

ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN APLIKASI POINT OF SALES MENGGUNAKAN ISO 27001

Gilis Fadhil Hisyam^{1*}, Muhammad Afdan Rojabi²

¹Universitas Mercu Buana, Jakarta, Indonesia

²Universitas Sains Indonesia, Bekasi, Indonesia

*Corresponding email: gilissaliti@gmail.com

Abstrak: Keamanan informasi menjadi aspek penting dalam operasional aplikasi *Point of Sales* (POS), mengingat sistem ini menangani data transaksi dan informasi pelanggan yang bersifat sensitif. Risiko kebocoran data, akses tidak sah, serta serangan siber dapat mengancam keberlanjutan bisnis yang menggunakan sistem POS. Penelitian ini menganalisis serta menerapkan sistem manajemen keamanan informasi berbasis standar ISO 27001:2022 pada aplikasi POS guna meningkatkan perlindungan data. Metode yang digunakan mencakup identifikasi risiko berdasarkan analisis kerentanan, penerapan kontrol keamanan sesuai dengan Annex A ISO 27001:2022, serta evaluasi efektivitas melalui audit keamanan dan uji penetrasi. Hasil penelitian menunjukkan bahwa penerapan kontrol seperti enkripsi data, manajemen akses berbasis peran, monitoring aktivitas sistem, serta peningkatan kesadaran keamanan dapat mengurangi potensi ancaman siber secara signifikan. Kesimpulan dari penelitian ini menegaskan bahwa implementasi ISO 27001:2022 pada sistem POS mampu meningkatkan keamanan informasi, mendukung kepatuhan terhadap standar internasional, serta memperkuat kepercayaan pelanggan.

Kata kunci: Keamanan Informasi, ISO 27001:2022, *Point of Sales*, Manajemen Risiko, Enkripsi Data.

Abstract: Information security is a crucial aspect of the operation of *Point of Sales* (POS) applications, as these systems handle transaction data and sensitive customer information. The risks of data breaches, unauthorized access, and cyberattacks can threaten the sustainability of businesses using POS systems. This study analyzes and implements an information security management system based on the ISO 27001:2022 standard in POS applications to enhance data protection. The methodology includes risk identification through vulnerability analysis, implementation of security controls following Annex A of ISO 27001:2022, and effectiveness evaluation through security audits and penetration testing. The results indicate that implementing controls such as data encryption, role-based access management, system activity monitoring, and increased security awareness can significantly reduce potential cyber threats. The study concludes that implementing ISO 27001:2022 in POS systems enhances information security, supports compliance with international standards, and strengthens customer trust.

Keywords: Information Security, ISO 27001:2022, *Point of Sales*, Risk Management, Data Encryption.

PENDAHULUAN

Dalam era digital yang semakin berkembang, penggunaan aplikasi *Point of Sales* (POS) dari PT XYZ menjadi bagian krusial dalam operasional bisnis, terutama di sektor ritel, perhotelan, dan layanan makanan (Panjaitan & Lupiana, 2023). Aplikasi POS tidak hanya berfungsi sebagai alat utama dalam pengelolaan transaksi keuangan, tetapi juga mencakup berbagai aspek bisnis seperti manajemen inventaris, pengolahan data pelanggan, serta analisis performa penjualan (Geni et al, 2024). Dengan semakin luasnya adopsi teknologi ini, keamanan informasi dalam aplikasi POS menjadi perhatian utama bagi perusahaan dalam menjaga integritas dan kepercayaan pelanggan. Aplikasi POS menangani berbagai jenis data sensitif, termasuk informasi keuangan, data kartu kredit pelanggan, serta rekam jejak transaksi yang bernilai strategis bagi bisnis (Ifadhila et al, 2024). Sayangnya, sistem POS sering menjadi target utama bagi pelaku kejahatan siber yang ingin mengeksploitasi kelemahan dalam sistem keamanan. Serangan seperti pencurian data pelanggan, malware pada terminal POS, serta manipulasi transaksi dapat menyebabkan kerugian finansial yang signifikan, merusak reputasi perusahaan, dan bahkan menimbulkan konsekuensi hukum akibat pelanggaran regulasi perlindungan data (Maulani et al, 2025).

ISO 27001 merupakan standar internasional yang menyediakan kerangka kerja sistem manajemen keamanan informasi (SMKI) untuk membantu organisasi dalam mengidentifikasi, mengelola, serta mengurangi risiko keamanan informasi (Kenyon, 2024). Standar ini mencakup serangkaian kontrol keamanan yang dirancang untuk melindungi data dari akses yang tidak sah, kebocoran informasi, serta ancaman lainnya yang dapat mengganggu operasional bisnis (Pratama et al, 2024). Implementasi ISO 27001 dalam aplikasi POS bertujuan untuk memastikan bahwa data transaksi dan informasi pelanggan dikelola dengan aman melalui penerapan kebijakan keamanan yang sistematis dan berkelanjutan. Dalam penelitian ini, akan dilakukan analisis dan penerapan sistem manajemen keamanan informasi pada aplikasi POS dengan mengacu pada standar ISO 27001 (Erwin et al, 2024). Studi ini mencakup identifikasi risiko keamanan yang dihadapi oleh sistem POS, penerapan kontrol yang relevan berdasarkan kerangka kerja ISO 27001, serta evaluasi efektivitas penerapan tersebut dalam meningkatkan keamanan informasi. Hasil penelitian ini diharapkan dapat memberikan panduan praktis bagi pengembang aplikasi POS, pelaku bisnis, serta pemangku kepentingan lainnya dalam mengimplementasikan strategi keamanan informasi yang lebih baik. Dengan menerapkan standar ISO 27001, diharapkan perusahaan dapat meningkatkan kepercayaan pelanggan, memenuhi persyaratan kepatuhan terhadap regulasi keamanan data, serta mengurangi dampak negatif dari ancaman keamanan yang berpotensi merugikan bisnis.

METODE

Penelitian ini menggunakan pendekatan studi kasus dengan menerapkan standar ISO 27001:2022 dalam sistem manajemen keamanan informasi pada aplikasi *Point of Sales* (POS). Metode yang digunakan dalam penelitian ini mencakup beberapa tahapan utama sebagai berikut:

1. Identifikasi Risiko Keamanan

Dalam upaya memastikan keamanan sistem *Point of Sales* (POS), dilakukan analisis menyeluruh terhadap berbagai ancaman dan kerentanan yang dapat memengaruhi integritas, kerahasiaan, dan ketersediaan informasi. Analisis ini mencakup identifikasi potensi serangan siber, kelemahan dalam kontrol akses, serta risiko yang timbul akibat kesalahan pengguna atau kegagalan sistem. Salah satu pendekatan yang digunakan dalam penilaian ini adalah metode analisis risiko berbasis ISO 27005, yang memberikan kerangka kerja sistematis dalam mengidentifikasi, menilai, dan mengelola risiko keamanan informasi. Sebagai bagian dari penerapan standar keamanan yang lebih luas, identifikasi risiko ini juga mengacu pada Klausul 6.1 *Tindakan untuk Mengatasi Risiko dan Peluang* dalam ISO 27001:2022. Klausul ini menekankan pentingnya pendekatan berbasis risiko dalam mengelola keamanan informasi, termasuk dengan mengembangkan kebijakan mitigasi risiko yang efektif dan menyesuaikan kontrol keamanan sesuai dengan tingkat ancaman yang dihadapi. Dengan menerapkan metode ini, organisasi dapat memastikan bahwa risiko yang teridentifikasi tidak hanya terdokumentasi dengan baik, tetapi juga diatasi melalui langkah-langkah mitigasi yang tepat guna, sehingga sistem POS menjadi lebih tahan terhadap potensi serangan atau insiden keamanan yang dapat mengganggu operasional bisnis.

2. Perancangan dan Implementasi Kontrol Keamanan

Dalam upaya meningkatkan keamanan sistem *Point of Sales* (POS), dilakukan perancangan dan implementasi kontrol keamanan yang mengacu pada Annex A ISO 27001:2022. Standar ini menyediakan kerangka kerja komprehensif yang mencakup berbagai aspek pengelolaan keamanan informasi. Beberapa kategori kontrol utama yang diadopsi dalam sistem POS meliputi:

- A.5 (Kontrol Organisasi): Menetapkan kebijakan dan prosedur keamanan informasi yang jelas, termasuk struktur tanggung jawab dalam pengelolaan keamanan serta mekanisme pemantauan kepatuhan terhadap kebijakan tersebut.
- A.6 (Kontrol Orang): Mengelola aspek keamanan yang berkaitan dengan pengguna, seperti pelatihan kesadaran keamanan bagi karyawan, manajemen akses berbasis peran (RBAC), serta penerapan prinsip *least privilege* untuk meminimalkan risiko akses yang tidak sah.
- A.7 (Kontrol Fisik): Mengamankan infrastruktur fisik terkait dengan sistem POS, termasuk pengelolaan akses ke perangkat keras, pemantauan area kerja, serta perlindungan terhadap pencurian atau manipulasi perangkat yang digunakan dalam operasional POS.
- A.8 (Kontrol Teknologi): Mengimplementasikan langkah-langkah teknis seperti enkripsi data transaksi, autentikasi multi-faktor (MFA), pemantauan sistem secara *real-time*, serta penerapan *firewall* dan sistem deteksi intrusi untuk mencegah serangan siber.

Selain mengadopsi kontrol berdasarkan Annex A, implementasi keamanan juga disesuaikan dengan kebutuhan spesifik dari aplikasi POS yang digunakan oleh perusahaan. Evaluasi dilakukan untuk menentukan kontrol yang paling relevan dan efektif dalam konteks operasional yang ada, sehingga setiap langkah mitigasi dapat diterapkan secara optimal tanpa menghambat fungsionalitas sistem. Dengan pendekatan ini, diharapkan sistem POS dapat lebih tangguh terhadap ancaman keamanan informasi serta memenuhi standar kepatuhan internasional yang ditetapkan dalam ISO 27001:2022.

3. Evaluasi dan Audit Keamanan

Sebagai bagian dari upaya memastikan efektivitas kontrol keamanan yang telah diterapkan, dilakukan audit internal secara berkala untuk menilai kepatuhan terhadap standar ISO 27001:2022. Audit ini mengacu pada Klausul 9.2 (Audit Internal) yang menetapkan persyaratan untuk melakukan evaluasi sistematis terhadap implementasi kebijakan, prosedur, dan kontrol keamanan yang telah diadopsi. Melalui audit internal, dapat diidentifikasi apakah terdapat kesenjangan dalam penerapan standar serta area yang memerlukan perbaikan guna meningkatkan tingkat kepatuhan dan efektivitas sistem manajemen keamanan informasi. Selain audit internal, sistem POS juga diuji menggunakan metode *penetration testing* (uji penetrasi) untuk mengukur ketahanan terhadap potensi serangan siber. Pengujian ini mengacu pada Annex A.8 (Kontrol Teknologi) dalam ISO 27001:2022, yang menekankan pentingnya perlindungan teknis terhadap aset informasi. Uji penetrasi dilakukan dengan mensimulasikan berbagai skenario serangan guna mengidentifikasi kelemahan yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

4. Peningkatan Berkelanjutan

Sebagai bagian dari komitmen terhadap keamanan informasi, organisasi menerapkan proses peningkatan berkelanjutan untuk memastikan sistem *Point of Sales* (POS) selalu sesuai dengan standar ISO 27001:2022 serta mampu menghadapi ancaman keamanan yang terus berkembang. Langkah pertama dalam upaya ini adalah menyusun rekomendasi perbaikan berdasarkan hasil evaluasi dan audit. Temuan dari audit internal dan uji penetrasi dianalisis secara mendalam untuk mengidentifikasi area yang memerlukan perbaikan, baik dalam aspek teknis maupun kebijakan keamanan informasi. Rekomendasi ini mencakup pembaruan kebijakan keamanan, peningkatan kontrol teknis, serta optimalisasi prosedur manajemen risiko guna menutup celah keamanan yang ditemukan. Selain itu, peningkatan kesadaran dan kompetensi sumber daya manusia juga menjadi fokus utama dalam perbaikan berkelanjutan. Oleh karena itu, organisasi melakukan pelatihan kepada staf dan pengguna sistem mengenai kesadaran keamanan informasi, mengacu pada Klausul 7.2 (Kompetensi) serta Annex A.6 (Kontrol Orang) dalam ISO 27001:2022. Pelatihan ini bertujuan untuk meningkatkan

pemahaman terkait kebijakan keamanan, praktik terbaik dalam penggunaan sistem POS, serta langkah-langkah yang harus diambil dalam menghadapi potensi ancaman siber. Dengan adanya peningkatan kompetensi ini, organisasi dapat membangun budaya keamanan informasi yang kuat, di mana setiap individu memiliki peran aktif dalam menjaga keamanan sistem.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini menunjukkan bahwa penerapan ISO 27001:2022 pada aplikasi POS memberikan peningkatan signifikan dalam keamanan informasi. Beberapa temuan utama yang diperoleh dalam audit dan evaluasi adalah sebagai berikut:

1. Identifikasi Risiko

Dalam proses analisis keamanan terhadap sistem *Point of Sales* (POS), ditemukan beberapa risiko yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data. Salah satu kelemahan utama yang teridentifikasi adalah praktik berbagi akun pengguna, di mana beberapa pengguna masih menggunakan *username* dan *password* yang sama untuk mengakses sistem. Selain itu, ditemukan juga penggunaan alamat email bersama untuk autentikasi, yang menyebabkan lemahnya pengendalian akses serta kesulitan dalam melakukan audit dan penelusuran aktivitas pengguna. Praktik ini bertentangan dengan prinsip *least privilege access* dan meningkatkan risiko penyalahgunaan akun, baik oleh pihak internal maupun eksternal. Selain itu, penggunaan akun bersama menyebabkan pencatatan log aktivitas menjadi tidak akurat, sehingga dalam situasi pelanggaran keamanan atau insiden keamanan informasi, sulit untuk mengidentifikasi individu yang bertanggung jawab atas suatu tindakan. Praktik ini juga membuka peluang bagi serangan *credential stuffing*, di mana kredensial yang telah bocor dapat digunakan kembali untuk mengakses sistem secara tidak sah. Oleh karena itu, perlu diterapkan kebijakan manajemen identitas yang lebih ketat, seperti mewajibkan setiap pengguna memiliki akun unik, melarang penggunaan akun bersama atau berbagi email untuk autentikasi, mengaktifkan *multi-factor authentication* (MFA), serta melakukan audit berkala terhadap aktivitas akun guna mengidentifikasi potensi penyalahgunaan akses.

Selain masalah terkait identitas dan autentikasi, ditemukan pula bahwa zona waktu yang dikonfigurasi pada server masih menggunakan GMT+8 (Shanghai), bukan zona waktu Indonesia yang sesuai, yaitu GMT+7 (WIB), GMT+8 (WITA), atau GMT+9 (WIT). Ketidaksesuaian ini dapat menyebabkan berbagai permasalahan, seperti ketidaktepatan dalam pencatatan log aktivitas yang dapat mempersulit analisis forensik dan audit keamanan. Jika terjadi insiden keamanan, tim investigasi akan mengalami kesulitan dalam merekonstruksi urutan kejadian karena perbedaan waktu pencatatan. Selain itu, ketidaksesuaian waktu transaksi dengan waktu aktual pelanggan dan sistem pembayaran dapat menyebabkan perbedaan dalam laporan transaksi serta menghambat proses rekonsiliasi data keuangan. Masalah ini juga dapat berdampak pada sistem monitoring dan notifikasi otomatis, yang bergantung pada waktu yang akurat untuk memberikan peringatan terhadap aktivitas anomali atau kegagalan sistem. Untuk mengatasi hal ini, perlu dilakukan konfigurasi ulang zona waktu server agar sesuai dengan zona waktu Indonesia, menerapkan *Network Time Protocol* (NTP) guna memastikan sinkronisasi waktu yang akurat di seluruh server dan perangkat terkait, serta melakukan validasi berkala terhadap pengaturan zona waktu guna memastikan tidak ada perubahan yang tidak terotorisasi.

2. Implementasi Kontrol Keamanan

Dalam upaya meningkatkan keamanan sistem *Point of Sales* (POS) dan memastikan kepatuhan terhadap standar ISO 27001:2022, telah diterapkan sejumlah kontrol keamanan yang bertujuan untuk mengurangi risiko yang telah diidentifikasi sebelumnya. Salah satu langkah utama yang diambil adalah penerapan manajemen identitas yang lebih ketat dengan

mewajibkan setiap personel yang memiliki akses ke aplikasi POS untuk menggunakan akun individu mereka sendiri. Dengan adanya akun khusus untuk setiap pengguna, perusahaan dapat memastikan bahwa setiap aktivitas dalam sistem dapat ditelusuri kembali ke individu yang bertanggung jawab, sehingga meningkatkan akuntabilitas dan mengurangi risiko penyalahgunaan akun bersama. Selain itu, penggunaan akun individu juga memungkinkan penerapan kontrol akses berbasis peran (*role-based access control*), di mana setiap personel hanya diberikan hak akses sesuai dengan tugas dan tanggung jawabnya. Langkah ini sejalan dengan kontrol dalam Annex A.5.9 terkait *Identity Management*, yang mengharuskan organisasi untuk memiliki sistem manajemen identitas yang efektif guna mencegah akses tidak sah ke informasi sensitif.

Selain perbaikan dalam manajemen identitas, sistem juga telah dikonfigurasi ulang agar sesuai dengan zona waktu Indonesia bagian barat (GMT+7), menggantikan pengaturan sebelumnya yang masih menggunakan GMT+8 (Shanghai). Kesalahan dalam pengaturan zona waktu sebelumnya dapat menyebabkan ketidaktepatan dalam pencatatan log aktivitas sistem, yang berisiko terhadap analisis forensik keamanan serta audit kepatuhan. Dengan menyesuaikan zona waktu, pencatatan log aktivitas kini lebih akurat dan selaras dengan waktu operasional perusahaan, sehingga memungkinkan investigasi insiden keamanan dilakukan dengan lebih efisien. Penerapan kontrol ini merujuk pada Annex A.8.17 *Clock Synchronization*, yang menekankan pentingnya sinkronisasi waktu dalam sistem informasi guna memastikan integritas dan akurasi pencatatan peristiwa dalam sistem.

Audit keamanan yang dilakukan selama implementasi juga menemukan adanya kelemahan dalam sistem pemantauan aktivitas yang dapat menghambat deteksi dini terhadap ancaman keamanan. Kelemahan ini termasuk kurangnya *logging* dan pemantauan terhadap akses serta perubahan data yang dilakukan oleh pengguna dengan hak istimewa (*privileged users*), sehingga dapat menyulitkan identifikasi aktivitas mencurigakan atau tidak sah dalam sistem. Sebagai langkah mitigasi, sistem pengawasan yang lebih ketat telah diterapkan dengan menambahkan fitur *real-time monitoring* dan analisis log otomatis untuk mendeteksi pola anomali dalam aktivitas pengguna. Selain itu, dilakukan *independent review* secara berkala untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan dan memastikan bahwa kebijakan serta prosedur keamanan tetap relevan dengan ancaman yang berkembang. Upaya ini sesuai dengan rekomendasi dalam Annex A.5.35 *Independent Review of Information Security*, yang menekankan perlunya tinjauan berkala terhadap keamanan informasi oleh pihak independen guna memastikan adanya pengawasan dan perbaikan yang berkelanjutan terhadap sistem keamanan yang diterapkan.

3. Evaluasi dan Peningkatan

Setelah implementasi berbagai kontrol keamanan yang direkomendasikan, dilakukan evaluasi untuk menilai efektivitas langkah-langkah yang telah diterapkan dalam meningkatkan keamanan sistem Point of Sales (POS). Evaluasi ini mencakup pengujian sistem, analisis log keamanan, serta wawancara dengan pengguna terkait penerapan kontrol yang telah dilakukan. Hasil evaluasi menunjukkan adanya peningkatan signifikan dalam kemampuan sistem untuk mendeteksi dan merespons potensi serangan siber. Sebelumnya, sistem memiliki keterbatasan dalam memonitor aktivitas pengguna dan mendeteksi anomali secara real-time. Namun, setelah implementasi mekanisme *real-time monitoring* dan *logging* yang lebih komprehensif, sistem mampu mengidentifikasi pola akses yang mencurigakan serta memberikan peringatan dini sebelum ancaman berkembang menjadi insiden keamanan yang lebih serius. Penerapan manajemen identitas yang lebih ketat juga telah mengurangi kemungkinan penyalahgunaan akun bersama, meningkatkan akuntabilitas pengguna, serta mengoptimalkan kontrol akses berdasarkan peran.

Selain peningkatan teknis dalam sistem keamanan, kesadaran staf terhadap kebijakan keamanan informasi juga mengalami perbaikan yang signifikan. Sebagai bagian dari upaya peningkatan keamanan, pelatihan mengenai praktik keamanan informasi telah diberikan kepada seluruh personel yang memiliki akses ke aplikasi POS. Pelatihan ini mencakup pemahaman mengenai pentingnya manajemen kredensial yang aman, praktik terbaik dalam penggunaan kata sandi, serta tindakan pencegahan terhadap serangan siber seperti *phishing* dan *social engineering*. Berdasarkan hasil survei dan tes evaluasi pasca-pelatihan, ditemukan bahwa tingkat pemahaman karyawan terhadap kebijakan keamanan meningkat secara signifikan, yang menunjukkan efektivitas dari program pelatihan yang telah diterapkan. Langkah ini selaras dengan rekomendasi dalam Annex A.6 *Organization of Information Security*, yang menekankan pentingnya peran dan tanggung jawab setiap individu dalam menjaga keamanan informasi, termasuk melalui peningkatan kesadaran dan edukasi terhadap ancaman keamanan siber.

Meskipun peningkatan yang dicapai cukup signifikan, evaluasi juga menunjukkan bahwa masih terdapat beberapa aspek yang perlu diperbaiki untuk mencapai standar keamanan yang lebih optimal. Salah satu area yang membutuhkan perhatian lebih lanjut adalah penguatan mekanisme audit dan tinjauan keamanan secara berkala. Untuk memastikan keberlanjutan dari implementasi kontrol yang telah diterapkan, disarankan agar perusahaan mengadopsi kebijakan *continuous security assessment*, di mana audit keamanan dan pengujian penetrasi dilakukan secara rutin guna mengidentifikasi potensi celah keamanan yang mungkin muncul akibat perubahan teknologi atau metode serangan yang semakin berkembang. Selain itu, diperlukan sistem umpan balik dari pengguna terkait kendala yang mereka hadapi dalam penerapan kebijakan keamanan agar dapat dilakukan penyesuaian kebijakan tanpa mengurangi efektivitas perlindungan terhadap sistem. Dengan evaluasi dan peningkatan yang berkelanjutan, sistem POS dapat terus beradaptasi terhadap dinamika ancaman keamanan siber yang berkembang, meningkatkan kepatuhan terhadap standar ISO 27001:2022, serta memastikan bahwa perlindungan terhadap data pelanggan dan transaksi bisnis tetap optimal dalam jangka panjang.

4. Dokumen Temuan

Hasil temuan dari aplikasi *Point of Sales* (POS) yang dimiliki PT XYZ setelah dilakukan analisis risiko dan evaluasi terhadap sistem keamanan informasi berdasarkan standar ISO 27001:2022 dapat dilihat pada Tabel 1.

Tabel 1. Dokumen Temuan Pada Aplikasi POS di PT XYZ

No	Klausul	Deskripsi Temuan	Unit Kerja	Kategori
1	A.5.9 (<i>Identity management</i>)	Terdapat adanya <i>username</i> dan <i>password sharing</i> dan juga <i>email sharing</i>	IT	Minor
2	A.8.17 (<i>Clock synchronization</i>)	Zona waktu server masih menunjukkan GMT+8 Shanghai, bukan zona waktu Indonesia	IT	Minor

Dokumen ini menjadi dasar bagi organisasi dalam melakukan peningkatan berkelanjutan pada keamanan aplikasi POS dan memastikan kepatuhan terhadap ISO 27001:2022.

SIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa penerapan ISO 27001:2022 pada aplikasi *Point of Sales* (POS) berperan penting dalam meningkatkan keamanan informasi secara signifikan. Identifikasi risiko yang telah dilakukan mengungkap beberapa celah keamanan yang dapat dieksploitasi oleh pihak tidak berwenang, seperti kelemahan dalam kontrol akses, penggunaan autentikasi yang kurang aman, serta kurangnya pemantauan aktivitas sistem. Namun, dengan penerapan kontrol keamanan yang tepat sesuai dengan standar ISO 27001:2022, risiko tersebut dapat diminimalkan, sehingga sistem menjadi lebih tangguh terhadap ancaman siber. Implementasi berbagai kontrol keamanan telah terbukti memberikan dampak positif dalam menjaga keamanan informasi pada sistem POS. Beberapa langkah yang diterapkan, seperti enkripsi data transaksi (Annex A.10) untuk melindungi informasi pelanggan, manajemen akses berbasis peran (Annex A.5.9) guna mencegah akses tidak sah, serta monitoring dan logging aktivitas sistem (Annex A.8.15 & A.8.16) untuk mendeteksi potensi ancaman lebih dini, telah meningkatkan efektivitas sistem dalam menghadapi ancaman keamanan. Selain itu, pelatihan dan peningkatan kesadaran keamanan (Annex A.6) yang diberikan kepada staf dan pengguna sistem turut berkontribusi dalam membangun budaya keamanan yang lebih baik dalam organisasi.

Evaluasi dan audit yang dilakukan selama penelitian ini juga memberikan gambaran yang lebih jelas mengenai efektivitas penerapan ISO 27001:2022, serta mengidentifikasi area yang masih memerlukan perbaikan lebih lanjut. Hasil audit internal menunjukkan bahwa masih terdapat aspek-aspek yang dapat ditingkatkan, seperti optimalisasi pengelolaan aset informasi (Annex A.8), penyelarasan kebijakan keamanan dengan standar terkini, serta implementasi sistem pemantauan keamanan yang lebih komprehensif. Ke depannya, perusahaan disarankan untuk terus melakukan pemantauan dan peningkatan berkelanjutan terhadap sistem keamanan informasi guna memastikan sistem POS tetap sesuai dengan perkembangan teknologi serta ancaman keamanan yang semakin kompleks. Penerapan siklus Plan-Do-Check-Act (PDCA) dalam manajemen keamanan informasi dapat menjadi strategi efektif dalam menjaga kepatuhan terhadap standar ISO 27001:2022, sekaligus memastikan bahwa kebijakan dan prosedur keamanan yang diterapkan selalu relevan dan adaptif terhadap perubahan lingkungan bisnis dan teknologi. Dengan komitmen terhadap keamanan informasi yang kuat serta penerapan ISO 27001:2022 secara berkelanjutan, perusahaan dapat tidak hanya meningkatkan perlindungan terhadap data transaksi dan pelanggan, tetapi juga membangun kepercayaan yang lebih tinggi dari pelanggan serta mitra bisnis dalam operasionalnya.

DAFTAR PUSTAKA

- Erwin, E., Judijanto, L., Anggraeni, A. F., Nurfaidah, N., Damayanti, F., Sari, H. E., & Indrayani, N. (2024). *Sistem Informasi Manajemen: Teori, Prinsip dan Penerapan*. Jambi: PT. Sonpedia Publishing Indonesia.
- Geni, B. Y., Ramayanti, D., & Ratnasari, A. (2024). IMPLEMENTASI SISTEM POIN OF SALE TERINTEGRASI BERBASIS PYTHON. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(4), 4387-4393. <https://doi.org/10.36040/jati.v8i4.9934>.
- Ifadhila, I., Rukmana, A. Y., Erwin, E., Ratnaningrum, L. P. R. A., Aprilia, M., Setiawan, R., & Setiawan, H. (2024). *Pemasaran Digital di Era Society 5.0: Transformasi Bisnis di Dunia Digital*. Jambi: PT. Sonpedia Publishing Indonesia.
- Kenyon, B. (2024). *ISO 27001 controls—A guide to implementing and auditing*. Cambridgeshire: IT Governance Ltd.
- Maulani, G., Kom, S., Kom, M., Mustakim, S., Kom, M., Putra, I. I. N. T. A., & SE, M. (2025). *PENGANTAR SISTEM INFORMASI*. Batam: Cendikia Mulia Mandiri.

- Panjaitan, W. J., & Lupiana, F. (2023). Penerapan Tranformasi Digital dan Hambatannya Pada Industri Kuliner di Indonesia. *Jurnal Riset Manajemen Dan Ekonomi (Jrime)*, 1(2), 278-301. <https://doi.org/10.54066/jrime-itb.v1i2.650>.
- Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Bandung: Kaizen Media Publishing.