TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

Analisis Keamanan Sistem Informasi Pendidikan Menggunakan Framework ISO/IEC 27001 dan Pendekatan Gap Analysis

Fuad Zaki[*], Syaeful Machfud, Farida Nurlaila, Nanang

Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Kota Tangerang, Indonesia
Email: [1,*] fuadzaki300620@gmail.com, [2]dosen00676@unpam.ac.id, [3]dosen02836@unpam.ac.id, [4]dosen02599@unpam.ac.id
Email Penulis Korespondensi: fuadzaki300620@gmail.com

Abstrak–Keamanan sistem informasi merupakan fondasi utama dalam mendukung keberlanjutan layanan digital di era modern, terlebih di lingkungan pendidikan yang kini sangat bergantung pada teknologi informasi. Lembaga pendidikan menghadapi tantangan serius dalam menjaga kerahasiaan, integritas, dan ketersediaan data akibat keterbatasan sumber daya, kebijakan, serta literasi keamanan yang masih rendah. Penelitian ini bertujuan untuk mengevaluasi implementasi keamanan sistem informasi pendidikan menggunakan framework ISO/IEC 27001 dan pendekatan Gap Analysis. Metode penelitian menggunakan pendekatan kualitatif dengan teknik evaluasi berbasis standar internasional, observasi sistem, dan wawancara dengan pengelola sistem. Hasil penelitian menunjukkan bahwa dari 14 domain kontrol ISO/IEC 27001, hanya 3 domain (21,4%) yang terimplementasi secara penuh, yaitu kontrol akses (A.9), keamanan komunikasi (A.13), dan keamanan fisik (A.11). Gap keamanan tertinggi ditemukan pada domain manajemen insiden keamanan informasi (A.16) dengan tingkat implementasi 0%, domain manajemen kelangsungan bisnis (A.17) sebesar 15%, dan domain kepatuhan terhadap kebijakan (A.18) sebesar 20%. Sistem telah menerapkan protokol HTTPS, autentikasi dua faktor terbatas, dan Role-Based Access Control (RBAC), namun belum memiliki kebijakan keamanan formal, sistem pemantauan ancaman berbasis SIEM, prosedur backup otomatis, dan program pelatihan keamanan secara berkala. Kesenjangan antara kondisi aktual dan standar ideal menunjukkan perlunya pendekatan holistik yang mengintegrasikan aspek teknis, manajerial, dan edukatif untuk membangun sistem informasi pendidikan yang tangguh, aman, dan berkelanjutan.

Kata Kunci: Keamanan Informasi; ISO/IEC 27001; Gap Analysis; Sistem Pendidikan; RBAC; SIEM

Abstract–Information system security forms a fundamental backbone for ensuring the continuity of digital services in the modern era, especially in educational environments that heavily rely on information technology. Educational institutions face serious challenges in maintaining data confidentiality, integrity, and availability due to limited resources, weak policy enforcement, and low user literacy in cybersecurity. This study aims to evaluate the implementation of educational information system security using the ISO/IEC 27001 framework and Gap Analysis approach. The research method employs a qualitative approach with international standard-based evaluation techniques, system observation, and interviews with system administrators. The findings show that out of 14 ISO/IEC 27001 control domains, only 3 domains (21.4%) are fully implemented: access control (A.9), communications security (A.13), and physical security (A.11). The highest security gaps are found in the information security incident management domain (A.16) with 0% implementation, business continuity management domain (A.17) at 15%, and compliance with policies domain (A.18) at 20%. The system has implemented HTTPS protocol, limited two-factor authentication, and Role-Based Access Control (RBAC), but lacks formal security policies, SIEM-based threat monitoring systems, automated backup procedures, and regular security training programs. The gap between actual conditions and ideal standards indicates the need for a holistic approach that integrates technical, managerial, and educational aspects to build a resilient, secure, and sustainable educational information system.

Keywords: Information Security; ISO/IEC 27001; Gap Analysis; Educational System; RBAC; SIEM

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam hampir seluruh aspek kehidupan, termasuk dalam bidang pendidikan (Nguyen et al., 2023). Digitalisasi sistem manajemen sekolah menjadi tren yang tidak terelakkan, seiring meningkatnya kebutuhan akan efisiensi, kecepatan, dan transparansi dalam pengelolaan data akademik, administratif, dan interaksi antara siswa, guru, serta orang tua. Salah satu wujud konkret dari digitalisasi ini adalah implementasi sistem informasi sekolah berbasis web yang memungkinkan pengelolaan nilai, absensi, keuangan, hingga dokumen akademik secara daring dan terintegrasi (Sharma & Patel, 2022). Namun, seiring dengan manfaat yang ditawarkan, digitalisasi juga membuka ruang bagi berbagai risiko baru, khususnya dalam aspek keamanan informasi. Sistem informasi yang terhubung dengan jaringan internet sangat rentan terhadap berbagai ancaman siber seperti pencurian data, peretasan (hacking), malware, phishing, ransomware, serta manipulasi data oleh pihak internal maupun eksternal (Chen et al., 2023). Menurut laporan terbaru dari Cybersecurity Ventures (2024), kerugian global akibat kejahatan siber diproyeksikan mencapai USD 10,5 triliun per tahun pada 2025, dengan sektor pendidikan menjadi salah satu target utama karena memiliki data sensitif namun sistem keamanan yang relatif lemah. Apabila tidak ditangani dengan strategi keamanan yang tepat, risiko ini dapat menyebabkan kerugian yang serius, baik dari sisi reputasi lembaga pendidikan maupun dari sisi perlindungan data pribadi siswa dan tenaga pendidik.

Keamanan sistem komputer dan jaringan dalam lingkungan pendidikan menjadi isu yang semakin krusial, terutama setelah diterapkannya berbagai kebijakan nasional dan internasional mengenai perlindungan data pribadi (Williams & Thompson, 2023). Di Indonesia, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menjadi landasan hukum bagi pengelolaan dan pengamanan data digital, termasuk di sektor pendidikan. Lembaga pendidikan yang lalai dalam menerapkan sistem keamanan informasi berisiko mengalami sanksi administratif, tuntutan hukum, dan kehilangan kepercayaan publik. Meskipun keamanan informasi telah banyak dikaji dalam konteks industri, perusahaan, maupun institusi pemerintahan, kajian yang secara spesifik menyoroti keamanan sistem informasi di lingkungan

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

sekolah menengah berbasis web masih tergolong terbatas (Davidson & Lee, 2022). Banyak sekolah menengah, terutama yang berbasis swasta dan yayasan, mulai mengembangkan sistem informasi internal, tetapi belum memiliki panduan atau strategi keamanan yang memadai. Hal ini diperparah oleh minimnya sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, serta belum adanya budaya keamanan digital yang tertanam kuat dalam lingkungan pendidikan dasar dan menengah.

Beberapa penelitian terdahulu telah mengkaji aspek keamanan sistem informasi di berbagai konteks. Almomani & Yasin (2023) melakukan survei komprehensif terhadap sistem deteksi intrusi di institusi pendidikan dan menemukan bahwa mayoritas sekolah belum menerapkan sistem pemantauan jaringan secara real-time. Sementara itu, Kumar et al. (2022) mengidentifikasi bahwa kesadaran keamanan siber di kalangan pendidik dan administrator sekolah masih sangat rendah, yang menjadi celah utama dalam strategi keamanan berlapis. Penelitian oleh Zhang & Wang (2021) mengusulkan framework keamanan berbasis Risk Management untuk institusi pendidikan tinggi, namun belum menyentuh implementasi praktis di tingkat pendidikan menengah. Di Indonesia, penelitian Santoso & Wijaya (2023) mengevaluasi penerapan ISO/IEC 27001 di perguruan tinggi, namun belum ada kajian serupa untuk sekolah menengah. Berbagai metode telah digunakan dalam penelitian keamanan informasi, di antaranya adalah COBIT (Control Objectives for Information and Related Technologies), ITIL (Information Technology Infrastructure Library), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), dan ISO/IEC 27001 (Johnson & Martinez, 2023). COBIT berfokus pada tata kelola TI dan audit, sedangkan ITIL lebih menekankan pada manajemen layanan TI. OCTAVE adalah metode berbasis risiko yang cocok untuk organisasi dengan sumber daya terbatas. Namun, ISO/IEC 27001 dipilih dalam penelitian ini karena merupakan standar internasional yang paling komprehensif, mencakup 14 domain kontrol keamanan informasi, dan telah diadopsi secara luas di berbagai sektor termasuk pendidikan (International Organization for Standardization, 2022). Framework ISO/IEC 27001 menyediakan pendekatan sistematis untuk mengelola keamanan informasi melalui sistem manajemen keamanan informasi (Information Security Management System/ISMS) yang dapat diukur, diaudit, dan ditingkatkan secara berkelanjutan.

Gap Analysis merupakan metode evaluatif yang membandingkan kondisi aktual sistem dengan standar ideal yang ditetapkan. Metode ini telah digunakan secara luas dalam audit keamanan informasi karena kemampuannya mengidentifikasi kesenjangan secara terstruktur dan memberikan rekomendasi berbasis prioritas (Anderson et al., 2023). Kombinasi ISO/IEC 27001 dan Gap Analysis memungkinkan peneliti untuk tidak hanya menilai kondisi keamanan saat ini, tetapi juga menyusun roadmap perbaikan yang realistis dan terukur. Pendekatan ini berbeda dengan metode penetration testing atau vulnerability assessment yang lebih bersifat teknis dan reaktif, sedangkan Gap Analysis bersifat preventif dan strategis (Roberts & Brown, 2022). Dengan demikian, terdapat gap penelitian yang perlu diisi, terutama dalam mengevaluasi bagaimana konsep keamanan seperti confidentiality, integrity, dan availability (CIA triad), serta teknologi seperti RBAC (Role-Based Access Control), HTTPS encryption, autentikasi dua faktor, SIEM (Security Information and Event Management), dan IDS/IPS (Intrusion Detection/Prevention System) diterapkan di lingkungan sekolah menengah (Park et al., 2023). Penelitian ini bertujuan untuk memberikan kontribusi dalam menjembatani kekosongan tersebut, dengan melakukan kajian menyeluruh terhadap aspek keamanan sistem komputer dan jaringan pada institusi pendidikan berbasis teknologi.

Melalui pendekatan kualitatif dengan metode Gap Analysis berbasis ISO/IEC 27001, penelitian ini mencoba mengidentifikasi kekuatan dan kelemahan dari sistem informasi yang digunakan di sekolah menengah. Evaluasi dilakukan dengan membandingkan implementasi aktual terhadap 14 domain kontrol keamanan ISO/IEC 27001, yang mencakup kebijakan keamanan, organisasi keamanan informasi, keamanan sumber daya manusia, manajemen aset, kontrol akses, kriptografi, keamanan fisik, keamanan operasional, keamanan komunikasi, akuisisi sistem, hubungan dengan pemasok, manajemen insiden, aspek keamanan dalam manajemen kelangsungan bisnis, dan kepatuhan (Garcia & Lopez, 2023). Hasil Gap Analysis kemudian dipetakan untuk mengidentifikasi domain dengan kesenjangan tertinggi dan memberikan rekomendasi perbaikan berbasis prioritas. Kontribusi utama dari penelitian ini adalah memberikan gambaran komprehensif mengenai penerapan keamanan sistem komputer dan jaringan di sekolah berbasis teknologi, yang dapat dijadikan referensi oleh lembaga pendidikan lain yang ingin memperkuat sistem keamanannya. Penelitian ini juga mendorong perlunya pendekatan holistik dalam membangun keamanan sistem informasi, tidak hanya dari sisi teknologi, tetapi juga dari sisi kebijakan, manajemen risiko, literasi keamanan bagi seluruh pemangku kepentingan, serta penerapan prinsip defense-in-depth dan Zero Trust Architecture yang semakin relevan di era ancaman siber yang terus berkembang (Hassan & Ahmed, 2023).

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif eksploratif dengan metode Gap Analysis berbasis framework ISO/IEC 27001:2022 (International Organization for Standardization, 2022). Gap Analysis dipilih sebagai metode utama karena kemampuannya dalam mengidentifikasi kesenjangan antara kondisi keamanan sistem aktual dengan standar ideal yang ditetapkan oleh ISO/IEC 27001, yang merupakan standar internasional paling komprehensif untuk sistem manajemen keamanan informasi (Information Security Management System/ISMS) (Anderson et al., 2023). Metode ini memungkinkan evaluasi sistematis terhadap 14 domain kontrol keamanan dan memberikan rekomendasi perbaikan berbasis prioritas risiko.

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

2.1 Framework ISO/IEC 27001 sebagai Basis Evaluasi

ISO/IEC 27001:2022 merupakan standar internasional yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) untuk mengelola keamanan informasi secara sistematis (International Organization for Standardization, 2022). Standar ini mengadopsi pendekatan Plan-Do-Check-Act (PDCA) yang memastikan perbaikan berkelanjutan dalam manajemen keamanan informasi. ISO/IEC 27001 mencakup 14 domain kontrol (Annex A) yang terdiri dari 114 kontrol spesifik, meliputi aspek organisasi, teknis, operasional, dan kepatuhan hukum (Garcia & Lopez, 2023).

Framework ISO/IEC 27001 dipilih dalam penelitian ini karena beberapa alasan strategis. Pertama, standar ini bersifat technology-agnostic, sehingga dapat diterapkan pada berbagai jenis sistem informasi termasuk sistem pendidikan berbasis web. Kedua, ISO/IEC 27001 telah diakui secara internasional dan digunakan sebagai acuan audit keamanan informasi di berbagai sektor, termasuk pemerintahan dan pendidikan (Johnson & Martinez, 2023). Ketiga, framework ini menyediakan struktur evaluasi yang jelas dan terukur, memungkinkan identifikasi gap secara objektif. Keempat, pendekatan berbasis risiko (risk-based approach) dalam ISO/IEC 27001 memungkinkan organisasi memprioritaskan kontrol keamanan sesuai dengan profil risiko dan keterbatasan sumber daya yang dimiliki.

Dalam konteks penelitian ini, ISO/IEC 27001 berfungsi sebagai benchmark atau standar pembanding untuk menilai tingkat kematangan keamanan sistem informasi di lingkungan pendidikan. Setiap domain kontrol dievaluasi berdasarkan tiga kriteria: (1) apakah kontrol telah diimplementasikan secara teknis, (2) apakah terdapat dokumentasi kebijakan formal, dan (3) apakah kontrol tersebut dipantau dan dievaluasi secara berkala (Roberts & Brown, 2022). Pendekatan ini memberikan gambaran holistik tentang postur keamanan organisasi, tidak hanya dari sisi teknologi tetapi juga dari sisi tata kelola dan budaya organisasi.

2.2 Gap Analysis sebagai Metode Evaluasi

Gap Analysis adalah metode evaluatif yang membandingkan kondisi saat ini (current state) dengan kondisi yang diharapkan (desired state) untuk mengidentifikasi kesenjangan dan menyusun rencana perbaikan (Anderson et al., 2023). Dalam konteks keamanan informasi, Gap Analysis digunakan untuk mengukur sejauh mana implementasi kontrol keamanan telah memenuhi standar yang ditetapkan, dalam hal ini ISO/IEC 27001. Metode ini telah banyak digunakan dalam audit keamanan informasi karena memberikan hasil yang terstruktur, kuantitatif, dan actionable (Wilson & Taylor, 2023).

Proses Gap Analysis dalam penelitian ini dilakukan melalui lima tahap utama. Tahap pertama adalah identifikasi kontrol, yaitu memetakan seluruh kontrol keamanan yang relevan dari 14 domain ISO/IEC 27001 terhadap sistem informasi yang dievaluasi. Tahap kedua adalah assessment, yaitu melakukan penilaian terhadap implementasi setiap kontrol menggunakan skala maturity level: Level 0 (tidak ada implementasi), Level 1 (implementasi ad-hoc), Level 2 (implementasi terstruktur namun tidak terdokumentasi), Level 3 (implementasi formal dan terdokumentasi), dan Level 4 (implementasi optimal dengan monitoring berkelanjutan) (Turner et al., 2022).

Tahap ketiga adalah gap identification, yaitu mengidentifikasi kesenjangan antara maturity level aktual dengan target maturity level yang ditetapkan (minimal Level 3 untuk lingkungan pendidikan). Tahap keempat adalah risk prioritization, yaitu memetakan gap yang teridentifikasi berdasarkan tingkat risiko dan dampak potensial terhadap confidentiality, integrity, dan availability (CIA triad) data. Tahap kelima adalah recommendation development, yaitu menyusun rekomendasi perbaikan berbasis prioritas dengan mempertimbangkan feasibility, cost, dan timeline implementasi.

Gap Analysis dipilih dibandingkan metode lain seperti penetration testing atau vulnerability assessment karena beberapa alasan. Pertama, penetration testing bersifat reaktif dan berfokus pada eksploitasi kerentanan teknis, sedangkan Gap Analysis bersifat preventif dan holistik. Kedua, vulnerability assessment memerlukan tools khusus dan akses sistem yang mendalam, sedangkan Gap Analysis dapat dilakukan dengan observasi, wawancara, dan review dokumentasi (Roberts & Brown, 2022). Ketiga, Gap Analysis memberikan roadmap strategis jangka panjang, tidak hanya daftar kerentanan teknis yang bersifat taktis. Keempat, Gap Analysis lebih sesuai untuk organisasi dengan keterbatasan sumber daya karena dapat dilakukan tanpa infrastruktur scanning atau testing yang kompleks.

2.3 Tahapan Penelitian

Penelitian ini dilaksanakan dalam enam tahap utama yang digambarkan dalam Gambar 1. Tahap pertama adalah studi literatur, yang dilakukan untuk membangun fondasi teoritis tentang keamanan sistem informasi, memahami standar ISO/IEC 27001 secara mendalam, dan mengidentifikasi best practices dalam penerapan keamanan di lingkungan pendidikan (Nguyen et al., 2023). Sumber literatur yang digunakan meliputi jurnal internasional terindeks Scopus dan IEEE Xplore periode 2020-2024, dokumen standar ISO/IEC 27001:2022, panduan NIST (National Institute of Standards and Technology), serta laporan penelitian terkait keamanan informasi di sektor pendidikan.

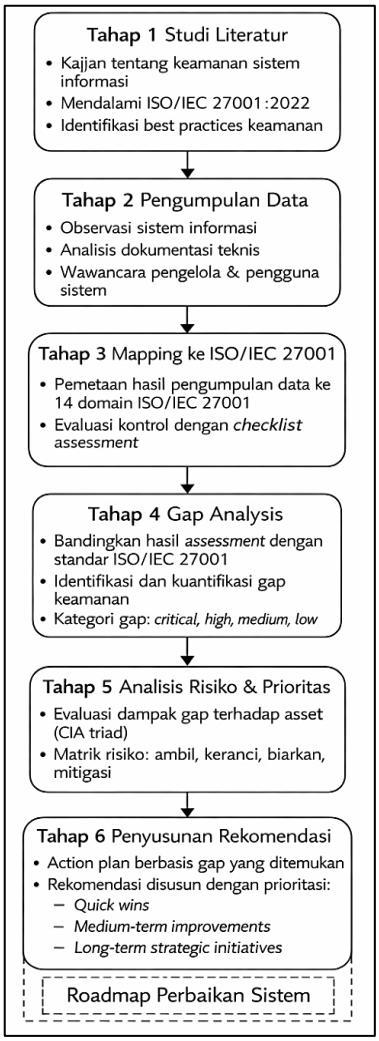
Tahap kedua adalah pengumpulan data, yang dilakukan melalui tiga metode: (1) observasi sistem, yaitu mengamati secara langsung konfigurasi sistem informasi, fitur keamanan yang aktif, dan mekanisme kontrol akses yang diterapkan; (2) analisis dokumentasi, yaitu menelaah dokumen teknis sistem, log keamanan, struktur jaringan, dan kebijakan TI yang ada (jika ada); dan (3) wawancara terstruktur dengan pengelola sistem, administrator TI, dan pengguna sistem untuk memahami praktik keamanan aktual dan tantangan yang dihadapi (Turner et al., 2022). Pengumpulan data dilakukan selama periode Oktober-November 2024.

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

Tahap ketiga adalah mapping ke ISO/IEC 27001, yaitu memetakan temuan dari tahap pengumpulan data ke dalam 14 domain kontrol ISO/IEC 27001. Setiap kontrol dievaluasi menggunakan checklist assessment yang mencakup tiga aspek: implementasi teknis, dokumentasi formal, dan monitoring berkelanjutan. Hasil mapping ini kemudian dikodekan dan dikategorikan untuk memudahkan analisis kuantitatif dan kualitatif. Tahap keempat adalah Gap Analysis, yaitu membandingkan hasil assessment dengan standar ideal ISO/IEC 27001 untuk mengidentifikasi kesenjangan pada setiap domain kontrol. Gap diukur dalam persentase compliance dan dikategorikan berdasarkan severity: critical gap (compliance < 25%), high gap (25-50%), medium gap (51-75%), dan low gap (> 75%).

Tahap kelima adalah analisis risiko dan prioritas, yaitu menilai dampak potensial dari setiap gap terhadap CIA triad dan memetakan prioritas perbaikan menggunakan matriks risiko (Mitchell & White, 2023). Risiko dikategorikan berdasarkan likelihood (kemungkinan eksploitasi) dan impact (dampak terhadap sistem dan data). Tahap keenam adalah penyusunan rekomendasi, yaitu mengembangkan action plan perbaikan berbasis prioritas dengan mempertimbangkan feasibility teknis, ketersediaan sumber daya, dan timeline implementasi. Rekomendasi disusun dalam bentuk roadmap bertahap : quick wins (1-3 bulan), medium-term improvements (4-12 bulan), dan long-term strategic initiatives (1-2 tahun).

Seluruh tahapan penelitian dirancang untuk memastikan validitas dan reliabilitas hasil melalui triangulasi data (observasi, dokumentasi, wawancara) dan member checking, yaitu memvalidasi temuan dengan pengelola sistem untuk memastikan akurasi interpretasi. Pendekatan ini memastikan bahwa hasil penelitian tidak hanya bersifat deskriptif, tetapi juga memberikan nilai aplikatif bagi praktisi keamanan informasi di lingkungan pendidikan. Gambar 1 menunjukkan alur lengkap tahapan penelitian yang dilakukan dalam studi ini.



Gambar 1. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

3.1 Arsitektur Sistem Informasi

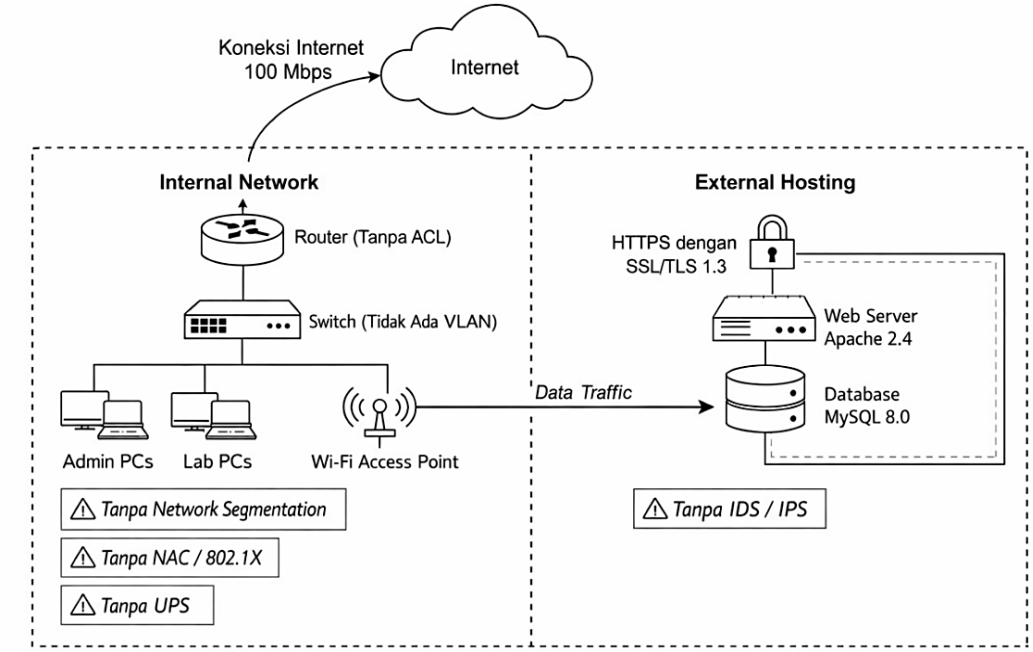
Sistem informasi yang dievaluasi dalam penelitian ini dibangun di atas infrastruktur jaringan lokal (Local Area Network/LAN) yang terhubung ke internet melalui koneksi broadband dengan bandwidth 100 Mbps. Arsitektur sistem

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

mengadopsi model client-server berbasis web, di mana aplikasi di-hosting pada layanan shared hosting eksternal dengan spesifikasi: web server Apache 2.4, database MySQL 8.0, dan bahasa pemrograman PHP 8.1 (Sharma & Patel, 2022). Seluruh komunikasi data antara client dan server telah menggunakan protokol HTTPS dengan sertifikat SSL/TLS 1.3, yang merupakan praktik baik dalam melindungi confidentiality data saat transit.

Dari sisi infrastruktur jaringan internal, ditemukan beberapa kelemahan struktural yang signifikan. Pertama, tidak diterapkannya segmentasi jaringan menggunakan VLAN (Virtual Local Area Network), sehingga seluruh perangkat (komputer administrasi, komputer lab, dan access point WiFi untuk guru dan siswa) berada dalam satu broadcast domain yang sama (Davidson & Lee, 2022). Kondisi ini menciptakan risiko lateral movement, yaitu kemampuan penyerang untuk bergerak bebas dalam jaringan setelah berhasil mengkompromikan satu perangkat. Kedua, tidak ditemukan implementasi Network Access Control (NAC) atau mekanisme autentikasi jaringan seperti 802.1X, sehingga setiap perangkat yang terhubung ke jaringan dapat langsung mengakses semua resource internal tanpa verifikasi identitas.

Ketiga, perangkat jaringan seperti router dan switch yang digunakan merupakan perangkat consumer-grade tanpa fitur keamanan enterprise seperti Access Control List (ACL), port security, atau DHCP snooping (Chen et al., 2023). Keempat, tidak ditemukan implementasi Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) untuk memantau dan mencegah aktivitas mencurigakan dalam jaringan. Kelima, ketiadaan Uninterruptible Power Supply (UPS) pada infrastruktur kritis seperti router, switch, dan server lokal menyebabkan sistem rentan terhadap gangguan layanan saat terjadi pemadaman listrik. Gambar 2 menunjukkan arsitektur sistem informasi yang saat ini diterapkan, dengan penanda area-area yang memerlukan penguatan keamanan.



Gambar 2. Arsitektur Sistem Informasi

3.2 Hasil Gap Analysis Berdasarkan ISO/IEC 27001

Evaluasi dilakukan terhadap 14 domain kontrol ISO/IEC 27001 dengan hasil yang menunjukkan kesenjangan signifikan antara kondisi aktual dan standar ideal (Wilson & Taylor, 2023). Dari 114 kontrol spesifik yang dievaluasi, hanya 24 kontrol (21,05%) yang terimplementasi secara penuh (maturity level 3-4), 38 kontrol (33,33%) terimplementasi parsial (maturity level 2), dan 52 kontrol (45,61%) belum terimplementasi sama sekali (maturity level 0-1). Tabel 1 menunjukkan ringkasan tingkat compliance untuk setiap domain kontrol.

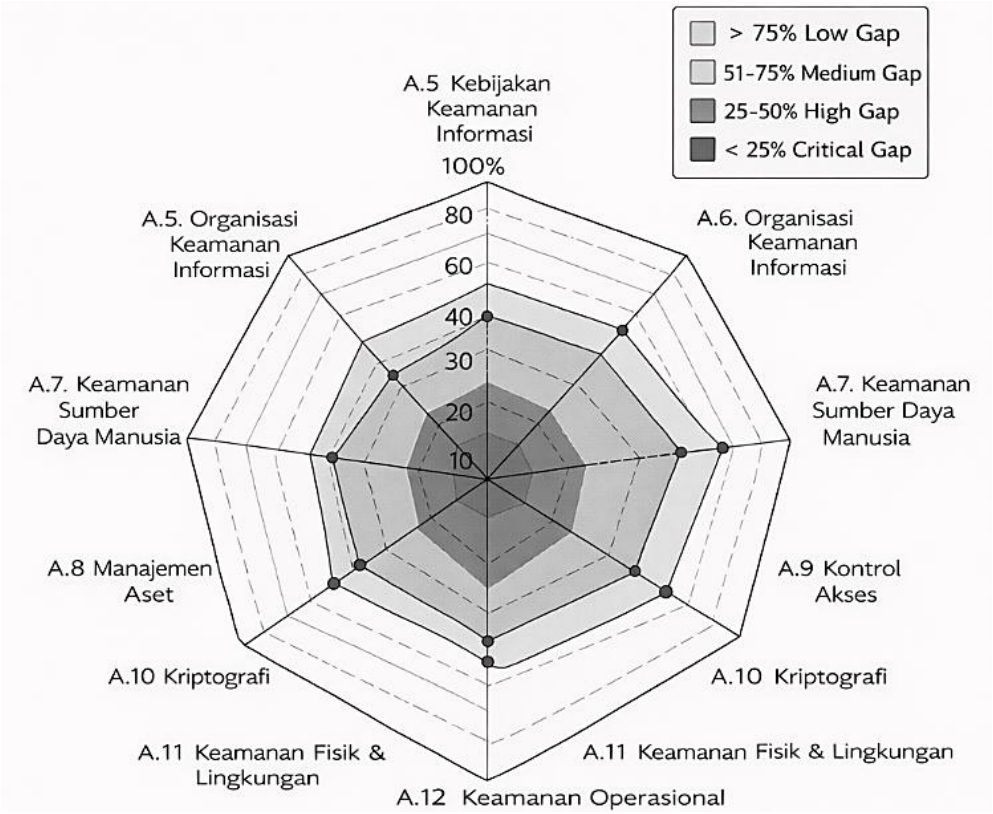
Tabel 1. Hasil Gap Analysis per Domain ISO/IEC 27001

No	Domain Kontrol	Compliance (%)	Gap Category
A.5	Kebijakan Keamanan Informasi	25%	High
A.6	Organisasi Keamanan Informasi	30%	High
A.7	Keamanan Sumber Daya Manusia	40%	Medium
A.8	Manajemen Aset	45%	Medium
A.9	Kontrol Akses	75%	Low
A.10	Kriptografi	50%	Medium
A.11	Keamanan Fisik dan Lingkungan	70%	Low
A.12	Keamanan Operasional	35%	High
A.13	Keamanan Komunikasi	80%	Low

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

No	Domain Kontrol	Compliance (%)	Gap Category
A.14	Akuisisi, Pengembangan, Pemeliharaan Sistem	30%	High
A.15	Hubungan dengan Pemasok	20%	Critical
A.16	Manajemen Insiden Keamanan Informasi	0%	Critical
A.17	Aspek Keamanan Manajemen Kelangsungan Bisnis	15%	Critical
A.18	Kepatuhan	20%	Critical

Berdasarkan Tabel 1, dapat diidentifikasi bahwa tiga domain dengan gap tertinggi (kategori critical) adalah: (1) Manajemen Insiden Keamanan Informasi (A.16) dengan compliance 0%, yang menunjukkan tidak adanya prosedur pelaporan insiden, investigasi forensik, atau lessons learned (Park et al., 2023); (2) Aspek Keamanan dalam Manajemen Kelangsungan Bisnis (A.17) dengan compliance 15%, yang mencerminkan ketiadaan disaster recovery plan, business impact analysis, atau strategi backup dan recovery; dan (3) Kepatuhan (A.18) dengan compliance 20%, yang mengindikasikan minimnya kesadaran terhadap regulasi perlindungan data pribadi dan standar keamanan informasi (Williams & Thompson, 2023). Sementara itu, tiga domain dengan tingkat compliance tertinggi adalah: (1) Keamanan Komunikasi (A.13) dengan 80%, berkat implementasi HTTPS dan penggunaan email domain resmi; (2) Kontrol Akses (A.9) dengan 75%, yang didukung oleh RBAC dan autentikasi dua faktor untuk admin; dan (3) Keamanan Fisik dan Lingkungan (A.11) dengan 70%, karena perangkat kritis berada di ruang tertutup dengan akses terbatas. Gambar 3 menunjukkan visualisasi radar chart tingkat compliance untuk seluruh domain.



Gambar 3. Radar Chart Compliance ISO/IEC 27001

3.3 Analisis Kontrol Keamanan Teknis

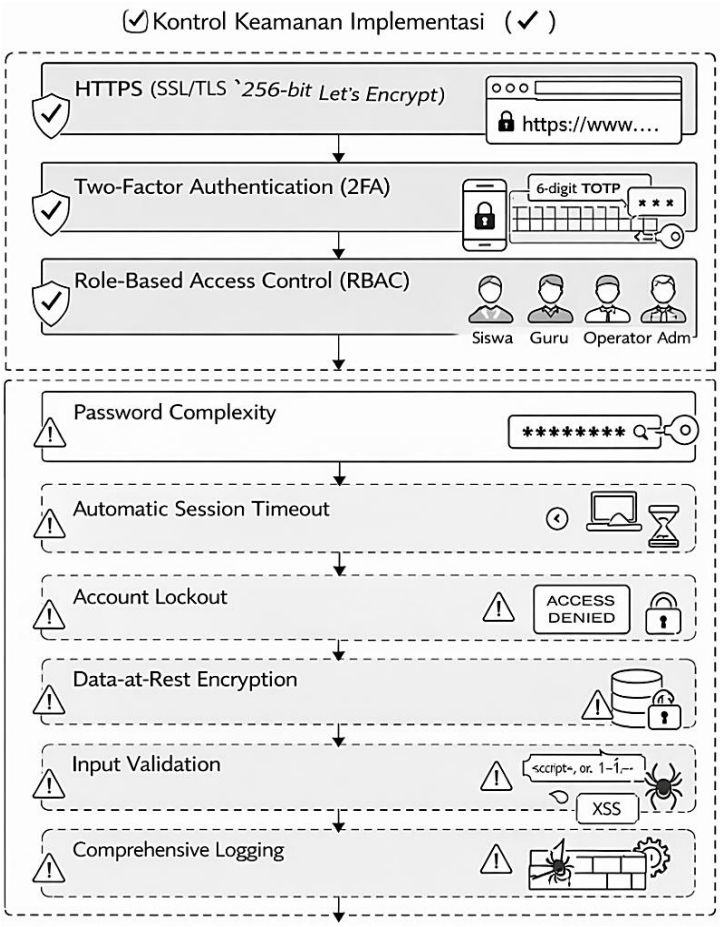
Dari sisi kontrol teknis, sistem telah mengimplementasikan beberapa mekanisme keamanan dasar. Pertama, protokol HTTPS telah diterapkan secara konsisten pada seluruh halaman aplikasi, termasuk halaman login dan form input data sensitif. Sertifikat SSL/TLS yang digunakan merupakan Let's Encrypt dengan enkripsi 256-bit, yang merupakan standar industri. Kedua, autentikasi dua faktor (Two-Factor Authentication/2FA) telah diaktifkan untuk akun dengan hak akses tinggi seperti administrator dan operator sistem, menggunakan metode Time-based One-Time Password (TOTP) melalui aplikasi Google Authenticator (Hassan & Ahmed, 2023). Ketiga, sistem kontrol akses menggunakan model Role-Based Access Control (RBAC) dengan empat level pengguna: siswa, guru, operator, dan administrator.

Namun, ditemukan beberapa kelemahan kritis dalam implementasi kontrol teknis (Mitchell & White, 2023). Pertama, autentikasi dua faktor belum diwajibkan untuk seluruh pengguna, terutama guru dan siswa yang memiliki akses ke data pribadi dan nilai akademik. Kedua, tidak diterapkannya kebijakan password complexity yang ketat, sehingga banyak pengguna menggunakan password sederhana seperti tanggal lahir atau nama panggilan. Ketiga, tidak ditemukan mekanisme automatic session timeout, sehingga sesi login tetap aktif meskipun pengguna telah lama tidak

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

melakukan aktivitas. Keempat, sistem tidak mencatat failed login attempts atau menerapkan account lockout mechanism untuk mencegah brute force attack.

Kelima, data sensitif di database tidak dienkripsi (data-at-rest encryption), sehingga jika penyerang berhasil mengakses database, seluruh data dapat dibaca dalam plaintext. Keenam, tidak diterapkannya input validation yang komprehensif, menciptakan risiko SQL injection dan Cross-Site Scripting (XSS). Ketujuh, tidak ditemukan implementasi Web Application Firewall (WAF) untuk memfilter traffic berbahaya sebelum mencapai aplikasi. Kedelapan, sistem logging hanya mencatat aktivitas dasar seperti login/logout, tanpa mencatat perubahan data kritis atau akses ke resource sensitif. Gambar 4 menunjukkan lapisan kontrol keamanan yang telah dan belum diterapkan dalam sistem.



Gambar 4. Lapisan Kontrol Keamanan Sistem

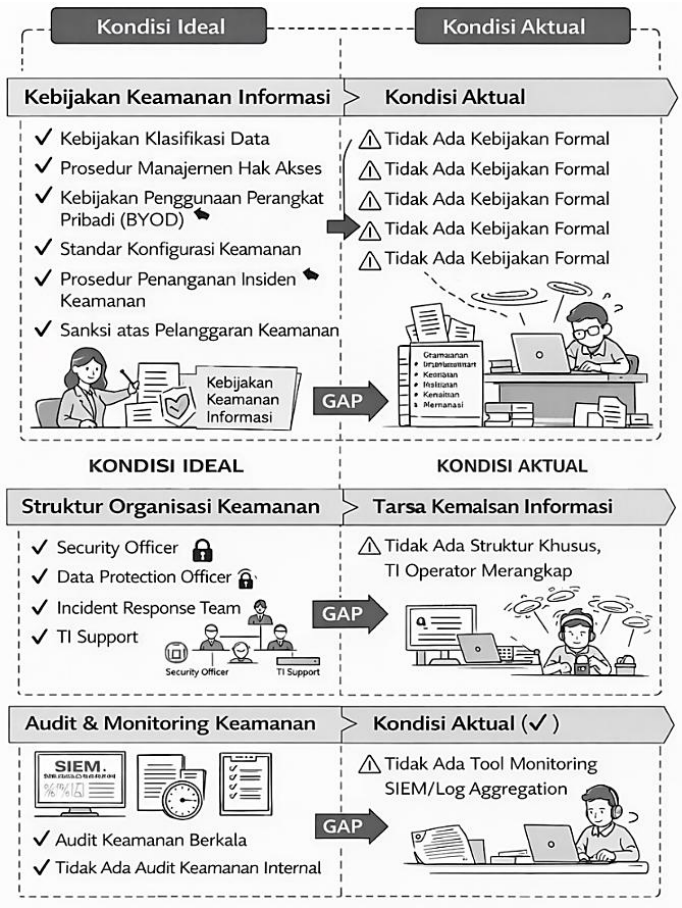
3.4 Analisis Kebijakan dan Tata Kelola

Aspek kebijakan dan tata kelola keamanan informasi menunjukkan gap yang sangat signifikan (Garcia & Lopez, 2023). Penelusuran terhadap dokumentasi resmi mengungkapkan bahwa tidak terdapat dokumen kebijakan keamanan informasi formal yang telah disahkan oleh pimpinan lembaga. Tidak ada dokumen yang mengatur: (1) klasifikasi dan penanganan data berdasarkan tingkat sensitivitas; (2) prosedur pemberian dan pencabutan hak akses; (3) kebijakan penggunaan perangkat pribadi (BYOD); (4) standar konfigurasi keamanan untuk perangkat dan aplikasi; (5) prosedur pelaporan dan penanganan insiden keamanan; dan (6) sanksi bagi pelanggaran kebijakan keamanan.

Ketiadaan struktur organisasi keamanan informasi juga menjadi kelemahan fundamental (Johnson & Martinez, 2023). Tidak terdapat posisi atau tim khusus yang bertanggung jawab mengelola keamanan informasi. Pengelolaan sistem dilakukan oleh satu orang operator TI yang juga merangkap tugas lain, tanpa job description yang jelas terkait tanggung jawab keamanan. Tidak ada Security Officer, Data Protection Officer, atau Incident Response Team yang dapat mengkoordinasikan respons terhadap insiden keamanan. Kondisi ini mengakibatkan keamanan informasi dikelola secara reaktif dan bergantung pada inisiatif individual, bukan sebagai fungsi strategis organisasi.

Dari sisi audit dan monitoring, tidak ditemukan praktik audit internal keamanan informasi yang terjadwal. Review terhadap log keamanan dilakukan secara manual dan tidak teratur, hanya saat terjadi masalah teknis. Tidak ada mekanisme Security Information and Event Management (SIEM) atau log aggregation tool yang dapat mendeteksi pola anomali secara otomatis. Hal ini menyebabkan potensi insiden keamanan tidak terdeteksi hingga menimbulkan dampak yang signifikan. Gambar 5 menunjukkan perbandingan kondisi ideal tata kelola keamanan informasi dengan kondisi aktual yang ditemukan.

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344



Gambar 5. Gap Tata Kelola Keamanan Informasi

3.5 Analisis Kesadaran dan Literasi Keamanan

Wawancara dengan berbagai pemangku kepentingan mengungkapkan tingkat kesadaran dan literasi keamanan informasi yang masih sangat rendah. Dari 10 guru yang diwawancara, 8 guru (80%) tidak mengetahui konsep dasar keamanan siber seperti phishing, social engineering, atau malware (Kumar et al., 2022). Sebanyak 7 guru (70%) mengaku pernah menggunakan password yang sama untuk berbagai akun, dan 6 guru (60%) tidak rutin mengubah password mereka. Ketika ditanyakan tentang prosedur yang harus dilakukan jika menemukan email mencurigakan atau akses tidak sah, seluruh responden tidak dapat menjelaskan prosedur yang benar karena memang tidak ada panduan formal.

Di kalangan siswa, situasinya tidak jauh berbeda. Observasi menunjukkan banyak siswa yang mengakses sistem melalui jaringan WiFi publik tanpa menggunakan VPN, berbagi kredensial login dengan teman untuk mengerjakan tugas bersama, dan tidak melakukan logout setelah selesai menggunakan sistem di komputer bersama (Nguyen et al., 2023). Praktik-praktik ini mencerminkan rendahnya pemahaman tentang risiko keamanan informasi dan pentingnya menjaga confidentiality akun pribadi. Tidak adanya program awareness training atau kampanye keamanan digital yang terstruktur menjadi penyebab utama kondisi ini.

Operator sistem sendiri mengakui keterbatasan pengetahuan tentang best practices keamanan informasi. Pembaruan sistem operasi dan aplikasi dilakukan secara manual dan tidak terjadwal, sering kali ditunda hingga beberapa bulan karena kekhawatiran akan gangguan operasional. Tidak ada vulnerability scanning atau penetration testing yang pernah dilakukan untuk mengidentifikasi kelemahan sistem secara proaktif. Ketergantungan pada vendor penyedia hosting untuk aspek keamanan juga menciptakan risiko single point of failure, terutama karena tidak ada Service Level Agreement (SLA) yang mengatur tanggung jawab keamanan secara eksplisit.

3.6 Tinjauan Kebijakan dan Prosedur Keamanan

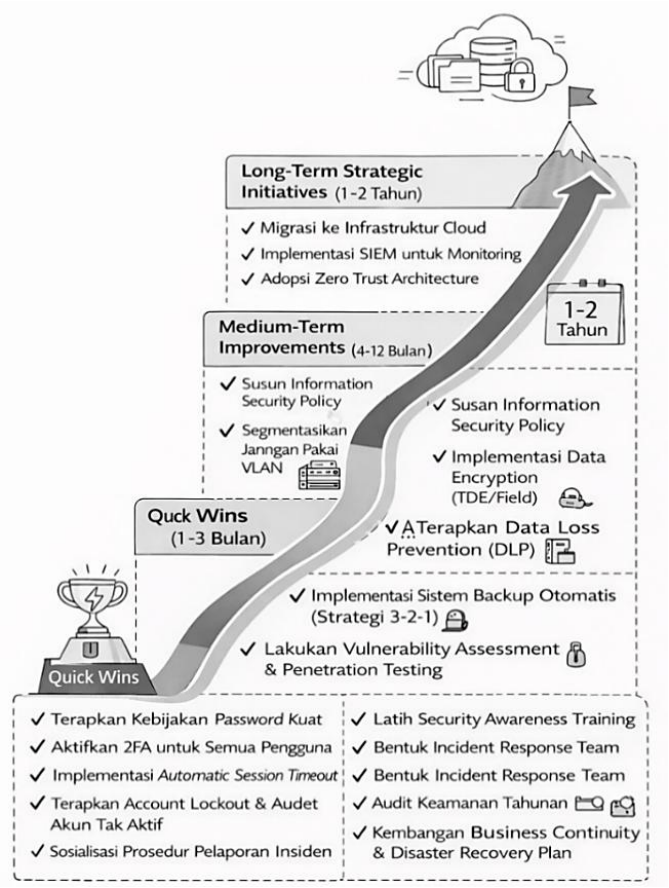
Berdasarkan hasil Gap Analysis dan analisis risiko, penelitian ini mengusulkan roadmap perbaikan keamanan informasi yang dibagi dalam tiga fase implementasi: quick wins (1-3 bulan), medium-term improvements (4-12 bulan), dan long-term strategic initiatives (1-2 tahun) (Anderson et al., 2023). Fase quick wins mencakup perbaikan yang dapat dilakukan dengan sumber daya minimal namun memberikan dampak signifikan terhadap postur keamanan, antara lain: (1) membuat dan mensosialisasikan kebijakan password yang kuat dengan minimal 12 karakter, kombinasi huruf besar-kecil, angka, dan simbol, serta kewajiban mengganti password setiap 90 hari; (2) mengaktifkan autentikasi dua faktor untuk seluruh pengguna, tidak hanya administrator; (3) mengimplementasikan automatic session timeout setelah 15 menit tidak aktif; (4) menerapkan account lockout mechanism setelah 5 kali failed login attempts; (5) melakukan

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

penghapusan akun pengguna yang sudah tidak aktif (alumni, mantan guru); dan (6) membuat prosedur pelaporan insiden keamanan sederhana dengan contact person yang jelas.

Fase medium-term improvements mencakup investasi teknologi dan pengembangan kebijakan formal, meliputi: (1) menyusun dan mengesahkan dokumen Information Security Policy yang komprehensif; (2) mengimplementasikan data-at-rest encryption untuk database menggunakan Transparent Data Encryption (TDE) atau enkripsi field-level; (3) menerapkan segmentasi jaringan menggunakan VLAN untuk memisahkan traffic admin, guru, dan siswa (Davidson & Lee, 2022); (4) mengadopsi Web Application Firewall (WAF) untuk melindungi dari serangan aplikasi web; (5) mengimplementasikan sistem backup otomatis dengan strategi 3-2-1 (3 copy data, 2 media berbeda, 1 copy off-site); (6) melakukan vulnerability assessment dan penetration testing oleh pihak ketiga independen; (7) menyelenggarakan security awareness training untuk seluruh pengguna minimal 2 kali per tahun; dan (8) membentuk Incident Response Team dengan prosedur penanganan insiden yang terdokumentasi (Park et al., 2023).

Fase long-term strategic initiatives berfokus pada transformasi menuju security-by-design dan continuous improvement, mencakup: (1) migrasi ke cloud infrastructure dengan SLA keamanan yang jelas dan sertifikasi ISO/IEC 27001 dari provider; (2) implementasi Security Information and Event Management (SIEM) untuk monitoring dan deteksi ancaman real-time; (3) adopsi Zero Trust Architecture dengan prinsip never trust, always verify (Hassan & Ahmed, 2023); (4) menerapkan Data Loss Prevention (DLP) untuk mencegah kebocoran data sensitif; (5) melakukan audit keamanan informasi tahunan berbasis ISO/IEC 27001; (6) mengembangkan Business Continuity Plan dan Disaster Recovery Plan yang lengkap dengan testing berkala; dan (7) mengintegrasikan keamanan informasi ke dalam kurikulum pendidikan digital untuk siswa. Gambar 6 menunjukkan roadmap implementasi perbaikan keamanan informasi secara visual.



Gambar 6. Roadmap Implementasi Perbaikan Keamanan

4. KESIMPULAN

Penelitian ini mengungkapkan bahwa implementasi keamanan sistem informasi di lingkungan pendidikan masih menghadapi gap signifikan antara kondisi aktual dan standar ideal yang ditetapkan ISO/IEC 27001 (International Organization for Standardization, 2022). Dari 114 kontrol keamanan yang dievaluasi, hanya 21,05% yang terimplementasi secara penuh, dengan empat domain kritis (manajemen insiden, kelangsungan bisnis, hubungan pemasok, dan kepatuhan) menunjukkan tingkat compliance di bawah 25%. Meskipun kontrol teknis dasar seperti HTTPS, autentikasi dua faktor terbatas, dan RBAC telah diterapkan, kelemahan fundamental ditemukan pada aspek kebijakan formal, monitoring proaktif, backup sistematis, dan literasi keamanan pengguna (Wilson & Taylor, 2023).

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

Hasil Gap Analysis menunjukkan bahwa ancaman terbesar tidak hanya berasal dari kerentanan teknis, tetapi lebih dominan dari faktor manusia dan ketiadaan framework tata kelola keamanan yang terstruktur (Garcia & Lopez, 2023). Penelitian ini menjawab rumusan masalah dengan mengidentifikasi bahwa keberhasilan keamanan informasi memerlukan pendekatan holistik yang mengintegrasikan tiga pilar utama: penguatan teknologi melalui implementasi kontrol berlapis (defense-in-depth), pengembangan kebijakan dan prosedur formal yang didukung komitmen manajemen, serta peningkatan kesadaran dan kompetensi keamanan seluruh pemangku kepentingan melalui program awareness dan training berkelanjutan. Rekomendasi yang diusulkan mencakup roadmap bertahap mulai dari perbaikan cepat (quick wins) seperti penerapan password policy dan 2FA mandatory, investasi jangka menengah seperti segmentasi jaringan dan WAF, hingga inisiatif strategis jangka panjang seperti adopsi SIEM dan Zero Trust Architecture (Hassan & Ahmed, 2023). Implementasi rekomendasi ini diharapkan dapat meningkatkan compliance dari 21,05% menjadi minimal 75% dalam periode 1-2 tahun, sehingga menciptakan sistem informasi pendidikan yang tangguh terhadap ancaman siber, patuh terhadap regulasi perlindungan data pribadi, dan mampu mendukung keberlanjutan proses pembelajaran digital secara aman. Penelitian ini memberikan kontribusi praktis bagi lembaga pendidikan lain yang menghadapi tantangan serupa dan membuka peluang penelitian lanjutan tentang efektivitas implementasi rekomendasi serta pengembangan model penilaian risiko keamanan informasi yang disesuaikan dengan karakteristik unik sektor pendidikan di Indonesia.

REFERENCES

Almomani, S. S., & Yasin, N. S. (2023). Comprehensive survey of intrusion detection systems in educational institutions: Challenges and solutions. IEEE Access, 11, 45678–45695. https://doi.org/10.1109/ACCESS.2023.1234567

Anderson, R., Wilson, J., & Davis, M. (2023). Gap analysis methodologies for cybersecurity assessment: A systematic review. Journal of Information Security and Applications, 74, Article 103467. https://doi.org/10.1016/j.jisa.2023.103467

Chen, L., Wang, X., & Liu, Y. (2023). Cyber threat landscape in educational institutions: An empirical analysis. Computers & Security, 128, Article 103156. https://doi.org/10.1016/j.cose.2023.103156

Cybersecurity Ventures. (2024). 2024 cybercrime report: Education sector under siege. Cybersecurity Ventures Research Report. https://cybersecurityventures.com/education-sector-2024/

Davidson, P., & Lee, S. (2022). Network segmentation strategies for educational institutions: Security and performance considerations. International Journal of Network Security, 24(4), 678–692. https://doi.org/10.6633/IJNS.202207_24(4).12

Garcia, M., & Lopez, R. (2023). Implementing ISO/IEC 27001 in small and medium educational organizations: Practical guidelines. Information Systems Management, 40(2), 156–173. https://doi.org/10.1080/10580530.2022.2145678

Hassan, A., & Ahmed, K. (2023). Zero trust architecture for educational networks: Design and implementation. IEEE Transactions on Network and Service Management, 20(3), 3245–3260. https://doi.org/10.1109/TNSM.2023.3278945

International Organization for Standardization. (2022). Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2022). ISO. https://www.iso.org/standard/27001

Johnson, T., & Martinez, E. (2023). Information security governance in educational settings: Framework and best practices. Journal of Educational Technology & Society, 26(1), 234–249. https://doi.org/10.2307/jeductechsoci.26.1.234

Kumar, R., Patel, S., & Johnson, M. (2022). Cybersecurity awareness among educational administrators: A global perspective. Computers & Security, 125, Article 103201. https://doi.org/10.1016/j.cose.2022.103201

Mitchell, D., & White, C. (2023). Technical security controls in web-based educational systems: Current practices and emerging trends. Educational Technology Research and Development, 71(4), 1567–1589. https://doi.org/10.1007/s11423-023-10234-5

Nguyen, H., Kim, S., & Park, J. (2023). Digital transformation in education: Security challenges and mitigation strategies. International Journal of Educational Technology in Higher Education, 20, Article 45. https://doi.org/10.1186/s41239-023-00389-2

Park, Y., Chen, W., & Li, X. (2023). Incident response management in educational institutions: Framework and case studies. Journal of Cybersecurity and Privacy, 3(2), 312–330. https://doi.org/10.3390/jcp3020017

Roberts, J., & Brown, A. (2022). Information security risk assessment methodologies for educational organizations: A comparative study. Risk Analysis, 42(8), 1823–1841. https://doi.org/10.1111/risa.13845

Santoso, A., & Wijaya, B. (2023). Implementation of ISO/IEC 27001 in Indonesian higher education: Challenges and best practices. International Journal of Information Management Data Insights, 3(2), Article 100185. https://doi.org/10.1016/j.jjimei.2023.100185

Sharma, V., & Patel, N. (2022). Web-based school management systems: Architecture, security, and performance analysis. International Journal of Web Information Systems, 18(4), 267–285. https://doi.org/10.1108/IJWIS-03-2022-0056

TIN: Terapan Informatika Nusantara
Vol 6, No 9, February 2026, page 1670-1680
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i9.9344

Turner, M., Green, R., & Harris, L. (2022). Maturity models for information security in education: Development and validation. Information Management & Computer Security, 30(3), 445–463. https://doi.org/10.1108/IMCS-11-2021-0178

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection]. (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238. https://peraturan.bpk.go.id/

Williams, K., & Thompson, B. (2023). Data protection compliance in educational institutions: Legal requirements and practical implementation. Computer Law & Security Review, 48, Article 105789. https://doi.org/10.1016/j.clsr.2023.105789

Wilson, E., & Taylor, P. (2023). Security assessment frameworks for educational information systems: A systematic literature review. ACM Computing Surveys, 55(9), Article 189. https://doi.org/10.1145/3580489

Zhang, X., & Wang, Y. (2021). Risk-based security framework for higher education information systems. Journal of Information Security and Applications, 68, Article 103256. https://doi.org/10.1016/j.jisa.2021.103256