Standar Keamanan Penyelenggara dan Tata Kelola Data dalam Teknik Informatika: Tinjauan Komprehensif dan Rekomendasi Implementasi

1. Pendahuluan

Pentingnya Keamanan Data dan Tata Kelola Data di Era Digital

Dalam lanskap digital kontemporer, data telah bertransformasi menjadi salah satu aset paling berharga bagi organisasi, yang seringkali melebihi nilai infrastruktur fisik yang menyimpannya.[1] Nilai intrinsik data ini mencakup beragam informasi krusial, mulai dari data pribadi karyawan dan pelanggan, informasi keuangan yang sensitif, catatan kesehatan, hingga kekayaan intelektual seperti rahasia dagang dan paten.[3] Pengelolaan dan perlindungan aset digital ini menjadi imperatif untuk keberlangsungan operasional dan reputasi organisasi.

Transformasi digital yang kian pesat telah membawa kemudahan dan efisiensi yang luar biasa dalam berbagai sektor, dari bisnis hingga pemerintahan.[4] Namun, kemajuan ini juga diiringi dengan peningkatan signifikan dalam risiko dan tantangan keamanan siber.[6] Ancaman siber terus berevolusi, menjadi semakin canggih dan merusak, mengancam kerahasiaan, integritas, dan ketersediaan data.[6] Insiden kebocoran data, serangan

malware, dan *phishing* adalah ancaman nyata yang dapat mengakibatkan kerugian finansial, kerusakan reputasi, dan hilangnya kepercayaan pelanggan.[6] Oleh karena itu, penerapan standar keamanan data yang efektif dan tata kelola data yang matang bukan hanya menjadi praktik terbaik, melainkan sebuah keharusan strategis untuk memastikan keberlanjutan bisnis, mengurangi risiko operasional, mengoptimalkan investasi teknologi informasi, dan menjaga kepercayaan seluruh pemangku

kepentingan.[1]

Ruang Lingkup Laporan

Laporan ini menyajikan tinjauan komprehensif mengenai standar keamanan penyelenggara dan tata kelola data, dengan fokus khusus pada konteks teknik informatika. Pembahasan akan mencakup definisi dan konsep dasar yang relevan, aspek-aspek teknis keamanan data, kerangka kerja dan standar internasional yang diakui, regulasi dan kewajiban hukum yang berlaku di Indonesia, metodologi dan praktik terbaik dalam tata kelola data, tantangan-tantangan umum yang dihadapi dalam implementasi, serta solusi praktis untuk mengatasinya. Laporan ini juga akan menyertakan studi kasus yang relevan di Indonesia untuk memberikan gambaran implementasi di lapangan. Tujuan utama dari laporan ini adalah untuk membekali para profesional di bidang teknologi informasi, keamanan siber, dan manajemen data, serta para pembuat keputusan strategis, dengan pemahaman yang mendalam dan rekomendasi yang dapat ditindaklanjuti untuk membangun postur keamanan dan tata kelola data yang tangguh dan adaptif di organisasi mereka.

2. Definisi dan Konsep Dasar

Keamanan Data dan Keamanan Informasi (InfoSec)

Keamanan Data secara spesifik berfokus pada perlindungan data itu sendiri, baik data yang disimpan (data *at rest*) maupun data yang sedang dalam perjalanan (data *in transit*).[3] Ini melibatkan proses identifikasi data yang dimiliki organisasi, lokasinya, dan penilaian risiko yang mengelilingi data tersebut.[3] Teknik-teknik yang diterapkan dalam keamanan data meliputi enkripsi, autentikasi dan otorisasi pengguna, deteksi risiko dari dalam (ancaman

insider), penerapan kebijakan pencegahan kehilangan data (DLP), pencadangan data

secara teratur, sistem peringatan *real-time*, penilaian risiko yang sistematis, dan pengauditan data secara berkala.[3] Semua langkah ini bertujuan untuk mencegah ekstraksi data sensitif oleh pihak yang tidak berwenang.[3]

Sementara itu, **Keamanan Informasi (InfoSec)** merupakan payung yang lebih luas yang mencakup perlindungan informasi sensitif di seluruh lingkungan digital organisasi, termasuk *cloud*, aplikasi, dan titik akhir.[11] InfoSec tidak hanya mencakup keamanan siber yang berfokus pada teknologi, tetapi juga aspek keamanan fisik dan lingkungan, serta kontrol akses.[11] Elemen inti dari InfoSec melibatkan penerapan kebijakan, prosedur, alat, dan praktik terbaik untuk melindungi aplikasi dan data yang terkait dengannya. Tujuannya adalah untuk menjaga akurasi, keandalan, dan ketersediaan informasi, memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses, mengubah, atau mencampuri data.[11]

Memahami hubungan antara keamanan data dan keamanan informasi sangat penting untuk merancang strategi perlindungan yang komprehensif. Keamanan informasi adalah domain yang lebih luas yang mencakup semua aspek perlindungan aset informasi, baik dalam bentuk digital maupun fisik. Keamanan siber, yang berfokus pada perlindungan teknologi dan sistem dari serangan digital, merupakan bagian integral dari keamanan informasi. Dalam konteks ini, keamanan data adalah subset yang lebih spesifik, yang secara langsung berkaitan dengan perlindungan aset data itu sendiri dari akses, penggunaan, modifikasi, atau penghancuran yang tidak sah. Dengan demikian, InfoSec menyediakan kerangka kerja menyeluruh yang memastikan bahwa semua dimensi perlindungan informasi, termasuk keamanan data, dipertimbangkan dan diimplementasikan secara terpadu. Pendekatan ini menghindari fokus yang terlalu sempit pada satu aspek keamanan, sehingga menghasilkan pertahanan yang lebih kuat dan berkelanjutan terhadap berbagai ancaman.

Tata Kelola Data (Data Governance)

Tata kelola data adalah disiplin manajemen data yang berfokus pada kualitas, keamanan, dan ketersediaan data organisasi.[12] Disiplin ini merupakan bagian integral dari manajemen data secara keseluruhan, yang meliputi praktik pengumpulan, pemrosesan, dan penggunaan data secara aman dan efisien untuk mendukung pengambilan keputusan strategis dan meningkatkan hasil bisnis.[12] Tujuan utamanya adalah untuk memastikan integritas data dan kepatuhan terhadap persyaratan peraturan yang berlaku.[13] Tata kelola data melibatkan perumusan proses, peran,

tanggung jawab, aturan, metrik, dan standar yang mengatur pengelolaan data dalam suatu organisasi guna mencapai tujuan bisnis.[13] Penerapan tata kelola data yang efektif membantu organisasi dalam memanfaatkan data berkualitas tinggi untuk inisiatif seperti Kecerdasan Buatan (AI) dan Pembelajaran Mesin (ML), sekaligus melindungi data tersebut dan memastikan kepatuhan terhadap peraturan yang relevan.[12]

Perbedaan dan Keterkaitan Konsep

Keamanan data merupakan komponen kunci dan esensial dari tata kelola data.[13] Tata kelola data menyediakan kerangka kerja yang terstruktur, termasuk kebijakan, prosedur, dan akuntabilitas, yang memandu bagaimana keamanan data harus diterapkan dan dikelola secara konsisten di seluruh organisasi. Ini berarti bahwa upaya keamanan data tidak boleh dilakukan secara ad-hoc, melainkan harus terintegrasi dalam strategi tata kelola data yang lebih besar.

Tata kelola data berfungsi sebagai fondasi untuk keberlanjutan keamanan data. Tanpa kerangka tata kelola yang kuat, inisiatif keamanan data mungkin akan menghadapi kendala dalam jangka panjang. Tata kelola data memastikan adanya panduan yang jelas, penetapan peran dan tanggung jawab yang eksplisit, serta alokasi sumber daya yang konsisten untuk mendukung praktik keamanan data. Misalnya, tata kelola data menetapkan siapa yang bertanggung jawab atas kepemilikan data, bagaimana data diklasifikasikan berdasarkan tingkat sensitivitas, dan prosedur apa yang harus diikuti untuk akses dan penggunaan data.[14] Hal ini menciptakan lingkungan di mana keamanan data bukan hanya tugas teknis, tetapi menjadi bagian integral dari budaya dan operasional organisasi. Dengan demikian, tata kelola data memastikan bahwa upaya keamanan data selaras dengan tujuan bisnis, memitigasi risiko secara efektif, dan menjaga kepercayaan pemangku kepentingan dalam jangka panjang.

3. Aspek Teknis Keamanan Data dalam Teknik Informatika

Aspek teknis keamanan data dalam teknik informatika melibatkan serangkaian teknologi dan metodologi yang dirancang untuk melindungi informasi dari berbagai

ancaman. Penerapan teknik-teknik ini secara komprehensif sangat penting untuk membangun pertahanan siber yang tangguh.

Teknologi Keamanan Data Esensial

Berbagai teknologi menjadi tulang punggung keamanan data modern:

- **Enkripsi Data:** Ini adalah proses fundamental yang mengubah data menjadi format kode yang tidak dapat dibaca tanpa kunci dekripsi yang benar.[2] Enkripsi efektif melindungi data baik saat disimpan (*data at rest*) maupun saat ditransmisikan (*data in motion*), memastikan bahwa meskipun data disadap, isinya tetap tidak dapat dipahami oleh pihak yang tidak berwenang.[3] Contoh penerapannya termasuk penggunaan HTTPS untuk lalu lintas web dan enkripsi *end-to-end* dalam komunikasi pesan.[8]
- **Autentikasi dan Otorisasi Pengguna:** Proses ini memverifikasi kredensial pengguna dan mengkonfirmasi bahwa hak akses telah ditetapkan dan diterapkan dengan benar.[3] Kontrol akses berbasis peran (*Role-Based Access Control/RBAC*) memungkinkan organisasi memberikan akses hanya kepada individu yang benar-benar membutuhkan data tersebut untuk menjalankan tugasnya.[3] Penggunaan mekanisme autentikasi yang kuat, seperti autentikasi dua faktor (2FA), juga krusial untuk menambah lapisan keamanan.[15]
- **Pencegahan Kehilangan Data (Data Loss Prevention/DLP):** Kebijakan dan teknologi DLP dirancang untuk mengidentifikasi, memantau, dan mencegah aktivitas berbagi atau penggunaan data sensitif yang tidak sah pada titik akhir, aplikasi, dan layanan.[3] Ini membantu mencegah kebocoran atau pencurian data yang tidak disengaja maupun disengaja.
- **Pencadangan Data (Data Backup) dan Pemulihan Bencana (Disaster Recovery):** Melakukan pencadangan salinan data organisasi secara rutin adalah langkah vital untuk memastikan kemampuan pemulihan jika terjadi kegagalan penyimpanan, pelanggaran data, atau bencana alam.[3] Pemulihan bencana melibatkan serangkaian metode untuk membangun kembali sistem teknologi fungsional setelah insiden yang mengganggu, memastikan ketersediaan informasi dalam situasi darurat.[10]
- **Peringatan Real-time dan Pemantauan Aktivitas Anomali:** Sistem ini mengotomatiskan pemberitahuan untuk potensi penyalahgunaan data dan mendeteksi perilaku yang tidak biasa atau mencurigakan dalam sistem.[3]

Kemampuan ini memungkinkan organisasi untuk mengambil tindakan segera dan proaktif untuk menghentikan serangan siber sebelum menyebabkan kerusakan signifikan.[3]

- **Penilaian Risiko:** Proses ini melibatkan pemahaman bagaimana karyawan, vendor, kontraktor, dan mitra menggunakan dan memiliki informasi tentang data dan praktik keamanan organisasi.[3] Tujuannya adalah untuk mengidentifikasi potensi penyalahgunaan data dan mengembangkan strategi mitigasi yang sesuai.

Keamanan Jaringan dan Infrastruktur

Keamanan jaringan adalah fondasi untuk melindungi data yang bergerak di dalam dan di antara sistem. Berbagai teknologi dan praktik diterapkan untuk mengamankan infrastruktur jaringan:

- **Firewall:** Berfungsi sebagai penghalang atau filter yang mengontrol akses ke jaringan, mencegah lalu lintas tidak sah masuk atau keluar dari sistem.[2] Firewall memeriksa lalu lintas jaringan berdasarkan protokol dan dapat memblokir *traffic* yang berpotensi membahayakan.[17]
- **Deteksi Intrusi (Intrusion Detection System/IDS) dan Pencegahan Intrusi (Intrusion Prevention System/IPS):** Sistem ini secara aktif memantau aktivitas jaringan dan sistem untuk mendeteksi perilaku yang tidak biasa, upaya masuk ilegal, atau aktivitas mencurigakan lainnya.[4] IPS secara khusus memiliki kemampuan untuk tidak hanya mendeteksi tetapi juga secara aktif mencegah serangan pada jaringan.[19]
- **VPN (Virtual Private Network):** Teknologi ini menciptakan koneksi jaringan yang aman melalui jaringan publik, menjaga lalu lintas data tetap terenkripsi dan aman.[4] Ini sangat penting untuk melindungi data di perangkat seluler atau dalam lingkungan kerja jarak jauh.
- **Analitik Perilaku:** Sistem keamanan ini menggunakan *anomaly detection engines* untuk menganalisis pola perilaku dalam jaringan dan sistem, mengidentifikasi aktivitas yang menyimpang dari norma yang mungkin mengindikasikan upaya akses ilegal.[17] Sistem ini memberikan notifikasi ketika perilaku mencurigakan terdeteksi.
- **Keamanan Nirkabel:** Mengatasi kerentanan inheren pada jaringan nirkabel yang seringkali memiliki konfigurasi dan jenis enkripsi yang lebih lemah dibandingkan jaringan kabel.[17] Ini melibatkan penerapan protokol keamanan nirkabel yang kuat dan manajemen akses yang ketat.

Efektivitas keamanan jaringan tidak bergantung pada satu teknologi saja, melainkan pada bagaimana teknologi-teknologi ini diintegrasikan dan saling melengkapi. Misalnya, *firewall* membatasi akses, IDS/IPS mendeteksi dan mencegah serangan, sementara VPN mengamankan koneksi. Hal ini mencerminkan prinsip "pertahanan berlapis" (*defense-in-depth*), di mana beberapa lapisan kontrol keamanan diterapkan untuk melindungi aset. Dalam pendekatan ini, kegagalan satu kontrol tidak berarti kegagalan sistem keseluruhan, karena ada lapisan lain yang dirancang untuk menangkap dan memitigasi ancaman. Pendekatan ini secara signifikan meningkatkan ketahanan sistem terhadap serangan yang kompleks dan multi-vektor.

Keamanan Aplikasi dan Siklus Hidup Pengembangan Perangkat Lunak (Secure SDLC)

Keamanan aplikasi menjadi semakin krusial karena aplikasi modern seringkali menjadi titik masuk utama bagi serangan siber dan menyimpan data pengguna yang sensitif.[17] Kerentanan pada aplikasi seringkali disebabkan oleh kelalaian dalam proses pengembangan, seperti celah

SQL Injection atau *Cross-Site Scripting*.[20]

Untuk mengatasi hal ini, diperlukan pendekatan **Secure SDLC (Secure Software Development Life Cycle)**, yaitu kerangka kerja pengembangan perangkat lunak yang memprioritaskan keamanan sepanjang seluruh siklus hidupnya.[21] Tujuannya adalah untuk mengurangi risiko keamanan pada aplikasi dan sistem yang dibangun, serta mencegah serangan siber dan pelanggaran keamanan.[21]

Tahapan integrasi keamanan dalam SDLC meliputi:

- **Perencanaan:** Tahap ini menetapkan dasar untuk pengembangan perangkat lunak yang aman. Ini melibatkan identifikasi persyaratan keamanan, penentuan tujuan keamanan (kerahasiaan, integritas, ketersediaan), identifikasi regulasi kepatuhan yang relevan, dan pelaksanaan model ancaman (*threat modeling*) untuk mengidentifikasi potensi kerentanan sejak dini.[22] Selain itu, rencana keamanan yang mencakup kebijakan dan strategi manajemen risiko harus dikembangkan.[22]
- **Desain:** Pada tahap desain, fokusnya adalah memasukkan langkah-langkah keamanan ke dalam arsitektur perangkat lunak. Ini termasuk penggunaan pola

dan prinsip desain yang aman, seperti prinsip hak akses paling rendah (*least privilege*), pertahanan berlapis, dan pengaturan *default* yang aman, serta merancang perlindungan data yang kuat.[22]

- **Implementasi/Coding:** Tahap ini melibatkan penerapan praktik pengkodean yang aman. Pengembang harus menggunakan *tools* untuk analisis kode statis (*Static Application Security Testing/SAST*) dan analisis komposisi perangkat lunak (*Software Composition Analysis/SCA*) untuk mendeteksi kerentanan dalam kode dan komponen pihak ketiga.[23]
- **Pengujian:** Pengujian keamanan harus dilakukan sesegera mungkin setelah tahap *coding* selesai.[23] Ini mencakup
  fuzz testing, *penetration testing*, *Dynamic Application Security Testing/DAST*, dan *Interactive Application Security Testing/IAST*.[22] Pengujian ini harus diintegrasikan ke dalam
  Continuous Integration/Continuous Delivery (CI/CD) *pipeline* untuk memastikan pemeriksaan keamanan otomatis dan berkelanjutan.[24] Model ancaman juga harus ditinjau dan diperbarui jika terjadi regresi.[23]
- **Penerapan dan Operasi:** Setelah aplikasi diterapkan, penting untuk memastikan konfigurasi yang aman, melakukan pemantauan berkelanjutan terhadap aktivitas sistem, memiliki kesiapan tanggap insiden yang cepat, dan memberikan pelatihan berkelanjutan kepada pengguna.[22]

Pendekatan ini mencerminkan paradigma "Keamanan Shift-Left", yang berarti memasukkan tindakan keamanan lebih awal dalam SDLC.[24] Secara historis, keamanan seringkali menjadi pertimbangan di akhir siklus pengembangan, yang menyebabkan biaya perbaikan yang lebih tinggi dan kerentanan yang lebih sulit diatasi. Pendekatan

shift-left menandai pergeseran fundamental menuju keamanan proaktif, di mana kerentanan diidentifikasi dan diperbaiki pada tahap awal, secara signifikan mengurangi risiko dan biaya dalam jangka panjang. Ini memastikan bahwa keamanan bukan hanya fitur tambahan, tetapi merupakan bagian intrinsik dari kualitas perangkat lunak.

Manajemen Kerentanan Sistem Informasi

Manajemen kerentanan adalah proses berkelanjutan yang melibatkan identifikasi, evaluasi, penanganan (remediasi), dan pelaporan kerentanan dalam sistem informasi.[25] Ini berbeda dengan penilaian kerentanan, yang merupakan tindakan

tunggal untuk menentukan profil risiko setiap kerentanan.[25] Manajemen kerentanan yang solid memberikan peningkatan keamanan dan kontrol, karena organisasi dapat mempersulit penyerang untuk mendapatkan akses ke dalam sistem dengan melakukan pemindaian rutin dan menerapkan

patch tepat waktu.[25]

Komponen utama program pengelolaan kerentanan yang efektif meliputi:

- **Penemuan dan Inventaris Aset:** Tim TI bertanggung jawab untuk melacak dan menjaga catatan semua perangkat, perangkat lunak, *server*, dan aset digital lainnya di seluruh lingkungan perusahaan.[25] Sistem manajemen inventaris aset membantu memberikan visibilitas tentang aset yang dimiliki, lokasinya, dan bagaimana aset tersebut digunakan.
- **Pemindaian Kerentanan:** Melakukan serangkaian pengujian terhadap sistem dan jaringan untuk mencari kelemahan atau kekurangan umum.[25] Pengujian ini dapat mencakup upaya untuk mengeksploitasi kerentanan yang diketahui atau mencoba mendapatkan akses ke area terbatas.
- **Pengelolaan Patch:** Memastikan sistem komputer tetap mutakhir dengan penambal keamanan terbaru untuk menutup celah keamanan yang ditemukan.[15] Solusi pengelolaan
  patch seringkali mengotomatiskan pemeriksaan pembaruan dan penyebaran *patch*.
- **Security Incident and Event Management (SIEM):** Perangkat lunak SIEM mengumpulkan dan menggabungkan informasi serta kejadian keamanan organisasi secara *real-time*.[24] Ini memberikan visibilitas menyeluruh tentang apa yang terjadi di seluruh infrastruktur digital, termasuk pemantauan lalu lintas, identifikasi perangkat yang mencoba terhubung ke sistem internal, dan pelacakan aktivitas pengguna.
- **Uji Penetrasi (Penetration Testing):** Mensimulasikan serangan untuk menemukan dan mengeksploitasi kerentanan dalam sistem komputer sebelum peretas sungguhan melakukannya.[23] Ini membantu mengidentifikasi kelemahan yang dapat dieksploitasi di dunia nyata.
- **Inteligensi Ancaman:** Perangkat lunak perlindungan terhadap ancaman menyediakan kemampuan untuk melacak, memantau, menganalisis, dan memprioritaskan potensi ancaman.[18] Solusi ini mengumpulkan data dari berbagai sumber untuk mengidentifikasi tren dan pola yang dapat mengindikasikan pelanggaran atau serangan keamanan di masa mendatang.
- **Remediasi Kerentanan:** Proses memprioritaskan kerentanan yang ditemukan, mengidentifikasi langkah-langkah perbaikan yang sesuai, dan membuat tiket

remediasi agar tim TI dapat melaksanakannya.[25] Pelacakan remediasi adalah alat penting untuk memastikan kerentanan atau kesalahan konfigurasi ditangani dengan benar.

Manajemen kerentanan sebagai proses yang terus-menerus mengidentifikasi, mengevaluasi, mengatasi, dan melaporkan kerentanan menunjukkan bahwa keamanan siber bukanlah proyek sekali jalan, melainkan siklus hidup yang berulang dan adaptif.[25] Hal ini menekankan pentingnya pemantauan berkelanjutan, pembaruan, dan respons terhadap ancaman yang terus berevolusi. Organisasi yang hanya melakukan penilaian kerentanan sesekali akan tertinggal dari ancaman baru, sementara organisasi yang menerapkan manajemen kerentanan secara berkelanjutan akan lebih tangguh dan proaktif dalam mempertahankan diri dari serangan.

Audit Keamanan Sistem Informasi

Audit keamanan sistem informasi adalah evaluasi sistematis dan independen terhadap keamanan komputer dan aplikasinya.[27] Tujuannya adalah untuk memastikan bahwa sistem tersebut mampu melindungi aset organisasi, menjaga integritas data, dan mendukung pencapaian tujuan organisasi secara efektif dan efisien.[28]

Manfaat utama dari audit keamanan meliputi:

- **Identifikasi Kerentanan:** Audit dapat menemukan celah keamanan yang mungkin tidak terlihat oleh pengelola sistem sehari-hari.[29]
- **Memastikan Kepatuhan:** Memastikan organisasi mematuhi regulasi dan standar keamanan yang berlaku.[29]
- **Meningkatkan Kepercayaan:** Memberikan jaminan kepada pelanggan dan mitra bisnis tentang keamanan data.[29]
- **Mencegah Insiden Keamanan:** Audit proaktif dapat mencegah serangan siber dan kebocoran data dengan mengidentifikasi dan memperbaiki kelemahan sebelum dieksploitasi.[29]

Tahapan audit keamanan sistem informasi umumnya mencakup:

- **Perencanaan Audit:** Menentukan ruang lingkup, tujuan, dan metode audit. Tahap ini juga melibatkan pemahaman bisnis auditi (kebijakan, struktur organisasi, praktik) dan analisis risiko audit pendahuluan.[29]
- **Pengumpulan Data:** Melakukan wawancara, observasi, dan pengumpulan

dokumen serta *log* sistem.[28]
- **Evaluasi dan Analisis:** Menganalisis data yang terkumpul untuk mengidentifikasi kelemahan dan risiko keamanan.[29]
- **Pelaporan:** Menyusun laporan hasil audit yang mencakup temuan, risiko, dan rekomendasi perbaikan.[29]
- **Tindak Lanjut:** Memastikan rekomendasi diterapkan dan melakukan audit ulang jika diperlukan untuk memverifikasi efektivitas perbaikan.[29]

Metodologi audit dapat memanfaatkan teknik audit berbantuan komputer (*Computer-Aided Auditing Techniques/CAATTs*) untuk menganalisis data dan menguji integritas data secara rinci.[28] Standar internasional seperti ISO 27001 sering digunakan sebagai kriteria audit untuk menilai tingkat kepatuhan dan kematangan keamanan.[31] Audit keamanan sistem informasi bukan sekadar pemeriksaan kepatuhan satu kali, melainkan merupakan alat diagnostik yang krusial untuk secara proaktif mengidentifikasi kelemahan, memvalidasi efektivitas kontrol keamanan, dan mendorong perbaikan berkelanjutan dalam postur keamanan organisasi. Audit yang rutin dan komprehensif adalah investasi dalam ketahanan siber, bukan hanya biaya operasional.

Arsitektur Keamanan Data

Desain arsitektur data yang buruk dapat menimbulkan masalah keamanan data yang serius, secara signifikan meningkatkan risiko kebocoran data.[9] Oleh karena itu, arsitektur data harus dirancang dengan mempertimbangkan aspek keamanan sejak awal untuk melindungi data dari akses yang tidak sah.[9] Ini adalah implementasi dari prinsip "keamanan berdasarkan desain" (

security by design), di mana keamanan diintegrasikan ke dalam setiap tahap siklus hidup sistem, bukan hanya ditambahkan di akhir.

Arsitektur data dan informasi adalah kerangka kerja yang mendefinisikan struktur, penyimpanan, integrasi, dan pengelolaan data dalam suatu sistem.[32] Dalam konteks Sistem Pemerintahan Berbasis Elektronik (SPBE), arsitektur keamanan SPBE merupakan dokumen yang mendeskripsikan pengendalian dan pengintegrasian keamanan data dan informasi, aplikasi SPBE, serta infrastruktur SPBE secara terpadu di tingkat nasional, menjadi acuan bagi instansi pemerintah.[33]

Tujuan dari arsitektur data yang baik meliputi:

- **Integrasi Data:** Memungkinkan entitas yang berbeda untuk berbagi data secara sinergis dan mengintegrasikan informasi dari berbagai sumber, menghindari duplikasi dan meningkatkan efisiensi.[32]
- **Pengelolaan Data yang Efisien:** Memfasilitasi pengumpulan, penyimpanan, pengolahan, dan pembaruan data yang optimal, memastikan integritas, kualitas, dan keamanan data yang tinggi.[32]
- **Dasar untuk Analisis Data:** Menyediakan fondasi yang kuat untuk analisis data, memungkinkan pemerintah memperoleh wawasan berharga dan membuat keputusan berbasis bukti.[32]

Prinsip "keamanan berdasarkan desain" menekankan bahwa keamanan tidak boleh menjadi fitur tambahan yang dipasang belakangan, tetapi harus menjadi bagian intrinsik dari desain sistem sejak tahap awal. Pendekatan ini jauh lebih efektif dan hemat biaya daripada mencoba memperbaiki kerentanan setelah sistem dibangun, karena masalah keamanan dapat diidentifikasi dan diatasi pada titik paling awal, mengurangi risiko dan kompleksitas perbaikan di kemudian hari.

Tabel 3: Teknik Keamanan Data Teknis dan Penerapannya

Teknik Keamanan	Deskripsi Singkat	Penerapan/Manfaat Utama	Sumber (Snippet ID)
Enkripsi Data	Mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci dekripsi.	Melindungi data saat disimpan dan ditransmisikan; mencegah akses tidak sah.	3
Autentikasi & Otorisasi	Memverifikasi identitas pengguna dan hak aksesnya.	Memastikan hanya pengguna berwenang yang mengakses data; kontrol akses berbasis peran (RBAC); autentikasi	3

		dua faktor (2FA).	
Pencegahan Kehilangan Data (DLP)	Mengidentifikasi dan mencegah transfer data sensitif yang tidak sah.	Mencegah kebocoran atau pencurian data pada titik akhir, aplikasi, dan layanan.	[3]
Pencadangan Data & Pemulihan Bencana	Membuat salinan data dan rencana untuk mengembalikan sistem setelah insiden.	Memastikan data dapat dipulihkan dari kegagalan penyimpanan, pelanggaran, atau bencana; menjaga ketersediaan.	[3]
Peringatan Real-time & Pemantauan Anomali	Otomatisasi notifikasi dan deteksi perilaku mencurigakan.	Memungkinkan tindakan cepat untuk menghentikan serangan siber; identifikasi penyalahgunaan data.	[3]
Penilaian Risiko	Proses mengidentifikasi dan mengevaluasi potensi ancaman terhadap data.	Memahami kerentanan dan potensi penyalahgunaan data oleh berbagai pihak.	[3]
Firewall	Penghalang jaringan yang mengontrol lalu lintas masuk dan keluar.	Mencegah akses tidak berwenang; memfilter lalu lintas berbahaya.	[2]
Deteksi Intrusi (IDS) / Pencegahan Intrusi (IPS)	Memantau jaringan untuk mendeteksi/mencega h aktivitas mencurigakan.	Mengidentifikasi dan menghentikan serangan siber secara proaktif.	[8]
VPN (Virtual Private Network)	Membuat koneksi aman melalui jaringan publik.	Mengamankan lalu lintas jaringan, terutama untuk kerja jarak jauh dan	[4]

		perangkat seluler.	
Secure SDLC	Mengintegrasikan keamanan di seluruh siklus hidup pengembangan perangkat lunak.	Mengurangi kerentanan aplikasi; mencegah serangan siber dari tahap awal pengembangan.	21
Manajemen Kerentanan	Proses berkelanjutan identifikasi, evaluasi, remediasi, dan pelaporan kerentanan.	Meningkatkan keamanan sistem secara terus-menerus; proaktif mengatasi kelemahan.	25
Audit Keamanan Sistem Informasi	Evaluasi sistematis keamanan sistem dan aplikasi.	Mengidentifikasi kelemahan, memastikan kepatuhan, meningkatkan kepercayaan, mencegah insiden.	27
Arsitektur Keamanan Data	Kerangka kerja untuk struktur, penyimpanan, integrasi, dan pengelolaan data yang aman.	Memastikan keamanan data dirancang sejak awal; mendukung integrasi dan pengelolaan data yang efisien.	9

4. Kerangka Kerja dan Standar Internasional

Penerapan standar dan kerangka kerja internasional sangat penting untuk membangun postur keamanan dan tata kelola data yang kuat dan diakui secara global.

ISO/IEC 27000 Series (Sistem Manajemen Keamanan Informasi - ISMS)

ISO (International Organization for Standardization) dan IEC (International Electrotechnical Commission) adalah organisasi internasional non-pemerintah yang berfokus pada standarisasi.[1] Dalam konteks keamanan informasi, seri standar ISO/IEC 27000 adalah yang paling dikenal.

ISO/IEC 27001 adalah standar internasional yang menyediakan persyaratan untuk Sistem Manajemen Keamanan Informasi (ISMS), menawarkan kerangka kerja terstruktur untuk melindungi aset informasi dan ISMS itu sendiri.[18] ISMS adalah sistem terpusat yang membantu organisasi mengumpulkan, meninjau, dan meningkatkan kebijakan serta prosedur InfoSec, memitigasi risiko, dan membantu manajemen kepatuhan.[11]

ISO/IEC 27001:2022 dan Kontrolnya:
Versi terbaru, ISO/IEC 27001:2022, menekankan pendekatan berbasis risiko yang komprehensif untuk meningkatkan manajemen keamanan informasi.18 Standar ini mengintegrasikan proses evaluasi risiko yang menyeluruh dan kontrol Annex A yang diperbarui.18 Kontrol Annex A telah diringkas dari 114 menjadi 93, dengan beberapa digabungkan, direvisi, atau ditambahkan baru untuk mencerminkan lingkungan keamanan siber saat ini.18
Kontrol-kontrol ini dikelompokkan menjadi empat kategori utama [18]:

- **Kontrol Organisasi (37 kontrol):** Meliputi kebijakan keamanan informasi, peran dan tanggung jawab, pemisahan tugas, intelijen ancaman (BARU), keamanan dalam manajemen proyek, inventaris dan penggunaan aset yang dapat diterima, klasifikasi informasi, transfer informasi, kontrol akses, manajemen identitas, keamanan dalam hubungan pemasok, pengelolaan keamanan informasi dalam rantai pasokan TIK, penggunaan layanan *cloud* (BARU), perencanaan dan persiapan manajemen insiden, kesiapan TIK untuk keberlangsungan bisnis (BARU), persyaratan hukum, peraturan, dan kontraktual, hak kekayaan intelektual, perlindungan catatan, privasi dan perlindungan PII, tinjauan independen keamanan informasi, kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi, dan prosedur operasi yang didokumentasikan.
- **Kontrol Sumber Daya Manusia (8 kontrol):** Mencakup *screening*, syarat dan ketentuan kerja, kesadaran, pendidikan dan pelatihan keamanan informasi, proses disipliner, tanggung jawab setelah pengakhiran atau perubahan pekerjaan, perjanjian kerahasiaan atau *non-disclosure*, kerja jarak jauh, dan pelaporan insiden keamanan informasi.
- **Kontrol Fisik (14 kontrol):** Termasuk perimeter keamanan fisik, masuk fisik, pengamanan kantor, ruangan dan fasilitas, pemantauan keamanan fisik (BARU),

perlindungan terhadap ancaman fisik dan lingkungan, bekerja di area aman, *clear desk* dan *clear screen*, penempatan dan perlindungan peralatan, keamanan aset di luar lokasi, media penyimpanan, utilitas pendukung, keamanan kabel, pemeliharaan peralatan, dan pembuangan atau penggunaan kembali peralatan yang aman.

- **Kontrol Teknologi (34 kontrol):** Meliputi perangkat titik akhir pengguna, hak akses istimewa, pembatasan akses informasi, akses ke kode sumber, autentikasi aman, manajemen kapasitas, perlindungan terhadap *malware*, manajemen kerentanan teknis, manajemen konfigurasi (BARU), penghapusan data (BARU), *data masking* (BARU), pencegahan kebocoran data (BARU), pencadangan informasi, redundansi fasilitas pemrosesan informasi, *logging*, pemantauan aktivitas (BARU), sinkronisasi jam, penggunaan program utilitas istimewa, instalasi perangkat lunak pada sistem operasional, keamanan jaringan, keamanan layanan jaringan, segregasi jaringan, *web filtering* (BARU), penggunaan kriptografi, siklus hidup pengembangan aman, persyaratan keamanan aplikasi, prinsip arsitektur dan rekayasa sistem aman, pengkodean aman (BARU), pengujian keamanan dalam pengembangan dan penerimaan, pengembangan *outsourced*, pemisahan lingkungan pengembangan, pengujian dan produksi, manajemen perubahan, informasi uji, dan perlindungan sistem informasi selama pengujian audit.

Sebanyak 11 kontrol baru yang diperkenalkan dalam ISO 27001:2022 secara khusus berfokus pada teknologi dan tantangan yang muncul, seperti layanan *cloud*, intelijen ancaman, kesiapan TIK, pemantauan keamanan fisik, pengkodean aman, dan pencegahan kebocoran data.[18] Penambahan ini menunjukkan adaptasi standar terhadap lanskap ancaman siber yang terus berkembang.

Manfaat Sertifikasi ISO 27001: Mencapai sertifikasi ISO 27001 memberikan berbagai keuntungan signifikan bagi organisasi. Ini termasuk efisiensi biaya melalui pencegahan pelanggaran keamanan yang mahal, percepatan pertumbuhan penjualan dengan mengurangi permintaan dokumentasi keamanan yang ekstensif dari klien, pembangunan kepercayaan klien yang kuat, peningkatan manajemen risiko yang sistematis, perolehan keunggulan kompetitif di pasar, dan jaminan kepatuhan terhadap regulasi yang kompleks seperti GDPR dan NIS 2.[18]

Pembaruan ISO 27001 ke versi 2022 dengan penambahan kontrol baru yang menargetkan teknologi dan tantangan yang muncul menunjukkan bahwa standar ini tidak statis, melainkan dirancang untuk beradaptasi dengan lanskap ancaman siber yang terus berubah. Pengelompokan kontrol ke dalam kategori Organisasi, Sumber Daya Manusia, Fisik, dan Teknologi menggarisbawahi pendekatan holistik ISO 27001. Ini mengakui bahwa keamanan informasi bukan murni masalah teknis, tetapi juga

sangat bergantung pada faktor manusia, proses, dan lingkungan fisik. Standar ini menyediakan kerangka kerja yang komprehensif dan adaptif, memungkinkan organisasi untuk secara efektif mengelola dan memitigasi risiko keamanan informasi secara menyeluruh.

NIST Cybersecurity Framework (CSF) 2.0

NIST Cybersecurity Framework (CSF) adalah kerangka kerja keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga standar teknologi terkemuka dari Amerika Serikat.[35] Kerangka kerja ini memberikan panduan kepada berbagai jenis organisasi, termasuk industri dan lembaga pemerintah, untuk mengelola risiko keamanan siber secara efektif.[34]

NIST CSF menawarkan taksonomi hasil keamanan siber tingkat tinggi yang dapat digunakan oleh organisasi apa pun, terlepas dari ukuran, sektor, atau tingkat kematangannya, untuk lebih memahami, menilai, memprioritaskan, dan mengkomunikasikan upaya keamanan siber mereka.[36] Kerangka kerja ini bersifat non-preskriptif; artinya, ia tidak meresepkan

bagaimana hasil harus dicapai, tetapi menghubungkan ke sumber daya *online* yang memberikan panduan tambahan tentang praktik dan kontrol yang dapat diterapkan.[36]

Fungsi Inti (Core Functions): Fungsi-fungsi ini mengorganisir hasil keamanan siber pada tingkat tertinggi dan membentuk inti dari NIST CSF [35]:

- **GOVERN (GV):** Fungsi ini berada di pusat kerangka kerja, memastikan bahwa strategi, ekspektasi, dan kebijakan manajemen risiko keamanan siber organisasi ditetapkan, dikomunikasikan, dan dipantau.[36] Fungsi ini menginformasikan bagaimana organisasi memprioritaskan dan mencapai hasil dari lima fungsi lainnya, mengintegrasikan keamanan siber ke dalam manajemen risiko perusahaan yang lebih luas.
- **IDENTIFY (ID):** Berfokus pada pemahaman risiko keamanan siber organisasi saat ini, termasuk aset (data, *hardware*, *software*, sistem, fasilitas, layanan, orang) dan pemasok.[35] Pemahaman ini krusial untuk memprioritaskan upaya keamanan yang konsisten dengan strategi manajemen risiko dan kebutuhan misi organisasi.
- **PROTECT (PR):** Melibatkan penggunaan pengamanan untuk mengelola risiko keamanan siber.[35] Setelah mengidentifikasi dan memprioritaskan aset dan risiko, fungsi PROTECT mendukung pengamanan aset tersebut untuk mencegah atau

menurunkan kemungkinan dan dampak dari peristiwa keamanan siber yang merugikan. Contoh aktivitas meliputi penerapan kontrol akses, enkripsi data, dan pelatihan kesadaran keamanan.[35]

- **DETECT (DE):** Fungsi ini memungkinkan penemuan dan analisis anomali, indikator kompromi, dan peristiwa lain yang berpotensi merugikan secara tepat waktu yang mungkin mengindikasikan serangan dan insiden keamanan siber.[35] Ini mendukung respons insiden dan aktivitas pemulihan yang berhasil. Contoh aktivitas termasuk mengaktifkan
  monitoring log dan menggunakan *Intrusion Detection System* (IDS).[35]
- **RESPOND (RS):** Melibatkan pengambilan tindakan terkait insiden keamanan siber yang terdeteksi untuk menahan dampaknya.[35] Hasil dalam fungsi ini mencakup manajemen insiden, analisis, mitigasi, pelaporan, dan komunikasi. Menyusun rencana respons insiden adalah contoh aktivitas penting.[35]
- **RECOVER (RC):** Fungsi ini mendukung pemulihan aset dan operasi yang terpengaruh oleh insiden keamanan siber secara tepat waktu untuk mengurangi dampaknya dan memungkinkan komunikasi yang tepat selama upaya pemulihan.[35] Melakukan
  data backup secara berkala dan menyusun rencana keberlangsungan bisnis (*Business Continuity Plan/BCP*) adalah contoh aktivitas.[35]

Tingkat Implementasi (Tiers): NIST CSF mengidentifikasi empat tingkat implementasi untuk membantu organisasi mengukur kemajuan mereka dalam mengelola risiko keamanan siber [37]:

- **Tier 1 – Partial:** Organisasi mungkin akrab dengan NIST CSF dan telah mengimplementasikan beberapa aspek kontrol di beberapa area infrastruktur, namun implementasi bersifat reaktif dan kesadaran risiko terbatas.
- **Tier 2 – Risk Informed:** Organisasi lebih sadar akan risiko keamanan siber dan berbagi informasi secara informal, namun belum memiliki proses manajemen risiko keamanan siber yang terencana, dapat diulang, dan proaktif di seluruh organisasi.
- **Tier 3 – Repeatable:** Organisasi dan eksekutif seniornya sadar akan risiko keamanan siber dan telah mengimplementasikan rencana manajemen risiko keamanan siber yang dapat diulang di seluruh organisasi. Tim keamanan siber memiliki rencana tindakan untuk memantau dan merespons serangan siber secara efektif.
- **Tier 4 – Adaptive:** Organisasi berketahanan siber, menggunakan pelajaran yang dipetik dan indikator prediktif untuk mencegah serangan siber. Tim keamanan siber terus meningkatkan dan memajukan teknologi dan praktik keamanan siber organisasi, serta beradaptasi dengan perubahan ancaman dengan cepat dan

efisien.

NIST CSF secara konsisten menekankan sifat non-preskriptifnya, yang berarti tidak mendikte bagaimana hasil harus dicapai, tetapi menyediakan taksonomi hasil yang fleksibel.[36] Penambahan konsep "Tiers" memungkinkan organisasi untuk menilai tingkat kematangan praktik keamanan siber mereka saat ini dan menetapkan target perbaikan yang realistis. Hal ini menjadikan NIST CSF alat yang sangat fleksibel untuk evaluasi diri dan perencanaan strategis, berbeda dengan standar yang lebih berorientasi sertifikasi seperti ISO 27001. Pendekatan ini memungkinkan organisasi untuk mengadaptasi kerangka kerja sesuai dengan risiko unik dan tujuan misi mereka, memfasilitasi peningkatan berkelanjutan dalam postur keamanan siber.

Kerangka Kerja Keamanan Data Lainnya

Selain ISO 27001 dan NIST CSF, terdapat beberapa kerangka kerja keamanan data lain yang relevan, terutama untuk kebutuhan spesifik industri atau teknologi:

- **SOC 2 (System and Organization Controls 2):** Kerangka kerja ini berfokus pada pengendalian layanan terkait keamanan, ketersediaan, integritas pemrosesan, kerahasiaan, dan privasi data.[34] Kepatuhan dengan SOC 2 sangat penting bagi penyedia layanan
  cloud untuk memastikan mereka memiliki kontrol yang tepat untuk melindungi data pelanggan mereka.
- **CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry):** Ini adalah program sertifikasi yang relevan untuk keamanan *cloud*, menunjukkan komitmen penyedia layanan *cloud* terhadap praktik keamanan terbaik.[34]

Kehadiran kerangka kerja seperti SOC 2 dan CSA STAR, di samping ISO 27001 dan NIST CSF, menunjukkan bahwa meskipun kerangka kerja umum memberikan fondasi yang kuat, ada kebutuhan yang berkembang untuk standar yang lebih spesifik industri atau teknologi, seperti yang berkaitan dengan layanan *cloud* atau penyedia layanan. Hal ini mengimplikasikan bahwa organisasi mungkin perlu mengadopsi kombinasi kerangka kerja untuk mencapai postur keamanan dan tata kelola data yang komprehensif, disesuaikan dengan konteks operasional dan jenis data yang mereka kelola. Pendekatan multi-kerangka kerja ini memungkinkan organisasi untuk mengatasi persyaratan kepatuhan yang beragam dan mengelola risiko secara lebih terperinci.

Tabel 1: Perbandingan Kerangka Kerja Keamanan Data Internasional (ISO 27001 vs. NIST CSF)

Aspek Perbandingan	ISO/IEC 27001:2022	NIST Cybersecurity Framework 2.0	Sumber (Snippet ID)
Tujuan Utama	Menyediakan persyaratan untuk Sistem Manajemen Keamanan Informasi (ISMS) dan sertifikasi.	Memberikan panduan untuk mengelola risiko keamanan siber; bersifat non-preskriptif.	18
Sifat	Standar sertifikasi internasional; audit eksternal untuk kepatuhan.	Kerangka kerja sukarela; alat untuk penilaian diri dan peningkatan berkelanjutan.	18
Fokus Utama	Manajemen keamanan informasi secara holistik (proses, orang, teknologi, fisik).	Manajemen risiko siber (Identifikasi, Lindungi, Deteksi, Respons, Pulihkan, Tata Kelola).	11
Pendekatan	Berbasis risiko; menetapkan kontrol Annex A yang spesifik.	Berbasis hasil; menyediakan taksonomi hasil keamanan siber tingkat tinggi.	18
Tingkat Kematangan	Tidak secara eksplisit memiliki "tingkat" kematangan internal, tetapi kepatuhan penuh adalah tujuannya.	Memiliki empat "Tiers" (Partial, Risk Informed, Repeatable, Adaptive) untuk mengukur kematangan.	36

Kepatuhan Regulasi	Membantu memenuhi berbagai regulasi global (misalnya GDPR, NIS 2).	Membantu memenuhi regulasi dan *compliance* di berbagai sektor, fleksibel.	[18]
Manfaat Utama	Efisiensi biaya, percepatan penjualan, kepercayaan klien, keunggulan kompetitif.	Peningkatan kesiapan, membangun budaya keamanan, fleksibel dan *scalable*.	[18]
Fleksibilitas	Memungkinkan penyesuaian kontrol berdasarkan penilaian risiko, namun tetap ketat untuk sertifikasi.	Sangat fleksibel, dapat disesuaikan dengan kebutuhan unik organisasi tanpa preskripsi cara.	[18]

5. Regulasi dan Kewajiban di Indonesia

Indonesia telah mengambil langkah signifikan dalam memperkuat kerangka hukum terkait perlindungan data dan penyelenggaraan sistem elektronik, dengan dua pilar utama: Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Peraturan Pemerintah (PP) No. 71 Tahun 2019.

Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022

Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 disahkan pada 17 Oktober 2022 dan mulai berlaku penuh pada Oktober 2024, dua tahun setelah pengesahannya.[38] Regulasi ini dirancang untuk mengatur secara komprehensif pengumpulan, penggunaan, pengungkapan, dan pemrosesan data pribadi oleh berbagai entitas, termasuk organisasi internasional serta lembaga pemerintah dan swasta di Indonesia.[40]

Jenis Data Pribadi: UU PDP mengklasifikasikan data pribadi menjadi dua kategori utama [39]:

- **Data pribadi yang bersifat spesifik:** Meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
- **Data pribadi yang bersifat umum:** Meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Hak Subjek Data: Setiap individu, sebagai pemilik data pribadi, diberikan hak fundamental yang kuat oleh UU PDP [38]:

- Hak untuk mengetahui bagaimana data pribadinya digunakan.
- Hak untuk meminta akses atau penghapusan data jika diperlukan (*right to be forgotten*).
- Hak untuk menarik persetujuan untuk pemrosesan data.
- Hak untuk keberatan terhadap pemrosesan data.

Kewajiban Pengendali Data (Data Controllers): Organisasi yang mengumpulkan dan menentukan tujuan pemrosesan data memiliki kewajiban yang ketat [38]:

- Wajib memperoleh persetujuan eksplisit dari subjek data sebelum memproses data pribadi.
- Harus menjamin keamanan data untuk mencegah kebocoran atau penyalahgunaan.
- Memiliki dasar hukum yang sah untuk pemrosesan data, serta memproses data secara terbatas, spesifik, sah, dan transparan.
- Memastikan akurasi, kelengkapan, dan konsistensi data pribadi.
- Mencatat semua aktivitas pemrosesan data pribadi.
- Melakukan Penilaian Dampak Perlindungan Data (*Data Protection Impact Assessment/DPIA*) untuk aktivitas pemrosesan berisiko tinggi.
- Wajib melaporkan kebocoran data pribadi dalam waktu 3x24 jam kepada subjek data dan otoritas yang berwenang.
- Menyediakan mekanisme pengaduan yang jelas bagi subjek data terkait pelanggaran data.
- Menghapus atau memusnahkan data pribadi ketika tidak lagi diperlukan.

Kewajiban Prosesor Data (Data Processors): Entitas yang memproses data atas nama pengendali data wajib memproses data hanya di bawah instruksi Pengendali Data dan memastikan kepatuhan terhadap regulasi selama pemrosesan.[41]

Ketentuan Penunjukan Petugas Perlindungan Data (DPO): Penunjukan DPO menjadi wajib bagi organisasi yang melakukan pemrosesan data pribadi skala besar, memproses data sensitif, atau data yang berkaitan dengan layanan publik atau tindak pidana.[41]

Transfer Data Internasional: Transfer data pribadi ke luar negeri diatur secara ketat. Organisasi harus memastikan bahwa negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi. Jika tidak, pengamanan tambahan harus diterapkan, termasuk memperoleh persetujuan subjek data.[41]

Sanksi: Pelanggaran terhadap UU PDP dapat dikenai sanksi administratif yang signifikan, termasuk peringatan tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan atau pemusnahan data pribadi, dan denda hingga 2% dari pendapatan tahunan. Selain itu, terdapat pula sanksi pidana berupa denda dan/atau penjara untuk pelanggaran terkait pengumpulan, pengungkapan, atau penyalahgunaan data yang melanggar hukum.[38]

UU PDP bukan hanya sekadar kerangka hukum tambahan, melainkan merupakan tonggak penting yang secara fundamental mengubah lanskap perlindungan data di Indonesia. Dengan memberikan hak-hak yang kuat kepada subjek data (seperti hak untuk dihapus atau menarik persetujuan) dan membebankan kewajiban yang ketat kepada pengendali/prosesor data (seperti persetujuan eksplisit, DPIA, dan pelaporan insiden 3x24 jam), UU ini mendorong organisasi untuk beralih dari pendekatan reaktif ke proaktif dalam mengelola privasi data. Kesamaan dengan GDPR menunjukkan upaya Indonesia untuk menyelaraskan diri dengan standar global, yang memiliki implikasi besar bagi bisnis yang beroperasi secara internasional, menuntut adaptasi kebijakan dan sistem yang komprehensif.

Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 mengatur secara rinci penyelenggaraan sistem dan transaksi elektronik di Indonesia.[42] Regulasi ini menetapkan berbagai kewajiban bagi Penyelenggara Sistem Elektronik (PSE) untuk memastikan keamanan dan keandalan operasional.

Kewajiban Penyelenggara Sistem Elektronik (PSE):

- **Rekam Jejak Audit:** PSE wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik. Rekam jejak ini digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.[43]
- **Edukasi Pengguna:** PSE wajib melakukan edukasi kepada Pengguna Sistem Elektronik. Edukasi ini minimal mencakup hak, kewajiban, dan tanggung jawab seluruh pihak terkait, serta prosedur pengajuan komplain.[43]
- **Informasi Perlindungan Pengguna:** Penyelenggara Agen Elektronik wajib memuat atau menyampaikan informasi untuk melindungi hak pengguna pada Agen Elektronik yang diselenggarakannya. Informasi ini meliputi identitas penyelenggara, objek transaksi, kelayakan atau keamanan Agen Elektronik, tata cara penggunaan perangkat, syarat kontrak, prosedur mencapai kesepakatan, jaminan privasi dan/atau perlindungan Data Pribadi, dan nomor telepon pusat pengaduan.[43]
- **Prinsip Kehati-hatian dan Pengamanan:** Dalam penyelenggaraan Agen Elektronik, PSE harus memperhatikan prinsip kehati-hatian, pengamanan dan terintegrasinya sistem Teknologi Informasi, pengendalian pengamanan atas aktivitas Transaksi Elektronik, efektivitas dan efisiensi biaya, serta perlindungan konsumen.[43]
- **Prosedur Standar Pengoperasian:** PSE wajib memiliki dan menjalankan prosedur standar pengoperasian yang memenuhi prinsip pengendalian pengamanan data pengguna dan Transaksi Elektronik. Prinsip pengendalian pengamanan data ini meliputi kerahasiaan, integritas, ketersediaan, keautentikan, otorisasi, dan kenirsangkalan (*non-repudiation*).[43]
- **Pengujian Keautentikan dan Otorisasi:** PSE wajib melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik yang melakukan Transaksi Elektronik.[43]
- **Penanganan Pencurian Data:** PSE wajib memiliki dan melaksanakan kebijakan dan prosedur untuk mengambil tindakan jika terdapat indikasi terjadi pencurian data.[43]
- **Pengendalian Akses:** Memastikan pengendalian terhadap otorisasi dan hak Akses terhadap sistem, *database*, dan aplikasi Transaksi Elektronik.[43]
- **Perlindungan Integritas Data:** Menyusun dan melaksanakan metode dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Transaksi Elektronik.[43]
- **Rencana Keberlangsungan Bisnis (BCP):** PSE wajib memiliki rencana keberlangsungan bisnis termasuk rencana kontingensi yang efektif untuk memastikan tersedianya sistem dan jasa Transaksi Elektronik secara berkesinambungan.[43]

- **Penanganan Insiden:** Memiliki prosedur penanganan kejadian tak terduga yang cepat dan tepat untuk mengurangi dampak suatu insiden, penipuan, dan kegagalan Sistem Elektronik.[43]

Kewajiban-kewajiban yang diatur dalam PP 71 Tahun 2019 ini menegaskan bahwa PSE memiliki tanggung jawab yang signifikan dalam menjaga keamanan operasional data. Regulasi ini tidak hanya berfokus pada perlindungan data pribadi, tetapi juga pada keandalan dan integritas seluruh sistem dan transaksi elektronik. Adanya kewajiban untuk menyediakan rekam jejak audit, melakukan edukasi pengguna, dan memiliki rencana keberlangsungan bisnis menunjukkan bahwa pemerintah mendorong pendekatan proaktif dan komprehensif dalam manajemen risiko teknologi informasi. Hal ini berarti PSE harus membangun sistem yang tidak hanya aman dari serangan eksternal, tetapi juga tangguh terhadap kegagalan internal dan mampu menjaga kepercayaan pengguna melalui transparansi dan mekanisme pengaduan yang efektif.

6. Metodologi dan Praktik Terbaik Tata Kelola Data

Penerapan tata kelola data yang efektif memerlukan pendekatan yang sistematis dan terstruktur, menggabungkan aspek manusia, proses, dan teknologi.

Pendekatan Holistik: People, Process, Technology (PPT)

Model *People, Process, Technology* (PPT) adalah pendekatan holistik yang diakui secara luas untuk peningkatan proses dan manajemen risiko.[44] Dalam konteks keamanan informasi dan tata kelola data, ketiga elemen ini harus bekerja secara sinergis untuk menciptakan pertahanan yang efektif terhadap ancaman siber dan memastikan pengelolaan data yang optimal.[5]

- **People (Orang):** Elemen manusia adalah garis pertahanan pertama dan seringkali yang terlemah.[46] Penting untuk menyadarkan dan melatih karyawan, pelanggan, dan masyarakat luas tentang pentingnya keamanan siber.[5] Edukasi mengenai
  phishing, *malware*, dan praktik keamanan lainnya dapat membantu individu mengenali dan menghindari ancaman.[5] Pelatihan berkala dan berkelanjutan

sangat penting untuk memastikan karyawan selalu *terupdate* dengan ancaman terbaru, yang terus berkembang.[47] Simulasi serangan siber, seperti simulasi *phishing*, adalah alat yang sangat efektif untuk menguji kesiapan karyawan dalam menghadapi ancaman nyata.[47] Membangun budaya keamanan yang kuat di dalam organisasi, di mana karyawan merasa menjadi bagian dari perlindungan aset informasi, adalah kunci keberhasilan.[7] Ini melibatkan semua tingkatan organisasi, dari pimpinan hingga karyawan di semua level.[47]

- **Process (Proses):** Organisasi perlu mengembangkan dan memelihara kebijakan keamanan yang mencakup penilaian risiko teratur, strategi mitigasi, dan protokol respons insiden.[5] Proses ini memastikan bahwa tindakan pencegahan tersedia dan respons yang cepat serta efektif dapat dilaksanakan saat insiden keamanan terjadi.[7] Pengembangan dan penerapan standar keamanan, audit berkala, serta latihan penanggulangan insiden adalah bagian penting dari proses ini.[7] Manajemen risiko harus menjadi bagian integral dari strategi bisnis organisasi, dengan identifikasi aset kritis, penilaian kerentanan, dan analisis dampak bisnis sebagai langkah-langkah kunci.[5] Memiliki rencana pemulihan bencana dan kelangsungan bisnis yang teruji juga memastikan operasi bisnis dapat dilanjutkan dengan minimal gangguan jika terjadi serangan siber.[5]
- **Technology (Teknologi):** Adopsi teknologi keamanan yang canggih sangat penting untuk menghadapi ancaman yang terus berkembang.[5] Ini mencakup pemantauan jaringan *real-time*, analitik prediktif, dan otomatisasi respons insiden.[5] Teknologi memfasilitasi proses dan didukung oleh orang. Namun, teknologi sendiri tidak akan menyelesaikan semua masalah; ia harus diintegrasikan dengan proses yang jelas dan orang-orang yang terlatih.[45]

Menciptakan kohesi antara ketiga elemen ini seringkali menjadi tantangan.[45] Pemimpin harus mendorong tim lintas fungsi untuk bekerja sama, mengidentifikasi masalah, menetapkan prioritas, dan mengatasi masalah manajemen risiko dari sudut pandang yang lebih luas, yang memperhitungkan tujuan bisnis, kepatuhan, dan keamanan.[45] Visibilitas perusahaan yang terpusat dan tersistematisasi dalam satu platform dapat membuat manajemen risiko lebih mudah dan efektif.[45]

DAMA-DMBOK (Data Management Body of Knowledge)

DAMA-DMBOK adalah kerangka kerja yang diakui secara global yang mendefinisikan

prinsip-prinsip inti, praktik terbaik, dan fungsi-fungsi penting manajemen data.[48] Dikembangkan oleh DAMA International, panduan ini menyediakan fondasi terstruktur bagi para profesional, organisasi, dan pendidik untuk memahami, mengimplementasikan, dan terus meningkatkan praktik manajemen data.[48]

DAMA-DMBOK mengorganisir manajemen data menjadi 11 area pengetahuan, dengan tata kelola data berfungsi sebagai fondasi yang mendukung semua fungsi lainnya.[49] Area pengetahuan utama meliputi:

- **Tata Kelola Data:** Menetapkan kebijakan, prosedur, dan tanggung jawab untuk mengelola data sebagai aset.[49]
- **Arsitektur Data:** Merancang dan memelihara kerangka struktural untuk data.[49]
- **Pemodelan dan Desain Data:** Mengembangkan model data untuk mendukung operasi bisnis dan analitik.[49]
- **Manajemen Kualitas Data:** Memastikan akurasi, konsistensi, dan keandalan data.[13]
- **Keamanan Data:** Melindungi data sensitif dan memastikan kepatuhan terhadap peraturan industri.[13]
- **Manajemen Metadata:** Mengkatalogkan, mengatur, dan melacak silsilah data.[13]
- **Manajemen Siklus Hidup Data:** Mengelola seluruh siklus hidup data untuk mengoptimalkan sumber daya dan meminimalkan risiko.[13]

Prinsip Tata Kelola Data DAMA-DMBOK:

- **Akuntabilitas:** Menetapkan peran dan tanggung jawab untuk kepemilikan dan *stewardship* data.[49]
- **Kebijakan dan Standar:** Mendefinisikan aturan untuk manajemen data guna memastikan kepatuhan dan konsistensi.[13]
- **Hak Keputusan:** Menetapkan otoritas untuk pengambilan keputusan terkait aset data.[49]
- **Metrik Kinerja:** Mengukur efektivitas tata kelola dan dampaknya terhadap tujuan organisasi.[49]

Langkah-langkah Adopsi Kerangka Kerja DAMA-DMBOK:

- **Mempersiapkan Organisasi:** Menilai kesiapan organisasi untuk perubahan, mengevaluasi praktik manajemen data saat ini, mengidentifikasi kesenjangan, dan mendefinisikan tujuan.[50] Ini juga melibatkan pembentukan struktur tata kelola data dan mendapatkan dukungan eksekutif.[50]
- **Mengimplementasikan Kerangka Kerja:** Menerapkan prinsip dan praktik yang digariskan dalam DAMA-DMBOK ke dalam proses manajemen data organisasi.[50] Ini mungkin memerlukan penetapan peran dan tanggung jawab baru, pembaruan

kebijakan dan prosedur, serta implementasi solusi teknologi.[50] Melibatkan semua pemangku kepentingan yang relevan untuk memastikan keselarasan dan mendapatkan dukungan adalah penting.[50]
- **Memantau dan Menyesuaikan:** Memantau dan mengevaluasi efektivitas kerangka kerja secara berkelanjutan.[50] Ini melibatkan penilaian dampak praktik yang diadopsi, pengukuran indikator kinerja utama, dan pengumpulan umpan balik dari pengguna dan pemangku kepentingan.[50] Berdasarkan temuan, penyesuaian dilakukan untuk mengoptimalkan kemampuan manajemen data.

DAMA-DMBOK adalah kerangka kerja yang komprehensif dan *scalable*, cocok untuk organisasi dengan berbagai ukuran dan industri.[49] Dengan menekankan nilai strategis data, DAMA-DMBOK memastikan inisiatif tata kelola selaras dengan tujuan bisnis, mendorong inovasi, dan keunggulan kompetitif.[48] Kerangka kerja ini juga mempromosikan praktik data yang konsisten di seluruh departemen, mengurangi redundansi, dan memungkinkan integrasi aset data yang mulus.[49] Melalui kebijakan yang kuat untuk keamanan, kualitas, dan kepatuhan, DAMA-DMBOK membantu organisasi memitigasi risiko terkait pelanggaran data, pelanggaran regulasi, dan pengambilan keputusan yang buruk.[49]

Praktik Terbaik dalam Membangun Kerangka Kerja Keamanan Data

Membangun kerangka kerja keamanan data yang efektif memerlukan kombinasi praktik teknis dan prosedural:

- **Manajemen Patch yang Andal:** Menerapkan proses manajemen *patch* yang andal sangat penting. Ini mencakup identifikasi kerentanan keamanan, penilaian risiko, pengujian dan penerapan *patch*, serta validasi bahwa *patch* telah berhasil diterapkan.[26] Audit rutin terhadap perangkat lunak *database* harus dilakukan untuk memverifikasi bahwa semua *patch* terbaru dan sesuai dengan rekomendasi vendor.[26]
- **Kontrol Autentikasi dan Otorisasi yang Kuat:** Penggunaan kontrol autentikasi dan otorisasi yang kuat sangat penting untuk mengamankan akses ke *database* dan menjaga data sensitif.[26] Ini memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi kritis.
- **Minimalisasi Permukaan Serangan:** Mengurangi permukaan serangan *database* sangat penting untuk meningkatkan keamanan.[26] Banyak *database* menyertakan fitur yang mungkin tidak diperlukan di lingkungan spesifik,

dan fitur-fitur ini dapat menjadi titik masuk yang tidak sengaja bagi penyerang. Menghapus fitur yang tidak digunakan dan mengkonfigurasi sistem dengan prinsip *least privilege* dapat secara signifikan mengurangi risiko.
- **Pemantauan Berkelanjutan:** Implementasi sistem pemantauan dan audit yang memeriksa aktivitas dalam sistem secara *real-time* membantu dalam mendeteksi aktivitas mencurigakan lebih awal.[15] Pemantauan berkelanjutan adalah kunci untuk respons cepat terhadap ancaman.

Praktik-praktik ini, ketika diterapkan secara terpadu, membentuk kerangka kerja komprehensif untuk mengamankan data dan aplikasi. Memastikan postur keamanan selalu *mutakhir*, efektif, dan mencerminkan kemajuan terkini dalam enkripsi dan keamanan jaringan adalah investasi dalam kelangsungan dan integritas bisnis.[8]

7. Tantangan Implementasi dan Solusi Praktis

Implementasi standar keamanan dan tata kelola data di lingkungan teknik informatika menghadapi berbagai tantangan, namun terdapat solusi praktis untuk mengatasinya.

Tantangan Umum Implementasi

- **Ancaman *Malware* dan Serangan Siber yang Terus Berkembang:** *Malware* dan serangan siber terus menjadi semakin canggih, mengancam keamanan data pengguna.[6] Serangan seperti *ransomware*, *phishing*, dan *DDoS* dapat melumpuhkan sistem dan mencuri data sensitif.[4]
- **Ketidakpatuhan Regulasi Privasi:** Adanya regulasi privasi yang ketat seperti GDPR di Eropa dan UU PDP di Indonesia menempatkan tekanan pada organisasi untuk mematuhi standar pengumpulan dan pemrosesan data.[6] Ketidakpatuhan dapat mengakibatkan sanksi administratif dan pidana yang berat.[41]
- **Penggunaan *Big Data*:** Penggunaan *big data* untuk analisis dapat menimbulkan risiko privasi data jika tidak dikelola dengan benar.[6] Kompleksitas dan volume data yang besar menambah tantangan dalam menjaga konsistensi dan keamanan.[32]
- **Kebocoran Data dan Serangan *Phishing*:** Ancaman kebocoran data dan serangan *phishing* terus merugikan pengguna dengan mengakses informasi

pribadi mereka.[6] Insiden seperti kebocoran data di Pusat Data Nasional dan layanan kesehatan digital di Indonesia menunjukkan kerentanan yang ada.[52]
- **Kurangnya Kesadaran Pengguna:** Banyak pengguna yang tidak sepenuhnya menyadari risiko keamanan dan tidak menerapkan praktik keamanan yang baik, seringkali menjadi penyebab utama pelanggaran data.[6]
- **Keterbatasan Sumber Daya:** Organisasi sering menghadapi kendala seperti kurangnya sumber daya finansial, keterbatasan SDM dengan *expertise* di bidang keamanan siber, dan kesulitan dalam mengintegrasikan berbagai teknologi yang ada.[35]

Solusi Strategis untuk Mengatasi Tantangan

Mengatasi tantangan ini memerlukan pendekatan multi-faceted yang mencakup teknologi, kebijakan, dan faktor manusia:

- **Keamanan Siber yang Komprehensif:** Mengadopsi pendekatan keamanan siber yang komprehensif dengan menggunakan perangkat lunak antivirus yang terkini, *firewall* yang kuat, dan pembaruan sistem secara teratur.[6] Investasi dalam sistem deteksi ancaman canggih juga penting untuk mendeteksi dan merespons serangan dengan cepat.[55]
- **Pematuhan Regulasi yang Ketat:** Melibatkan tim keamanan dan privasi data yang berkompeten untuk memastikan pemenuhan regulasi privasi dan peraturan lainnya.[6] Ini mencakup pemahaman mendalam tentang persyaratan hukum dan penerapannya dalam konteks operasional.
- **Pengelolaan *Big Data* yang Aman:** Menerapkan protokol keamanan data yang ketat dan menggunakan solusi enkripsi untuk melindungi integritas data saat digunakan untuk analisis *big data*.[6] Klasifikasi data berdasarkan sensitivitas juga membantu dalam pengelolaan yang aman.[12]
- **Pendidikan dan Pelatihan Keamanan Berkelanjutan:** Meningkatkan kesadaran pengguna melalui kampanye pendidikan dan pelatihan keamanan yang teratur.[6] Mengajarkan karyawan untuk mengidentifikasi serangan *phishing* dan praktik keamanan lainnya dapat mengurangi risiko yang disebabkan oleh kesalahan manusia.[8] Simulasi serangan siber juga efektif untuk menguji kesiapan.[47]
- **Penerapan Teknologi Enkripsi:** Menggunakan teknologi enkripsi untuk melindungi data saat berada dalam penyimpanan dan perpindahan, memastikan bahwa bahkan jika terjadi kebocoran data, informasi yang dicuri tetap tidak dapat

diakses atau dipahami.[6]

- **Pengelolaan Akses Pengguna yang Ketat:** Menerapkan kontrol akses yang ketat dan memberikan hak akses yang sesuai dengan pekerjaan dan tanggung jawab individu dalam organisasi.[6] Kontrol akses berbasis peran (RBAC) adalah praktik terbaik dalam hal ini.[3]
- **Audit Keamanan Rutin:** Melakukan audit keamanan rutin untuk mendeteksi dan merespons ancaman keamanan dengan cepat sebelum dapat menyebabkan kerugian yang signifikan.[6] Audit membantu mengidentifikasi potensi celah keamanan dan mendorong tindakan perbaikan.[29]
- **Prinsip Privasi Terbuka:** Menerapkan prinsip privasi terbuka dengan memberikan informasi yang jelas kepada pengguna tentang bagaimana data mereka dikumpulkan, digunakan, dan disimpan.[6] Ini membangun kepercayaan dan akuntabilitas.

Studi Kasus Kegagalan Implementasi di Indonesia

Beberapa insiden di Indonesia menyoroti pentingnya keamanan data dan tata kelola yang kuat:

- **Insiden Kebocoran Data Pusat Data Nasional (Juni 2024):** Insiden ini menjadi salah satu krisis siber terbesar dalam sejarah transformasi digital pemerintah Indonesia.[52] Penyebab utama kebocoran data teridentifikasi pada manajemen keamanan yang lemah, ketiadaan cadangan data yang memadai, dan implementasi tata kelola sistem digital yang buruk.[52] Studi ini merekomendasikan pembaruan kebijakan nasional, peningkatan kapasitas sumber daya manusia, dan adopsi teknologi keamanan canggih untuk memperkuat ketahanan siber pemerintah.[52]
- **Kebocoran Data Layanan Telemedisin (termasuk e-HAC dan rekam medis COVID-19):** Perkembangan layanan telemedisin di Indonesia, meskipun inovatif, dihadapkan pada masalah hukum serius terkait kebocoran data pribadi pasien yang belum tertangani secara memadai.[53] Meskipun kerangka hukum formal ada, implementasi praktisnya masih lemah, terbukti dari berbagai insiden kebocoran data.[53] Regulasi teknis yang ada dinilai belum cukup mengatasi kompleksitas sistem digital, sementara kesadaran penyedia layanan mengenai prinsip privasi dan akuntabilitas masih kurang.[53] Perlindungan data pasien harus menjadi bagian integral dari layanan medis digital melalui penegakan hukum yang efektif dan penguatan tata kelola data yang etis dan transparan.[53]

Kasus-kasus ini menunjukkan bahwa meskipun kerangka hukum dan standar telah ada, implementasi yang lemah, kurangnya kesadaran, dan investasi yang tidak memadai dalam manajemen keamanan dan tata kelola data dapat menyebabkan konsekuensi yang merugikan. Ini menggarisbawahi bahwa keamanan siber dan tata kelola data bukan hanya masalah kepatuhan, tetapi juga masalah operasional dan strategis yang memerlukan komitmen berkelanjutan dari semua tingkatan organisasi.

8. Studi Kasus Implementasi Berhasil di Indonesia

Meskipun tantangan implementasi keamanan data dan tata kelola data masih ada, beberapa organisasi di Indonesia telah menunjukkan keberhasilan dalam menerapkan standar dan kerangka kerja internasional.

Implementasi ISO 27001 di Perusahaan Teknologi

Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi telah terbukti meningkatkan keamanan informasi melalui penerapan kontrol yang sistematis dan terstruktur, serta membantu kepatuhan regulasi.[57] Sebuah perusahaan teknologi besar di Indonesia melaporkan penurunan kejadian keamanan setelah menerapkan standar ini, yang juga berdampak positif pada peningkatan kepercayaan pelanggan dan pendapatan mereka.[57]

Contoh nyata keberhasilan ini adalah **Telkom Indonesia** yang meraih sertifikasi ISO 27001:2013 seri Biometrik untuk produk Picaso e-KYC mereka.[58] Picaso e-KYC adalah produk

Big Data yang memanfaatkan *Artificial Intelligence* untuk mengolah data gambar dan video, seperti *Optical Character Recognition* (OCR) untuk ekstraksi data KTP, *Face Recognition* (FR) untuk identifikasi wajah, dan *Object Detection* (OD) untuk analisis lalu lintas atau kerumunan.[58] Pencapaian sertifikasi ini menunjukkan komitmen Telkom dalam mengamankan data biometrik yang sangat sensitif, yang masih langka di Indonesia.[58] Penggunaan FR, misalnya, memungkinkan akses yang lebih mudah, cepat, dan aman ke aplikasi atau layanan finansial tanpa perlu mengingat kata sandi, dengan

verifikasi yang terintegrasi dengan data Dukcapil.[58] Keberhasilan ini tidak hanya meningkatkan keamanan, tetapi juga efisiensi operasional dan pengalaman pengguna.

Penerapan NIST Cybersecurity Framework di Indonesia

Penerapan NIST Cybersecurity Framework (CSF) di Indonesia, meskipun tidak selalu dalam bentuk sertifikasi formal seperti ISO 27001, telah menjadi acuan penting bagi berbagai organisasi untuk mengelola risiko siber.[35] NIST CSF membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan aset informasi dari ancaman siber.[35]

Manfaat implementasi NIST CSF di Indonesia meliputi peningkatan kesiapan menghadapi ancaman siber yang terus berkembang, membantu memenuhi regulasi dan kepatuhan di berbagai sektor, serta membangun budaya keamanan siber di lingkungan kerja.[35] Kerangka kerja ini fleksibel dan

scalable, sehingga dapat diterapkan di berbagai skala bisnis.[35] Meskipun ada kendala seperti keterbatasan SDM dan

expertise, serta biaya implementasi, tips sukses mencakup memulai dengan penilaian keamanan awal, memprioritaskan area berisiko tinggi, melibatkan seluruh level organisasi, dan melakukan pelatihan keamanan siber secara berkala.[35] Ini menunjukkan bahwa organisasi di Indonesia dapat memanfaatkan NIST CSF sebagai panduan strategis untuk terus meningkatkan postur keamanan siber mereka.

Implementasi Tata Kelola Data di Sektor Keuangan dan Pemerintahan

Sektor keuangan di Indonesia menunjukkan komitmen terhadap tata kelola data yang baik, terutama dengan adopsi teknologi seperti Kecerdasan Buatan (AI). Otoritas Jasa Keuangan (OJK) telah menyusun *Artificial Intelligence Governance for Indonesian Banking* sebagai pedoman bagi bank-bank di Indonesia.[59] Pedoman ini memastikan bahwa teknologi AI dikembangkan dan diimplementasikan secara bertanggung jawab, dengan pengelolaan risiko yang terkendali, untuk melindungi nasabah dan menjaga stabilitas sistem perbankan.[59] Ini mencerminkan upaya proaktif untuk

mengintegrasikan tata kelola data ke dalam inovasi teknologi yang lebih luas.

Di sektor pemerintahan, upaya digitalisasi layanan publik juga menunjukkan implementasi tata kelola data. Misalnya, di Kabupaten Serang, penerapan digitalisasi layanan publik melalui aplikasi terintegrasi telah berhasil meningkatkan efisiensi layanan.[60] Meskipun masih ada tantangan dalam infrastruktur, literasi digital masyarakat, dan ego sektoral, studi menunjukkan bahwa digitalisasi layanan publik mampu meningkatkan transparansi, efisiensi, dan aksesibilitas layanan.[60] Ini menggarisbawahi pentingnya dukungan dari berbagai pihak dan ketersediaan infrastruktur teknologi informasi yang memadai sebagai kunci keberhasilan implementasi tata kelola data di tingkat lokal.[61]

Studi kasus ini menunjukkan bahwa dengan komitmen manajemen puncak, investasi yang tepat dalam teknologi dan sumber daya manusia, serta pendekatan yang sistematis terhadap standar dan regulasi, organisasi di Indonesia dapat mencapai keberhasilan signifikan dalam memperkuat keamanan data dan tata kelola data mereka. Keberhasilan ini tidak hanya terbatas pada sektor teknologi, tetapi juga meluas ke sektor keuangan dan pemerintahan, menunjukkan relevansi dan adaptabilitas kerangka kerja global dalam konteks lokal.

9. Kesimpulan dan Rekomendasi

Keamanan data dan tata kelola data merupakan dua pilar fundamental yang saling terkait dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi di era digital yang kompleks. Keamanan data berfokus pada perlindungan teknis terhadap aset data, sementara tata kelola data menyediakan kerangka kebijakan, proses, dan akuntabilitas yang memastikan upaya keamanan data terstruktur, konsisten, dan selaras dengan tujuan bisnis organisasi. Pemahaman akan hierarki perlindungan informasi, di mana keamanan data adalah bagian dari keamanan siber, yang pada gilirannya merupakan bagian dari keamanan informasi yang lebih luas, sangat penting untuk pendekatan yang komprehensif.

Indonesia telah menunjukkan komitmen yang kuat terhadap perlindungan data melalui pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Peraturan Pemerintah (PP) No. 71 Tahun 2019. Regulasi ini memberikan hak-hak yang kuat kepada subjek data dan membebankan kewajiban yang ketat kepada pengendali dan prosesor data, mendorong transformasi paradigma menuju pendekatan proaktif

dalam privasi dan keamanan data. Namun, studi kasus di Indonesia juga menyoroti bahwa kerangka hukum saja tidak cukup; implementasi yang lemah, kurangnya kesadaran, dan investasi yang tidak memadai dapat menyebabkan insiden kebocoran data yang merugikan.

Kerangka kerja internasional seperti ISO/IEC 27001 dan NIST Cybersecurity Framework menawarkan panduan yang sistematis dan adaptif untuk membangun sistem manajemen keamanan informasi yang tangguh. ISO 27001, dengan pendekatan berbasis risikonya dan kontrol Annex A yang diperbarui, memberikan kerangka kerja untuk sertifikasi dan kepatuhan global. Sementara itu, NIST CSF, dengan sifat non-preskriptif dan tingkat implementasinya, memungkinkan organisasi untuk menilai kematangan keamanan siber mereka dan merencanakan perbaikan secara fleksibel. Pendekatan "keamanan berdasarkan desain" dan "shift-left security" juga menjadi prinsip penting dalam pengembangan sistem dan aplikasi yang aman sejak awal.

Berdasarkan analisis komprehensif ini, beberapa rekomendasi kunci dapat diajukan untuk memperkuat standar keamanan penyelenggara dan tata kelola data dalam teknik informatika di Indonesia:

1. **Perkuat Komitmen Manajemen Puncak dan Budaya Keamanan:** Keamanan data dan tata kelola data harus menjadi prioritas strategis yang didukung penuh oleh manajemen puncak. Ini harus diwujudkan dalam alokasi sumber daya yang memadai dan pembangunan budaya keamanan yang kuat di seluruh organisasi, di mana setiap karyawan memahami peran dan tanggung jawab mereka dalam melindungi data. Pelatihan berkelanjutan dan simulasi serangan siber sangat penting untuk meningkatkan kesadaran dan kesiapan.
2. **Integrasikan Keamanan Sepanjang Siklus Hidup Sistem:** Terapkan prinsip *security by design* dan *Secure SDLC* secara menyeluruh. Keamanan tidak boleh menjadi fitur tambahan, melainkan harus diintegrasikan dari tahap perencanaan, desain, implementasi, pengujian, hingga operasional sistem dan aplikasi. Ini akan mengurangi kerentanan dan biaya perbaikan di kemudian hari.
3. **Adopsi dan Adaptasi Kerangka Kerja Internasional:** Organisasi disarankan untuk mengadopsi kerangka kerja keamanan informasi yang diakui secara internasional seperti ISO/IEC 27001 untuk sertifikasi dan kepatuhan yang ketat, serta NIST CSF untuk penilaian kematangan dan peningkatan berkelanjutan. Fleksibilitas NIST CSF memungkinkan adaptasi sesuai dengan profil risiko dan tujuan bisnis yang unik.
4. **Patuhi Regulasi Nasional secara Proaktif:** Pastikan kepatuhan penuh terhadap UU PDP No. 27 Tahun 2022 dan PP No. 71 Tahun 2019. Ini mencakup pemenuhan kewajiban seperti memperoleh persetujuan eksplisit, melakukan DPIA untuk

pemrosesan berisiko tinggi, memiliki rekam jejak audit, dan melaporkan insiden kebocoran data dalam batas waktu yang ditentukan. Penunjukan Petugas Perlindungan Data (DPO) bagi organisasi yang memenuhi kriteria adalah langkah krusial.

5. **Terapkan Teknologi Keamanan Data Esensial:** Investasikan pada teknologi keamanan data yang terbukti efektif, termasuk enkripsi data, autentikasi dan otorisasi yang kuat (termasuk 2FA), solusi DLP, sistem pencadangan dan pemulihan bencana yang andal, *firewall*, IDS/IPS, dan alat manajemen kerentanan. Integrasi teknologi ini dalam pendekatan pertahanan berlapis akan meningkatkan ketahanan sistem.
6. **Lakukan Audit dan Pemantauan Berkelanjutan:** Audit keamanan sistem informasi secara rutin dan independen harus dilakukan untuk mengidentifikasi kelemahan, memvalidasi efektivitas kontrol, dan memastikan kepatuhan. Pemantauan aktivitas sistem secara *real-time* dan analitik perilaku akan memungkinkan deteksi dini anomali dan respons cepat terhadap potensi ancaman.
7. **Manfaatkan Tata Kelola Data sebagai Enabler Keamanan:** Tata kelola data harus dipandang sebagai fondasi yang memungkinkan keamanan data yang efektif. Dengan menetapkan kebijakan data yang jelas, peran dan tanggung jawab yang terdefinisi, serta prosedur untuk manajemen siklus hidup data, organisasi dapat memastikan bahwa data dikelola secara aman, berkualitas tinggi, dan tersedia sesuai kebutuhan.

Dengan menerapkan rekomendasi ini secara komprehensif dan berkelanjutan, organisasi di Indonesia dapat membangun postur keamanan dan tata kelola data yang tangguh, tidak hanya untuk mematuhi regulasi, tetapi juga untuk melindungi aset paling berharga mereka dan menjaga kepercayaan di era digital yang terus berkembang.

Karya yang dikutip

1. KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI UNTUK MENUNJANG IMPLEMENTASI E-LEARNING PADA PERGURUAN TINGGI - Jurnal Undira, diakses Juli 28, 2025, https://jurnal.undira.ac.id/jurnaltera/article/download/128/127/919
2. Keamanan Data & Informasi - Badan Kepegawaian dan Pengembangan SDM Daerah, diakses Juli 28, 2025, https://bkpsdmd.babelprov.go.id/content/keamanan-data-informasi
3. Apa Itu Keamanan Data? | Microsoft Security, diakses Juli 28, 2025, https://www.microsoft.com/id-id/security/business/security-101/what-is-data-security

4. Keamanan Siber Di Teknik Informatika Untuk Menghadapi Ancaman Serangan Digital, diakses Juli 28, 2025, https://iti.ac.id/keamanan-siber-untuk-menghadapi-ancaman-serangan-digital/
5. Transformasi Digital dan Cybersecurity: Pendekatan Holistik dalam Menghadapi Tantangan Keamanan Siber - Swiss German University, diakses Juli 28, 2025, https://sgu.ac.id/id/transformasi-digital-dan-cybersecurity-pendekatan-holistik-dalam-menghadapi-tantangan-keamanan-siber/
6. Tantangan dan Solusi Terkait dengan Keamanan Data dan Privasi Pengguna, diakses Juli 28, 2025, https://online.ciputra.ac.id/keamanan-data/
7. Transformasi Digital dan Cybersecurity: Pendekatan Holistik dalam Menghadapi Tantangan Keamanan Siber - Tekno Kompas, diakses Juli 28, 2025, https://tekno.kompas.com/read/2024/07/25/17243797/transformasi-digital-dan-cybersecurity-pendekatan-holistik-dalam-menghadapi
8. Teknik-Teknik Keamanan Data yang Efektif - Widya Security, diakses Juli 28, 2025, https://widyasecurity.com/2023/12/18/teknik-teknik-keamanan-data-yang-efektif/
9. Apa itu Arsitektur Data ? Arti, Karakteristik dan Komponen, diakses Juli 28, 2025, https://www.fanruan.com/id/glossary/analisis-statistik/arsitektur-data
10. Keamanan Sistem Informasi Manajemen • Fakultas Ekonomi Terbaik di Sumut, diakses Juli 28, 2025, https://ekonomi.uma.ac.id/2024/01/16/keamanan-sistem-informasi-manajemen/
11. Apa itu keamanan informasi (InfoSec)? | Microsoft Security, diakses Juli 28, 2025, https://www.microsoft.com/id-id/security/business/security-101/what-is-information-security-infosec
12. Apa yang dimaksud dengan tata kelola data? | IBM, diakses Juli 28, 2025, https://www.ibm.com/id-id/topics/data-governance
13. Apa itu Tata Kelola Data? - Solix Technologies, diakses Juli 28, 2025, https://www.solix.com/id/kb/data-governance/
14. Apa itu Tata Kelola Data? - Microsoft Azure, diakses Juli 28, 2025, https://azure.microsoft.com/id-id/resources/cloud-computing-dictionary/what-is-a-data-governance
15. Mengatasi Tantangan Keamanan Data dengan Software Bisnis yang Tepat | ALPHASOFT, diakses Juli 28, 2025, https://alphasoft.id/blog/bisnis-5/mengatasi-tantangan-keamanan-data-dengan-software-bisnis-yang-tepat-117
16. Keamanan Digital: Definisi, Cara Melindungi, dan Manfaat - Vida, diakses Juli 28, 2025, https://vida.id/id/blog/keamanan-digital
17. 10 Sistem Keamanan Jaringan Komputer yang Banyak Digunakan - Eduparx Blog, diakses Juli 28, 2025, https://eduparx.id/blog/insight/10-sistem-keamanan-jaringan-komputer/
18. What is ISO/IEC 27001, The Information Security Standard, diakses Juli 28, 2025, https://www.isms.online/iso-27001/
19. KEAMANAN JARINGAN INFORMASI MENGGUNAKAN METODE IPS - Fakultas Teknik Terbaik di Medan Sumatera Utara, diakses Juli 28, 2025, https://teknik.uma.ac.id/2024/01/18/keamanan-jaringan-informasi-menggunakan-metode-ips/

20. ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY | Jurnal Inovatif : Inovasi Teknologi Informasi dan Informatika, diakses Juli 28, 2025, https://ejournal.uika-bogor.ac.id/index.php/INOVA-TIF/article/view/4127
21. Secure SDLC Based on ISO 27002:2022 | Cyber Academy Indonesia, diakses Juli 28, 2025, https://www.cyberacademy.id/corporate-training/secure-sdlc-based-on-iso-27002-2022/batch-1
22. Bagaimana Mengintegrasikan Keamanan dalam Setiap Tahap Siklus Hidup Pengembangan Perangkat Lunak, dari Perencanaan hingga Operasi - Btech, diakses Juli 28, 2025, https://btech.id/id/news/how-to-integrate-security-into-each-phase-of-the-software-development-lifecycle-from-planning-to-operating/
23. Security Software Development Life Cycle | by Radinal Dwiki Novendra, S.T., M.T. | Medium, diakses Juli 28, 2025, https://medium.com/@radinaldn/security-software-development-life-cycle-2e9278417e70
24. Pendekatan untuk Mengintegrasikan Alat dan Teknologi Keamanan ke dalam Alur Kerja Pengembangan dan Operasi yang Ada - Btech, diakses Juli 28, 2025, https://btech.id/id/news/approaches-for-integrating-security-tools-and-technologies-into-existing-development-and-operations-workflows/
25. Apa itu Pengelolaan Kerentanan? | Microsoft Security, diakses Juli 28, 2025, https://www.microsoft.com/id-id/security/business/security-101/what-is-vulnerability-management
26. 10 Praktik Terbaik Keamanan Basis Data yang Harus Anda Ketahui - AppMaster, diakses Juli 28, 2025, https://appmaster.io/id/blog/praktik-keamanan-basis-data
27. Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 ... - OJS Unud, diakses Juli 28, 2025, https://ojs.unud.ac.id/index.php/merpati/article/download/45473/27587
28. Audit Keamanan Sistem Informasi Oke | PDF - Scribd, diakses Juli 28, 2025, https://id.scribd.com/presentation/697878459/Audit-Keamanan-Sistem-Informasi-Oke
29. Audit Keamanan Informasi: Langkah Penting Menjamin Integritas Sistem - UTI-TTIS, diakses Juli 28, 2025, https://csirt.teknokrat.ac.id/audit-keamanan-informasi-langkah-penting-menjamin-integritas-sistem/
30. TAHAPAN TAHAPAN AUDIT SISTEM INFORMASI - OSF, diakses Juli 28, 2025, https://osf.io/3erdb/download
31. 1 AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA PT. BPR JATIM 1)Fine Ermana 2)Haryanto Tanuwijaya 3)Ignatiu - Neliti, diakses Juli 28, 2025, https://media.neliti.com/media/publications/253000-audit-keamanan-sistem-informasi-berdasar-2ffbc758.pdf
32. arsitektur data spbe kabupaten tanah laut, diakses Juli 28, 2025, https://portal.tanahlautkab.go.id/asset/files/arsitektur-data-spbe-kabupaten-tana

h-laut_1723435472.pdf
33. Arsitektur Keamanan SPBE - Inixindo Jogja, diakses Juli 28, 2025, https://inixindojogja.co.id/it-consultant/arsitektur-keamanan-spbe/
34. 13 Kerangka Kepatuhan yang Wajib Diketahui oleh Organisasi Berbasis Cloud, diakses Juli 28, 2025, https://integrasolusi.com/keamanan/pentest/13-kerangka-kepatuhan-yang-wajib-diketahui-oleh-organisasi-berbasis-cloud/
35. NIST Cybersecurity Framework: Mengenal Pilar Keamanan Siber Modern - Logique, diakses Juli 28, 2025, https://www.logique.co.id/blog/2025/05/22/nist-cybersecurity-framework/
36. The NIST Cybersecurity Framework (CSF) 2.0 - NIST Technical ..., diakses Juli 28, 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
37. What is the NIST Cybersecurity Framework? - IBM, diakses Juli 28, 2025, https://www.ibm.com/think/topics/nist
38. Hukum Perlindungan Data: Regulasi di Indonesia dan Dunia - MyData, diakses Juli 28, 2025, https://mydata2018.org/berita-terkini/hukum-perlindungan-data-regulasi-di-indonesia-dan-dunia/
39. UU No. 27 Tahun 2022 - Peraturan BPK, diakses Juli 28, 2025, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022
40. PDP Law (Indonesia) - Compliance - Google Cloud, diakses Juli 28, 2025, https://cloud.google.com/security/compliance/indonesia-pdpl
41. UU Perlindungan Data Pribadi - Bitlion, diakses Juli 28, 2025, https://www.bitlion.io/framework/uu-perlindungan-data-pribadi
42. PERATURAN PEMERINTAH REPUBLIK INDONESIA NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK - Regulasip, diakses Juli 28, 2025, https://www.regulasip.id/book/16516/read
43. Peraturan Pemerintah Nomor 71 Tahun 2019 - JDIH Kominfo - Komdigi, diakses Juli 28, 2025, https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019
44. Three New Dimensions to People, Process, Technology Improvement Model, diakses Juli 28, 2025, https://www.researchgate.net/publication/283226690_Three_New_Dimensions_to_People_Process_Technology_Improvement_Model
45. People, Process, Technology: Optimizing Risk Management Initiatives, diakses Juli 28, 2025, https://www.corporatecomplianceinsights.com/people-process-technology-optimizing-risk-management-initiatives/
46. How to Maintain ISO 27001 Compliance: 17 Pro Strategies - SecureSlate - Medium, diakses Juli 28, 2025, https://secureslate.medium.com/how-to-maintain-iso-27001-compliance-17-pro-strategies-eb1165c7dc2e
47. Cara Efektif Membangun Budaya Security Awareness di Kantor - SiberMate, diakses Juli 28, 2025,

https://sibermate.com/hrmi/cara-efektif-membangun-budaya-security-awareness-di-kantor
48. Data Management Body of Knowledge (DAMA-DMBOK, diakses Juli 28, 2025, https://dama.org/learning-resources/dama-data-management-body-of-knowledge-dmbok/
49. Data Governance Frameworks - The DAMA DMBoK - Sogeti Labs, diakses Juli 28, 2025, https://labs.sogeti.com/data-governance-frameworks-the-dama-dmbok/
50. DAMA-DMBOK Framework: What It Is and How To Adopt It? - CastorDoc, diakses Juli 28, 2025, https://www.castordoc.com/data-strategy/dama-dmbok-framework-what-it-is-and-how-to-adopt-it
51. Scaling data sharing through data management best practices - Opendatasoft, diakses Juli 28, 2025, https://www.opendatasoft.com/en/blog/scaling-data-sharing-through-data-management-best-practices/
52. Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN) - Kampus Akademik, diakses Juli 28, 2025, https://ejurnal.kampusakademik.co.id/index.php/jiem/article/download/5266/4577/20412
53. Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia, diakses Juli 28, 2025, https://ojs.daarulhuda.or.id/index.php/MHI/article/download/1465/1601
54. Memahami NIST Cybersecurity Framework untuk Keamanan Siber - Widya Security, diakses Juli 28, 2025, https://widyasecurity.com/2025/07/21/memahami-nist-cybersecurity-framework-untuk-keamanan-siber/
55. Mengatasi Keamanan Data dan Privasi dalam Penerapan TIK di Pemerintahan, diakses Juli 28, 2025, https://seputarbirokrasi.com/mengatasi-keamanan-data-dan-privasi-dalam-penerapan-tik-di-pemerintahan/
56. 5 Kasus Cybercrime di Indonesia yang Menyerang Server - AMT IT Solutions, diakses Juli 28, 2025, https://amt-it.com/blog/kasus-cybercrime-di-indonesia/
57. Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala, diakses Juli 28, 2025, https://journal.fkom.uniku.ac.id/ilkom/article/download/205/49/764
58. Telkom Raih ISO 27001:2013 Seri Biometrics yang Masih Langka di Indonesia - Medium, diakses Juli 28, 2025, https://medium.com/leaptelkom/telkom-raih-iso-27001-2013-seri-biometrics-yang-masih-langka-di-indonesia-c0a5e5f4cff6
59. Tata Kelola Kecerdasan Artifisial Perbankan Indonesia - OJK, diakses Juli 28, 2025, https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata%20Kelola%20Kecerdasan%20Artifisial%20Perbankan%20Indonesia.pdf
60. Digital Governance: Studi Kasus Digitalisasi Pelayanan Publik Terpadu di Kabupaten Serang - Jurnal Sosial Teknologi, diakses Juli 28, 2025, https://sostech.greenvest.co.id/index.php/sostech/article/download/31861/1447/73

55
61. Penerapan E-Government pada Sektor Pelayanan Publik (Studi Kasus Aplikasi OpenSID di Desa Tondowolio Kecamatan Tanggetada, diakses Juli 28, 2025, https://ejurnal.teraskampus.id/index.php/bangsa/article/download/256/110/905