulauan masih menunjukkan tingkat kematangan yang relatif lebih rendah, mencerminkan keterbatasan struktural dan kapasitas lokal dalam pengelolaan keamanan siber.

Kesenjangan tersebut mengindikasikan bahwa budaya keamanan siber tidak tumbuh dalam ruang hampa, melainkan sangat dipengaruhi oleh ekosistem digital lokal. Faktor-faktor seperti ketersediaan dan kualitas infrastruktur TIK, kapasitas sumber daya manusia, tingkat literasi digital masyarakat, serta komitmen dan kepemimpinan pemerintah daerah memainkan peran penting dalam membentuk perilaku aman digital. Temuan ini sejalan dengan arah kebijakan dalam Rencana Strategis BSSN yang menegaskan bahwa penguatan keamanan siber nasional memerlukan pendekatan kolaboratif, lintas sektor, dan lintas wilayah, bukan semata-mata intervensi yang bersifat terpusat dan seragam.

Dalam perspektif strategis nasional, kesenjangan antarprovinsi tersebut menimbulkan risiko fragmentasi ketahanan siber nasional. Daerah dengan tingkat kematangan budaya keamanan siber yang rendah berpotensi menjadi titik lemah (*weak link*) dalam sistem keamanan siber nasional yang saling terhubung. Mengingat karakter ruang siber yang tidak mengenal batas administratif, kerentanan di satu wilayah dapat dimanfaatkan sebagai pintu masuk untuk menyerang sistem di wilayah lain, termasuk sektor-sektor strategis dan lintas pemerintahan.

Ketimpangan budaya keamanan siber antarprovinsi juga berpotensi memperlebar kesenjangan manfaat transformasi digital. Wilayah dengan budaya keamanan siber yang lebih matang akan lebih siap memanfaatkan teknologi digital secara aman dan produktif, sementara wilayah dengan tingkat kematangan rendah berisiko tertinggal serta lebih rentan terhadap dampak negatif ruang siber. Kondisi ini dapat menghambat upaya pemerataan pembangunan digital nasional dan melemahkan kohesi ketahanan siber secara keseluruhan.

Oleh karena itu, hasil kajian ini memperkuat urgensi perlunya strategi diferensial dan afirmatif dalam program peningkatan budaya keamanan siber. BSSN perlu mendorong model intervensi yang berbasis klaster wilayah, tingkat risiko, dan kapasitas daerah, dengan pendekatan yang disesuaikan terhadap karakteristik lokal. Strategi tersebut sejalan dengan kerangka penguatan kapasitas daerah dalam RPJMN 2025–2029 serta Rencana Aksi Nasional Keamanan Siber, yang menekankan pentingnya penguatan peran pemerintah daerah sebagai garda terdepan dalam pembangunan ketahanan siber nasional. Dengan demikian, kesenjangan budaya keamanan siber antarprovinsi bukan semata persoalan disparitas teknis, tetapi merupakan tantangan strategis nasional yang memerlukan kebijakan terarah, pendampingan berkelanjutan, serta koordinasi yang kuat antara pemerintah pusat dan daerah.

5.3 Tantangan Implementasi Program Budaya Keamanan Siber

Meskipun berbagai regulasi, kebijakan, dan program peningkatan budaya keamanan siber telah disusun dan diimplementasikan oleh Badan Siber dan Sandi Negara (BSSN), pelaksanaannya di lapangan masih menghadapi sejumlah tantangan strategis yang bersifat struktural, kultural, dan operasional. Tantangan-tantangan ini menunjukkan bahwa pembangunan budaya keamanan siber merupakan proses jangka panjang yang tidak dapat dicapai hanya melalui pendekatan regulatif atau kampanye sesaat.

Tantangan pertama adalah pergeseran literasi dari aspek pengetahuan menuju perubahan perilaku. Hasil pengukuran IKBKS menunjukkan bahwa literasi keamanan siber telah menjangkau masyarakat secara relatif luas, tetapi dampaknya terhadap praktik dan perilaku aman digital masih belum optimal. Kondisi tersebut mengindikasikan adanya kesenjangan antara pengetahuan dan tindakan. Hal ini menunjukkan bahwa pemahaman terhadap risiko siber belum sepenuhnya diterjemahkan ke dalam kebiasaan yang konsisten. Oleh karena itu, diperlukan transformasi pendekatan literasi dari yang semula bersifat informatif menjadi edukatif, partisipatif, dan kontekstual, dengan menyesuaikan karakteristik pengguna, latar sosial budaya, serta tingkat kematangan digital di masing-masing wilayah.

Tantangan kedua berkaitan dengan koordinasi lintas pemangku kepentingan. Budaya keamanan siber bukan semata tanggung jawab BSSN sebagai otoritas nasional, melainkan memerlukan keterlibatan aktif dan berkelanjutan dari kementerian/lembaga, pemerintah daerah, sektor swasta, dunia pendidikan, komunitas, serta media. Tanpa mekanisme orkestrasi yang kuat dan terintegrasi, berbagai program literasi, sosialisasi, dan pembinaan berpotensi berjalan secara parsial, tumpang tindih, atau tidak berkelanjutan. Kondisi ini dapat mengurangi efektivitas intervensi serta menyulitkan pengukuran dampak program secara komprehensif.

Tantangan ketiga adalah ketimpangan kapasitas sumber daya manusia dan kelembagaan di daerah. Implementasi kebijakan dan program budaya keamanan siber di tingkat daerah sangat bergantung pada kesiapan aparatur, ketersediaan anggaran, serta komitmen pimpinan daerah. Di sejumlah wilayah, keterbatasan kapasitas teknis dan manajerial masih menjadi kendala utama dalam menerjemahkan kebijakan nasional ke dalam program yang operasional dan berkelanjutan. Oleh karena itu, penguatan peran pembinaan, asistensi, dan pendampingan dari pemerintah pusat menjadi sangat penting, sebagaimana telah menjadi salah satu fokus dalam Rencana Strategis BSSN 2025–2029.

Selain itu, tantangan strategis yang tidak kalah penting adalah kecepatan evolusi ancaman siber. Dinamika ancaman yang semakin kompleks, adaptif, dan lintas batas menuntut budaya keamanan siber yang responsif dan berkelanjutan. Budaya keamanan siber tidak dapat dibangun hanya melalui kepatuhan sesaat terhadap kebijakan atau program tertentu, tetapi harus berkembang menjadi sistem nilai dan kebiasaan yang mampu beradaptasi terhadap perubahan lanskap ancaman secara berkesinambungan.

Secara keseluruhan, paparan ini menegaskan bahwa budaya keamanan siber merupakan fondasi strategis ketahanan siber nasional. Hasil pengukuran IKBKS tidak hanya berfungsi sebagai alat evaluasi, tetapi juga sebagai instrumen perumusan kebijakan berbasis bukti (evidence-based policy) bagi BSSN dan seluruh pemangku kepentingan. Dengan mengintegrasikan hasil indeks ke dalam perencanaan strategis nasional, Indonesia memiliki peluang besar untuk mendorong transformasi—dari sekadar aware society menuju resilient digital society—selaras dengan visi Indonesia Digital dan Indonesia Emas 2045.

BAB VI

REKOMENDASI

MATURITY

bukan sekadar aman, tapi berkelanjutan

6.1 Ringkasan Indeks Nasional

Hasil pengukuran IKBKS Tahun 2025 menunjukkan bahwa secara nasional Indonesia berada pada skor 2,32 dengan predikat “Sadar”. Capaian ini menandakan bahwa kesadaran terhadap pentingnya keamanan siber telah terbentuk secara luas, baik di tingkat masyarakat maupun pemerintah daerah. Namun demikian, kesadaran tersebut belum sepenuhnya terinternalisasi menjadi perilaku aman digital yang konsisten dan berkelanjutan.

Sebagian besar provinsi berada pada predikat “Baik”, sementara hanya beberapa provinsi yang telah mencapai tingkat “Sangat Baik”. Kondisi ini menunjukkan adanya kemajuan yang positif, tetapi juga menegaskan masih kuatnya ketergantungan pada pendekatan literasi yang bersifat informatif dan reaktif.

Dengan demikian, indeks nasional memberikan gambaran bahwa Indonesia sedang berada pada fase transisi strategis, yaitu dari tahap peningkatan kesadaran menuju tahap pembudayaan keamanan siber. Fase ini membutuhkan intervensi kebijakan yang lebih terarah, terukur, dan berorientasi pada perubahan perilaku.

6.2 Arah Pengembangan Pengukuran

Berdasarkan evaluasi terhadap hasil indeks dan dinamika implementasi di lapangan, pengukuran IKBKS ke depan perlu dikembangkan secara lebih komprehensif dan adaptif. Beberapa arah pengembangan yang direkomendasikan dipaparkan sebagai berikut.

Pertama, penguatan orientasi perilaku dalam pengukuran. Indikator perlu lebih menekankan pada praktik nyata pengguna ruang siber, bukan hanya pada tingkat pengetahuan atau paparan literasi. Hal ini penting untuk memastikan bahwa peningkatan skor indeks benar-benar mencerminkan perubahan budaya.

Kedua, penerapan pendekatan diferensial berbasis risiko dan wilayah. Pengukuran perlu mempertimbangkan karakteristik daerah, tingkat kematangan digital, serta potensi ancaman yang berbeda antarprovinsi sehingga hasil indeks dapat menjadi dasar kebijakan yang lebih kontekstual.

Ketiga, integrasi indeks budaya keamanan siber dengan kerangka pengukuran ketahanan siber nasional. Dengan demikian, IKBKS tidak berdiri sendiri, tetapi menjadi bagian dari sistem pemantauan keamanan siber nasional yang utuh dan berkesinambungan.

Keempat, penguatan mekanisme evaluasi longitudinal sehingga indeks tidak hanya menggambarkan kondisi sesaat, tetapi mampu menangkap tren perubahan budaya keamanan siber dari waktu ke waktu.

6.3 Rekomendasi

6.3.1 Pemerintah Pusat: Strategi Nasional

Pemerintah Pusat, khususnya melalui BSSN, perlu menjadikan IKBKS sebagai instrumen kebijakan strategis dalam perencanaan dan evaluasi keamanan siber nasional. Strategi nasional diarahkan pada penguatan budaya keamanan siber sebagai pilar utama ketahanan siber nasional, sejalan dengan Renstra BSSN dan RPJMN. Selain itu, diperlukan penguatan koordinasi lintas kementerian/lembaga untuk memastikan bahwa program literasi, regulasi, dan pengamanan teknis berjalan secara terpadu. Pendekatan nasional perlu bergeser dari kampanye kesadaran menuju internalisasi nilai dan pembiasaan perilaku aman digital.

6.3.2 Pemerintah Daerah: Penguatan Program Regional

Pemerintah daerah didorong untuk mengintegrasikan budaya keamanan siber ke dalam kebijakan pembangunan daerah, khususnya pada sektor pelayanan publik dan transformasi digital. Program literasi dan pembinaan perlu disesuaikan dengan karakteristik sosial, geografis, dan tingkat kematangan digital masing-masing daerah. Bagi daerah dengan tingkat indeks rendah atau menengah, diperlukan pendekatan afirmatif melalui pendampingan, peningkatan kapasitas SDM, serta kolaborasi dengan perguruan tinggi dan komunitas lokal. Pemerintah daerah juga perlu didorong menjadi agen utama dalam membangun budaya keamanan siber di wilayahnya.

6.3.3 Masyarakat dan Komunitas: Perilaku Aman di Ruang Siber

Masyarakat dan komunitas memiliki peran kunci dalam pembentukan budaya keamanan siber. Upaya peningkatan literasi perlu diarahkan pada pembiasaan perilaku aman digital, seperti perlindungan data pribadi, kewaspadaan terhadap ancaman siber, serta etika berinteraksi di ruang digital. Komunitas digital, organisasi masyarakat, dan dunia pendidikan perlu dilibatkan secara aktif sebagai mitra strategis dalam menyebarluaskan praktik baik keamanan siber. Pendekatan berbasis komunitas diyakini lebih efektif dalam membangun norma sosial yang mendukung keamanan digital.

6.3.4 Industri Teknologi: Peningkatan Perlindungan Pengguna

Industri teknologi memiliki tanggung jawab strategis dalam menciptakan ekosistem digital yang aman. Rekomendasi diarahkan pada penerapan prinsip *security by design* dan *privacy by default*--serta penyediaan fitur keamanan yang mudah dipahami dan digunakan oleh pengguna. Selain itu, industri diharapkan berperan aktif dalam edukasi keamanan siber kepada pengguna, termasuk melalui kampanye, pembaruan sistem yang proaktif, dan mekanisme perlindungan yang adaptif terhadap ancaman baru.

6.3.5 Prioritas Program Tahun Berikutnya

Berdasarkan hasil kajian ini, prioritas program pada tahun berikutnya perlu difokuskan pada:

- a. Transformasi literasi keamanan siber menjadi literasi berbasis perilaku.
- b. Penguatan program afirmatif untuk daerah dengan indeks kematangan rendah.
- c. Integrasi IKBKS ke dalam sistem perencanaan dan evaluasi nasional.
- d. Penguatan kolaborasi lintas sektor dalam pembangunan budaya keamanan siber.
- e. Pengembangan narasi nasional budaya keamanan siber yang inklusif dan berkelanjutan.

Secara keseluruhan, rekomendasi dalam paparan di atas menegaskan bahwa peningkatan budaya keamanan siber merupakan proses jangka panjang yang memerlukan komitmen bersama seluruh pemangku kepentingan. Dengan menjadikan IKBKS sebagai alat ukur sekaligus instrumen kebijakan, Indonesia memiliki landasan yang kuat untuk membangun ruang siber nasional yang aman, resilien, dan berkelanjutan.

Daftar Pustaka

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98.
- Armoogum, S., Armoogum, V., Chandra, A., Dewi, D. A., Kurniawan, T. B., Bappoo, S., Mohd Salikon, M. Z., & Alanda, A. (2025). A comprehensive review of cyber hygiene practices in the workplace for enhanced digital security. *JOIV: International Journal on Informatics Visualization*, 9(1), 137–145.
- Artina, B. S., Desnasari, D., Fitriyah, F., & Rizkita, R. G. (2020). The workforce in Indonesian organizations: An analysis based upon the cultural dimensions of Hofstede's model. *Journal of International Conference Proceedings*, 3(1), 56–64.*
- Badan Siber dan Sandi Negara. (2020). *Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 menggunakan Indeks Keamanan Informasi (Indeks KAMI)*. Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2020). *Rencana Strategis Badan Siber dan Sandi Negara 2020–2024*. Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2024). *Rencana Aksi Nasional Keamanan Siber 2024–2028*. Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2025). *Pedoman pengisian instrumen Indeks Keamanan Informasi (Indeks KAMI) versi 5.0 untuk pemerintah daerah*. Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2025). *Rencana Strategis Badan Siber dan Sandi Negara 2025–2029*. Badan Siber dan Sandi Negara.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.
- Brown, D., & Pytlak, A. (2020). *Why gender matters in international cyber security*. Women's International League for Peace and Freedom; Association for Progressive Communications.
- Burns, T., & Gottschalk, F. (Eds.). (2019). *Educating 21st century children: Emotional well-being in the digital age*. OECD Publishing.
- Cloramidine, F., & Badaruddin, M. (2023). Mengukur keamanan siber Indonesia melalui indikator pilar kerjasama dalam Global Cybersecurity Index (GCI). *Populis: Jurnal Sosial dan Humaniora*, 8(1), 57–73.



- Da Veiga, A., & Martins, N. (2015a). *Improving the information security culture through monitoring and implementation actions illustrated through a case study*. *Computers & Security*, 49, 162–176.
- Da Veiga, A., & Martins, N. (2015b). *Information security culture and information protection culture: A validated assessment instrument*. *Computer Law & Security Review*, 31(2), 243–256.
- Electronic Frontier Foundation. (2023). *The growing threat of cybercrime law abuse: LGBTQ+ rights in MENA and the UN cybercrime draft convention*.
- Fertig, T., & Schütz, A. E. (2020). *About the measuring of information security awareness: A systematic literature review*. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 1–10).
- Flew, T. (2021). *The global trust deficit disorder: A communications perspective on trust in the time of global pandemics*. *Journal of Communication*, 71(2), 163–186.*
- Global Partners Digital, & ARTICLE 19 West Africa. (2024). *An ever-tightening net: Restrictions on online expression under cybercrime laws and content restrictions in Africa, the Middle East and Türkiye*.
- Goldsmith, A., & Hutchings, A. (2025). *Beyond fraud and identity theft: assessing the impact of data breaches on individual victims*. *Security Journal*.
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind* (3rd ed.). McGraw–Hill.
- Human Rights Watch. (2024a). *Treacherous internet: Cyber-criminalization of LGBT people*.
- Internet Society. (2019). *The state of user privacy and trust online*.
- International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. International Telecommunication Union.
- KnowBe4. (2023). *2023 phishing by industry benchmarking report*. KnowBe4.
- National Cyber Security Alliance, & CybSafe. (2021). *Oh, Behave! The annual cybersecurity attitudes and behaviors report 2021*. National Cyber Security Alliance.
- National Cyber Security Centre. (2025). *Cyber security culture principles*. National Cyber Security Centre.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*. *Computers & Security*, 42, 165–176.

- Pavlova, P. (2025). *Intersectional feminist perspectives on cybercrime law: Toward an effective and human rights-respecting implementation of the United Nations Cybercrime Convention*. Centre for Feminist Foreign Policy; Heinrich-Böll-Stiftung.
- Permadi, R. B., & Ramli, K. (2024). Analysis of measuring information security awareness for employees at institution XYZ. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 4(4), 1330–1338.
- Perkasa, D. A., & Setiawan, B. (2024). Measuring information security awareness level of high school students. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 4(4), 1301–1308. <https://doi.org/10.57152/malcom.v4i4.1461>
- Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585.
- Rizal, M. A., & Setiawan, B. (2024). Information security awareness literature review: Focus area for measurement instruments. *Procedia Computer Science*, 234, 1420–1427.
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Luimula, M. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), e14234.
- Setyaningrum, R., Wijaya, A. R., & Subagyo, S. (2022). The characteristics of society in Indonesian based on the Hofstede cultural dimensions: Measuring the five Indonesian islands. *International Journal of Culture and Art Studies*, 6(1), 60–74.*
- Yunita, A., & Nurdeni, D. A. (2023). Research review on measuring information security awareness. *Journal of Science and Informatics for Society*, 1(2).

INDEKS KEMATANGAN BUDAYA KEAMANAN SIBER 2025

