BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer
Vol. 7, No. 1, Maret 2026, hlm. 01-07
e-ISSN: 2722-0850

Perancangan Sistem Pengamanan Data Berdasarkan Standar ISO 27001 pada Lingkungan Laboratorium Teknik Informatika

Taufiq Timur Warisaji [1], Guruh Wijaya [2], Lintang Setyo Kurniawati[3]
[1]Teknik Informatika, Universitas Muhammadiyah Jember, *taufiqtimur@unmuhjember.ac.id*
[2]Teknik Informatika, Universitas Muhammadiyah Jember, *guruh.wijaya@unmuhjember.ac.id*
[3]Teknik Informatika, Universitas Muhammadiyah Jember, *lintang@unmuhjember.ac.id*

Keywords :

ISO 27001,
Information Security,
Informatics Engineering Laboratory,
Data Encryption,
Risk Management,

ABSTRACT

This study addresses the problem of inadequate information security systems in Informatics Engineering laboratories, which leads to high risks of data leakage, unauthorized access, and low user awareness of information security. The aim of this research is to design and implement an information security system based on the ISO/IEC 27001 standard to enhance the protection of information assets and establish sustainable security governance. The research employs a descriptive qualitative method consisting of literature review, needs analysis, risk assessment using a Risk Assessment Matrix, system design and implementation of security controls, and system evaluation through penetration testing and user compliance surveys. The results show that the implementation of technical security controls, such as data encryption, firewalls, and access management, significantly reduces data leakage risks and improves user compliance and awareness of information security practices. The study concludes that ISO/IEC 27001 is effective in establishing a structured and sustainable information security management system within the Informatics Engineering laboratory environment

Kata Kunci

ISO 27001,
keamanan informasi,
laboratorium TI,
enkripsi data,
manajemen risiko,

ABSTRAK

Penelitian ini membahas permasalahan belum optimalnya sistem pengamanan informasi di laboratorium Teknik Informatika yang menyebabkan tingginya risiko kebocoran data, akses tidak sah, serta rendahnya kesadaran pengguna terhadap keamanan informasi. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pengamanan informasi berbasis standar ISO/IEC 27001 guna meningkatkan perlindungan aset informasi dan tata kelola keamanan data yang berkelanjutan. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan tahapan studi literatur, analisis kebutuhan, penilaian risiko menggunakan Risk Assessment Matrix, perancangan dan implementasi kontrol keamanan, serta evaluasi sistem melalui pengujian penetrasi dan survei kepatuhan pengguna. Hasil penelitian menunjukkan bahwa penerapan kontrol keamanan teknis seperti enkripsi data, firewall, dan manajemen akses mampu menurunkan risiko kebocoran data serta meningkatkan kepatuhan dan kesadaran pengguna terhadap keamanan informasi. Kesimpulan penelitian menunjukkan bahwa standar ISO/IEC 27001 efektif dalam membangun sistem manajemen keamanan informasi yang terstruktur dan berkelanjutan di lingkungan laboratorium Teknik Informatika.

Korespondensi Penulis:

Lintang Setyo Kurniawati,
Alifiasi, Universitas Muhammadiyah Jember
Telepon : +6287712444003
Email: *lintang@unmuhjember.ac.id*

Submitted: 07-11-2025; Accepted: 21-01-2026;
Published: 26-01-2026

1. PENDAHULUAN

Laboratorium Teknik Informatika memiliki peran yang sangat penting sebagai pusat penelitian dan pengembangan teknologi informasi. Menurut [1], laboratorium ini menyimpan berbagai jenis data sensitif seperti hasil penelitian, kode sumber, serta data mahasiswa yang memerlukan perlindungan ketat. Data tersebut memiliki nilai strategis yang tinggi dan rentan terhadap risiko keamanan informasi, termasuk akses tidak sah, kebocoran data, hingga potensi kerusakan sistem. Seiring dengan semakin kompleksnya ancaman siber dan kemajuan teknologi informasi,

laboratorium dihadapkan pada tantangan serangan siber yang semakin canggih dan sulit dideteksi [2]. Selain itu, meningkatnya kesadaran publik terhadap pentingnya perlindungan data pribadi juga menuntut laboratorium untuk menerapkan sistem pengamanan informasi yang tangguh, terstruktur, dan dapat dipertanggungjawabkan[3].

Permasalahan keamanan informasi di lingkungan laboratorium tidak hanya berkaitan dengan aspek teknis, tetapi juga dengan lemahnya tata kelola keamanan informasi secara menyeluruh. Banyak laboratorium masih menerapkan pengamanan yang bersifat parsial dan reaktif, tanpa didukung oleh kebijakan, prosedur, serta mekanisme evaluasi yang sistematis. Kondisi ini menyebabkan pengelolaan keamanan informasi sulit diukur tingkat efektivitasnya dan berpotensi menimbulkan celah keamanan yang signifikan. Oleh karena itu, diperlukan suatu kerangka kerja keamanan informasi yang mampu mengintegrasikan aspek teknis, administratif, dan manajerial secara komprehensif.

ISO 27001 hadir sebagai kerangka kerja internasional yang telah diakui secara luas dalam pengelolaan keamanan informasi [4]. tandar ini menyediakan panduan sistematis bagi organisasi dalam mengidentifikasi, menilai, dan mengelola risiko keamanan informasi melalui pendekatan berbasis risiko (risk-based approach). ISO 27001 mencakup berbagai kontrol keamanan, seperti kebijakan akses data, manajemen risiko, serta prosedur keamanan operasional yang relevan untuk diterapkan di lingkungan laboratorium Teknik Informatika [5]. Dengan mengadopsi standar ini, laboratorium diharapkan mampu meningkatkan perlindungan terhadap berbagai bentuk ancaman, meminimalkan potensi kebocoran data, serta membangun kepercayaan pemangku kepentingan terhadap pengelolaan informasi yang dilakukan. Sebagaimana dikemukakan dalam [6], sistem pengamanan berbasis ISO 27001 memungkinkan organisasi menyesuaikan protokol keamanan mereka dengan praktik terbaik internasional.

Penerapan sistem pengamanan informasi berbasis ISO 27001 tidak hanya menekankan pada penerapan kontrol teknis, tetapi juga menuntut komitmen organisasi secara menyeluruh, mulai dari kebijakan manajemen hingga perilaku individu yang terlibat di dalamnya. Standar ini menekankan pentingnya identifikasi dan evaluasi risiko terhadap aset informasi sebagai dasar dalam penetapan kontrol keamanan yang tepat. Proses tersebut meliputi asesmen risiko, identifikasi kerentanan, serta penentuan kontrol keamanan yang mencakup pengelolaan akses, pengawasan aktivitas sistem, penggunaan enkripsi, dan peningkatan kesadaran keamanan informasi. Keseluruhan elemen ini membentuk fondasi Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur dan selaras dengan kerangka ISO 27001.

Keberhasilan penerapan ISO 27001 juga sangat dipengaruhi oleh budaya keamanan informasi yang berkembang di lingkungan laboratorium. Rendahnya kesadaran pengguna sering kali menjadi faktor utama terjadinya insiden keamanan, seperti penggunaan kata sandi yang lemah atau pengabaian prosedur pencadangan data [7]. Oleh karena itu, penguatan aspek sumber daya manusia melalui pelatihan dan sosialisasi keamanan informasi menjadi bagian yang tidak terpisahkan dari penerapan ISO 27001. Pendekatan ini sejalan dengan prinsip ISO 27001 yang menekankan keterlibatan seluruh pihak dalam menjaga keamanan informasi secara berkelanjutan.

Dalam konteks lingkungan akademik, adopsi standar ISO/IEC 27001 tidak hanya berfungsi sebagai pedoman dalam penerapan kontrol keamanan informasi, tetapi juga menjadi tolok ukur kesiapan organisasi dalam menghadapi ancaman siber yang terus berkembang. Tingkat kesiapan ini mencerminkan kematangan tata kelola keamanan informasi, yang meliputi kelengkapan kebijakan, efektivitas pengelolaan risiko, konsistensi penerapan kontrol keamanan, serta keberlangsungan proses evaluasi dan perbaikan sistem keamanan. Untuk menilai tingkat kematangan tersebut, institusi akademik sering menggunakan Indeks Keamanan Informasi (KAMI) sebagai instrumen evaluasi yang disusun berdasarkan kriteria dan prinsip ISO/IEC 27001. Penggunaan Indeks KAMI memungkinkan organisasi melakukan penilaian secara sistematis terhadap kondisi keamanan informasi yang ada, mengidentifikasi kesenjangan antara praktik yang diterapkan dan standar yang diharapkan, serta menjadi dasar dalam merumuskan strategi peningkatan keamanan informasi secara berkelanjutan[8].

Dalam konteks lingkungan akademik, adopsi standar ISO/IEC 27001 tidak hanya berperan sebagai acuan dalam penerapan pengamanan informasi, tetapi juga berfungsi sebagai tolok ukur kesiapan organisasi dalam menghadapi ancaman siber yang terus berkembang. Tingkat kesiapan ini mencerminkan kematangan tata kelola keamanan informasi, yang meliputi aspek kebijakan, manajemen risiko, penerapan kontrol keamanan, serta mekanisme evaluasi dan peningkatan berkelanjutan. Untuk menilai tingkat kematangan tersebut, institusi akademik sering menggunakan Indeks Keamanan Informasi (KAMI) sebagai instrumen evaluasi yang disusun berdasarkan kriteria ISO/IEC 27001. Instrumen ini memungkinkan organisasi melakukan penilaian secara sistematis terhadap kondisi keamanan informasi yang berjalan, mengidentifikasi kesenjangan antara praktik yang diterapkan dan standar yang diharapkan, serta menjadi dasar dalam perencanaan peningkatan keamanan informasi secara berkelanjutan[9].

Selain meningkatkan keamanan internal, penerapan ISO 27001 juga memberikan dampak positif terhadap reputasi dan kredibilitas laboratorium Teknik Informatika. Keberadaan sistem manajemen keamanan informasi yang terdokumentasi menunjukkan komitmen institusi terhadap pengelolaan data yang profesional dan bertanggung jawab. Hal ini menjadi nilai tambah dalam kerja sama penelitian serta meningkatkan kepercayaan mitra akademik dan industri. Lebih lanjut, penerapan ISO 27001 berpotensi meningkatkan efisiensi sistem informasi, menurunkan insiden keamanan, serta mendukung keberlangsungan operasional laboratorium secara berkelanjutan [10]. Berdasarkan kondisi tersebut, penelitian ini difokuskan pada perancangan sistem pengamanan informasi yang efektif dan terstruktur berdasarkan standar ISO/IEC 27001, dengan tujuan memperkuat tata kelola keamanan data di lingkungan

laboratorium Teknik Informatika. Pembahasan mengenai implementasi teknis dan evaluasi efektivitas sistem akan diuraikan pada bagian selanjutnya.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dengan metode kualitatif yang bertujuan untuk merancang sistem pengamanan data berbasis standar ISO 27001 pada lingkungan laboratorium Teknik Informatika. Metode ini dipilih untuk memberikan pemahaman menyeluruh terhadap proses perancangan sistem pengamanan informasi yang sesuai dengan kerangka kerja standar internasional. Adapun tahapan-tahapan penelitian yang dilakukan dijelaskan sebagai berikut:

1. Studi Literatur : Tahap awal penelitian diawali dengan penelusuran literatur yang berkaitan dengan standar ISO 27001, sistem manajemen keamanan informasi (*Information Security Management System*/ISMS), serta teknik dan teknologi pengamanan data yang relevan. Studi literatur ini bertujuan untuk memperoleh pemahaman mendalam mengenai prinsip-prinsip keamanan informasi, kerangka kerja ISO 27001, serta praktik terbaik yang dapat diterapkan di lingkungan akademik. Literatur yang dikaji berasal dari jurnal ilmiah, buku teks, standar internasional, serta hasil penelitian terdahulu yang relevan. Referensi tersebut juga digunakan sebagai dasar pembanding dan validasi terhadap pendekatan yang diambil dalam penelitian ini.
2. Analisis Kebutuhan : Pada tahap ini dilakukan untuk mengidentifikasi pengamanan informasi di laboratorium teknik informatika melalui data primer dan sekunder. Data primer diperoleh dari 50 responden yang terdiri atas dosen, laboran, asisten, dan mahasiswa pengguna laboratorium dengan metode purposive sampling. Pengambilan data dilakukan melalui observasi, wawancara terstruktur, dan kuesioner guna mengidentifikasi kondisi sistem, kebijakan, serta tingkat kepatuhan pengguna. Data yang diperoleh dianalisis menggunakan analisis risiko berdasarkan kerangka ISO/IEC 27001, mencakup identifikasi aset, ancaman, dan kerentanan. Hasil analisis digunakan sebagai dasar penentuan prioritas pengamanan dan pemilihan kontrol keamanan untuk mitigasi risiko secara sistematis dan berkelanjutan.
3. Perancangan Sistem Pengamanan : Berdasarkan hasil analisis kebutuhan, selanjutnya dilakukan perancangan sistem pengamanan data yang terstruktur sesuai standar ISO 27001. Perancangan mencakup pemilihan kontrol keamanan yang meliputi pengendalian akses, manajemen hak pengguna, enkripsi data, audit log, serta pemantauan sistem. Selain aspek teknis, perancangan juga melibatkan penyusunan kebijakan keamanan informasi, prosedur operasional standar (SOP), serta peran dan tanggung jawab personel yang terlibat. Tujuan dari tahap ini adalah menyusun sistem pengamanan yang tidak hanya sesuai standar, tetapi juga dapat diterapkan secara realistis di lingkungan laboratorium.
4. Implementasi : Setelah sistem pengamanan dirancang, tahap berikutnya adalah implementasi di lingkungan laboratorium Teknik Informatika. Implementasi dilakukan melalui pemasangan perangkat lunak keamanan, konfigurasi sistem dan jaringan, pengaturan hak akses pengguna, serta penyusunan dokumentasi kebijakan. Selain itu, dilakukan pelatihan dan sosialisasi kepada staf dan pengguna laboratorium untuk memastikan pemahaman serta kepatuhan terhadap sistem yang diterapkan. Implementasi ini bertujuan untuk memastikan sistem berjalan sesuai desain dan dapat dioperasikan dengan baik oleh seluruh pengguna.
5. Evaluasi Sistem : Tahap akhir penelitian adalah evaluasi terhadap sistem pengamanan yang telah diimplementasikan. Evaluasi dilakukan untuk menilai efektivitas kontrol keamanan berdasarkan indikator keberhasilan yang telah ditentukan sebelumnya. Metode evaluasi dapat berupa pengujian sistem, simulasi serangan (*penetration test*), maupun audit keamanan internal. Evaluasi ini juga mencakup peninjauan ulang terhadap kebijakan dan prosedur yang telah disusun untuk memastikan kesesuaian dengan kebutuhan dan standar ISO 27001. Hasil evaluasi digunakan untuk menentukan apakah sistem perlu diperbaiki, disempurnakan, atau dikembangkan lebih lanjut.

3. HASIL DAN ANALISIS

3.1. Studi Literatur

Keamanan informasi merupakan bagian krusial dalam sistem manajemen teknologi informasi, terutama dalam lingkungan laboratorium yang menangani data sensitif. Standar internasional seperti ISO/IEC 27001 digunakan sebagai acuan dalam membangun sistem manajemen keamanan informasi (*Information Security Management System*/ISMS) secara menyeluruh (ISO/IEC, 2013). Menurut Rizki [11], risiko keamanan informasi dapat dikategorikan ke dalam tiga aspek utama:

a. Ancaman Fisik : mencakup kehilangan perangkat keras dan akses tidak sah secara langsung.
b. Ancaman Teknis : termasuk serangan *malware*, eksploitasi jaringan, dan enkripsi lemah.
c. Ancaman Organisasi/Internal/Manusia : seperti *human error*, kebocoran informasi oleh karyawan, dan penggunaan perangkat ilegal.

Sementara itu, [12] Sintiya menyatakan bahwa penerapan kontrol keamanan teknis seperti enkripsi data, autentikasi ganda, dan *firewall* akan meningkatkan pertahanan berlapis dalam sistem informasi.

3.2. Identifikasi Risiko Keamanan Data

Proses identifikasi risiko dilaksanakan melalui pendekatan *Risk Assessment* yang merujuk pada kerangka kerja ISO 27005 untuk memastikan analisis dilakukan secara sistematis dan terukur. Tahapan utama yang dilakukan meliputi:

- *Asset Identification* (Identifikasi Aset) : yaitu mengumpulkan dan memetakan seluruh aset informasi yang memiliki nilai strategis bagi organisasi, termasuk data, perangkat keras, perangkat lunak, serta sumber daya pendukung.
- *Threat Identification* (Identifikasi Ancaman) : yakni mengidentifikasi berbagai potensi ancaman, baik yang berasal dari faktor internal maupun eksternal, yang dapat mengganggu keamanan aset tersebut.
- *Vulnerability Assessment* (Kelemahan Sistem) : yaitu mengevaluasi titik lemah pada sistem, proses, maupun infrastruktur yang memungkinkan ancaman mengeksploitasi celah keamanan.
- *Risk Estimation & Evaluation* : yaitu menetapkan tingkat kemungkinan dan dampak dari setiap risiko, kemudian melakukan penilaian menyeluruh untuk menentukan prioritas mitigasi dan strategi pengendalian yang paling efektif bagi organisasi.

3.3. Identifikasi Aset dan Ancaman

Identifikasi aset dan ancaman dilakukan untuk menentukan komponen-komponen penting dalam sistem yang berpotensi terdampak oleh insiden keamanan. Tahap ini bertujuan untuk memperoleh pemahaman menyeluruh mengenai aset yang harus dilindungi, jenis ancaman yang mungkin muncul, serta kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Proses ini menjadi dasar dalam menentukan tingkat risiko serta merumuskan strategi pengendalian keamanan yang tepat.

Tabel *1* Aset dan Ancaman

No	Aset Sistem	Ancaman Potensial	Kerentanan
1	Server & Data Center	Akses fisik ilegal, pencurian perangkat	Tidak ada sistem akses terkontrol
2	Jaringan Komputer	*Malware, sniffing, data breach*	Jaringan terbuka tanpa *firewall*
3	Sistem Informasi	SQL *injection, phishing*	Input tidak tervalidasi
4	Data Laboratorium	Pencurian, modifikasi tanpa izin	Tidak dienkripsi
5	Pengguna Sistem	*Human error, insider threat*	Kurangnya pelatihan keamanan

3.4. Penilaian Risiko (*Risk Assessment Matrix*)

Penilaian risiko dilakukan untuk menentukan tingkat ancaman terhadap aset dengan menggunakan pendekatan *Risk Assessment Matrix* [13]. Perhitungan risiko mengacu pada formula:

$$Risk\ Score = Likelihood\ (L) \times Impact\ (I)$$

Skala penilaian ditetapkan dari **1 hingga 5**, di mana nilai **1** menunjukkan tingkat kemungkinan atau dampak yang rendah, sedangkan nilai **5** menggambarkan tingkat yang sangat tinggi. Hasil penilaian ini berfungsi untuk mengidentifikasi prioritas mitigasi serta menentukan langkah pengendalian keamanan yang diperlukan.

Tabel 2 Penilaian Resiko

Risiko	L	I	Skor	Kategori Risiko
Akses tidak sah ke ruang server	4	5	20	Sangat Tinggi
Serangan *malware*	5	5	25	Sangat Tinggi
Human error (hapus data)	4	4	16	Tinggi
Pencurian data melalui jaringan	5	5	25	Sangat Tinggi
Penggunaan perangkat tanpa izin	3	4	12	Tinggi

Berdasarkan hasil perhitungan keseluruhan, diperoleh nilai rata-rata risiko:
Rata-rata risiko = (20 + 25 + 16 + 25 + 12) / 5 = 19,6
Dengan nilai tersebut, tingkat risiko masuk dalam kategori **Tinggi hingga Sangat Tinggi**, sehingga diperlukan penerapan kebijakan pengamanan yang lebih ketat serta pengembangan kontrol keamanan tambahan untuk menurunkan potensi insiden yang dapat mengganggu operasional sistem.

3.5. Implementasi Sistem Pengamanan Data

Berdasarkan hasil penilaian risiko yang telah dilakukan serta merujuk pada ketentuan dalam standar ISO 27001, perancangan sistem keamanan dilakukan dengan menerapkan pendekatan *defense-in-depth* sebagai strategi

utama. Pendekatan ini bertujuan untuk menyediakan mekanisme perlindungan berlapis sehingga setiap potensi ancaman dapat dihadapi pada berbagai titik kontrol keamanan. Dengan adanya lapisan pertahanan yang saling melengkapi, organisasi diharapkan mampu meminimalkan dampak insiden keamanan, meningkatkan ketahanan sistem, serta memastikan kontinuitas layanan. Rincian implementasi dari strategi tersebut disajikan sebagai berikut:

Tabel 3 Pendekatan *defense-in-depth*

No	Komponen Implementasi	Fungsi
1	Autentikasi Dua Faktor (2FA)	Memastikan hanya pengguna sah yang dapat mengakses sistem
2	Role-Based Access Control	Pembatasan hak akses berdasarkan level pengguna
3	Enkripsi AES-256	Mengamankan data sensitif dari penyadapan atau pencurian
4	Firewall dan IDS	Deteksi dan pencegahan serangan dari jaringan eksternal
5	Backup Otomatis	Perlindungan data jika terjadi insiden atau kehilangan

3.6. Evaluasi Keamanan Sistem

Tahap akhir penelitian adalah evaluasi terhadap sistem pengamanan yang telah diimplementasikan. Evaluasi dilakukan untuk menilai efektivitas kontrol keamanan berdasarkan indikator keberhasilan yang telah ditentukan sebelumnya. Metode evaluasi dapat berupa pengujian sistem, simulasi serangan (penetration test), maupun audit keamanan internal. Evaluasi ini juga mencakup peninjauan ulang terhadap kebijakan dan prosedur yang telah disusun untuk memastikan kesesuaian dengan kebutuhan dan standar ISO 27001. Hasil evaluasi digunakan untuk menentukan apakah sistem perlu diperbaiki, disempurnakan, atau dikembangkan lebih lanjut. Sehingga dalam tahap evaluasi sistem, penelitian ini menilai efektivitas kontrol keamanan yang telah diimplementasikan. Evaluasi keamanan sistem dilakukan untuk menilai efektivitas penerapan kontrol keamanan yang telah diimplementasikan. Proses evaluasi mencakup pengujian teknis serta penilaian tingkat kepatuhan pengguna terhadap prosedur keamanan yang baru diterapkan. Hasil evaluasi ini menjadi dasar untuk menentukan apakah sistem telah mencapai tingkat keamanan yang diharapkan dan area mana yang masih memerlukan perbaikan.

3.6.1. Pengujian Penetrasi

Pengujian penetrasi dilakukan menggunakan metode *Black Box Testing* dan *White Box Testing* guna mengidentifikasi celah keamanan dari sudut pandang eksternal maupun internal. Pengujian ini memberikan gambaran mengenai efektivitas kontrol keamanan yang diterapkan sebelum dan sesudah implementasi. Adapun hasil pengujian dirangkum dalam tabel berikut:

Tabel 4 *Black Box* dan *White Box Testing*

Parameter Evaluasi	Sebelum Implementasi	Setelah Implementasi	Efektivitas
Kebocoran Data (insiden/bulan)	60	9	↓ 85%
Deteksi Ancaman Jaringan	20 insiden/bulan	35 insiden/bulan	↑ 75%
Kecepatan Respon	3 jam	45 menit	↑ 75%

3.6.2. Evaluasi Kepatuhan Pengguna

Selain pengujian teknis, evaluasi juga dilakukan melalui survei terhadap 50 pengguna laboratorium untuk menilai sejauh mana prosedur keamanan baru diterapkan. Aspek yang dinilai meliputi penggunaan autentikasi dua faktor, perilaku penyimpanan data, serta pelaporan insiden keamanan. Hasil evaluasi ditampilkan pada tabel berikut:

Tabel 5 Evaluasi Kepatuhan Pengguna

Aspek Kepatuhan	Sebelum Implementasi	Setelah Implementasi	Kenaikan (%)
Penggunaan 2FA	40%	92%	+52%
Penyimpanan data aman	55%	90%	+35%
Pelaporan insiden	30%	75%	+45%

Peningkatan tingkat kepatuhan ini menunjukkan bahwa implementasi kebijakan keamanan tidak hanya berdampak pada infrastruktur teknis, tetapi juga pada perilaku pengguna dalam menjaga keamanan informasi.

3.7. Pembahasan

Penerapan sistem pengamanan berbasis ISO 27001 menunjukkan efektivitas signifikan dalam menurunkan tingkat risiko keamanan informasi, baik pada aspek teknis maupun perilaku pengguna. Standar ini menyediakan kerangka kerja *Information Security Management System* (ISMS) yang komprehensif dan mendukung mekanisme

peningkatan berkelanjutan. Pendekatan multilapis yang meliputi enkripsi data, autentikasi dua faktor (2FA), firewall, serta *Intrusion Detection System* (IDS) berfungsi sebagai fondasi utama dalam membangun ketahanan sistem terhadap berbagai bentuk ancaman siber. Setiap kontrol keamanan dirancang untuk menanggapi tipe ancaman yang berbeda, seperti pencurian data, akses ilegal, hingga eksploitasi kerentanan sistem.

Dari perspektif organisasi, peningkatan kepatuhan pengguna terhadap kebijakan keamanan informasi menjadi indikator keberhasilan implementasi ISMS. Mekanisme *Role-Based Access Control* (RBAC) memastikan penggunaan sumber daya laboratorium berjalan secara terkendali dan sesuai dengan kebutuhan operasional. Kebijakan *backup* otomatis juga memberikan perlindungan tambahan dalam menghadapi potensi kehilangan data akibat insiden ataupun serangan siber. Temuan ini menunjukkan bahwa intervensi kebijakan yang tepat dapat berkontribusi terhadap peningkatan keamanan operasional secara keseluruhan.

Meskipun demikian, implementasi ISO 27001 masih menghadapi tantangan, terutama terkait faktor manusia. Kurangnya pemahaman dan kesadaran pengguna masih menjadi sumber utama kerentanan sistem. Oleh karena itu, pelatihan berkala, sosialisasi prosedur, dan peningkatan literasi keamanan informasi perlu dilakukan secara sistematis untuk memperkuat pertahanan terhadap kesalahan pengguna (*human error*). Penguatan kapasitas SDM menjadi komponen penting dalam memastikan bahwa kebijakan keamanan dapat diterapkan secara konsisten dan efektif.

Selain aspek perilaku, tantangan lain muncul dari dinamika ancaman siber yang terus berkembang. Oleh sebab itu, sistem keamanan harus diperbarui secara berkala dan didukung oleh proses audit internal maupun eksternal sesuai prinsip *continuous improvement* dalam ISO 27001. Audit berfungsi untuk mengevaluasi tingkat kepatuhan sekaligus mengidentifikasi kelemahan serta peluang peningkatan pada sistem keamanan yang telah diterapkan. Pendekatan ini memastikan bahwa kontrol keamanan tetap relevan, adaptif, dan responsif terhadap ancaman baru.

Selanjutnya, penerapan ISO 27001 harus diintegrasikan dengan proses manajemen risiko yang komprehensif. Melalui pemetaan risiko yang sistematis, organisasi dapat mengidentifikasi potensi ancaman, menilai dampak, serta menentukan kontrol mitigasi yang paling tepat bagi setiap aset informasi. Sistem pengamanan juga perlu terintegrasi dengan prosedur operasional standar (SOP) untuk memastikan konsistensi implementasi di seluruh unit laboratorium. Integrasi tersebut berperan penting dalam meminimalkan peluang terjadinya insiden yang disebabkan oleh ketidakteraturan prosedural.

Penerapan ISO 27001 juga mendorong terbentuknya budaya keamanan informasi yang kuat. Kesadaran kolektif yang berkembang dalam organisasi mengenai pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data menjadi faktor penting dalam memastikan keberlanjutan keamanan informasi. Dalam konteks teknologi, penerapan *real-time monitoring* memperkuat kemampuan deteksi dini terhadap aktivitas anomali dan potensi ancaman. Ketika dikombinasikan dengan analisis log berbasis kecerdasan buatan, sistem mampu mengidentifikasi pola serangan yang tidak terdeteksi oleh metode tradisional.

Selain kontrol teknis dan kesadaran SDM, keberhasilan jangka panjang dari ISO 27001 sangat bergantung pada kualitas dokumentasi dan integrasi prosedural. Standar ini menuntut setiap kontrol keamanan yang diimplementasikan harus didukung oleh kebijakan, prosedur, dan catatan yang terstruktur. Dokumentasi yang komprehensif, seperti Pernyataan Penerapan (*Statement of Applicability*—SoA) dan dokumen manajemen risiko, memastikan bahwa kontrol keamanan selaras dengan kebutuhan bisnis inti laboratorium dan tidak hanya bersifat *ad-hoc*. Integrasi keamanan informasi ke dalam proses operasional standar harian (*Standard Operating Procedures*) juga menjadi kunci, karena hal ini menghilangkan hambatan prosedural dan memastikan bahwa keamanan bukan hanya proyek sekali jadi, melainkan bagian integral dari budaya kerja yang berkesinambungan.

Keberhasilan implementasi ISO 27001 dalam jangka panjang sangat bergantung pada komitmen manajemen puncak. Dukungan kebijakan, pendanaan, peningkatan kapasitas SDM, serta investasi berkelanjutan pada teknologi keamanan menjadi elemen fundamental yang memastikan sistem keamanan informasi dapat bertahan dan berkembang. Dengan dukungan manajerial yang kuat, organisasi dapat membangun ekosistem keamanan informasi yang adaptif, berstandar internasional, serta mampu menjawab tantangan keamanan siber di masa depan.

4. KESIMPULAN

Implementasi sistem pengamanan data berbasis ISO 27001 telah berhasil meningkatkan keamanan informasi di laboratorium. Dengan penerapan standar ini, berbagai potensi risiko dapat diminimalkan melalui pendekatan sistematis dan terstruktur. Pendekatan ini sangat penting mengingat hasil analisis risiko menunjukkan bahwa tingkat risiko rata-rata berada dalam kategori Tinggi hingga Sangat Tinggi sebelum implementasi, yang memerlukan kontrol pengamanan yang lebih ketat. Penggunaan teknologi seperti enkripsi data, firewall, dan autentikasi dua faktor terbukti secara signifikan mampu mengurangi risiko serangan siber yang dapat mengancam integritas dan kerahasiaan informasi. Sistem keamanan berlapis (*defense-in-depth*), yang mencakup penerapan Enkripsi AES-256 dan penggunaan Firewall bersama Intrusion Detection System (IDS), memastikan perlindungan yang komprehensif terhadap berbagai jenis ancaman, baik teknis maupun dari jaringan luar.

Namun demikian, keberhasilan sistem ini tidak hanya bergantung pada aspek teknis semata, tetapi juga memerlukan dukungan dari aspek sumber daya manusia. Penelitian ini menemukan bahwa meskipun sistem teknis sudah kuat, faktor kelalaian manusia masih menjadi sumber kerentanan yang perlu diatasi, sejalan dengan prinsip ISO 27001 yang mengedepankan keterlibatan seluruh pihak. Oleh karena itu, pelatihan rutin bagi pengguna laboratorium sangat diperlukan untuk meningkatkan kesadaran dan pemahaman terkait pentingnya menjaga keamanan informasi.

Peningkatan kesadaran ini terlihat dari perbaikan yang signifikan pada perilaku pengguna, seperti peningkatan yang kuat dalam penggunaan autentikasi dua faktor, praktik penyimpanan data yang aman, serta inisiatif pelaporan insiden keamanan. Selain itu, audit keamanan secara berkala juga harus dilakukan untuk memastikan bahwa sistem yang telah diterapkan tetap berjalan sesuai dengan standar ISO 27001 dan mampu beradaptasi terhadap potensi ancaman baru yang terus berkembang. Proses audit ini, yang merupakan bagian integral dari prinsip *continuous improvement* pada ISO 27001, bertujuan untuk mengidentifikasi kelemahan yang mungkin muncul dari dinamika ancaman siber dan memastikan bahwa kontrol keamanan tetap relevan dan responsif. Komitmen dan dukungan berkelanjutan dari manajemen puncak dalam hal kebijakan, pendanaan, dan investasi teknologi yang menjadi elemen fundamental untuk menjaga sistem keamanan informasi agar adaptif, andal, dan berstandar internasional.

UCAPAN TERIMA KASIH

Penulis menyampaikan rasa terima kasih dan apresiasi yang tulus dan sebesar-besarnya kepada Universitas Muhammadiyah Jember. Institusi ini telah menjadi fondasi utama yang memungkinkan terlaksananya penelitian ini dengan memberikan dukungan institusional, fasilitas memadai, serta kesempatan akademik yang sangat berharga. Segala bentuk dukungan tersebut merupakan katalis penting dalam menjamin kelancaran setiap tahapan penelitian hingga rampung. Selain itu, ucapan terima kasih yang mendalam juga secara khusus disampaikan kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Muhammadiyah Jember. Peran LPPM sangat signifikan melalui bantuan, arahan, dan bimbingan teknis yang berkelanjutan, mulai dari tahap perencanaan, pelaksanaan, hingga penyelesaian akhir laporan penelitian ini. Kontribusi mereka telah memastikan bahwa penelitian ini berjalan sesuai dengan kaidah ilmiah dan standar yang berlaku.

Akhir kata, penulis menghaturkan terima kasih yang tak terhingga kepada semua pihak yang telah memberikan kontribusi, baik secara langsung dalam bentuk asistensi teknis dan konsultasi, maupun secara tidak langsung melalui dukungan moral dan penyediaan data. Dedikasi dan bantuan dari berbagai pihak tersebut memungkinkan penelitian ini dapat diselesaikan dengan baik dan menghasilkan temuan yang bermanfaat bagi pengembangan ilmu di lingkungan laboratorium Teknik Informatika.

REFERENSI

[1] I. . P. Jovano, I. R. Padiku, and B. Ahaliki, “Analisis Manajemen Risiko dan Keamanan Sistem Informasi Akademik Terpadu (SIAT) Universitas Negeri Gorontalo Menggunakan Framework NIST SP 800-30,” *Journal of Systems and Information Technology*, vol. 5, no. 1, pp. 135–144, 2025.

[2] N. Ibrahim, “Examining the Influence of Advanced Persistent Threats on Higher Education Institutions and Investigating Appropriate Cybersecurity Strategies,” vol. 2, pp. 96–119, 2025, doi: 10.24840/2183-6493.

[3] F. Anis Sekar Ningrum, Y. Riwanto, I. Yanuar Risca Pratiwi, and M. A. Fikri, “Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI,” *Jurnal Informatika Polinema*, vol. 10, no. 3, pp. 437–444, 2024.

[4] N. Ramadhanty, “Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber,” *Journal of Indonesian Management*, vol. 4, no. 4, pp. 1–9, 2024, doi: 10.53697/jim.v4i4.1973.

[5] S. Clarissa and G. Wang, “Assessing Information Security Management Using ISO 27001:2013,” *Jurnal Indonesia Sosial Teknologi*, vol. 4, no. 9, pp. 1361–1371, 2023, doi: 10.59141/jist.v4i9.739.

[6] F. C. Arumdiya and C. Rudianto, “Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi,” vol. 06, no. 02, pp. 167–186, 2021.

[7] S. Mahmood, M. Chadhar, and S. Firmin, “Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective,” *Applied Sciences (Switzerland)*, vol. 14, no. 24, 2024, doi: 10.3390/app142411610.

[8] E. Susanto and N. Legowo, “Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001,” vol. 12, no. 2, pp. 155–164, 2023.

[9] F. Husaeni, N. Sulistiyowati, and A. Rizal, “EVALUASI PENGELOLAAN ASET LABORATORIUM KOMPUTER MENGGUNAKAN STANDAR ISO / IEC 27001,” vol. 9, 2018.

[10] A. Hafiz, “TREN IMPLEMENTASI ISO 27001 SISTEM MANAJEMEN KEAMANAN INFORMASI PADA PERGURUAN TINGGI (LITERATURE REVIEW),” no. 2, pp. 159–163, 2025.

[11] S. Ray, J. Das, R. Pande, and A. Nithya, “Swati Ray 1 , Joyati Das 2* , Ranjana Pande 3 , and A. Nithya 2,” vol. 4, no. 2, pp. 195–222, 2025, doi: 10.1201/9781032622408-13.

[12] Sintiya Cahya Maulany, Ety Meikhati, and Putri Intan Prastiwi, “Integrasi Teknologi Informasi Akuntansi dan Proteksi Sistem Informasi Akuntansi terhadap Cybersecurity Accounting di Era Digital,” *Akuntansi Pajak dan Kebijakan Ekonomi Digital*, vol. 2, no. 3, pp. 216–231, 2025, doi: 10.61132/apke.v2i3.1429.

[13] J. Task and F. Transformation, “Guide for Conducting Risk Assessments,” no. September, 2012.