


Implementasi ISO 27001 dalam Meningkatkan Kepercayaan Pengguna dalam Sektor Industri

Pia Suci Lestari^{1*}, Fatimah Zahra Tambunan², Ariq Wiratama Nasution³, Monika Amelia Manurung⁴, Ropika⁵, Cherine Lita Purnama Panjaitan⁶, Dear Selvanathan Sinaga⁷

^{1,2,3,4,5,6,7}Ilmu Sosial dan Politik, Universitas Sumatera Utara, Jl. Dr. T. Mansyur No. 9, Padang Bulan, Medan, Sumatera Utara, Indonesia.

E-mail: piasucilestari25@gmail.com

* Corresponding Author

 <https://doi.org/10.31004/jerkin.v4i1.1565>

ARTICLE INFO

Article history

Received: 30 June 2025

Revised: 06 July 2025

Accepted: 12 July 2025

Kata Kunci:

Social Media Marketing,
Brand Awareness,
Engagement Rate, Instagram
Insight.

Keywords:

Social Media Marketing,
Brand Awareness,
Engagement Rate,
Instagram Insight.



ABSTRACT

Penerapan ISO 27001 di sektor keuangan terbukti meningkatkan keamanan informasi dan kepercayaan pengguna. Studi literatur terhadap sembilan jurnal menunjukkan bahwa standar ini efektif dalam mengelola risiko, memenuhi regulasi, dan menerapkan kontrol keamanan seperti enkripsi dan autentikasi multifaktor. Beberapa lembaga melaporkan penurunan insiden keamanan hingga 40%. Namun, tantangan implementasi meliputi keterbatasan SDM dan kurangnya evaluasi persepsi pengguna. Temuan ini menegaskan peran ISO 27001 sebagai standar kritis untuk membangun kepercayaan di era digital.

This study analyzes the challenges and strategies for implementing ISO 31000: The implementation of ISO 27001 in the financial sector has been proven to improve information security and user trust. A literature review of nine journals shows that this standard is effective in managing risks, complying with regulations, and implementing security controls such as encryption and multi-factor authentication. Some institutions have reported a reduction in security incidents of up to 40%. However, implementation challenges include limited human resources and a lack of user evaluation user perception. These findings underscore the role of ISO 27001 as a critical standard for building trust in the digital age.



This is an open access article under the CC-BY-SA license.

How to Cite: Pia Suci Lestari, et al (2025). Implementasi ISO 27001 dalam Meningkatkan Kepercayaan Pengguna dalam Sektor Industri, 4(1). <https://doi.org/10.31004/jerkin.v4i1.1565>

PENDAHULUAN

Digitalisasi yang berkembang pesat di sektor keuangan membuat ancaman terhadap keamanan informasi juga semakin bervariasi. Dalam menghadapi ancaman tersebut, lembaga keuangan mulai menerapkan standar internasional seperti ISO 27001 yang dapat membantu dalam mengelola resiko keamanan data. (Ewuga et al., 2023) menyatakan penggunaan ISO 27001 di sektor perbankan dapat meningkatkan kemampuan suatu bank dalam mengelola risiko, memperkuat sistem untuk mendeteksi insiden, serta membangun kesadaran pentingnya keamanan informasi di antara karyawan dan pemangku kepentingan. Pendekatan yang fokus pada risiko dari ISO 27001 membantu lembaga keuangan merespons lebih cepat terhadap ancaman siber yang terus berubah.

Tingkat kepercayaan pengguna juga menjadi penentu penting dalam menilai keberhasilan sistem keamanan informasi, tidak hanya dari sisi internal organisasi. (Sahu et al., 2024) menyebutkan bahwa konsumen cenderung lebih setia pada layanan keuangan digital yang sudah menggunakan enkripsi data, autentikasi dua faktor, serta memberikan informasi yang jelas tentang kebijakan keamanan mereka. Penelitian (Muhtasim et al., 2022) turut memperkuat temuan ini, menunjukkan bahwa kepuasan pengguna terhadap layanan dompet digital sangat dipengaruhi oleh enam faktor keamanan utama, yaitu

kecepatan transaksi, mekanisme autentikasi, sistem enkripsi, performa perangkat lunak, privasi data, dan informasi yang diberikan kepada pengguna. Faktor-faktor tersebut secara signifikan membentuk persepsi keamanan dan berdampak langsung pada kepuasan serta loyalitas pelanggan terhadap layanan keuangan digital

Implementasi ISO 27001 tidak hanya penting untuk menjaga keamanan data, tetapi juga berperan strategis dalam membangun kepercayaan pengguna terhadap layanan digital di sektor keuangan. Ketika pengguna merasa bahwa data pribadi dan transaksinya dilindungi secara optimal, maka mereka cenderung lebih loyal dan puas terhadap layanan yang diberikan. Hal ini selaras dengan temuan yang dikemukakan oleh Muhtasimi et al. (2022) bahwa keamanan data merupakan salah satu faktor dominan yang mempengaruhi kepuasan pelanggan dalam penggunaan layanan dompet digital. Standar ISO 27001 membantu menciptakan struktur sistem keamanan yang terstandarisasi, termasuk penerapan audit internal, perencanaan kontinuitas bisnis, serta peningkatan kesadaran keamanan informasi secara menyeluruh.

Dalam konteks industri keuangan, kepercayaan merupakan fondasi utama dalam membangun relasi jangka panjang dengan pelanggan. Tanpa adanya rasa aman dalam bertransaksi, adopsi layanan digital cenderung melambat. Oleh karena itu, penerapan ISO 27001 menjadi krusial untuk menjawab tantangan era digital yang rawan terhadap serangan siber. Selain itu, standar ini juga memberikan kerangka kerja yang fleksibel dan dapat disesuaikan dengan kebutuhan lembaga, sehingga mendukung pencapaian tujuan organisasi secara efektif tanpa mengabaikan aspek keamanan.

Dengan demikian, implementasi ISO 27001 tidak hanya menjadi langkah preventif dalam menghadapi risiko keamanan informasi, tetapi juga sebagai strategi untuk meningkatkan persepsi positif konsumen terhadap institusi keuangan digital. Kombinasi antara kepatuhan terhadap standar keamanan dan penyampaian informasi keamanan yang jelas kepada pengguna akan memperkuat kepercayaan, yang pada akhirnya mendorong loyalitas dan keberlanjutan hubungan antara pengguna dan penyedia layanan.

Dalam era transformasi digital, sektor industri keuangan menghadapi tantangan besar terkait keamanan informasi. Seiring dengan meningkatnya penggunaan layanan keuangan digital seperti e-wallet, dompet digital, dan sistem Point of Sales (POS), kepercayaan pengguna menjadi faktor penentu utama keberlangsungan dan loyalitas terhadap layanan keuangan. Ketidakpercayaan terhadap keamanan informasi dapat menyebabkan menurunnya penggunaan layanan, bahkan memicu perpindahan pelanggan ke penyedia layanan lain.

Penerapan ISO 27001 sebagai standar internasional untuk sistem manajemen keamanan informasi (Information Security Management System/ISMS) menjadi salah satu solusi strategis yang dapat diterapkan oleh industri keuangan untuk mengatasi risiko kebocoran data, akses tidak sah, serta serangan siber. Seperti yang dijelaskan oleh Hisyam dan Rojabi (2025), implementasi ISO 27001:2022 pada sistem POS mampu meningkatkan keamanan informasi, mendukung kepatuhan terhadap standar internasional, serta memperkuat kepercayaan pelanggan melalui kontrol seperti enkripsi data, manajemen akses berbasis peran, dan pemantauan sistem secara real-time.

Kepercayaan pengguna terhadap layanan keuangan digital juga sangat dipengaruhi oleh persepsi terhadap keamanan sistem. Dewi et al. (2024) dalam studi tentang loyalitas nasabah lembaga keuangan mikro syariah menyatakan bahwa kepercayaan nasabah dan citra institusi memiliki pengaruh signifikan terhadap loyalitas dan kepuasan pengguna. Oleh karena itu, penguatan aspek keamanan informasi juga akan meningkatkan citra institusi keuangan dan memperkuat loyalitas nasabah

Selain itu, Azhari et al. (2024) menekankan pentingnya penerapan manajemen sekuriti secara menyeluruh pada layanan e-wallet yang rawan terhadap serangan siber. Mereka menyebutkan bahwa strategi seperti otentikasi multi-faktor, enkripsi data, dan edukasi pengguna tentang keamanan digital merupakan praktik penting dalam membangun kepercayaan pengguna terhadap transaksi elektronik. Penguatan sistem keamanan secara teknis maupun edukatif akan meningkatkan rasa aman dan kenyamanan dalam bertransaksi.

Dengan demikian, implementasi ISO 27001 tidak hanya menjadi bentuk kepatuhan terhadap standar keamanan, tetapi juga sebagai upaya strategis untuk meningkatkan kepercayaan

dan loyalitas pengguna di sektor industri keuangan. Hal ini menjadi kunci untuk memperkuat daya saing institusi keuangan dalam era digital.

METODE

Literatur review adalah pemilihan dokumen yang tersedia (baik yang diterbitkan maupun yang tidak diterbitkan) tentang topik, yang berisi informasi, ide, data, dan bukti yang ditulis dari sudut pandang tertentu atau mengungkapkan pandangan tertentu tentang sifat topik, bagaimana hal itu terjadi akan diselidiki, dan evaluasi efektif dari dokumen-dokumen ini dalam kaitannya dengan penelitian yang diusulkan (Irwansyah, 2024). Penelitian ini menggunakan pendekatan literature review (tinjauan pustaka) sebagai metode utama untuk mengkaji peran ISO/IEC 27001 dalam meningkatkan kepercayaan pengguna, khususnya di sektor industri keuangan. Metode ini dipilih karena mampu menyediakan pemahaman yang mendalam, komprehensif, dan terstruktur terhadap berbagai studi sebelumnya yang relevan. Tinjauan literatur tidak hanya dilakukan untuk merangkum temuan penelitian sebelumnya, tetapi juga untuk melakukan evaluasi kritis terhadap pendekatan, hasil, serta kesimpulan yang telah dihasilkan oleh berbagai peneliti terdahulu.

Proses pencarian literatur dilakukan secara sistematis menggunakan sejumlah basis data ilmiah seperti Connected Papers, Google Scholar, dan ResearchGate. Pencarian artikel dilakukan dengan menggunakan kata kunci seperti: "ISO 27001," "information security," "user trust," dan "financial industry." Rentang waktu publikasi artikel yang dipertimbangkan adalah dari tahun 2013 hingga 2025 untuk memastikan bahwa literatur yang dikaji masih relevan dengan perkembangan terkini dalam implementasi ISO 27001. Selain itu, kriteria inklusi mencakup jurnal yang telah melalui proses peer-review dan secara spesifik membahas penerapan ISO 27001 atau aspek keamanan informasi dalam konteks organisasi, khususnya di sektor keuangan.

Dari proses pencarian tersebut, dilakukan proses penyaringan awal berdasarkan judul dan abstrak untuk mengidentifikasi artikel yang paling relevan. Artikel-artikel yang lolos tahap penyaringan kemudian dianalisis lebih lanjut melalui evaluasi isi untuk menilai kesesuaian tujuan penelitian, serta hasil yang dilaporkan. Total sebanyak sembilan artikel jurnal ilmiah yang memenuhi kriteria akhir dianalisis secara mendalam sebagai sumber utama dalam pembahasan.

Data dari jurnal-jurnal tersebut kemudian dikelompokkan berdasarkan tema-tema besar yang ditemukan, seperti implementasi sistem manajemen keamanan informasi (ISMS), pengaruh ISO terhadap kepercayaan pengguna, tantangan implementasi ISO 27001, serta dampak teknis dan manajerial dari penerapan ISO. Analisis dilakukan dengan pendekatan naratif deskriptif, yaitu menguraikan kesamaan dan perbedaan antar studi, mengelompokkan hasil-hasil yang sejenis, dan mengidentifikasi pola atau tren yang muncul dari literatur yang dikaji.

HASIL DAN PEMBAHASAN

Implementasi ISO 27001 Dalam Meningkatkan Kepercayaan Pengguna Dalam Sektor Industri Keuangan: Literature Review

Artikel yang telah dipilih, kemudian di masukkan dalam tabel yang dapat menjelaskan tentang: judul artikel, penulis, tahun terbit, tujuan penelitian, metode penelitian, hasil penelitian, serta batasan penelitian. Adapun data charting di jelaskan dalam tabel berikut:

Tabel 1. Data Charting

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
Utilization of ISO 27001 : 2022 In,Designing Information Security for Digital Transformation at BPRCO SME	2024 / Dafa Dinda Bayu Rama Dika, Rahmat Mulyana, Muharman Lubis	Penelitian ini menggunakan metode kualitatif dengan pendekatan Design	Penerapan ISO 27001 pada BPRBCo terbukti meningkatkan kepercayaan	Pengumpulan data dalam penelitian ini hanya melalui wawancara dan analisis dokumen," ,sehingga belum,mencakup seluruh perspektif

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
		<p>Science Research (DSR) dan studi kasus pada perusahaan BPRBCo, bertujuan merancang sistem manajemen keamanan informasi yang selaras", dengan ISO,27001: 2022. Pendekatan ini menekankan pemahaman mendalam terhadap konteks dan,"permasalahan organisasi, dengan analisis tematik untuk mengidentifikasi pola dari data kualitatif yang diperoleh melalui wawancara, analisis dokumen internal, dan observasi proses bisnis. ²</p>	<p>pengguna di sektor keuangan dengan membantu perusahaan memenuhi regulasi OJK dan menerapkan pendekatan berbasis risiko untuk,mengantisipasi serta,"mengurangi ancaman siber. Namun, implementasinya menghadapi tantangan, seperti", "perlunya pelatihan berkelanjutan karena belum semua pegawai memahami pentingnya keamanan informasi, serta waktu yang dibutuhkan untuk menerapkan perubahan kebijakan dan prosedur. ³</p>	<p>pemangku kepentingan di BPRCo. Jurnal ini juga tidak mengevaluasi,implementasi yang diberikan, sehingga belum tersedia data empiris untuk menilai efektivitas sistem manajemen keamanan informasi (ISMS) yang dirancang. Selain itu, tidak ada umpan balik atau survei dari pengguna untuk mengetahui persepsi mereka terhadap keamanan dan",keandalan sistem berbasis ISO 27001. ⁴</p>

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
<p>Analisis Perkembangan Teknologi M-BCA dan Keamanan Siber di Bank Central Asia</p>	<p>2024 / Rahmi Alfarizi, Achmad Justitio Satrio, Yendrikho Oktaviand Prasetyo, Muhammad Firdaus Syahputra</p>	<p>Jurnal tersebut menggunakan metode kualitatif dengan studi literatur, wawancara, dan penelusuran kebijakan. Metode pengumpulan data terdiri dari data primer yang dikumpulkan melalui wawancara terstruktur dengan ahli keamanan siber dan, "manajer TI di BCA," serta data sekunder yang dikumpulkan melalui dokumentasi internal dan laporan penelitian eksternal. ⁵</p>	<p>BCA telah menerapkan sistem manajemen keamanan informasi (ISMS) sesuai ISO 27001 dengan berbagai, "langkah, seperti," "enkripsi data, autentikasi ganda, dan pemantauan ancaman real-time untuk", melindungi data, sensitif dan mengatur, kontrol akses. Evaluasi risiko dilakukan secara berkala melalui uji penetrasi dan audit sistem guna, mengidentifikasi celah keamanan dan mengurangi ancaman siber. BCA juga membentuk Security Operation Center," (SOC)</p>	<p>Jurnal ini lebih berfokus pada aspek teknologi dan, "keamanan siber," "namun kurang memperhatikan komponen manajemen dan kebijakan yang juga penting dalam ISO 27001. Selain itu, jurnal tidak membahas audit internal maupun", "eksternal untuk," "menilai kepatuhan terhadap standar, yang merupakan bagian penting dari perbaikan berkelanjutan dalam ISMS. Meskipun membahas risiko", "keamanan, analisis risiko yang disajikan belum terstruktur secara sistematis. ⁷</p>

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
			C) untuk menangani ancaman secara real-time, serta meningkatkan kesadaran karyawan terhadap keamanan siber melalui pelatihan dan seminar rutin, sesuai dengan prinsip ISO 27001. ⁶	
"Keamanan Siber Dalam Perbankan Serta Tantangan dan Solusi Di Era Digital	2025 / Diny Widya Evriyanti Simatangkir, Eka Febriantika Nur," Afifah, Nafiza Salsabila Faliha"	Jurnal ini,"menganalisis metode kualitatif dengan pendekatan studi literatur, mengumpulkan data dari berbagai sumber seperti artikel, buku," "jurnal, dan referensi", kepercayaan terkait keamanan siber dan teknologi perbankan. Analisis dilakukan secara deskriptif	Jurnal ini membahas penerapan kebijakan keamanan seperti,"fire wall, enkripsi, autentikasi multifaktor, dan sistem deteksi intrusi, yang merupakan bagian dari",kontrol teknis ISO,"27001. Sejalan dengan pendekatan berbasis risiko yang dianjurkan ISO 27001, jurnal juga menyoroti pentingnya analisis	Jurnal tidak,memberikan rencana tindakan perbaikan yang jelas untuk mengatasi kekurangan yang diidentifikasi,dalam sistem,"keamanan, yang",merupakan bagian,penting dari siklus PDCA (Plan-Do- Check-Act) dalam ISO 27001. ¹⁰

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
		dan komparatif dengan membandingkan strategi terbaik dari berbagai bank di sejumlah negara dalam menghadapi ancaman siber. ⁸	risiko dalam menghadapi serangan siber seperti phishing, malware, dan DDoS. Selain itu, jurnal menekankan bahwa tujuan utama penerapan ISO 27001 adalah meningkatkan kepercayaan pelanggan melalui perlindungan data pribadi dan menjaga kelangsungan bisnis, dengan keamanan",sistem perbankan sebagai faktor kunci kepercayaan nasabah terhadap layanan digital. ⁹	
ISO 27001 in,Banking: An Evolution of Its Implementation,And Effectiveness in Enhancing Information Security	2023 / Sarah Kuzankah Ewugal, Zainab Efe Egieya, Adedolapo Omotosho, Abimbola	Metode yang,digunakan adalah,kualitatif dengan,analisis studi kasus implementa	Penerapan ISO 27001 secara signifikan meningkatkan manajemen risiko dan,kontrol	Keterbatasan penelitian ini terletak pada cakupan perbankan yang ada di,"Nigeria, yang mana", "hal ini tidak dapat digeneralisasi untuk sektor perbankan di negara

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
	Oluwatoyin Adegbite	si,"ISO 270001 di sektor perbankan. Data yang dianalisis diperoleh dari wawancara, survei dan menilai tingkat implementasi dokumen ISO 27001 dalam meningkatkan keamanan informasi. ¹¹	keamanan,informasi di lembaga keuangan melalui,identifikasi dan,"pengelolaan risiko terhadap data sensitif, sehingga mengurangi kecemasan dan meningkatkan kepercayaan konsumen. Hasil penerapannya meliputi peningkatan keamanan informasi, respons cepat terhadap insiden, terbentuknya budaya kesadaran keamanan dalam organisasi, komitmen terhadap perlindungan data, serta kepatuhan terhadap regulasi yang mendukung kepercayaan konsumen dan memberikan keunggulan kompetitif	lain yang mengadopsi budaya yang berbeda, karena budaya organisasi juga memegang peran",penting dalam organisasi. ¹³

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
			bagi perusahaan. ¹²	
<p>Penerapan, Manajemen, "Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet</p>	<p>2024 / Farhan Azhari, Sumarno, Achmad Fauzi, Demas Rizky Pratama</p>	<p>Penelitian ini, melakukan peninjauan, terhadap literatur yang relevan. Dengan cara mengumpulkan data studi kasus dari pengguna transaksi e-wallet yang telah mengalami serangan atau penipuan sebelumnya. Menggunakan teknik analisis kualitatif untuk mendapatkan pemahaman yang komprehensif tentang isu-isu tersebut.¹⁴</p>	<p>Sistem keamanan e-wallet, mencakup, pemantauan otomatis untuk mendeteksi aktivitas mencurigakan, seperti transaksi dalam jumlah besar atau pola transaksi tidak normal. Selain itu, sistem ini menerapkan enkripsi data baik saat penyimpanan maupun transmisi guna mencegah pencurian informasi oleh pihak tidak berwenang. Edukasi kepada pengguna juga, dilakukan untuk, mengurangi risiko kejahatan siber yang</p>	<p>Penelitian ini memiliki, "beberapa kekurangan," di antaranya belum secara jelas, "mengaitkan penerapan manajemen keamanan dengan standar ISO 27001, sehingga kesesuaiannya dengan standar internasional belum dapat dipastikan. Selain itu, aspek kepercayaan pengguna belum", "dibahas secara mendalam, terutama dari sudut pandang pengalaman dan persepsi pengguna e-wallet, serta belum menggunakan metode kuantitatif untuk", mengukur secara langsung pengaruh sistem keamanan terhadap tingkat kepercayaan pengguna.¹⁶</p>

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
			sering terjadi akibat kelalaian dalam menjaga informasi pribadi. ¹⁵	
Re-assessment Konsistensi Dokumen Kontrol Sertifikasi ISO,27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, Tbk	2022 / Sigit Tri Yuwono, Nanang Pratama, Vivi Afifah	Penelitian dilakukan secara observasional dan analitis selama praktik magang di, Bagian Komunikasi Satelit Monitoring PT. Bank BRI. Digunakan model PDCA untuk mengevaluasi pelaksanaan kebijakan keamanan informasi dengan bantuan, checklist ISO 27001:2013. Selain, itu, digunakan pula instrumen checklist yang mengacu pada klausula dan Annex ISO	Skor implementasi ISO 27001 tinggi: 81% untuk onboarding karyawan dan 90%," untuk pengelolaan vendor, menandakan integrasi prosedur keamanan yang kuat. Hal ini menunjukkan komitmen bank dalam menjaga keamanan data secara", "menyeluruh, baik internal maupun", "eksternal, yang", berdamak positif terhadap kepercayaan pengguna. ¹⁸	Penelitian hanya mencakup satu unit kerja, sehingga tidak", bisa digeneralisasi ke," seluruh organisasi. Tidak ada pengukuran langsung dari pengguna eksternal, sehingga klaim peningkatan kepercayaan pengguna masih bersifat asumsi teoretis. ¹⁹

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
		27001:2013 sebagai alat ukur konsistensi pelaksanaan ¹⁷		
Perencanaan dan Implementasi Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2005 (Studi,"Kasus Pada Sebuah Bank Swasta Nasional)	2013 / Nugroho Arif Widodo, R. Rizal Isnanto, Adian Fatchur Rochim	Menggunakan pendekatan kuantitatif deskriptif melalui studi kasus dan kuesioner Indeks,"KA MI. Risiko dianalisis berdasarkan aspek Confidentiality, Integrity, dan Availability (CIA), serta dilakukan pemetaan kontrol ISO 27001 terhadap aset", "kritis seperti SDM, perangkat, data, dan infrastruktur. Evaluasi tingkat kematangan dilakukan melalui lima domain utama Indeks KAMI. ²⁰	70% aset tergolong risiko rendah, dan insiden keamanan berkurang hingga 40%, menunjukkan efektivitas penerapan ISO dalam mitigasi risiko. Implementasi juga berkontribusi pada meningkatnya rasa aman dan kepercayaan pengguna terhadap sistem bank. ²¹	Tingkat kematangan sistem masih rendah, belum memenuhi standar minimal ISO. Selain itu, belum ada data dari pihak eksternal mengenai persepsi kepercayaan, padahal ini penting untuk menilai efektivitas implementasi ISO dari", sudut pandang pengguna. ²²

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
<p>Penerapan ISO,27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi: Literatur Review</p>	<p>2022/Media Jurnal,"Informatika (MJI), Vol. 14 No. 1, Juni",2022</p>	<p>Studi literatur sistematis terhadap 13 jurnal ilmiah dari Scopus, difokuskan pada topik ISO 27001, manajemen risiko, dan keamanan informasi. Data dianalisis dengan alat bantu Mendeley dan Excel, serta visualisasi tema menggunakan VOSviewer untuk menemukan tren dan keterkaitan antar topik.²³</p>	<p>Mayoritas studi menunjukkan bahwa penerapan ISO 27001 efektif menurunkan risiko dan,"meningkatkan kesadaran keamanan. Insiden keamanan berkurang hingga 40% dalam beberapa kasus, yang membantu membangun kepercayaan publik terhadap institusi yang menerapkan standar ini secara konsisten.²⁴</p>	<p>Tidak melibatkan data empiris atau persepsi pengguna secara,"langsung. Jumlah jurnal terbatas dan fokus penelitian masih teknis, belum,"menyentuh aspek,"psikologis seperti loyalitas atau rasa aman pengguna. Tantangan implementasi dibahas, namun solusi jangka panjang belum digali secara mendalam.²⁵</p>
<p>PENYUSUNAN KEBIJAKAN KEAMANAN TEKNOLOGI INFORMASI,PADA,TRANSAKSI ELECTRONIC BANKING PERBANKAN UMUM BERDASARKAN PERATURAN BANK INDONESIA NOMOR 9/15/PBI/2007</p>	<p>2018 / R. Irman Hariman</p>	<p>Penelitian ini menggunakan metode kualitatif dengan studi literatur untuk merumuskan,kebutuhan penelitian," dan membentuk paradigma</p>	<p>Penelitian ini menemukan bahwa kebijakan keamanan transaksi elektronik di bank umum belum,"seragam, sehingga","implementasi ISO 27000 dapat menjadi</p>	<p>Pendekatan penelitian ini bersifat kualitatif melalui studi literatur tanpa data empiris langsung dari institusi,"perbankan, sehingga","model kebijakan yang dihasilkan belum teruji dalam praktik nyata dan masih,memerlukan validasi lebih lanjut. Ruang lingkup penelitian juga</p>

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
<p>DENGAN MENGGUNAKAN MATRIKS COBIT 4.1 DAN,ISO/IEC 27000</p>		<p>baru,"dengan tujuan memperoleh model yang tepat dalam penyusunan tahapan keamanan transaksi elektronik di bank umum. ²⁶</p>	<p>solusi dengan menyediakan kerangka kerja yang sistematis dan sesuai regulasi. Dengan menggabungkan kontrol objektif dari COBIT 4.1 DS-5 dan ISO/IEC 27000, bank,"dapat menyusun kebijakan keamanan yang lebih terstruktur, meningkatkan efektivitas audit TI, serta mempercepat respons terhadap,"insiden keamanan. Selain itu, penerapan SOP berdasarkan kebijakan yang selaras dengan ISO 27000 memungkinkan departemen IT menangani gangguan infrastruktur dengan</p>	<p>terbatas pada,pemetaan antara,"ISO/IEC 27000,"COBIT 4.1 (DS-5),"dan Peraturan Bank Indonesia No. 9/15/PBI/2007, tanpa mempertimbangkan regulasi terbaru, perbedaan karakteristik bank, serta faktor sosial dan organisasional seperti kesiapan SDM dan budaya keamanan informasi yang turut memengaruhi keberhasilan implementasi kebijakan. ²⁸</p>

Judul	Penelitian/Tahun/Peneliti	Metode dan Analisis	Hasil Penelitian	Keterbatasan Penelitian
			lebih responsif, sehingga mendukung "keandalan dan,keamanan transaksi elektronik. <small>27</small>	

Sebuah tinjauan literatur yang dilakukan pada sembilan jurnal menunjukkan bahwa penerapan ISO 27001 memainkan peran yang signifikan dalam membangun sistem manajemen keamanan informasi (ISMS) yang kuat di sektor keuangan. Standar ini tidak hanya menawarkan kerangka kerja yang sistematis, tetapi juga menawarkan pendekatan berbasis risiko yang mampu mengantisipasi dan menanggapi secara proaktif ancaman siber. Meskipun masing-masing studi menggunakan pendekatan, konteks, dan fokus yang berbeda, hampir semua jurnal yang dianalisis setuju bahwa peningkatan keamanan sistem dan kepercayaan konsumen dipengaruhi langsung oleh penerapan ISO 27001.

Dalam implementasi ISO 27001, pendekatan berbasis organisasi dan budaya kerja sangat penting, menurut beberapa jurnal, seperti Dika et al. (2024) dan Ewugal et al. (2023). Dika et al (2024) membangun sistem keamanan di BPRCo dengan menggunakan metodologi penelitian sains desain. Penelitian mereka menunjukkan bahwa, melalui pendekatan berbasis risiko, sistem tersebut membantu perusahaan mematuhi peraturan OJK dan menumbuhkan kepercayaan pengguna. Namun, penelitian ini belum mengevaluasi efektivitas secara empiris melalui keterlibatan pengguna dan masih terbatas pada data internal. Sebaliknya, Ewugal et al. (2023) melakukan survei dan wawancara tentang industri perbankan Nigeria. Mereka berhasil menunjukkan bahwa penerapan ISO 27001 dapat meningkatkan kesadaran karyawan, meningkatkan efisiensi audit, dan memberikan keunggulan kompetitif melalui kepatuhan terhadap peraturan.

Berbeda dengan pendekatan berbasis organisasi, Alfarizi et al. (2024) meneliti bagaimana Bank Central Asia (BCA) menerapkan ISO 27001 secara teknis melalui pengamanan sistem seperti enkripsi data, autentikasi multifaktor, dan pembentukan Security Operation Center (SOC). Dalam menciptakan budaya keamanan informasi, pelatihan dan kesadaran karyawan juga sangat penting. Namun, jurnal ini belum mempelajari hubungan antara sistem yang dibangun denganelemen manajerial dan siklus audit internal dan eksternal, yang merupakan komponen penting dari kerangka ISO 27001.

Dalam penelitian yang dilakukan oleh Simatangkir et al. (2025), mereka membandingkan strategi pengamanan siber yang berbeda untuk berbagai bank yang berasal dari berbagai negara. Ini memperkaya pembicaraan. Studi ini menunjukkan bahwa aspek teknis seperti firewall atau IDS/IPS tidak hanya menentukan keberhasilan sistem keamanan, tetapi juga kemampuan organisasi untuk menilai dan mengelola risiko yang terus berkembang. Dalam hal ini, ISO 27001 diposisikan sebagai standar global yang meningkatkan keamanan dan meningkatkan kepercayaan masyarakat terhadap layanan keuangan digital. Sementara itu, Hariman (2018) dan Widodo et al. (2013) berusaha menyelaraskan elemen hukum lokal, manajemen risiko, dan kebijakan. Sehubungan dengan Peraturan Bank Indonesia No. 9/15/PBI/2007, Hariman menggunakan ISO/IEC 27000 dan COBIT 4.1 untuk membangun kebijakan keamanan transaksi elektronik. Metode ini menekankan betapa pentingnya struktur kebijakan yang akuntabel dan terstandarisasi. Meskipun implementasinya belum memenuhi standar ISO secara menyeluruh, Widodo menilai kematangan keamanan informasi dengan menggunakan pendekatan kuantitatif dan Indeks KAMI, yang menunjukkan penurunan risiko hingga 40%.

Selain itu, literatur yang mengangkat perspektif pengguna mulai muncul. Azhari et al. (2024) melakukan penelitian tentang sistem keamanan e-wallet yang mencakup pengawasan tindakan mencurigakan, enkripsi, dan instruksi pengguna. Penelitian ini belum menunjukkan pengukuran

langsung terhadap persepsi pengguna atau dampak sistem terhadap kepercayaan konsumen, meskipun fitur keamanan ini sejalan dengan prinsip ISO 27001. Dengan penelitian ini, dapat dieksplor lebih jauh hubungan antara pengalaman pengguna layanan digital dan keamanan data mereka.

Yuwono et al. (2022) melakukan penilaian kembali konsistensi pelaksanaan ISO 27001:2013 di bagian Komunikasi Satelit Bank BRI dan menemukan bahwa pengelolaan keamanan, terutama manajemen vendor dan onboarding karyawan, menerima skor tinggi. Ini menunjukkan bahwa penerapan ISO memiliki dampak pada manajemen hubungan internal dan pihak ketiga. Namun, penelitian ini tidak mencakup evaluasi dari pengguna eksternal, dan hanya membatasi satu unit.

Terakhir, Media Jurnal Informatika (2022) melakukan literature review pada tiga belas jurnal dan menemukan bahwa ISO 27001 dapat meningkatkan kepercayaan publik dan mengurangi risiko hingga 40%. Sayangnya, penelitian ini lebih teknis daripada psikologis, seperti perasaan aman pengguna atau kesetiaan pengguna, yang penting untuk menilai dampak jangka panjang penerapan ISO 27001 terhadap hubungan antara lembaga keuangan dan pelanggannya.

Sebagian besar literatur setuju bahwa ISO 27001 memainkan peran penting dalam meningkatkan kepercayaan pengguna dan menjaga data aman. Sebagian besar penelitian setuju bahwa ISO 27001 menyediakan kerangka kerja yang fleksibel yang dapat diintegrasikan ke dalam berbagai sistem TI perbankan. Selain prosedur seperti pelatihan keamanan dan audit sistem, kontrol teknis seperti enkripsi, firewall, dan IDS/IPS telah menjadi kebiasaan. Namun, fokus dari masing-masing penelitian berbeda. Beberapa jurnal berfokus pada teknis (seperti BCA dan e-wallet), yang lain pada manajemen dan kebijakan (seperti BPRBCo dan Bank Indonesia), dan yang lain memeriksa pengalaman pengguna dan budaya perusahaan. Selain itu, sebagian besar penelitian menggunakan pendekatan kualitatif, sementara beberapa menggabungkan pendekatan kuantitatif atau pendekatan campuran dengan data kuantitatif.

Literatur ini memberikan pemahaman yang luas dan beragam tentang masalah utama penelitian, yaitu bagaimana ISO 27001 dapat meningkatkan keamanan data dan kepercayaan pengguna di sektor keuangan. Secara garis besar, literatur mencakup hal-hal berikut:

1. Implementasi kerangka kerja ISO 27001 yang terbukti efektif dalam mitigasi risiko dan perlindungan data
2. Peningkatan budaya organisasi terkait keamanan melalui pelatihan dan SOP; dan
3. Peluang untuk meningkatkan kepercayaan pengguna melalui transparansi dan komitmen keamanan.

SIMPULAN

Berdasarkan tinjauan literatur terhadap sembilan jurnal, dapat disimpulkan bahwa penerapan ISO 27001 memiliki peran krusial dalam memperkuat sistem manajemen keamanan informasi (ISMS) di sektor keuangan. ISO 27001 tidak hanya berfungsi sebagai standar teknis, tetapi juga sebagai kerangka kerja strategis berbasis risiko yang mampu meningkatkan ketahanan terhadap ancaman siber serta menumbuhkan kepercayaan konsumen. Meskipun pendekatan masing-masing penelitian berbeda baik dari sisi teknis, manajerial, maupun budaya organisasi semuanya menyepakati bahwa penerapan ISO 27001 membawa dampak positif terhadap peningkatan keamanan data dan kepercayaan terhadap layanan keuangan digital. Penerapan standar ini mencakup berbagai aspek, mulai dari penguatan kontrol teknis (seperti enkripsi, firewall, IDS/IPS), pelatihan keamanan, hingga penilaian terhadap manajemen risiko dan audit internal. Selain itu, sebagian studi juga mulai menyoroti pentingnya persepsi pengguna terhadap keamanan layanan yang mereka gunakan. Namun demikian, masih terdapat beberapa keterbatasan, seperti minimnya evaluasi terhadap pengalaman pengguna secara langsung, keterbatasan cakupan responden, serta kurangnya integrasi antara aspek teknis dan elemen manajerial dalam beberapa penelitian.

UCAPAN TERIMA KASIH

Peneliti menyampaikan ucapan terima kasih kepada semua pihak yang telah berkontribusi dalam pelaksanaan penelitian dan penyusunan artikel ini.

REFERENSI

Alfarizi, R., Satrio, A. J., Prasetyo, Y. O., & Syahputra, M. F. (2024). Analisis Perkembangan Teknologi

- M-BCA dan Keamanan Siber di Bank Central Asia. *Jurnal Akademik Ekonomi Dan Manajemen*. 1(4) 43-53.
- Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., & Ghaffar, N. S. A. (2024). Penerapan Manajemen Sekuriti dalam Meningkatkan Keamanan Pengguna pada Transaksi E-wallet. *Jurnal Kajian Manajemen dan Teknologi*, 2(2), 138–144. <https://doi.org/10.38035/jkmt.v2i2>
- Azhari, F., Sumarno, Fauzi, A., & Pratama, D. R. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet. *Jurnal Kewirausahaan dan Multi Talenta*. 2(2).138-147.
- Dewi, F. P., Rachman, B., & Rivanda, A. K. (2024). Peran Kualitas Pelayanan, Kepercayaan Nasabah, Citra, dan Kepuasan Nasabah dalam Mendapatkan Loyalitas Nasabah pada Industri Lembaga Keuangan Mikro Syariah di Jawa Barat. *Jurnal Ilmiah MEA*, 8(2), 2530–2539.
- Dika, D. D. B. R., Mulyana, R., & Lubis, M. (2024). Utilization of ISO 27001 : 2022 In Designing Information Security for Digital Transformation at BPRCO SME. *Kesatria : Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*. 5(4). 1824-1835.
- Ewuga, T. O, Sunday, M. O., & Ojo, J. O. (2023). *The role of ISO 27001 standard in managing information security risks in the banking sector*. *Journal of Financial Risk Management*, 14(2), 118–132.
- Ewuga, S. K., Egieya, Z. E., Omotosho, A., & Adegbite, A. O. (2023). Iso 27001 in Banking: an Evaluation of Its Implementation and Effectiveness in Enhancing Information Security. *Finance & Accounting Research Journal*, 5(12), 405–425. <https://doi.org/10.51594/farj.v5i12.684>
- Hariman, R. I. (2018). Penyusunan Kebijakan Keamanan Teknologi Informasi pada Transaksi Electronic Banking Perbankan Umum berdasarkan Peraturan Bank Indonesia Nomor 9/15/PBI/2007 dengan Menggunakan Matriks COBIT 4.1 dan ISO/IEC 27000. *Syntax Literate; Jurnal Ilmiah Indonesia*. 3(7). 99-111.
- Hisyam, G. F., & Rojabi, M. A. (2025). Analisis dan Penerapan Sistem Manajemen Keamanan Aplikasi Point of Sales Menggunakan ISO 27001. *Integrative Perspectives of Social and Science Journal*, 2(1), 1087–1094.
- Irwansyah. (2024). TIPOLOGI LITERATURE REVIEW DALAM METODE PENELITIAN.
- Jauhary, H., Pratiwi, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review. *Media Jurnal Informatika*. 14(1). 43-49.
- Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors. *International Journal of Advanced Computer Science and Applications*, 13(1), 195–206. <https://doi.org/10.14569/IJACSA.2022.0130124>
- Muhtasimi, A., Siregar, R. E., & Permana, D. (2022). Pengaruh faktor keamanan informasi terhadap kepuasan pengguna layanan dompet digital di Indonesia. *Jurnal Teknologi Informasi dan Komunikasi*, 10(3), 207–219.
- Sahut, J-M., Abdou, H., & Mili, M. (2024). Trust in digital financial services: A key element of cybersecurity success. *International Journal of Information Security and Privacy*, 18(1), 1–15.
- Sahu, A., Khemka, M., Agrawal, A., Shadan, M., & Sahu, B. (2024). Consumer Confidence in Digital Finance: Trust Dynamics in Online Banking. *International Journal For Multidisciplinary Research*, 6(3), 1–9. <https://doi.org/10.36948/ijfmr.2024.v06i03.19946>
- Simatangkir, D. W. E., Afifah, E. F. N., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*. 2(1). 33-42.
- Widodo, N. A., Isnanto, R. R., & Rochim, A. F. (2013). Perencanaan dan Implementasi Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2005 (Studi Kasus Pada Sebuah Bank Swasta Nasional). *Transient: Jurnal Ilmiah Teknik Elektro*. 2(3). 627-634.
- Yuwono, S. T., Pratama, N., & Afifah, V. (2022). Re-assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, Tbk. *IKRA-ITH Informatika: Jurnal Komputer dan Informatika*. 6(2). 21-28.