Jurnal Teknologi dan Manajemen Industri Terapan (JTMIT) Vol. 4, No. 3, September 2025 pp. 766 - 776
P-ISSN: 2829-0232 E-ISSN: 2829-0038

Model Tata Kelola TI Terintegrasi untuk Keamanan Informasi di Sektor *Fintech*

Merryana Lestari[1], Maria Entina Puspita[2], Agustinus Fritz Wijaya[3], Vicky[4]
[1, 4)] Information System, Universitas Bunda Mulia, Jakarta, Indonesia
Email: mlestari@bundamulia.ac.id, 31220073@student.ubm.ac.id
[2)] Accounting, STIE "AMA" Salatiga, Indonesia
Email: mariaentina@stieama.ac.id
[3)] Informatics, Universitas Bunda Mulia, Jakarta, Indonesia
Email: agustinus.wijaya@bundamulia.ac.id

ABSTRAK

Penelitian ini menggali penerapan *framework* tata kelola TI yang tepat khususnya untuk keamanan informasi yaitu dengan mengkombinasikan ISO/IEC 27001:2022, ISO/IEC 27005:2018 dan NIST Cybersecurity *Framework* 2.0 dalam konteks Perusahaan *fintech*, serta bagaimana prinsip-prinsip tersebut membantu dalam mitigasi risiko terkait ancaman keamanan informasi. Model tata kelola tersebut terdiri dari 6 (enam) tahapan praktis untuk memperkuat keamanan informasi yang cocok diterapkan khususnya pada Perusahaan *fintech*, yaitu Inisiasi dan Tata Kelola Perusahaan, Desain dan Implementasi keamanan informasi, Penguatan sumber daya manusia, Keamanan operasional, Keamanan pengembangan, serta Evaluasi dan peningkatan. Model tata kelola ini mendukung perusahaan *fintech* dalam membangun sistem keamanan informasi yang tangguh, adaptif, dan berkelanjutan, yang mampu melindungi aset, menjaga kepercayaan pelanggan, serta dapat memastikan kelangsungan operasional di tengah ancaman siber yang terus berkembang.

Kata kunci: *Fintech*, Keamanan Informasi, ISO/IEC, NIST, Tata Kelola Teknologi Informasi.

ABSTRACT

This research explores the implementation of an appropriate IT governance framework for information security by integrating ISO/IEC 27001:2022, ISO/IEC 27005:2018, and the NIST Cybersecurity Framework 2.0 within the context of fintech companies, and examines how these principles assist in mitigating information security risks. The governance model consists of six practical stages to strengthen information security, specifically suited for fintech companies: Initiation and Corporate Governance, Design and Implementation of Information Security, Human Resource Strengthening, Operational Security, Secure Development, and Evaluation and Improvement. This model supports fintech companies in building resilient, adaptive, and sustainable information security systems capable of protecting assets, maintaining customer trust, and ensuring operational continuity amid evolving cyber threats.

Keywords: *Fintech, Information Security, ISO/IEC, NIST, Information Technology Governance.*

Pendahuluan

Perkembangan pesat industri *fintech* (financial technology) telah membawa dampak signifikan pada sektor keuangan global, termasuk di Indonesia [1]. *Fintech* menawarkan kemudahan akses layanan keuangan digital yang cepat, murah, dan inklusif, sehingga mampu menjangkau segmen masyarakat yang sebelumnya sulit terlayani oleh lembaga keuangan konvensional [2]. Menurut laporan kantor akuntan publik, PricewaterhouseCoopers (PwC) tahun 2022, 58% perusahaan *fintech* global melaporkan adanya ancaman keamanan siber yang mengganggu operasional mereka [3]. Ancaman ini dapat berupa peretasan, pencurian data pribadi, serangan malware, hingga pelanggaran kebijakan privasi yang dapat merugikan pengguna dan merusak reputasi Perusahaan [4]. Seiring dengan meningkatnya kompleksitas ancaman terhadap data dan informasi, pemahaman dan implementasi tata kelola TI yang baik menjadi krusial. Namun, banyak pelaku *fintech* yang masih menghadapi kesulitan dalam merumuskan kebijakan dan strategi keamanan yang efektif [4]. Masalah utama yang dihadapi oleh banyak perusahaan *fintech* adalah kurangnya model tata kelola teknologi informasi (*IT governance*) yang memadai dalam pengelolaan risiko-risiko keamanan informasi [5], [6]. Selain itu, lemahnya regulasi dan perlindungan konsumen terhadap *cybercrime* masih menjadi kendala utama yang menghambat perkembangan *fintech* secara optimal di beberapa negara, termasuk Indonesia [7].

Tata kelola teknologi informasi yang baik sangat penting dalam menciptakan keamanan dan keberlanjutan operasional *fintech*. Menurut ISACA (2021), perusahaan *fintech* perlu mengadopsi *best practices*

dalam tata kelola TI untuk dapat mengidentifikasi, mengelola, dan mengurangi risiko yang terkait dengan ancaman siber. Pengabaian terhadap tata kelola yang baik dapat menyebabkan kerugian dalam bidang finansial, hukum, dan reputasi yang serius [8]. Tata kelola TI yang baik membantu perusahaan *fintech* dalam merumuskan kebijakan, prosedur, dan kontrol keamanan yang komprehensif, sekaligus memastikan kepatuhan terhadap regulasi yang berlaku, seperti sertifikasi ISO/IEC 27001 yang kini menjadi salah satu persyaratan utama untuk memperoleh izin usaha dari Otoritas Jasa Keuangan (OJK) di Indonesia [7], [9].

Implementasi standar ISO/IEC 27001 terbukti mampu meningkatkan kepercayaan pelanggan dan mitra bisnis melalui penguatan perlindungan data dan pengelolaan risiko keamanan informasi secara sistematis. Studi empiris pada perusahaan *fintech* menunjukkan bahwa penerapan sistem manajemen keamanan informasi berbasis ISO/IEC 27001 dengan pendekatan siklus *Plan-Do-Check-Act* (PDCA) dapat meningkatkan tingkat kematangan keamanan informasi dan mengurangi insiden kebocoran data [7], [9]. Selain itu, manajemen risiko yang terstruktur sesuai ISO/IEC 27005:2018 memberikan panduan metodologis untuk mengidentifikasi, menganalisis, dan mengelola risiko secara efektif, sehingga *fintech* dapat menentukan prioritas mitigasi risiko yang tepat dan mengurangi potensi kerugian finansial maupun operasional akibat serangan siber [10]. *Framework* NIST Cybersecurity *Framework* (CSF) juga banyak diadopsi sebagai kerangka kerja yang fleksibel dan praktis dalam mengelola risiko keamanan siber secara menyeluruh, mulai dari identifikasi aset, perlindungan, deteksi, respons, hingga pemulihan pasca insiden [11], [12]. Integrasi NIST CSF dengan ISO/IEC 27001 memungkinkan perusahaan *fintech* untuk membangun sistem keamanan yang adaptif dan berkelanjutan, sesuai dengan dinamika ancaman yang terus berkembang [13]. Selain aspek teknis, pelatihan dan peningkatan kesadaran keamanan bagi sumber daya manusia juga menjadi faktor penting dalam mengurangi risiko kesalahan manusia yang sering menjadi celah keamanan [14].

Penelitian ini bertujuan untuk mengkaji kebijakan, prosedur, dan standar operasional yang diterapkan untuk mengelola dan melindungi keamanan informasi serta sistem informasi di sektor *fintech*. Penelitian ini juga akan menggali penerapan *framework* tata kelola TI yang tepat khususnya untuk keamanan informasi yaitu dengan mengkombinasikan ISO/IEC 27001:2022, ISO/IEC 27005:2018 dan NIST *Cybersecurity Framework* 2.0 dalam konteks Perusahaan *fintech*, serta bagaimana prinsip-prinsip tersebut membantu dalam mitigasi risiko terkait ancaman keamanan informasi, seperti *fraud*, peretasan, kebocoran data, atau serangan siber lainnya. Fokus mitigasi dalam penelitian ini yaitu untuk memahami langkah-langkah preventif, detektif, dan responsif yang diterapkan oleh perusahaan *Fintech*, serta untuk menilai sejauh mana praktik-praktik ini berkontribusi pada pengurangan kerentanan terhadap ancaman yang semakin kompleks termasuk didalamnya mengenai evaluasi terhadap penerapan teknologi keamanan terkini, pelatihan SDM, serta aspek kepatuhan (*compliance*) terhadap regulasi yang relevan, seperti peraturan perlindungan data pribadi [15].

Metode Penelitian

Penerapan kebijakan keamanan yang berbasis pada analisis ancaman dan kerentanannya juga telah terbukti efektif dalam mengurangi potensi risiko [16]. Model *Risk-Based Approach* yang disarankan oleh ISO/IEC 27005:2018 mengusulkan bahwa organisasi harus memprioritaskan mitigasi terhadap ancaman yang memiliki dampak terbesar terhadap operasi mereka, dengan menggunakan analisis kuantitatif maupun kualitatif untuk menilai dan mengelola risiko [17], [18], [19]. Pemanfaatan teknologi terkini yang digunakan dalam sektor *fintech* juga dinilai mampu untuk meningkatkan keamanan informasi diantaranya teknologi yang mencakup solusi berbasis kecerdasan buatan (AI), *blockchain* dan *machine learning* [20], [21]. Solusi berbasis teknologi AI dan *machine learning* digunakan untuk mendeteksi pola serangan siber secara lebih cepat dan akurat, serta untuk menganalisis anomali dalam transaksi keuangan, sedangkan, teknologi *blockchain* semakin banyak digunakan dalam sektor *fintech* untuk meningkatkan transparansi dan keamanan transaksi, dimana memungkinkan pencatatan transaksi yang aman, tidak dapat diubah, dan terdesentralisasi, yang mengurangi potensi *fraud*, *data breaching* dan penyalahgunaan atau penipuan [20], [22], [23]. Penerapan *blockchain* pada *fintech* memberikan lapisan tambahan untuk memastikan keamanan data dan integritas transaksi [24], [25].

ISO/IEC 27001:2022 telah banyak dikaji dalam literatur sebagai standar utama sistem manajemen keamanan informasi (ISMS) yang efektif untuk berbagai organisasi di tengah meningkatnya ancaman siber dan tuntutan kepatuhan regulasi. Penerapan ISO/IEC 27001:2022 memperkuat tata kelola keamanan melalui integrasi kebijakan, prosedur, dan kontrol ke dalam proses bisnis. Penelitian ini juga mengidentifikasi komponen penting seperti konteks organisasi, kepemimpinan, perencanaan, dukungan, operasi, evaluasi kinerja, dan perbaikan berkelanjutan sebagai kunci keberhasilan implementasi [26]. Tingkat kematangan organisasi dalam menerapkan ISO/IEC 27001:2022 masih bervariasi, dengan banyak perusahaan yang masih berada pada tahap awal dan membutuhkan perbaikan kebijakan serta prosedur agar dapat memenuhi standar ini secara optimal [27]. Selain itu, penelitian aplikasi ISO/IEC 27001:2022 pada instansi pemerintah menunjukkan bahwa proses manajemen risiko yang terstruktur mampu mengidentifikasi berbagai ancaman dan dampak terhadap sistem informasi,

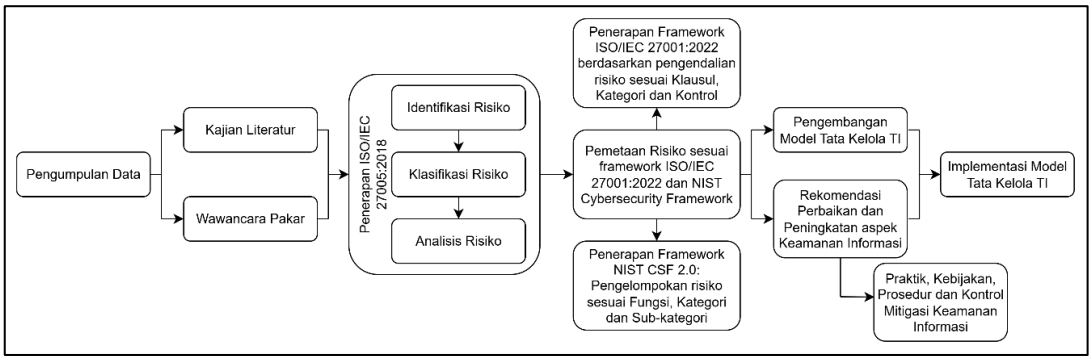
sehingga langkah mitigasi dapat dirancang secara lebih efektif sehingga menegaskan pentingnya pendekatan berbasis risiko dan perlunya evaluasi berkala untuk memastikan efektivitas pengendalian yang diterapkan [28].

ISO/IEC 27005:2018 diposisikan sebagai standar pendukung ISO/IEC 27001 yang secara khusus membahas manajemen risiko keamanan informasi. Pentingnya penyesuaian proses manajemen risiko sesuai ISO/IEC 27005:2018, mulai dari penetapan konteks, identifikasi dan analisis risiko, penentuan perlakuan risiko, hingga dokumentasi dan komunikasi risiko secara komprehensif. Hasil pemetaan risiko yang didasarkan pada standar ini memberikan gambaran detail mengenai risiko yang harus dimitigasi dan diterima oleh manajemen, serta menegaskan perlunya dokumentasi yang baik dalam seluruh proses manajemen risiko [10]. ISO/IEC 27005:2018 menawarkan pendekatan sistematis dan komprehensif untuk mengidentifikasi, menilai, dan menangani risiko keamanan informasi, serta selaras dengan standar ISO 31000 untuk manajemen risiko secara umum [29]. Hal ini memudahkan organisasi dalam memilih strategi mitigasi yang paling tepat sesuai konteks dan kebutuhan.

NIST *Cybersecurity Framework* (CSF) telah diadopsi secara luas di berbagai sektor sebagai kerangka kerja sukarela yang efektif dalam meningkatkan postur keamanan siber organisasi. Studi sistematis menunjukkan bahwa NIST CSF, dengan enam fungsi utamanya (*Identify, Protect, Detect, Respond, Recover,* dan *Govern*), memberikan fleksibilitas tinggi dan dapat diintegrasikan dengan standar lain seperti ISO/IEC 27001 [11][12]. *Framework* ini membantu organisasi dalam mengelola risiko siber secara menyeluruh, mulai dari identifikasi aset hingga pemulihan pasca-insiden. Penelitian juga menyoroti keunggulan NIST CSF dalam hal struktur yang mudah dipahami, skalabilitas, dan kemampuannya untuk diadaptasi sesuai kebutuhan spesifik tiap organisasi. Namun, beberapa literatur juga menyoroti tantangan dalam penerapan *framework* ini secara konsisten, terutama pada organisasi dengan sumber daya terbatas atau tingkat kematangan tata kelola TI yang masih rendah.

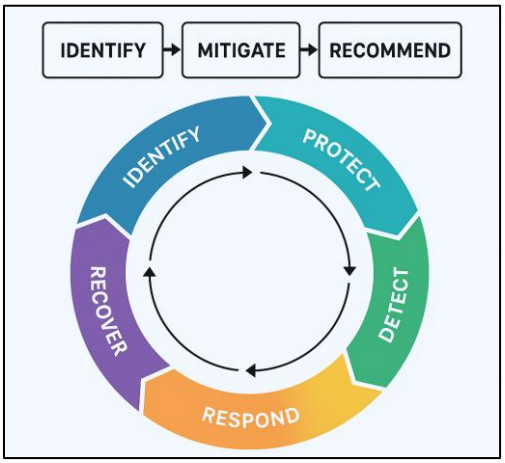
Melalui integrasi antara ISO/IEC 27001:2022, ISO/IEC 27005:2018, dan NIST CSF dapat memberikan hasil yang lebih optimal dalam tata kelola keamanan informasi [17], [30]. Dimana ISO/IEC 27001:2022 memberikan fondasi sistem manajemen, ISO/IEC 27005:2018 memperdalam aspek manajemen risiko, sementara NIST CSF menawarkan kerangka praktis dan adaptif yang mudah diimplementasikan di berbagai sektor [31].

Metode yang digunakan dalam penelitian ini bersifat deskriptif-kualitatif dengan pendekatan studi kasus pada beberapa perusahaan *fintech* yang ada di Indonesia, untuk mengidentifikasi dan menganalisis *best practices* tata kelola TI yang efektif dalam memitigasi ancaman terhadap keamanan informasi di sektor *fintech* [32], [33]. Oleh karena itu, penelitian ini akan menyoroti peran tata kelola TI yang baik dalam memastikan mitigasi ancaman keamanan informasi.



Gambar 1. Tahapan Penelitian

Tahapan penelitian ini melibatkan berbagai pendekatan yang mencakup pengumpulan data, berupa kajian literatur dan wawancara dengan pakar terkait risiko-risiko keamanan informasi di Perusahaan *fintech*, proses *expert judgement* untuk mengidentifikasi masalah yang berupa risiko-risiko pelanggaran keamanan informasi yang mungkin terjadi pada Perusahaan *fintech* dan tren ancaman yang berkembang saat ini, seperti serangan siber, kebocoran data, dan *fraud*. Termasuk didalamnya penerapan *framework* ISO/IEC 27005:2018 didalamnya termasuk proses pengidentifikasian risiko secara preventif, detektif, dan korektif dengan segala kemungkinan yang terjadi, kemudian dilanjutkan proses untuk mengklasifikasikan dan menganalisis risiko kedalam jenis ancaman dan dampak potensial yang akan ditimbulkannya. Setelah proses identifikasi masalah tersebut, kemudian dilanjutkan proses pemetaan risiko ke dalam *framework* NIST *Cybersecurity Framework* (NIST CSF 2.0) dan *framework* ISO/IEC 27001:2022, dimana dalam *framework* tersebut setiap risiko akan dikelompokan kedalam fungsi, klausul, kategori dan sub-kategori serta analisis bagaimana kontrol pengendaliannya. Setelah dilakukan pemetaan risiko, kemudian dilanjutkan proses rekomendasi untuk perbaikan dan peningkatan aspek keamanan informasi berdasarkan panduan kontrol pengendalian yang terdapat pada *framework* ISO/IEC 27001:2022 dan NIST CSF 2.0 berupa praktik, kebijakan, prosedur dan kontrol mitigasi keamanan informasi pengembangan model tata kelola TI dengan fokus keamanan informasi dan tahap terakhir dilakukan proses uji coba implementasi model tata kelola TI di Perusahaan *fintech,* yang dapat dilihat pada Gambar 1. Berikut model proses identifikasi, mitigasi, dan rekomendasi yang merupakan alur integrasi *framework* NIST Cybersecurity *Framework* (NIST CSF 2.0) dan ISO/IEC 27001:2022 ke dalam model 6 tahapan seperti pada Gambar 2.



Gambar 2. Model Proses Identifikasi, Mitigasi, dan Rekomendasi

Hasil dan Pembahasan

Berdasarkan hasil wawancara dengan praktisi dan pakar keamanan informasi didapatkan hasil yaitu pengelompokan beberapa permasalahan yang umumnya berisiko dan mengancam keamanan informasi di lembaga sektor finansial dan teknologi yang dikelompokan menjadi 2 (dua) yaitu ancaman *insider* dan ancaman *outsider*. Ancaman *insider* umumnya terjadi karena kurangnya kesadaran dan kepatuhan para karyawan, kontraktor, mitra bisnis, dan pihak internal lainnya yang secara sah memiliki akses langsung ke data, sistem maupun jaringan yang ada dalam perusahaan. Beberapa permasalahan yang sering terjadi diantaranya berupa kelalaian pegawai yang mengakibatkan pelanggaran keamanan informasi, seperti *information security breaches*, pencurian data, sabotase, penipuan dan bahkan spionase. Ancaman *outsider* umumnya lebih mengarah pada ancaman-ancaman keamanan informasi yang diakibatkan serangan dari luar, seperti serangan *malware*, *ransomware*, virus komputer, dan peretasan oleh hacker seperti *phising* dan *magecarting*. Ancaman-ancaman tersebut sangat berisiko untuk keberlangsungan perusahaan, berpotensi mengakibatkan kerugian finansial yang signifikan salah satunya yaitu berkurangnya kepercayaan para investor, tuntutan hukum dan pelanggaran terhadap regulasi, yang akan berdampak negatif pada hilangnya reputasi dan kepercayaan nasabah terhadap perusahaan.

Seiring dengan meningkatnya risiko keamanan informasi di sektor keuangan dan teknologi, kepatuhan terhadap regulasi pada sektor keuangan dan Undang-Undang Pelindungan Data Pribadi (UU PDP) menjadi sangat penting. Regulasi-regulasi pada sektor keuangan seperti kebijakan *macroprudential*, kebijakan *microprudential* dan UU PDP hadir sebagai langkah penting untuk memperkuat keamanan data dan memberikan sanksi terhadap pelanggaran keamanan informasi di Indonesia. Selain itu, regulasi global juga memainkan peran penting dalam meningkatkan standar keamanan siber, di mana regulator menuntut Lembaga sektor *fintech* untuk mematuhi standar keamanan tertentu, melakukan audit keamanan berkala, dan melaporkan insiden siber yang terjadi. Regulasi memberikan ruang bagi inovasi dan pertumbuhan *fintech* sambil memastikan bahwa pengembangannya tetap mematuhi prinsip-prinsip persyaratan kepatuhan dan pengawasan keuangan yang aman dan terpercaya. Lembaga sektor *fintech* harus mematuhi berbagai peraturan dan standar keamanan diantaranya seperti *Payment Card Industry Data Security Standard* (PCI-DSS), *General Data Protection Regulation* (GDPR), dan regulasi lokal terkait dengan privasi data seperti Otoritas Jasa Keuangan (OJK). Beberapa regulasi yang menjadi perhatian dalam penelitian ini diantaranya adalah cara penanganan dalam pengumpulan data nasabah dan transaksi keuangan, cara penyimpanan dan perlindungan terhadap data nasabah dan data keuangan, dan proses validasi kepatuhan serta proses auditing terhadap aspek kontrol keamanan informasi.

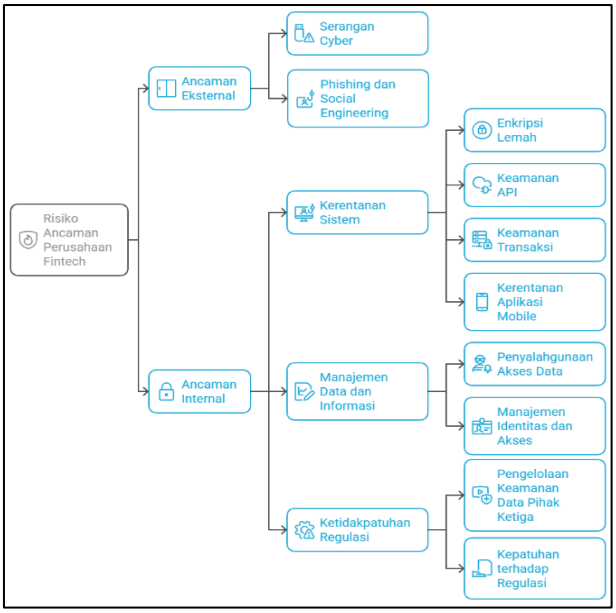
Berdasarkan beberapa regulasi yang berlaku mengenai perlindungan data pribadi, regulasi tersebut dapat dikelompokan menjadi beberapa pokok bagian yaitu regulasi yang membahas mengenai bagaimana data nasabah dikumpulkan dan dikelola, regulasi yang membahas mengenai bagaimana data nasabah dijamin keamanannya dan regulasi yang mengatur bagaimana aspek kepatuhan dilaksanakan sesuai dengan standar yang ditetapkan. Melalui regulasi mengenai pengumpulan dan pengelolaan data, proses pengumpulan dan pengelolaan data harus dilakukan berdasarkan asas kepastian hukum, kepentingan umum, dan aspek kerahasiaan. Dalam prosesnya, calon nasabah akan mengisi terlebih dahulu diminta persetujuan akan data pribadinya seperti data pribadi, data *biometric* dan data transaksi keuangan supaya dapat diolah dan dikelola oleh pengendali data secara transparan, yang berupa lembaga perbankan, dan lembaga non-perbankan seperti perusahaan keuangan, perusahaan sekuritas ataupun perusahaan asuransi dimana berkewajiban untuk menjaga kerahasiaan dan keamanan datanya. Dengan regulasi untuk jaminan keamanan data, pengendali data memiliki kewajiban untuk menerapkan langkah-langkah

keamanan dan mitigasi untuk melindungi datanya dari berbagai risiko yang mungkin terjadi. Sedangkan melalui regulasi aspek kepatuhan, maka pengendali data wajib mematuhi semua ketentuan keamanan informasi dan perlindungan data yang berlaku, termasuk didalamnya melaporkan aktivitas pelanggaran data yang terjadi kepada otoritas yang berwenang supaya ditindak lanjuti dan diberikan sanksi. Berdasarkan pengelompokan tersebut dapat diidentifikasikan beberapa ancaman yang sering terjadi khususnya ditinjau dari sisi keamanan informasinya. Berikut pada Tabel 1 adalah ancaman-ancaman yang berhubungan dengan keamanan informasi baik dari sisi perusahaan, regulator maupun pengguna yang berhasil diidentifikasi.

Tabel 1. Identifikasi Risiko Ancaman Keamanan Informasi pada Fintech

Ancaman Keamanan	Deskripsi	Dampak Potensial
Serangan Siber (*Hacking*)	Upaya eksploitasi kerentanan sistem oleh pihak luar melalui jaringan atau sistem aplikasi *fintech*.	Pencurian data pengguna, kerusakan sistem, dan kerugian finansial yang signifikan.
Backdoor* dan *Malware	Penyisipan perangkat lunak berbahaya (*malware*) atau *backdoor* dalam sistem yang memungkinkan akses tidak sah ke data dan sistem oleh pihak yang tidak berwenang.	Eksfiltrasi data sensitif, pengambil alihan sistem, dan potensi penyebaran *malware* ke jaringan internal.
Phishing* dan *Social Engineering	Teknik manipulasi psikologis yang digunakan untuk memperoleh kredensial pengguna atau akses ke sistem secara tidak sah.	Akses illegal ke akun pengguna, pencurian data, pencurian dana, dan eksploitasi identitas.
Enkripsi yang Lemah	Sistem *fintech* yang tidak mengenkripsi data secara memadai, baik data dalam transit maupun data yang tersimpan.	Kebocoran data, penyadapan informasi dan manipulasi data oleh pihak ketiga yang tidak berwenang.
Penyalahgunaan Akses Data	Penggunaan data oleh pihak internal yang tidak berwenang, misalnya karyawan yang memiliki akses ke data sensitif pelanggan.	Pelanggaran privasi, kerugian reputasi, risiko hukum.
Pengelolaan Keamanan Data Pihak Ketiga	Kelemahan keamanan dari vendor atau mitra eksternal dan ketidakmampuan dalam mengelola hubungan dengan pihak ketiga.	Kebocoran data, pelanggaran perjanjian kontrak dengan pengguna.
Manajemen Identitas dan Akses (IAM)	Pengelolaan kontrol akses yang buruk, seperti penggunaan kata sandi yang lemah atau tidak adanya autentikasi multi-faktor.	Peningkatan risiko akses yang tidak sah, pencurian data pengguna.
Keamanan API	Kerentanan pada API yang dapat diakses secara tidak sah atau tidak dilindungi dengan baik, memungkinkan pencurian atau manipulasi data.	Eksposur data pelanggan, akses tanpa izin ke sistem *backend*.
Keamanan Transaksi	Risiko terhadap transaksi finansial yang tidak sah atau manipulasi transaksi yang disebabkan oleh celah di sistem pembayaran atau perbankan digital.	Kerugian finansial, kehilangan kepercayaan pelanggan.
Kerentanan pada Mobile App	Masalah keamanan yang ada pada aplikasi mobile *fintech*, misalnya adanya celah di sistem otentikasi atau perangkat yang digunakan untuk mengakses aplikasi.	Pencurian akun pengguna, penyalahgunaan aplikasi.
***Compliance* dan Regulasi**	Ketidakpatuhan terhadap regulasi dan standar keamanan yang berlaku, seperti GDPR, PCI-DSS, atau OJK.	Denda besar, masalah hukum, hilangnya lisensi atau izin operasional.

Berdasarkan hasil analisis dan evaluasi dari risiko ancaman keamanan informasi yang berhasil diidentifikasi pada Tabel 1, maka risiko ancaman tersebut dapat dikelompokan menjadi beberapa kategori yaitu risiko ancaman dari pihak luar atau serangan siber, risiko ancaman yang berasal dari kerentanan sistem atau aplikasi *fintech*, risiko ancaman yang berasal dari manajemen pengelolaan data perusahaan maupun pengelolaan keamanan informasi dari pihak ketiga dan risiko ancaman yang berasal dari ketidakpatuhan terhadap regulasi. Dengan menggunakan *framework* ISO/IEC 27005:2018 didapatkan pemetaan dari risiko ancaman keamanan informasi seperti pada Gambar 3.



Gambar 3. Pemetaan Risiko

Kemudian, berdasarkan pemetaan risiko pada Gambar 3, dilakukan pemetaan terhadap *framework* NIST CSF 2.0 dan ISO 27001:2022 untuk mendapatkan klausul-klausul mana yang terdapat dalam *framework* tersebut yang berhubungan dengan jenis ancaman dan bentuk risiko terkait. Setelah didapatkan klausul dan kategori dari tiap *framework*, dilakukan proses analisis dengan mengkombinasikan hasil hasil penerapan keamanan informasi yang disarankan oleh tiap tiap *framework* tersebut, kemudian dilakukan proses analisis untuk menimbang saran terbaik dari penerapan keamanan informasi yang sudah di analisis, sehingga dapat disimpulkan rekomendasi-rekomendasi penerapan keamanan informasi terbaik yang dapat dilakukan untuk mengatasi risiko-risiko yang sering terjadi pada perusahaan *fintech* berdasarkan *framework* NIST CSF 2.0 dan ISO 27001:2022, yang dapat dilihat pada Tabel 2.

Tabel 2. Kombinasi Penerapan Best Practice Keamanan Informasi

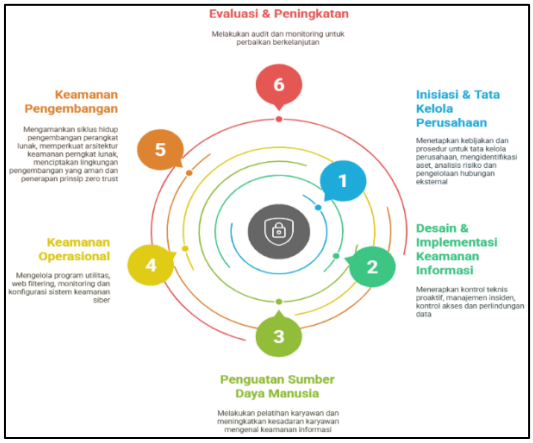
Jenis Ancaman	Bentuk Ancaman	Kategori NIST CSF 2.0	Klausul ISO 27001:2022	Rekomendasi Penerapan keamanan informasi
Ancaman Eksternal	Serangan *Cyber*	DE.DP (*Detection Process*) DE.AE (*Anomalies and Events*) DE.CM (*Security Continous Monitoring*)	A5.7 *Threat intelligence* A5.24. *Information security incident management planning and preparation* A5.26. *Response to information security incidents* A5.27. *Learning from information security incidents* A8.7 *Protection against malware* A8.8 *Management of technical vulnerabilities* A8.9 *Configuration management* A8.12 *Data leakage prevention* A8.15 *Logging* & A8.16 *Monitoring activities* A8.16. *Monitoring*	- Memantau, mengumpulkan dan menganalisis informasi terkait ancaman keamanan untuk mendukung langkah pencegahan dan penanganan (A5.7) - Manajemen Insiden Keamanan Informasi mulai dari perencanaan, persiapan, respon dan penanganan insiden ancaman keamanan informasi (A5.24, A5.26, A5.27) - Penguatan pada kontrol teknis, *monitoring* dan upaya upaya preventif, detektif dan korektif dalam pencegahan proaktif (A8.7, A8.8, A8.9, A8.12, A8.15, A8.16, A8.20, A8.21, A8.23, A8.24, DE.DP, DE.AE, DE.CM)

			activities A8.20 *Networks Security* A8.21 *Security of Network Services* A8.23 *Web Filtering* A8.24 *Use of Cryptography*	
	Social Engineering	PR.AT (*Awareness and Training*) ID.RA (*Risk Assesment*)	A5.7 *Threat Intelligence* A6.3 *Information Security Awareness, Education and Training* A6.6 *Confidentiality or Non-Disclosure Agreements* A6.8 *Information Security Event Reporting* A7.5. *Protecting against physical and environmental threats* A8.18. *Use of privileged utility programs* A8.23 *Web Filtering*	- Meningkatkan kesadaran dan kemampuan karyawan melalui program pelatihan dan edukasi yang terstruktur agar mereka memahami risiko keamanan informasi dan peran mereka dalam menjaga keamanan organisasi (A6.3, A6.6, A6.8, A7.5, PR.AT, ID.RA) - Mengelola dan mengontrol penggunaan program utilitas dan Mengimplementasikan mekanisme penyaringan web untuk membatasi akses ke situs web berbahaya untuk mencegah penyalahgunaan yang dapat membahayakan keamanan informasi pada perusahaan (A5.7, A8.18, A8.23)
Ancaman Internal	Kerentanan Sistem	PR.PT (*Protective Technology*) PR.IP (*Information Protection Process and Procedures*) PR.MA (*Maintenance*)	A5.8. *Information security in project management* A5.23. *Information security for use of cloud services* A8.4. *Access to source code* A8.8 *Management of technical vulnerabilities* A8.9 *Configuration management* A8.7 *Protection against malware* A8.25 *Secure development life cycle* A8.26. *Application security requirements* A8.27. *Secure system architecture and engineering principles* A8.28 *Secure coding* A8.29 *Security testing in development and acceptance* A8.31 *Separation of Development, Test and Production Environments*	- Mengintegrasikan praktik keamanan pada setiap tahap pengembangan perangkat lunak, mulai dari perencanaan, desain, pengkodean, pengujian, hingga pemeliharaan, guna meminimalkan risiko kerentanannya (A5.8, A8.4, A8.8, A8.9, A8.25, A8.26, PR.MA) - Mengadopsi pendekatan *zero trust* dalam keamanan lingkungan pengembangan (A5.23, A8.7, A8.27, A8.28, A8.29, A8.31, PR.PT, PR.IP)

Kelemahan dalam Manajemen Data dan Informasi	PR.AC (*Identity Management and Access Control*) PR.DS (*Data Security*) ID.AM (*Asset Management*)	A5.9 *Inventory of Information and other associated assets* A5.12 *Classification of Information* A5.13 *Labelling of Information* A5.15. *Access control* A5.16. *Identity management* A5.17. *Authentication information* A5.18. *Access rights* A5.33 *Protection of records* A5.34 *Privacy and protection of PII* A6.5. *Responsibilities after termination or change of employment* A6.6. *Confidentiality or non-disclosure agreements* A8.2. *Privileged access rights* A8.10 *Information deletion* A8.11 *Data masking* A8.12 *Data leakage prevention* A8.13 *Information Backup* A8.14 *Redudancy of Information Processing Facilities* A8.15. *Logging*	- Pengelolaan aset informasi untuk memastikan pengendalian dan perlindungan yang tepat (A5.9, A5.12, A5.13, ID.AM) - Menerapkan *monitoring*, kontrol dan manajemen identitas yang terintegrasi guna mengelola siklus hidup akun pengguna dan pembatasan akses sesuai dengan kebutuhan (A5.15, A5.16, A5.17, A5.18, A6.5, A6.6, A8.2, A8.15, PR.AC) - Memastikan perlindungan dalam keamanan siklus hidup data terjamin melalui upaya preventif dan proaktif dalam semua skenario insiden keamanan data (A5.33, A5.34, A8.10, A8.11, A8.12, A8.13, A8.14, PR.DS)
Ketidak patuhan terhadap Regulasi	ID.GV (*Governance*) ID.RA (*Risk Assesment*)	A5.1. *Policies for information security* A5.5. *Contact with authorities* A5.6. *Contact with special interest groups* A5.31 *Legal, statutory, regulatory and contractual requirements* A5.35 *Independent review of information security* A5.36 *Compliance with policies, rules and standards for information security* A5.37 *Documented operating procedures*	- Merencanakan, menyusun, menetapkan dan mendokumentasikan kebijakan keamanan informasi untuk seluruh prosedur operasional terkait keamanan informasi yang jelas, komprehensif, dan disesuaikan dengan kebutuhan organisasi (A5.1, A5.36, A5.37, ID.GV, ID.RA) - Melakukan *monitoring* dan audit internal berkala untuk memastikan kepatuhan dan mengidentifikasi pelanggaran sejak dini (A5.37, ID.GV) - Membangun dan memelihara hubungan baik dengan otoritas terkait baik regulator maupun mitra pihak ketiga (A5.5, A5.6) - Identifikasi dan pantau secara

	berkala semua persyaratan hukum, peraturan, dan kontrak yang relevan dengan keamanan informasi organisasi dan Memastikan kebijakan dan praktik organisasi selalu diperbarui agar sesuai dengan perubahan regulasi (A5.31, ID.GV, ID.RA)

Berdasarkan rekomendasi penerapan keamanan informasi terbaik untuk perusahaan *fintech* pada Tabel 2, dapat digambarkan model tata kelola terbaik untuk keamanan informasi perusahaan *fintech* yang terdiri dari 6 (enam) tahapan yaitu Pertama, tahap inisiasi dan tata kelola Perusahaan terdiri dari kebijakan, prosedur, identifikasi aset, analisis risiko, hubungan eksternal. Kedua adalah tahap desain dan implementasi keamanan informasi terdiri dari kontrol teknis proaktif, manajemen insiden, perlindungan data, kontrol akses. Ketiga adalah tahap penguatan sumber daya manusia terdiri dari pelatihan, peningkatan *awareness*, *Non-Disclosure Agreement*, kebijakan pasca-terminasi. Keempat adalah tahap keamanan operasional terdiri dari pengelolaan program utilitas, *web filtering*, konfigurasi *cyber security system*, monitoring dan *vulnerability testing*. Kelima adalah tahap Keamanan Pengembangan terdiri dari Secure Software Development Life Cycle, Arsitektur Keamanan, Secure *development and testing environment*, penerapan prinsip *zero trust*. Terakhir atau tahap keenam yaitu evaluasi dan peningkatan berupa audit, *monitoring*, *review*, dan perbaikan berkelanjutan. Model tata kelola TI dengan fokus keamanan informasi pada Perusahaan *fintech* dapat dilihat pada Gambar 4.



Gambar 4.Model Tata Kelola TI untuk Keamanan Informasi Fintech

Pada model tata kelola TI keamanan informasi setiap tahapannya dapat dirincikan ke dalam beberapa aktivitas-aktivitas pada Tabel 3 berikut.

Tabel 3. Tahapan Rekomendasi Model Tata Kelola TI

No.	Tahapan	Fokus Utama	Aktivitas Kunci
1	Inisiasi dan Tata Kelola Perusahaan	Pondasi kebijakan & struktur tata kelola keamanan informasi	- Merumuskan kebijakan dan prosedur keamanan sesuai visi-misi - Identifikasi aset informasi penting - Analisis risiko dan penetapan prioritas pengamanan - Pengelolaan hubungan eksternal dengan pihak ketiga, regulator, dan mitra - Kepatuhan terhadap ISO/IEC 27001 & UU PDP
2	Desain & Implementasi Keamanan	Penerapan kontrol teknis & prosedural untuk melindungi aset digital	- Penerapan kontrol teknis (firewall, enkripsi, MFA) - Deteksi dini, otomatisasi, dan mitigasi cepat insiden - Penyiapan prosedur respons insiden

			(deteksi, pelaporan, pemulihan) - Perlindungan data dengan enkripsi & kebijakan data sensitif - Kontrol akses untuk pihak berwenang
3	Penguatan Sumber Daya Manusia	Sumber daya manusia sebagai lini pertahanan utama	- Pelatihan rutin keamanan informasi bagi karyawan - Peningkatan security awareness (phishing, social engineering) - Penandatanganan NDA - Kebijakan pasca-terminasi (pencabutan akses, penghapusan data)
4	Keamanan Operasional	Pengelolaan & pemantauan sistem TI secara berkelanjutan	- Pengelolaan utilitas perangkat lunak - Web filtering - Konfigurasi sistem keamanan (IDS/IPS, endpoint protection) - Monitoring & vulnerability testing berkala
5	Keamanan Pengembangan	Integrasi keamanan dalam siklus pengembangan perangkat lunak (SSDLC)	- Perancangan arsitektur keamanan aplikasi - Penerapan lingkungan pengembangan & pengujian aman - Pengujian keamanan setiap perubahan kode - Penerapan prinsip zero trust (verifikasi & pengawasan ketat antar komponen sistem)
6	Evaluasi & Peningkatan	Evaluasi efektivitas dan relevansi sistem keamanan secara berkala	- Audit keamanan berkala - Monitoring sistem & aktivitas pengguna - Review & perbaikan berdasarkan hasil audit dan insiden - Peningkatan adaptasi terhadap ancaman baru

Simpulan

Berdasarkan model tata kelola TI yang dibangun dengan mengkombinasikan penerapan aspek preventif, detektif, dan korektif dalam pengendalian keamanan informasi melalui tiga framework global mengenai keamanan informasi, yaitu ISO/IEC 27001:2022, ISO/IEC 27005:2018, dan NIST Cybersecurity Framework (NIST CSF 2.0), didapatkan enam tahapan praktis untuk memperkuat keamanan informasi khususnya pada perusahaan fintech. Tahapan-tahapan tersebut meliputi: Inisiasi dan Tata Kelola Perusahaan, Desain dan Implementasi Keamanan Informasi, Penguatan Sumber Daya Manusia, Keamanan Operasional, Keamanan Pengembangan, serta Evaluasi dan Peningkatan. Melalui penelitian ini juga diberikan beberapa rekomendasi untuk praktik dalam penerapan keamanan informasi pada perusahaan fintech, yaitu berupa aktivitas-aktivitas yang sebaiknya dilakukan dalam mengendalikan risiko-risiko keamanan informasi. Model ini memberikan kontribusi teoritis melalui integrasi tiga framework global dalam satu kerangka tata kelola keamanan informasi yang komprehensif. Selain itu, terdapat kontribusi praktis berupa model aplikatif yang dapat dijadikan panduan oleh manajemen perusahaan fintech dalam memperkuat postur keamanan informasinya. Namun demikian, penelitian ini memiliki keterbatasan, yaitu studi ini masih terbatas pada konteks kasus di Indonesia dan belum dilakukan pengujian secara kuantitatif untuk mengukur efektivitas implementasi model secara lebih luas. Oleh karena itu, penelitian lanjutan diperlukan untuk melakukan validasi empiris dan generalisasi model ini dalam konteks internasional dan dengan pendekatan kuantitatif.

Daftar Pustaka

[1] Omolara Patricia Olaiya, Temitayo Oluwadamilola Adesoga, Adefisayo Ojo, Oluwabusola Dorcas Olagunju, Olajumoke Oluwagbemisola Ajayi, and Yusuf Olalekan Adebayo, “Cybersecurity strategies in fintech: safeguarding financial data and assets,” *GSC Adv. Res. Rev.*, vol. 20, no. 1, pp. 050–056, 2024,

doi: 10.30574/gscarr.2024.20.1.0241.

[2] L. L. Hafifah, N. W. Utami, and I. G. A. P. Dwi Putri, "Analisis Faktor Yang Mempengaruhi Behavioral Intention Dan User Behavior Pada Fintech Shopeepay Menggunakan Model Unified Theory of Acceptance and Use of Technology (Utaut)," *J. Akunt. Bisnis*, vol. 15, no. 2, pp. 102–117, 2022, doi: 10.30813/jab.v15i2.3574.

[3] A. Anggono, "Cybercrime dan Cybersecurity pada Fintech : Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech : A Systematic Literature Review," *J. Manaj. dan Organ.*, vol. 12, no. 3, pp. 239–251, 2021, doi: https://doi.org/10.29244/jmo.v12i3.33528.

[4] D. U. Maheswari S, "Cybersecurity Challenges In Fintech: Assessing Threats And Mitigation Strategies For Financial Institutions," *Educ. Adm. Theory Pract.*, vol. 30, no. 5, pp. 1063–1071, 2024, doi: 10.53555/kuey.v30i5.3010.

[5] R. A. Prayudi, R. Mulyana, and R. Fauzi, "SEIKO : Journal of Management & Business Pengendalian Digitalisasi FintechCo Melalui Perancangan Pengelolaan Keamanan Informasi Berbasis COBIT 2019 Information Security Focus Area," *SEIKO J. Manag. Bus.*, vol. 6, no. 2, pp. 388–406, 2023.

[6] N. Habibi, F. Ali Akbar, and A. Lina Nurlaili, "Analisis Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 551–560, 2024, doi: 10.36040/jati.v8i1.8349.

[7] Gatot Efrianto and Nia Tresnawaty, "Pengaruh Privasi, Keamanan, Kepercayaan Dan Pengalaman Terhadap Penggunaan Fintech Di Kalangan Masyarakat Kabupaten Tangerang Banten," *J. Liabilitas*, vol. 6, no. 1, pp. 53–72, 2021, doi: 10.54964/liabilitas.v6i1.71.

[8] M. Lestari, A. Iriani, and H. Hendry, "Information Technology Governance Design in DevOps-Based E-Marketplace Companies Using COBIT 2019 Framework," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 6, no. 2, pp. 233–252, 2022, doi: 10.29407/intensif.v6i2.18104.

[9] C. D. A. Ua, J. A. C. Likadja, and R. P. Leo, "Perlindungan Data Pribadi Konsumen Finansial Technology (Fintech) Berdasarkan Peraturan Otoritas Jasa Keuangan Nomor: 77/Pojk. 01/2016 dan Peraturan Bank Indonesia Nomor: 22/20/PBI/2020," *Madani J. Ilm. Multidisiplin*, vol. 1, no. 5, pp. 228–240, 2023, doi: e-ISSN: 2986-6340 DOI: https://doi.org/10.5281/zenodo.8009991.

[10] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahyu, "Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department," *Int. J. Electr. Comput. Biomed. Eng.*, vol. 2, no. 3, pp. 395–413, 2024, doi: 10.62146/ijecbe.v2i3.81.

[11] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 6, pp. 723–735, 2025, doi: 10.14569/IJACSA.2025.0160672.

[12] T. Moore, "The NIST Cybersecurity," 2024. doi: https://doi.org/10.6028/NIST.CSWP.29.

[13] J. Edwards and G. Weaver, " NIST Cybersecurity Framework ," *Cybersecurity Guid. to Governance, Risk, Compliance*, vol. 10, no. 8, pp. 191–207, 2024, doi: 10.1002/9781394250226.ch11.

[14] D. B. Putra, M. A. M. Hakim, and B. Nurdewanto, "Implementasi Electronic-Know Your Customer pada aplikasi Fintech untuk meningkatkan keamanan akun user," *J. Inf. Syst. Appl. Dev.*, vol. 1, no. 2, pp. 111–120, 2023, doi: 10.26905/jisad.v1i2.11112.

[15] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model," *J. Inf. Syst. Informatics*, vol. 6, no. 2, pp. 1052–1069, 2024, doi: 10.51519/journalisi.v6i2.754.

[16] J. F. Andry *et al.*, "Kebijakan Keamanan Teknologi Informasi Pada Perangkat Keras Di Perusahaan Distributor Sepatu," *J. Pengabdi. dan Kewirausahaan*, vol. 7, no. 2, pp. 118–133, 2023, doi: http://dx.doi.org/10.30813/jpk.v7i2.4775.

[17] M. Amirinnisa[1] and R. Bisma[2], "Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun," *Jeisbi*, vol. 04, no. 04, 2023.

[18] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis Manajemen Risiko Informasi Menggunakan Iso/Iec 27005:2018 (Studi Kasus: Pt.Xyz)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 728–734, 2024, doi: 10.29100/jipi.v9i2.4709.

[19] Bintang Rahmat Riadi, "Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018," *INOVTEK Polbeng - Seri Inform.*, vol. 10, no. 1, pp. 225–236, 2025, doi: 10.35314/pq4jhh89.

[20] T. D. Farah Labibah Caseba, "Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): a Systematic Literature Review," *Diponegoro J. Account.*, pp. 1–15, 2024.

[21] R. Amaliyah, "Efektivitas Penggunaan Teknologi Artificial Intelligence Terhadap Proteksi Keamanan Sistem Tata Kelola Perusahaan (Sektor Perbankan)," *Info Kripto*, vol. 19, no. 1, pp. 49–60, 2025, doi: 10.56706/ik.v19i1.121.

[22] Zulmedia, "Dampak Artificial Financial Intelligence dalam Fintech Payments Terhadap Kinerja Keuangan Perbankan Indonesia: A Sytematic Literatur Review," *J. Ilm. Raflesia Akunt.*, vol. 11, no. 1, pp. 45–52, 2025, doi: 10.53494/jira.v11i1.824.

[23] Erizal Candra Efendi, Irwandi Jaswir, Ahmad Wira, and Aidil Novia, "Optimalisasi Teknologi Financial Intelligence dalam Deteksi dan Pencegahan Fraud di Fintech Syariah 1 Istithmar : Jurnal Studi Ekonomi Syariah Article History," *J. Stud. Ekon. Syariah*, vol. 9, no. 9, pp. 1–14, 2025, [Online]. Available: http://jurnalfebi.iainkediri.ac.id/index.php/istithmarDOI:http://doi.org/10.30762/istithmar.v9i1.33

[24] U. Z. Agustiana, "Pemanfaatan Blockchain untuk Meningkatkan Keamanan Siber dalam Pembayaran Lintas Batas di Industri Fintech," *J. Bisnis, Ekon. Syariah, dan Pajak*, vol. 1, pp. 206–215, 2024.

[25] R. Mustaqim Handoko *et al.*, "Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia)," *J. Ilmu Tek. dan Inform.*, vol. 4, pp. 64–74, 2024.

[26] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *Nuansa Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.

[27] A. Apriany and A. Wibowo, "Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 18, no. 4, pp. 417–428, 2024, doi: 10.22146/ijccs.100385.

[28] J. S. S. Kanka Wiemas N. G., "Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022," *Syntax Lit. J. Ilm. Indones.*, vol. 7, no. 11, 2022, doi: 10.14341/conf05-08.09.22-132.

[29] N. L. Putri and A. F. Wijaya, "Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework," *J. Inf. Syst. Informatics*, vol. 5, no. 2, pp. 630–649, 2023, doi: 10.51519/journalisi.v5i2.468.

[30] A. Aminudin and A. Supriyanto, "Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah)," *Aiti*, vol. 21, no. 2, pp. 210–229, 2024, doi: 10.24246/aiti.v21i2.210-229.

[31] Eleonora Anggi Ardhaninggar and Kallamulah Ramli, "A Review of Cybersecurity Framework Implementation for Retail Industry-Challenges and Recommendation," *ARRUS J. Eng. Technol.*, vol. 4, no. 2, pp. 211–219, 2024, doi: 10.35877/jetech3434.

[32] Maniah; Shiyami, "Matriks dan Pengukuran Terhadap Kinerja Tata Kelola Teknologi Informasi," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 100–109, 2020, doi: 10.35957/jatisi.v7i1.224.

[33] F. L. Farah, Rahmat Mulyana, and Luthfi Ramadhani, "Studi Kasus Pengaruh Tata Kelola Ti Terhadap Transformasi Digital Dan Kinerja Bank B," *Zo. J. Sist. Inf.*, vol. 4, no. 2, pp. 100–116, 2022, doi: 10.31849/zn.v4i2.11085.