TADWIN : Jurnal Ilmu Perpustakaan dan Informasi
Available online at: https://jurnal.radenfatah.ac.id/index.php
Vol. 6 No. 1, Juni 2025, halaman: 141-154
Copyright ©2020, ISSN: 27232409 print/online 2774-8936
https://doi.org/xx

Evaluasi Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001 di Perpustakaan Universitas Nasional

Afifah Nur Fadilah[1], Dwi Fajar Saputra[2*], Ibnu Fyras Maulana[3], Muhammad Jordan A. N[4], Dzaki Rizky Jumayyil[5], Sarah Aurelia T. M. S[6], Saffana Mufiddah Adhayanti[7], Saffana Mufiddah Adhayanti[8]

[1234567] Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia
*Korespondensi email: dwifajar@upnvj.ac.id

Information

Submited: 27-05-2025
Revised: 26-06-2025
Accepted: 8-07-2025

How to cite: Evaluasi Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001 di Perpustakaan UNAS. (2025). *TADWIN: Jurnal Ilmu Perpustakaan Dan Informasi*, *6* (1), 141-154. https://doi.org/xx

DOI:

First Publication Right:
Tadwin: Jurnal Ilmu Perpustakaan dan Informasi Program Studi Ilmu Perpustakaan, Fakultas Adab dan Humaniora, UIN Raden Fatah Palembang, Indonesia

ABSTRACT

As the utilization of digital systems continues to grow, libraries must strengthen their information management systems to protect against threats such as cyberattacks and data breaches. This study employed a descriptive qualitative approach using interviews, observation, and documentation. The findings indicate that several ISO/IEC 27001 based controls have been implemented, including firewalls, encryption, and regular audits. However, security gaps remain, such as weak credentials, the absence of multi-factor authentication, and limited real-time monitoring and data backup. Major risks include malware, network attacks, and system failures. Although the National University (UNAS) Cyber Library has developed a Disaster Recovery Plan (DRP), improvements in formal documentation and user digital literacy are still needed. These findings serve as a strategic evaluation basis for enhancing the effectiveness of information security governance in academic library environments.

Keywords: *Information Security; ISO/IEC 27001;Library*

Abstrak

Pemanfaatan terhadap sistem digital, perpustakaan perlu memperkuat sistem pengelolaan informasi agar terlindung dari ancaman seperti serangan siber dan kebocoran data. Penelitian dilakukan dengan pendekatan kualitatif deskriptif melalui wawancara, observasi, dan dokumentasi. Hasilnya menunjukkan bahwa beberapa kontrol berbasis ISO/IEC 27001 telah diterapkan, seperti firewall, enkripsi, dan audit berkala. Namun, ditemukan celah keamanan berupa lemahnya kredensial, absennya autentikasi ganda, serta keterbatasan pemantauan dan pencadangan data secara real-time. Risiko utama meliputi malware, serangan jaringan, dan kegagalan sistem. Meskipun Perpustakaan Cyber Library UNAS telah memiliki rancangan Disaster Recovery Plan (DRP), penguatan dokumentasi dan peningkatan literasi digital pengguna masih diperlukan. Temuan ini menjadi dasar evaluasi strategis dalam pengembangan tata kelola keamanan informasi yang lebih efektif di lingkungan perpustakaan perguruan tinggi.

Kata kunci: ISO/IEC 27001; Keamanan Informasi; Perpustakaan

1. PENDAHULUAN

Perkembangan teknologi informasi semakin pesat, keamanan informasi merupakan hal krusial yang perlu diperhatikan setiap institusi, termasuk perguruan tinggi (Cheng & Wang, 2022). Saat ini, informasi merupakan aset penting yang harus dijaga (Farid et al., 2023), mengacu pada keamanan informasi yaitu perlindungan terhadap kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* data (Rahmat, 2019). Tanpa perlindungan yang memadai, sistem akan rentan terhadap berbagai ancaman, mulai dari kebocoran data hingga serangan siber yang tidak hanya dapat mengganggu operasional, tetapi juga dapat menyangkut dengan reputasi institusi (Aslan et al., 2023). Perpustakaan universitas merupakan salah satu unit kerja yang kini juga turut mengandalkan sistem informasi dalam mendukung operasional sehari-hari (Spring et al., 2022).

Transformasi digital mendorong perpustakaan untuk berperan sebagai pusat informasi yang berbasis teknologi (Ikenwe & Udem, 2022), layanan perpustakaan tidak lagi terbatas hanya penyedia koleksi fisik (Ruthven et al., 2023), tetapi juga menjadi pusat informasi digital dan memiliki peran penting dalam pengelolaan aset perpustakaan, seperti koleksi pustaka, arsip, identitas pengguna, dan data sensitif lainnya (Onunka et al., 2023). Tantangan keamanan informasi kini tidak semata hanya dari sisi teknis, melainkan juga dari lemahnya tata kelola atau minimnya regulasi internal (Dunn Cavelty & Smeets, 2023). Keamanan informasi juga menuntut struktur manajemen risiko, perencanaan pemulihan bencana, serta keterlibatan aktif seluruh pemangku kepentingan, termasuk pengguna layanan (AL-Dosari & Fetais, 2023). Oleh karena itu, sistem informasi serta pengelolaan menjadi hal penting yang harus diperhatikan dan dikelola agar tidak hanya berjalan secara efisien (Mehmood, 2021), tetapi juga mampu menjamin keamanan data yang disimpan (Taherdoost, 2023). Untuk memastikan hal itu, dibutuhkan penerapan standar manajemen keamanan informasi yang terstruktur (Folorunso et al., 2024).

Salah satu standar yang banyak digunakan adalah SNI ISO/IEC 27001, yang menyediakan kerangka kerja sistematis dalam menerapkan serta memelihara sistem manajemen keamanan informasi (SMKI) atau *Information Security Management System (ISMS)* (Jevelin & Faza, 2023). Beberapa penelitian sudah banyak yang mengkaji mengenai penerapan ISO/IEC 27001 dalam bidang perpustakaan. Salah satunya adalah penelitian yang dilakukan oleh Bahrudin & Firmansyah (2018), yang membahas mengenai penerapan ISO/IEC 27001 pada perpustakaan, hasilnya menunjukkan bahwa penerapan standar ini dapat membantu perpustakaan dalam memperkuat kontrol keamanan informasi, tetapi mereka juga menemukan kendala seperti minimnya sumber daya manusia (SDM), infrastruktur yang kurang memadai, dan kurangnya pelatihan teknis yang menjadi hambatan utama dalam proses implementasinya.

Sementara itu Fattah Ys et al. (2024) melakukan penelitian pada perpustakaan nasional RI yang juga menyebut bahwa dengan adanya ISO 27001 memberikan kerangka kerja yang lebih terstruktur bagi perpusnas, Fattah et al juga menyoroti lemahnya dokumentasi aset informasi, masih rentannya serangan hacker karena kurangnya pemantauan dalam pengelolaan informasi, dan untuk semua server belum tersedia kembali ke server *back-up*. Kedua penelitian tersebut memberikan gambaran mengenai manfaat dan hambatan dalam penerapan ISO/IEC 27001 dalam tata kelola keamanan informasi di lingkungan perpustakaan. Melihat pentingnya kebutuhan akan penguatan keamanan informasi di lingkungan perpustakaan, artikel ini disusun untuk mengevaluasi sejauh mana penerapan SNI ISO/IEC 27001 telah diimplementasikan dalam tata kelola keamanan informasi di perpustakaan Universitas Nasional (UNAS). Selain itu, artikel ini juga memberikan kontribusi dengan menyusun rekomendasi strategis untuk meningkatkan efektivitas pengelolaan keamanan informasi yang relevan dengan kondisi aktual institusi tersebut. Dengan menggunakan pendekatan kualitatif melalui wawancara dan observasi,

artikel ini diharapkan dapat memberikan gambaran nyata mengenai tingkat kesiapan, hambatam, serta peluang untuk peningkatan keamanan informasi.

2. TINJAUAN PUSTAKA

1. ISO/IEC 27001 dan Sistem Manajemen Keamanan Informasi (SMKI)

   ISO/IEC 27001 adalah standar internasional yang menyediakan kerangka kerja lengkap untuk manajemen keamanan data. Untuk melindungi kerahasiaan, integritas, dan ketersediaan data, organisasi harus menerapkan Information Security Management System (ISMS) sesuai dengan standar ini International Organization for Standardization (2013) Untuk melindungi koleksi digital, data pengguna, dan sistem layanan informasi yang semakin terintegrasi secara digital, SMKI menjadi sangat penting bagi perpustakaan (International Organization for Standardization, 2013). ISO/IEC 27001 memungkinkan organisasi untuk mengidentifikasi ancaman secara sistematis, menetapkan kontrol keamanan yang relevan, dan melakukan audit dan pemantauan kebijakan secara berkala. Sebagai bagian dari strategi keamanan yang menyeluruh, standar ini mencakup perlindungan teknis selain kebijakan internal, prosedur operasional, dan instruksi staf. Ini menciptakan lingkungan informasi yang aman dan andal bagi seluruh pemustaka.

2. Tata Kelola Keamanan Informasi di Institusi Pendidikan

   Menurut Posthumus & von Solms (2004), manajemen bertanggung jawab untuk mengatur dan memantau kebijakan, peran, dan proses yang berkaitan dengan perlindungan informasi. Tugas ini disebut tata kelola keamanan informasi (Posthumus & von Solms, 2004). Ini termasuk prosedur operasi standar (SOP), pelatihan rutin, dan mekanisme kontrol akses di perpustakaan. Galih (2020) menyatakan bahwa beberapa faktor yang dapat mengganggu keamanan sistem perpustakaan termasuk kegagalan firewall, kebijakan internal yang tidak konsisten, dan kurangnya instruksi staf. Akibatnya, untuk mendukung penerapan SMKI yang efektif, diperlukan penguatan tata Kelola (Galih, 2020).

3. Riset Terkait Perpustakaan Berbasis ISO/IEC 27001

   Kerangka kerja COBIT (Control Objectives for Information and Related Technologies) dan ISO/IEC 27001 merupakan dua pendekatan penting dalam mendukung tata kelola teknologi informasi di organisasi, termasuk di lingkungan perpustakaan. COBIT, yang dikembangkan oleh ISACA, menyediakan panduan menyeluruh untuk menyelaraskan strategi TI dengan tujuan bisnis melalui pengelolaan risiko, pemantauan operasional, dan evaluasi kinerja keamanan (ISACA, 2019). Sementara itu, ISO/IEC 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) yang berfokus pada perlindungan kerahasiaan, integritas, dan ketersediaan data (CIA triad). Standar ini menggunakan pendekatan manajemen risiko dan siklus PDCA (Plan-Do-Check-Act) untuk mengelola keamanan informasi secara menyeluruh (International Organization for Standardization, 2013). Integrasi keduanya dapat memperkuat implementasi keamanan informasi sekaligus memperjelas struktur tata kelola, peran dan tanggung jawab, serta sistem audit dan pengukuran kinerja secara berkala. Dalam konteks perpustakaan, sinergi ini memungkinkan sistem informasi dikelola secara strategis dan berkelanjutan, sejalan dengan nilai transparansi dan akuntabilitas lembaga.

4. Perancangan Disaster Recovery Plan (DRP) di Institusi Informasi

Literasi digital merupakan komponen kunci dalam keberhasilan implementasi keamanan informasi, terutama di era digital yang sarat risiko. Literasi ini tidak hanya mencangkup kemampuan teknis untuk menggunakan perangkat, tetapi juga pengetahuan tentang ancaman siber, etika penggunaan data, dan cara menyaring data dengan aman. Menurut San Nicolas-Rocca & Burkhard (2019) literasi digital harus menjadi komponen penting dari strategi keamanan organisasi. Literasi digital dalam perpustakaan berarti mendidik karyawan dan pengguna tentang bahaya digital seperti keamanan akun, perlindungan data, dan cara menghindari phishing (San Nicolas-Rocca & Burkhard, 2019). Menurut penelitian Perpustakaan UNAS, meskipun sistem keamanan telah dimulai, orang masih kurang memahami tentang keamanan data. Oleh karena itu, untuk mendukung sistem keamanan informasi yang berkelanjutan dan menyeluruh, pelatihan rutin, sosialisasi kebijakan, dan pelatihan pengguna harus dipromosikan.

5. Peran Literasi Digital dan Edukasi Pengguna

Studi tentang penerapan ISO/IEC 27001 di perpustakaan telah menunjukkan bahwa ada peningkatan besar dalam keamanan data. Menurut Bahrudin & Firmansyah (2018) standar ini membantu memperkuat kontrol sistem dan mengurangi risiko kebocoran data. Namun, ada kendala seperti kurangnya pelatihan teknis dan dokumentasi yang tidak sesuai (Bahrudin & Firmansyah, 2018). Selain itu, Fattah Ys et al.(2024) melakukan penelitian di Perpustakaan Nasional RI menemukan bahwa, meskipun sebagian besar kontrol telah dirancang, mereka masih kurang dalam hal evaluasi risiko berbasis aset dan penanganan insiden (Fattah Ys et al, 2024). Hasil ini sejalan dengan situasi di Perpustakaan UNAS, di mana sistem keamanan telah dimulai dengan backup data, firewall, dan log sistem, tetapi dokumentasi DRP dan pemantauan insiden masih kurang. Hal ini menunjukkan bahwa penerapan pendekatan sistematis dan manajerial sangat penting untuk menerapkan ISO 27001.

Perbandingan Manajemen Kelola Sebelum dan Sesudah Implementasi ISO/IEC 27001 di Perpustakaan UNAS

Sebagai bentuk review terhadap dua program dalam objek penelitian yang sama, kajian ini membandingkan kondisi keamanan informasi Perpustakaan Universitas Nasional (UNAS) sebelum dan sesudah adanya proses penerapan standar ISO/IEC 27001. Perbandingan ini dilakukan untuk menilai efektivitas perubahan kebijakan, infrastruktur, serta kesiapan sumber daya yang diimplementasikan seiring dengan adopsi standar internasional tersebut. Sebelum menerapkan ISO/IEC 27001, sistem keamanan informasi di Perpustakaan UNAS belum memiliki kerangka kerja yang baku. Tidak terdapat regulasi resmi mengenai kekuatan password, proses backup data dilakukan secara manual dan tidak terjadwal, serta belum tersedia sistem pemantauan lalu lintas secara real-time.

Selain itu, dokumentasi risiko dan prosedur pemulihan pasca-insiden belum diatur secara formal, sehingga potensi gangguan pada layanan perpustakaan cukup tinggi.Setelah implementasi standar, terjadi transformasi yang signifikan. Perpustakaan UNAS mulai menggunakan *Web Application Firewall (WAF)* untuk melindungi sistem dari serangan injeksi perintah dan XSS, menerapkan enkripsi data SSL/TLS, serta menyusun kerangka *Disaster Recovery Plan* (DRP) meskipun masih dalam tahap dokumentasi lanjutan. Audit keamanan juga telah dilakukan secara berkala, dan sistem monitoring sudah mulai difungsikan untuk mendeteksi anomali secara real-time. Walaupun penerapannya masih bertahap, sistem telah menunjukkan peningkatan kapabilitas dalam mitigasi risiko keamanan informasi. Berikut ini adalah perbandingan sistem keamanan informasi sebelum dan sesudah adanya proses penerapan ISO/IEC 27001:

Tabel 1. Perbandingan Tinjauan Pustaka

No	Aspek	Sebelum ISO/IEC 27001	Setelah adanya Proses Penerapan ISO/IEC 27001
1.	Kebijakan Password	Belum ada standar	Ditetapkan kebijakan password kuat
2.	Sistem Backup	Manual, tidak terjadwal	Mingguan, dengan disiapkan server cadangan
3.	Monitoring Sistem	Tidak tersedia	Pemantauan real-time dengan perangkat lunak
4.	Prosedur Pemulihan (DRP)	Belum tersedia	Disusun dalam bentuk rencana terstruktur
5.	Perlindungan Data	Tidak ada enkripsi	Menggunakan SSL/TLS untuk proteksi data
6.	Pelatihan Staf	Belum dilakukan	Mulai dilakukan secara bertahap

Perbandingan internal di Perpustakaan UNAS menunjukkan bahwa meskipun belum sepenuhnya ideal, implementasi ISO/IEC 27001 telah memberikan arah perbaikan yang signifikan terhadap pengelolaan keamanan informasi. Analisis dua kondisi sistem ini juga memberikan pembelajaran berharga mengenai pentingnya kebijakan, infrastruktur, serta kesiapan sumber daya manusia dalam membangun sistem yang tangguh

3. METODE PENELITIAN

Di dalam penelitian ini, peneliti menggunakan pendekatan kualitatif deskriptif yang memungkinkan untuk mendapatkan informasi yang lebih mendalam mengenai implementasi dan evaluasi keamanan informasi berbasi ISO/IEC 27001 pada perpustakaan UNAS. Creswell menjelaskan dalam bukunya yang berjudul Research Design bahwa penelitian kualitatif merupakan suatu pendekatan untuk mengeksplorasi dan memahami makna yang diberikan individu atau kelompok terhadap suatu masalah sosial atau manusia yang melibatkan metode pengumpulan data seperti wawancara, observasi, dan analisis dokumen, yang kemudian dianalisis secara induktif untuk membentuk tema atau pola tertentu (Creswell & Creswell, 2017).

Teknik yang digunakan pada penelitian ini untuk mendapatkan data yang mendalam untuk menjawab pertanyaan penelitian yaitu:

1. Wawancara

   Menurut Yusuf (2016), wawancara (*Interview)* merupakan suatu proses interaksi antara pewawancara *(interviewer)* dan narasumber *(interviewee)* melalui komunikasi langsung (Yusuf, 2016) . wawancara ini merupakan salah satu alat yang paling sering digunakan pada penelitian kualitatif. Dalam penelitian ini wawancara yang dilakukan oleh peneliti adalah wawancara terencana - terstruktur dimana kami sebagai peneliti membuat pedoman pertanyaan, membacakan pertanyaan sesuai urutan dan mencatat hasil wawancara. Wawancara dilakukan pada hari Kamis, 19 Juni 2025 di *Digital Library* Perpustakaan UNAS. Pemilihan informan peneliti serahkan kepada pihak perpustakaan UNAS, namun kriteria dari peneliti ialah seseorang yang sesuai dengan bidang fokus penelitian peneliti. Dalam hal ini peneliti mewawancarai dua pustakawan dari perpustakaan UNAS yaitu Y dan R, yang keduanya dibantu oleh jawaban dari BPTSI UNAS sesuai pertanyaan yang sudah kami kirim sebelumnya.

2. Dokumentasi

Dokumentasi adalah Metodologi yang digunakan untuk akuisisi data memfasilitasi pemeriksaan catatan sejarah. Dokumen yang berkaitan dengan individu atau kolektif, serta peristiwa atau insiden dalam konteks sosial, sangat bermanfaat untuk penyelidikan kualitatif (Yusuf, 2016). Dalam penelitian ini peneliti menggunakan teknik dokumentasi untuk mengumpulkan data sekunder dari jurnal, arsip, dan buku untuk mendukung penelitian ini.

Dalam penelitian ini teknik analisis data yang digunakan menggunakan model dari Miles, Huberman, & Saldaña (2014) yang membagi analisis data menjadi tiga alur kegiatan, yaitu reduksi data (data reduction), penyajian data (data display), serta penarikan kesimpulan atau verifikasi (Miles, Huberman, & Saldaña, 2014).

1. Reduksi Data
   Reduksi data dikonseptualisasikan sebagai proses metodologis pemilihan dan berkonsentrasi pada penyederhanaan, abstraksi, dan transformasi data "mentah" yang berasal dari pengamatan lapangan. Proses reduksi data dimulai bersamaan dengan inisiasi pengumpulan data, meliputi kegiatan seperti pembuatan ringkasan, pengkodean, eksplorasi tematik, dan komposisi memo, di antara tugas-tugas lainnya. Tujuan reduksi data adalah untuk menghilangkan data atau informasi asing, setelah itu data yang tersisa menjalani proses verifikasi.

2. Penyajian data
   Penyajian data merupakan penjelasan dari kumpulan informasi yang disintesis yang memungkinkan derivasi kesimpulan dan pelaksanaan tindakan. Representasi data kualitatif diartikulasikan dalam bentuk teks naratif, dengan tujuan menggabungkan informasi secara koheren dan dapat dipahami.

3. Penarikan kesimpulan atau verifikasi
   Kesimpulan mewakili sintesis hasil penelitian yang mengartikulasikan pernyataan akhir berdasarkan deskripsi atau penentuan sebelumnya yang diperoleh melalui metodologi penalaran induktif atau deduktif. Kesimpulan yang ditetapkan harus berkaitan dengan topik penelitian, tujuan penelitian, dan temuan penelitian yang telah ditafsirkan dan dibahas. Akibatnya, kesimpulan dalam penelitian kualitatif memang dapat mengatasi formulasi masalah yang diajukan di awal; Namun, mereka mungkin sama-sama gagal melakukannya, karena telah diindikasikan sebelumnya bahwa masalah dan formulasi masalah dalam penelitian kualitatif masih bersifat sementara dan berkembang begitu peneliti terlibat dalam kerja lapangan atau memulai penyelidikan mereka.

4. HASIL DAN PEMBAHASAN

Penelitian ini mengevaluasi bagaimana Perpustakaan Universitas Nasional (UNAS) menerapkan prinsip-prinsip tata kelola keamanan informasi berdasarkan kerangka kerja ISO/IEC 27001. Temuan dikategorikan ke dalam empat aspek utama, yaitu:

Kebijakan dan Prosedur Keamanan Informasi

Perpustakaan Universitas Nasional (UNAS) telah menerapkan kebijakan dan prosedur keamanan informasi yang merujuk pada prinsip-prinsip ISO/IEC 27001. Kebijakan ini ditujukan untuk menjaga integritas, kerahasiaan dan ketersediaan informasi dalam pengelolaan arsip digital maupun fisik. Beberapa prosedur utama yang dijalankan mencakup enkripsi data, otorisasi berbasis peran hingga

pemantauan sistem secara real-time. Perpustakaan UNAS juga menetapkan penggunaan SSL/TLS untuk menjamin enkripsi data dalam transmisi, serta enkripsi penyimpanan untuk melindungi arsip digital yang sensitif. Untuk membatasi akses, diterapkan Role Based Access Control (RBAC) yang memastikan bahwa hanya pengguna dengan hak tertentu yang dapat mengakses atau mengelola data. Perpustakaan unas dari sisi perlindungan fisik menjaga ketat akses ke ruang arsip dan coba dibatasi hanya personel yang berwenang. Ruangan dilengkapi dengan sistem keamanan seperti CCTV, kunci khusus, serta pengaturan suhu dan kelembaban guna menjaga kondisi dokumen fisik.

Kebijakan keamanan juga mencakup pelaksanaan backup data secara rutin setiap minggu serra penggunaan sistem deteksi dini seperti firewall dan sistem pemantauan intrusi (Intrusion Detection System/IDS) yang mampu mendeteksi upaya akses tidak sah. Dalam menghadapi insiden keamanan, perpustakaan UNAS memiliki prosedur respons insiden yang dimulai dari deteksi insiden isolasi sistem terdampak hingga pemulihan sistem. seluruh insiden didokumentasikan agar menjadi evaluasi untuk mencegah hal serupa. Audit internal dilaksanakan setiap bulan untuk menilai tingkat kepatuhan terhadap kebijakan serta efektivitas kontrol yang diterapkan . Selain itu, untuk mendukung implementasi kebijakan, perpustakaan UNAS juga menggunakan ISMS tools yang memungkinkan pemantauan dan pelaporan secara sistematis terhadap seluruh proses keamanan informasi.

Struktur Organisasi dan Peran Sumber Daya Manusia

Dalam penerapan tata kelola keamanan informasi berbasis ISO/IEC 27001, Struktur organisasi di perpustakaan Universitas Nasional (UNAS) memiliki peranan yang cukup penting dalam menjamin efektivitas implementasi kebijakan keamanan. peran penting dalam menjamin efektivitas implementasi kebijakan keamanan. Struktur ini tidak hanya menggambarkan pembagian tanggung jawab, tetapi juga mendukung kolaborasi lintas bagian untuk menjawab tantangan keamanan informasi yang kompleks dan dinamis.

Perpustakaan UNAS memiliki tim sistem informasi yang terdiri dari tenaga profesional di bidang IT dan keamanan informasi. Tim ini bertanggung jawab atas perencanaan, pelaksanaan, serta pemantauan kontrol keamanan informasi. Mereka juga memimpin proses audit internal, mitigasi risiko, serta respons terhadap insiden keamanan. Peran-peran utama dalam SDM yang terlibat meliputi:

1. Administrator Sistem: Bertugas mengelola server, sistem penyimpanan arsip digital, firewall, dan sistem enkripsi. Mereka memastikan stabilitas dan keamanan sistem operasional harian.
2. Tim Respons Insiden: Berperan aktif dalam menangani kejadian pelanggaran keamanan, mulai dari deteksi, isolasi, investigasi, hingga pemulihan dan pelaporan.
3. Petugas Pengelola Arsip: Bertanggung jawab dalam menjaga keamanan arsip fisik maupun digital, termasuk memastikan prosedur backup berjalan sesuai jadwal dan protokol akses diikuti dengan ketat.
4. Staf Keamanan Fisik dan Fasilitas: Memastikan pengawasan terhadap ruangan penyimpanan arsip non-digital dengan sistem kunci, kontrol akses, dan pemantauan CCTV.
5. Pengguna Layanan (end-user): Diberikan pelatihan dasar mengenai kebijakan penggunaan akun, tata cara unggah file yang aman, serta pentingnya menjaga keamanan kredensial pribadi.

Meskipun demikian, wawancara menunjukkan bahwa tantangan utama yang masih dihadapi adalah keterbatasan jumlah personel yang secara khusus ditugaskan dalam pengelolaan keamanan informasi. Hal ini menuntut efisiensi kerja dan kolaborasi yang tinggi antar unit kerja. Oleh karena itu, Perpustakaan UNAS menerapkan strategi pelatihan berkala untuk meningkatkan kapasitas staf dalam memahami dan melaksanakan kebijakan keamanan informasi yang telah ditetapkan. Penguatan peran

SDM ini menjadi pondasi penting dalam menjaga integritas sistem keamanan informasi di lingkungan perpustakaan, sejalan dengan prinsip *people, process, and technology* dalam kerangka kerja ISO/IEC 27001

Kesadaran dan Literasi Keamanan Informasi

Salah satu aspek penting dalam tata kelola keamanan informasi di Perpustakaan UNAS adalah kesadaran dan literasi pengguna terhadap risiko serta prosedur keamanan informasi. Berdasarkan hasil wawancara dengan tim pengelola sistem informasi, ditemukan bahwa rendahnya kesadaran pengguna menjadi salah satu faktor risiko utama dalam pengelolaan arsip digital. Pengguna sering kali mengunggah file tanpa terlebih dahulu memverifikasi keamanannya, serta menggunakan kredensial yang lemah seperti kombinasi username dan password yang mudah ditebak. Hal ini menunjukkan bahwa kelemahan bukan hanya bersumber dari sistem teknis, melainkan juga dari aspek perilaku manusia (human factor) dalam ekosistem informasi.

Perpustakaan UNAS sendiri telah melakukan beberapa upaya untuk membangun budaya keamanan melalui edukasi internal. Misalnya, penguatan kebijakan penggunaan password yang kuat dan himbauan penggunaan autentikasi dua faktor (2FA) telah diterapkan, meskipun belum secara menyeluruh. Namun, keterbatasan dalam pelatihan formal dan sosialisasi rutin menyebabkan tingkat literasi digital pengguna belum merata di semua kalangan sivitas akademika.

San Nicolas-Rocca & Burkhard (2019) menekankan bahwa literasi keamanan informasi harus menjadi bagian dari literasi digital secara menyeluruh, mencakup pemahaman terhadap risiko siber, praktik etis dalam penggunaan sistem informasi, serta keterampilan mengamankan data pribadi dan institusional. Dalam konteks perpustakaan, literasi ini sangat penting karena pengguna berinteraksi langsung dengan sistem digital, termasuk mengakses koleksi elektronik, menyimpan data riset, hingga mengelola akun pengguna.

Untuk mengatasi permasalahan ini, Perpustakaan UNAS disarankan untuk mengembangkan program literasi digital yang berkelanjutan, misalnya melalui pelatihan daring, infografis edukatif di portal pengguna, serta penyuluhan periodik tentang praktik keamanan yang baik. Langkah ini tidak hanya meningkatkan kepatuhan terhadap standar ISO/IEC 27001, tetapi juga menciptakan budaya tangguh terhadap ancaman siber di lingkungan kampus. Peningkatan kesadaran ini juga akan mendukung efektivitas teknis sistem keamanan informasi yang telah diterapkan, seperti firewall, enkripsi, dan sistem pemantauan real-time. Tanpa perilaku pengguna yang sadar risiko, teknologi yang paling canggih sekalipun tetap rentan terhadap celah keamanan akibat kelalaian individu.

Penilaian Risiko (*Risk Assessment*) Sistem Informasi

Menurut Nugroho & Legowo (2022) risk assessment adalah sebuah prosedur sistematis yang bertujuan untuk mengidentifikasi, mengukur, dan menentukan skala prioritas risiko pada aspek-aspek yang dapat di audit di sebuah Perusahaan (Nugroho & Legowo, 2022). Risk assessment adalah tahapan awal dalam penyusunan Disaster Recovery Plan (DRP) yang bertujuan untuk mengidentifikasi, menilai, dan mengevaluasi tingkat kerentanan serta dampak dari berbagai ancaman terhadap aset informasi, sesuai dengan kerangka metodologi ISO 27001 yang telah banyak diterapkan dalam pengelolaan keamanan informasi (Clarissa & Wang, 2023). Aset-aset informasi yang ada di Perpustakaan Universitas Nasional (UNAS) tersebut mencakup arsip digital, akun pengguna, sistem jaringan, serta koleksi fisik yang terintegrasi dalam sistem layanan informasi perpustakaan.

Penilaian risiko difokuskan pada ancaman siber seperti file berisi malware, penggunaan kredensial lemah, serangan eksternal terhadap aplikasi web, serta gangguan fisik terhadap ruang arsip. Informasi ini diperoleh berdasarkan hasil wawancara langsung dengan tim pengelola sistem informasi, Sebagai bagian dari proses tata kelola risiko yang selaras dengan ISO/IEC 27001, Perpustakaan UNAS melakukan pemetaan risiko terhadap aset informasi utama. Tujuannya bukan hanya untuk identifikasi teknis semata, tetapi sebagai dasar penyusunan kebijakan mitigasi berbasis dampak dan probabilitas risiko terhadap operasional layanan informasi.serta disusun dalam bentuk tabel seperti berikut.

Tabel 2. Risk Assessment

No	Ancaman	Ancaman Yang Terjadi	Kerentanan	Aset Kritis	Konsekuensi	Tingkat Resiko
1	File malware	File yang diunggah pengguna mengandung virus/malware	Tidak adanya filter otomatis saat unggah; pengguna tidak melakukan verifikasi	Sistem arsip digital, server, jaringan	Gangguan sistem, kerusakan data, risiko penyebaran malware	Tinggi
2	Kredensial lemah	Penggunaan username/password sederhana oleh pengguna	Tidak ada kebijakan enforce password kuat secara menyeluruh	Akun pengguna , sistem informasi pengguna	Akun pengguna, sistem informasi pengguna	Tinggi
3	Serangan siber	Upaya SQL injection dan XSS dari pihak luar	Keterbatasan pemantauan manual, WAF belum terupdate	Aplikasi web perpustakaan	Gangguan layanan, kompromi data sensitif	Tinggi
4	Kegagalan sistem/server	Gangguan listrik atau server down	Tidak adanya pemulihan cepat atau failover otomatis	Server, jaringan, backup data	Gangguan operasional, kehilangan akses data sementara	Sedang
5	Insiden Fisik	Akses tidak sah ke ruang penyimpanan, risiko bencana	Pengawasan fisik terbatas, akses belum menggunakan log digital	Arsip fisik, ruang server, koleksi non-digital	Kerusakan koleksi, kehilangan arsip, penghentian operasional	Rendah-Sedang

Hasil risk assessment menunjukkan bahwa sebagian besar ancaman berada pada tingkat risiko tinggi, yang menandakan pentingnya intervensi kebijakan dan penguatan prosedur manajerial. Tanpa pengintegrasian hasil penilaian risiko ke dalam struktur pengambilan keputusan organisasi, upaya pengamanan akan bersifat reaktif dan kurang berkelanjutan. Sebagian besar risiko berada pada kategori tinggi dan perlu ditindaklanjuti secara terstruktur. Tindakan mitigasi yang telah diterapkan UNAS merupakan langkah yang tepat, namun perlu diperkuat melalui dokumentasi DRP formal, edukasi

pengguna, serta simulasi pemulihan bencana. Ke depannya, integrasi sistem log, pemantauan berbasis AI, dan penguatan kebijakan pengguna menjadi kunci dalam menciptakan ekosistem perpustakaan yang aman, tanggap, dan berkelanjutan terhadap gangguan maupun ancaman siber.

Rancangan Disaster Recovery Plan (DRP)

Rencana Pemulihan Bencana (Disaster Recovery Plan/DRP) merupakan salah satu elemen kunci dalam tata kelola keamanan informasi yang proaktif. Dalam strategi bisnis DRP merupakan rencana yang dirancang untuk memastikan kelangsungan operasional sistem dan information teknologi informasi suatu organisasi setelah terjadinya bencana atau kejadian yang dapat mengancam integritas, ketersediaan, dan keamanan sistem IT (Nur Fa'izi, 2024). DRP ditujukan agar sistem tetap beroperasi meskipun ada gangguan dan selamatnya sistem informasi dari bencana (Wibowo, n.d.).

Berdasarkan hasil temuan yang dilakukan telah menunjukkan kesesuaian dengan standar SNI ISO/IEC 27001. Perpustakaan UNAS telah menyusun langkah-langkah strategis sebagai respons terhadap skenario gangguan operasional yang dapat terjadi akibat insiden teknis maupun non-teknis. Tabel berikut merangkum elemen-elemen DRP yang dirancang untuk menjamin keberlangsungan layanan informasi.

Tabel 3. Disaster Recovery Plan

No	Gangguan	Kendala	*Proses Recovery*
1.	Kegagalan sistem atau Server Down	a. Server mengalami kerusakan dan down, menyebabkan tidak bisa diakses oleh pengguna b. Tidak adanya cadangan server aktif c. Backup tidak dilakukan secara real time, hanya seminggu sekali	a. Mengaktifkan backup server mingguan b. menyiapkan server cadangan untuk pemulihan lebih cepat
2.	File terinfeksi virus atau malware	a. Pengguna mengunggah tanpa pemindaian b. Tidak semua file otomatis terdeteksi antivirus	a. Instalasi sistem pemindaian otomatis b. Pembersihan virus dan restorasi dari backup
3.	Akun pengguna diretas oleh akses ilegal	a. Banyak pengguna menggunakan password yang lemah b. Belum semua akun memakai autentikasi ganda (2FA)	a. Implementasi kebijakan password yang kuat dan 2FA b. Reset akun terdampak dan audit keamanan.
4.	Serangan siber (SQL Injection, XSS, dll)	a. Perlindungan sistem belum sepenuhnya dilengkapi Web Application Firewall atau WAF b. Sistem rentan terhadap injeksi perintah	a. Aktivasi firewall dan Web Application Firewall (WAF) b. Monitoring aktivitas dan penambalan celah keamanan
5.	Keterbatasan personil saat insiden	a. Jumlah staff IT tidak memadai untuk merespons cepat b. Penanganan insiden memerlukan koordinasi ekstra	a. Pembentukan tim respons insiden b. SOP penanganan insiden harus dijalankan dengan sesuai
6.	Ancaman fisik pada arsip non-	a. Kelembapan ruang tidak stabil b. Akses keruangan arsip tidak	a. Penyesuaian suhu dan kelembaban ruang arsip

	digital	dibatasi	b. Pembatasan akses dan pemasangan CCTV
7.	Kegagalan sistem akibat human error	a. Salah konfigurasi sistem b. Penghapusan arsip tidak sengaja oleh operator	a. Perlu adanya pelatihan rutin untuk staff b. Audit konfigurasi dan backup pemulihan

Rencana Pemulihan Bencana (Disaster Recovery Plan/DRP) yang tersaji dalam tabel tersebut belum sepenuhnya terdokumentasi dalam bentuk kebijakan formal dan belum dilakukan simulasi berkala untuk menguji kesiapan tim pengelola. Ini menunjukkan bahwa tata kelola pemulihan bencana di UNAS masih perlu diperkuat melalui SOP tertulis, penentuan peran yang jelas, serta pelatihan staf secara periodik untuk mengantisipasi potensi insiden.

Evaluasi Risiko dan Analisis Tindak Lanjut

Berdasarkan hasil evaluasi terhadap penerapan tata kelola keamanan informasi di Perpustakaan Universitas Nasional (UNAS), ditemukan bahwa pendekatan kelembagaan terhadap pengelolaan risiko dan perlindungan informasi masih berada pada tahap awal. Meskipun telah diterapkan kontrol teknis seperti firewall, enkripsi, serta penyusunan Disaster Recovery Plan (DRP), belum semua upaya tersebut diformalkan dalam kerangka kebijakan dan struktur organisasi yang komprehensif. Oleh karena itu, beberapa tindak lanjut strategis diperlukan untuk memperkuat efektivitas tata kelola keamanan informasi:

1. Formalisasi Dokumen Kebijakan dan SOP Tata Kelola Keamanan Informasi
   Diperlukan penyusunan kebijakan keamanan informasi secara menyeluruh yang mencakup klasifikasi aset, pengelolaan hak akses, pengendalian perubahan sistem, serta prosedur tanggap insiden. Semua kebijakan ini harus terdokumentasi, disahkan oleh manajemen, dan diterapkan melalui SOP yang terukur agar tata kelola berjalan konsisten dan terstandar.

2. Pembentukan Struktur Organisasi Keamanan Informasi
   Saat ini belum ada unit formal yang bertanggung jawab penuh atas pengawasan keamanan informasi. Maka dari itu, pembentukan Tim Keamanan Informasi atau *Information Security Governance Unit* menjadi krusial untuk menjamin keberlangsungan implementasi ISO/IEC 27001. Tim ini akan berperan dalam koordinasi audit, pengelolaan risiko, edukasi staf, dan peninjauan kebijakan berkala.

3. Integrasi Risk Assessment ke dalam Proses Perencanaan Strategis
   Hasil risk assessment yang dilakukan belum digunakan secara optimal sebagai dasar pengambilan keputusan strategis dan alokasi sumber daya keamanan. Perlu dibangun *risk register* institusional yang diintegrasikan ke dalam proses perencanaan tahunan dan diawasi oleh unit manajemen risiko universitas.

4. Penguatan Fungsi DRP sebagai Kebijakan Tata Kelola Risiko Operasional
   DRP perlu dilengkapi dan diuji secara berkala melalui simulasi insiden serta pelibatan aktif seluruh pemangku kepentingan. DRP sebaiknya tidak hanya menjadi respons teknis, tetapi bagian dari perencanaan keberlanjutan layanan informasi dan perlindungan reputasi institusi.

5. Peningkatan Literasi Keamanan Informasi dan Budaya Organisasi

Kurangnya kesadaran pengguna dan staf terhadap praktik keamanan menjadi tantangan utama. Maka, pelatihan berkelanjutan, kampanye kesadaran, dan integrasi keamanan informasi dalam program pengembangan SDM harus menjadi agenda tetap dalam tata kelola institusi.

6. Monitoring dan Evaluasi Kelembagaan Secara Berkelanjutan
   Perlu dibentuk mekanisme evaluasi berkala terhadap implementasi kebijakan keamanan, efektivitas kontrol, dan kepatuhan unit kerja terhadap standar ISO/IEC 27001. Evaluasi ini menjadi dasar dalam proses *continual improvement* sebagaimana dimandatkan dalam ISO/IEC 27001:2013.

4. KESIMPULAN

Berdasarkan hasil penelitian evaluasi terhadap penerapan tata kelola keamanan informasi di Perpustakaan Universitas Nasional (UNAS) menunjukkan bahwa institusi telah mengambil sejumlah inisiatif penting dalam menerapkan kontrol berbasis ISO/IEC 27001. Di antaranya adalah penggunaan firewall, sistem enkripsi, pemantauan sistem, hingga penyusunan Disaster Recovery Plan (DRP). Namun demikian, temuan lapangan juga menunjukkan bahwa sebagian besar kontrol tersebut masih berada dalam tahap teknis dan belum didukung oleh struktur tata kelola kelembagaan yang komprehensif.

Kebijakan keamanan informasi belum sepenuhnya terdokumentasi, belum terdapat unit formal pengelola keamanan informasi, dan hasil risk assessment belum diintegrasikan ke dalam proses perencanaan strategis. DRP yang telah disusun pun masih membutuhkan legalisasi formal dan simulasi berkala. Di sisi lain, rendahnya literasi keamanan informasi di kalangan staf dan pengguna menambah tantangan dalam membangun budaya keamanan yang adaptif dan berkelanjutan.

Dengan demikian, dapat disimpulkan bahwa keberhasilan implementasi ISO/IEC 27001 tidak hanya bergantung pada adopsi kontrol teknis, tetapi juga pada kapasitas manajemen untuk mengembangkan kebijakan, struktur organisasi, serta kesadaran kolektif dalam melindungi aset informasi. Penguatan tata kelola kelembagaan menjadi kunci agar Perpustakaan UNAS mampu mewujudkan sistem keamanan informasi yang efektif, berkelanjutan, dan tangguh menghadapi risiko yang terus berkembang.

REFERENSI

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, *12*(17), 3629. DOI 10.3390/electronics12173629

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. DOI 10.3390/electronics12061333

Bahrudin, M., & Firmansyah, F. (2018). Manajemen keamanan informasi di perpustakaan menggunakan Framework SNI ISO/IEC 27001. *Media Pustakawan*, *25*(1), 43-50. DOI 10.37014/medpus.v25i1.191

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. DOI 10.3390/ info13040192

Clarissa, S., & Wang, G. (2023). *Assessing Information Security Management Using ISO 27001:2013 | Jurnal Indonesia Sosial Teknologi*. DOI 10.59141/jist.v4i9.739

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications. https://books.google.co.id/books?hl=en&lr=&id=335ZDwAAQBAJ

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330-1352. DOI 10.1080/13501763.2023.2173274

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 01655515231160026. DOI 10.1177/01655515231160026

Fattah Ys, Moh. A., Parga Zen, B., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security Dan Forensik Digital*, *6*(2), 76-82. DOI 10.14421/csecurity.2023.6.2.4190

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582-2595. DOI 10.30574/wjarr.2024.24.1.3169

Galih, A. P. (2020). Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas. *AL Maktabah*, *5*(1), 10. DOI 10.29300/mkt.v5i1.3086

Ikenwe, I. J., & Udem, O. K. (2022). Innovative digital transformation for dynamic information service sustainability in university libraries in Nigeria. DOI 10.12775/FT.2022.004

International Organization for Standardization. (2013). *ISO/IEC 27001:2013(en), Information technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISACA. (2019). *COBIT | Control Objectives for Information Technologies*, ISACA. https://www.isaca.org/resources/cobit

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, *5*(4), 1240-1256. DOI 10.51519/journalisi.v5i4.572

Mehmood, T. (2021). Does information technology competencies and fleet management practices lead to effective service delivery? Empirical evidence from e-commerce industry. *International Journal of Technology Innovation and Management (IJTIM)*, *1*(2), 14-41. DOI 10.54489/ijtim.v1i2.26

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Arizona State University. https://books.google.co.id/books?id=p0wXBAAAQBAJ

Nugroho, A. R., & Legowo, N. (2022). Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022. *Syntax Literate; Jurnal Ilmiah Indonesia*,

7(12), 20307–20324. https://jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/15349

Nur Fa'izi, M. B. (2024, October 17). *Strategi Pentingnya Disaster Recovery Plan dalam IT Bisnis*. https://cyberhub.id/pengetahuan-dasar/disaster-recovery-plan

Onunka, O., Onunka, T., Fawole, A. A., Adeleke, I. J., & Daraojimba, C. (2023). Library and information services in the digital age: Opportunities and challenges. *Acta Informatica Malaysia*, *7*(1), 113-121. DOI 10.26480/aim.02.2023.113.121

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23* (8), 638-646. DOI 10.1016/j.cose.2004.10.006

Rahmat, D. (2019). Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Iso/Iec 27001: 2013. *COMPUTING | Jurnal Informatika*, *6* (2), 37-41. DOI 10.55222/computing.v6i2.203

Ruthven, I., Robinson, E., & McMenemy, D. (2023). The value of digital and physical library services in UK public libraries and why they are not interchangeable. *Journal of Librarianship and Information Science*, *55*(4), 1143-1154. DOI 10.1177/09610006221127027

San Nicolas-Rocca, T., & Burkhard, R. J. (2019). Information Security in Libraries. *Information Technology and Libraries*, *38*(2), 58–71. DOI 10.6017/ital.v38i2.10973

Spring, M., Faulconbridge, J., & Sarwar, A. (2022). How information technology automates and augments processes: Insights from Artificial-Intelligence-based systems in professional service operations. *Journal of Operations Management*, *68*(6-7), 592-618. DOI 10.1002/joom.1215

Taherdoost, H. (2023). An overview of trends in information systems: Emerging technologies that transform the information technology industry. *Taherdoost, H. (2023). An overview of trends in information systems: emerging technologies that transform the information technology industry. Cloud Computing and Data Science*, 1-16. DOI 10.37256/ccds.4120231653

Wibowo, A. M. (n.d.). *Business Continuity Plan & Disaster Recovery Plan*.

Yusuf, A. M. (2016). *Metode penelitian kuantitatif, kualitatif & penelitian gabungan*. Prenada Media. https://books.google.co.id/books?id=RnA-DwAAQBAJ