KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.3 Juni 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 333-345
DOI : https://doi.org/10.61722/jssr.v4i3.10330

Analisis Kapabilitas Keamanan Sistem Informasi Perbankan dalam Menghadapi Evolusi Kejahatan Siber

Dio Rendra Rinanto*[1], Evy Nurmiati[2]

[1,2] Prodi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
*Penulis Korespondensi: [1]dio.rendra24@mhs.uinjkt.ac.id, [2]evy.nurmiati@uinjkt.ac.id

Abstract. *Digital transformation in the banking industry has provided significant service efficiency, while simultaneously triggering the evolution of increasingly complex cybercrimes. This study aims to analyze the development of cyber threats in the banking sector, evaluate the applied information system security capabilities, and identify strategies to enhance cyber resilience in the digital era. The research method employed is qualitative with a literature study approach, examining various scientific journals, cybersecurity reports, and information security standard documents. The results indicate that the banking sector faces primary threats such as phishing, malware/ransomware, DDoS attacks, and social engineering. Although banks have integrated modern technologies like multi-factor authentication (MFA), firewalls, and artificial intelligence (AI), and adopted international standards such as ISO 27001 and NIST, human error and infrastructure complexity remain major challenges. The conclusion of this study emphasizes that future cyber resilience strategies must involve a comprehensive approach through the Zero Trust Security concept, strengthening IT governance, improving security literacy, and sustained cross-sector collaboration.*

Keywords: *Information system security, banking, cybercrime, digital tranformation, cyber resilience*

Abstrak. *Transformasi digital dalam industri perbankan memberikan efisiensi layanan namun sekaligus memicu evolusi kejahatan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis perkembangan ancaman siber pada sektor perbankan, mengevaluasi kapabilitas keamanan sistem informasi yang diterapkan, serta mengidentifikasi strategi peningkatan ketahanan siber di era digital. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi literatur, yang menelaah berbagai jurnal ilmiah, laporan keamanan siber, dan dokumen standar keamanan informasi. Hasil penelitian menunjukkan bahwa sektor perbankan menghadapi ancaman utama berupa phishing, malware/ransomware, serangan DDoS, dan social engineering. Meskipun perbankan telah mengintegrasikan teknologi modern seperti multi-factor authentication (MFA), firewall, dan kecerdasan buatan (AI) serta mengadopsi standar internasional seperti ISO 27001 dan NIST, faktor kesalahan manusia (human error) dan kompleksitas infrastruktur tetap menjadi tantangan utama. Kesimpulan dari penelitian ini menekankan bahwa strategi ketahanan siber masa depan harus melibatkan pendekatan komprehensif melalui konsep Zero Trust Security, penguatan tata kelola TI, peningkatan literasi keamanan, serta kolaborasi lintas sektor yang berkelanjutan*.

Kata kunci: *Keamanan sistem informasi, perbankan, kejahatan siber, transformasi digital, ketahanan siber*

1. LATAR BELAKANG

Perkembangan teknologi digital di Indonesia membawa banyak manfaat dalam kehidupan masyarakat, mulai dari pendidikan, perbankan, komunikasi, hingga bisnis(Guntara, n.d.). Transformasi digital mendorong bank untuk menghadirkan layanan yang lebih cepat, praktis, dan efisien melalui pemanfaatan teknologi berbasis internet.

Naskah Masuk: 25 Mei 2026; Revisi: 25 Mei 2026; Diterima: 26 Mei 2026; Terbit: 27 Mei 2026

Berbagai layanan seperti *internet banking, mobile banking, automated teller machine* (ATM), hingga pembayaran digital kini menjadi bagian penting dalam aktivitas transaksi masyarakat sehari-hari. Kehadiran layanan digital tersebut memberikan kemudahan bagi nasabah karena transaksi dapat dilakukan kapan saja dan di mana saja tanpa harus datang langsung ke kantor bank(Nur, 2023).

Transformasi digital telah menjadi fondasi utama dalam perkembangan sektor perbankan Indonesia, menjadikan sistem informasi sebagai tulang punggung operasional perbankan(Evy Nurmiati et al., 2025). Namun, di balik berbagai kemudahan dan manfaat yang diperoleh dari digitalisasi, sektor perbankan juga menghadapi tantangan besar berupa meningkatnya ancaman kejahatan siber(Cantika Sarma Seicilia Silalahi et al., 2024). Seiring berkembangnya teknologi, metode serangan yang digunakan pelaku kejahatan siber juga semakin kompleks, terorganisasi, dan sulit dideteksi. Sektor perbankan menjadi salah satu target utama serangan siber karena menyimpan data sensitif nasabah, informasi transaksi keuangan, serta memiliki nilai ekonomi yang tinggi. Serangan terhadap sistem informasi perbankan tidak hanya menimbulkan kerugian finansial, tetapi juga dapat merusak reputasi institusi dan menurunkan tingkat kepercayaan masyarakat terhadap layanan perbankan digital.

Kejahatan siber yang menyerang sektor perbankan memiliki berbagai bentuk dan karakteristik. Salah satu ancaman yang paling umum adalah *phishing*, yaitu upaya penipuan yang dilakukan dengan menyamar sebagai pihak resmi untuk memperoleh data penting nasabah seperti *username*, *password*, PIN, maupun kode OTP. Selain *phishing*, serangan ransomware yang mengeksploitasi volume data besar menjadi salah satu ancaman paling mematikan(Sya et al., 2026). Pelaku kejahatan siber juga semakin sering memanfaatkan teknik social engineering untuk memanipulasi pengguna agar memberikan akses terhadap informasi rahasia secara sukarela. Bahkan, perkembangan teknologi kecerdasan buatan mulai dimanfaatkan untuk menciptakan serangan siber yang lebih canggih dan sulit dikenali.

Meningkatnya intensitas dan kompleksitas serangan siber menunjukkan bahwa keamanan sistem informasi merupakan aspek yang sangat krusial dalam industri perbankan. Sistem keamanan informasi tidak hanya berfungsi untuk melindungi data dan transaksi nasabah, tetapi juga menjaga kerahasiaan, integritas, dan ketersediaan informasi

dalam sistem perbankan. Oleh karena itu, institusi perbankan perlu memiliki kapabilitas keamanan yang kuat dan adaptif terhadap perkembangan ancaman siber yang terus berubah. Kapabilitas tersebut mencakup penggunaan teknologi keamanan modern, penerapan kebijakan keamanan informasi, penguatan tata kelola teknologi informasi, serta peningkatan kesadaran keamanan bagi pengguna dan pegawai.

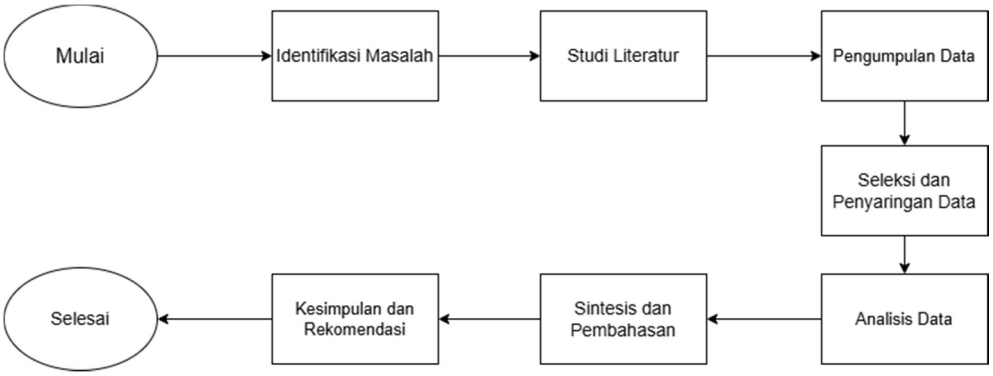
Dalam menghadapi ancaman siber yang semakin berkembang, berbagai standar dan *framework* keamanan informasi mulai diterapkan oleh industri perbankan. *Framework* seperti ISO 27001, NIST *Cybersecurity Framework*, dan COBIT digunakan sebagai pedoman dalam mengelola risiko keamanan informasi dan meningkatkan ketahanan sistem terhadap serangan siber. Selain itu, penerapan teknologi seperti *multi-factor authentication* (MFA), *intrusion detection system* (IDS), enkripsi data, serta pemantauan keamanan secara real-time menjadi langkah penting dalam meminimalkan risiko kebocoran data dan penyalahgunaan sistem.

Meskipun berbagai upaya pengamanan telah diterapkan, ancaman kejahatan siber masih terus berkembang seiring dengan kemajuan teknologi digital. Hal ini menunjukkan bahwa keamanan sistem informasi perbankan memerlukan pendekatan yang berkelanjutan dan adaptif agar mampu menghadapi berbagai bentuk ancaman baru. Oleh karena itu, diperlukan analisis yang mendalam mengenai kapabilitas keamanan sistem informasi perbankan dalam menghadapi evolusi kejahatan siber, sehingga dapat diketahui tingkat kesiapan industri perbankan dalam menjaga keamanan data, transaksi, dan layanan digital yang digunakan masyarakat.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis perkembangan ancaman kejahatan siber pada sektor perbankan, mengevaluasi kapabilitas keamanan sistem informasi yang diterapkan, serta mengidentifikasi strategi yang dapat digunakan untuk meningkatkan ketahanan siber industri perbankan di era transformasi digital. Penelitian ini diharapkan dapat memberikan wawasan mengenai pentingnya keamanan sistem informasi serta menjadi referensi dalam pengembangan strategi keamanan siber pada sektor perbankan di masa mendatang

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan studi literatur. Metode ini dipilih karena penelitian berfokus pada analisis berbagai teori, konsep, dan hasil penelitian terdahulu yang berkaitan dengan keamanan sistem informasi dan kejahatan siber pada sektor perbankan. Data yang digunakan dalam penelitian diperoleh dari berbagai sumber seperti jurnal ilmiah, artikel akademik, laporan lembaga keamanan siber, serta dokumen standar keamanan informasi.



Gambar 1. Alur Penelitian

Pengumpulan data dilakukan melalui studi pustaka dengan menelaah berbagai referensi yang relevan terhadap topik penelitian. Literatur yang digunakan mencakup pembahasan mengenai ancaman siber di sektor keuangan, implementasi *framework* keamanan informasi, serta strategi perlindungan sistem informasi perbankan. Selain itu, penelitian juga mengkaji beberapa kasus serangan siber yang pernah terjadi pada institusi perbankan sebagai bahan analisis.

Teknik analisis data *framework* dilakukan secara deskriptif dengan mengidentifikasi bentuk ancaman siber, mengevaluasi penerapan keamanan sistem informasi, serta membandingkan berbagai keamanan yang digunakan dalam industri perbankan. Hasil analisis kemudian digunakan untuk menggambarkan tingkat kesiapan dan kapabilitas keamanan sistem informasi dalam menghadapi evolusi kejahatan siber..

3. HASIL DAN PEMBAHASAN

Perkembangan teknologi digital dalam industri perbankan telah memberikan dampak signifikan terhadap peningkatan kualitas layanan keuangan. Berbagai inovasi seperti *mobile banking, internet banking, digital payment,* dan layanan transaksi berbasis aplikasi telah mengubah pola interaksi masyarakat dengan layanan perbankan menjadi

lebih cepat, fleksibel, dan efisien. Namun, kemajuan tersebut juga diikuti dengan meningkatnya ancaman kejahatan siber yang terus berkembang dari waktu ke waktu. Sektor perbankan menjadi salah satu target utama serangan siber karena memiliki aset bernilai tinggi berupa data nasabah, data transaksi, dan sistem keuangan yang terhubung secara digital.

3.1. Bentuk Kejahatan Siber

Sindikat kejahatan siber menerapkan beragam strategi manipulatif untuk menembus pertahanan sistem dan mengakses data sensitif secara ilegal. Bentuk-bentuk kejahatan siber bisa meliputi:

A. Phising

Phishing adalah jenis kejahatan siber yang bekerja dengan mengelabui korban untuk mengirimkan informasi sensitif seperti kata sandi atau data keuangan melalui situs atau pesan palsu yang terlihat seperti halaman resmi(Anjheli, 2025). Metode ini masih menjadi ancaman utama karena memanfaatkan kurangnya kesadaran keamanan digital pengguna. Banyak nasabah yang belum mampu membedakan antara layanan resmi dan layanan palsu sehingga mudah menjadi korban pencurian data.

B. Malware dan Ransomware

Malware adalah perangkat lunak khusus yang dirancang untuk masuk, merusak, atau melakukan tindakan ilegal pada jaringan komputer tanpa izin pemiliknya(Fauziah, n.d.). Saat ini, varian *malware* yang paling banyak ditemukan dan berbahaya adalah ransomware, yaitu jenis *malware* yang mengenkripsi data korban hingga tidak bisa diakses, kecuali korban membayar uang tebusan.

C. Serangan Ddos (*Distributed Denial of Service*)

Serangan DDoS (*Distributed Denial of Service*) adalah salah satu ancaman terbesar dalam keamanan siber, terutama bagi sektor perbankan. Serangan ini melibatkan membanjiri server atau jaringan dengan lalu lintas palsu, sehingga mengganggu layanan yang sah(Diny et al., 2024).

D. Social Engineering

Kejahatan siber modern juga semakin memanfaatkan teknik *social engineering*, yaitu metode manipulasi psikologis terhadap pengguna agar secara sukarela memberikan akses atau informasi rahasia kepada pelaku. Teknik ini sering kali dilakukan melalui telepon, media sosial, atau pesan instan dengan mengatasnamakan pihak bank. Pelaku biasanya memanfaatkan rasa panik, takut, atau ketidaktahuan korban untuk memperoleh akses terhadap akun perbankan. Dalam banyak kasus, keberhasilan serangan tidak sepenuhnya disebabkan oleh kelemahan sistem teknologi, melainkan akibat rendahnya kesadaran keamanan pengguna.

3.2. Kapabilitas Keamanan Sistem Informasi Perbankan

Dalam menghadapi perkembangan ancaman kejahatan siber yang semakin kompleks, industri perbankan terus meningkatkan kapabilitas keamanan sistem informasinya melalui penerapan berbagai teknologi, kebijakan, dan prosedur keamanan. Kapabilitas keamanan sistem informasi merupakan kemampuan organisasi dalam melindungi kerahasiaan, integritas, dan ketersediaan data serta layanan digital dari berbagai ancaman internal maupun eksternal. Pada sektor perbankan, keamanan sistem informasi menjadi aspek yang sangat penting karena berkaitan langsung dengan perlindungan data nasabah, transaksi keuangan, serta stabilitas operasional perusahaan.

Salah satu bentuk penguatan keamanan yang umum diterapkan oleh perbankan adalah penggunaan teknologi firewall. Salah satu teknologi *firewall* yang dapat digunakan yaitu AVG Antivirus. Salah satu fitur utama AVG Antivirus adalah kemampuannya untuk mendeteksi dan menghapus ancaman yang ada di komputer(Rahmatullah Rizki., 2023).

Selain teknologi firewall, bentuk penguatan keamanan yang umum diterapkan oleh perbankan adalah penggunaan sistem autentikasi berlapis atau *multi-factor authentication* (MFA). Teknologi ini mengharuskan pengguna untuk melewati lebih dari satu tahap verifikasi sebelum dapat mengakses sistem atau melakukan transaksi. Selain penggunaan password, sistem biasanya memanfaatkan kode OTP, biometrik, atau autentikasi melalui perangkat tertentu. Penerapan MFA dinilai mampu mengurangi risiko pencurian akun akibat kebocoran password atau serangan *phishing*. Selain itu, Edukasi mengenai *phishing, social engineering*, dan perlindungan data pribadi harus dilakukan agar pegawai

mampu mengenali serta mencegah potensi serangan yang dapat mengancam keamanan organisasi.

3.3. Analisis Kelemahan dan Tantangan Keamanan Siber Perbankan

Meskipun sektor perbankan telah menerapkan berbagai teknologi dan strategi keamanan informasi, masih terdapat sejumlah kelemahan dan tantangan yang dapat memengaruhi efektivitas perlindungan sistem informasi. Kompleksitas ancaman siber yang terus berkembang menyebabkan sistem keamanan harus selalu diperbarui agar mampu menghadapi berbagai metode serangan baru. Dalam praktiknya, tidak semua institusi perbankan memiliki tingkat kesiapan keamanan yang sama, sehingga masih terdapat celah yang dapat dimanfaatkan oleh pelaku kejahatan siber.

Salah satu kelemahan utama dalam keamanan sistem informasi perbankan adalah faktor manusia atau *human error*. Banyak kasus serangan siber berhasil terjadi bukan karena lemahnya teknologi keamanan, tetapi akibat kurangnya kesadaran pengguna terhadap ancaman digital. Nasabah maupun pegawai sering kali menjadi target serangan *phishing* dan *social engineering* karena kurang memahami cara mengenali tindakan penipuan digital. Penggunaan *password* yang lemah, membagikan kode OTP, serta mengakses tautan mencurigakan menjadi contoh perilaku yang dapat meningkatkan risiko kebocoran data dan penyalahgunaan akun.

Selain faktor manusia, tantangan lain yang dihadapi sektor perbankan adalah kompleksitas infrastruktur teknologi yang digunakan. Sistem perbankan modern umumnya terintegrasi dengan berbagai layanan digital, aplikasi pihak ketiga, serta jaringan komunikasi yang luas(S. Siregar, 2020). Semakin kompleks sistem yang digunakan, maka semakin besar pula potensi munculnya celah keamanan yang dapat dimanfaatkan oleh pelaku serangan siber. Integrasi antar sistem juga menyebabkan proses pengawasan dan pengelolaan keamanan menjadi lebih sulit dilakukan.

Ancaman *insider threat* atau ancaman internal juga menjadi tantangan serius dalam keamanan informasi perbankan. Risiko ini muncul ketika pegawai atau pihak internal organisasi menyalahgunakan hak akses yang dimiliki untuk kepentingan tertentu. Selain tindakan sengaja, ancaman internal juga dapat terjadi akibat kelalaian pegawai dalam menjaga kerahasiaan data dan prosedur keamanan. Karena memiliki akses langsung

terhadap sistem organisasi, ancaman internal sering kali lebih sulit dideteksi dibandingkan ancaman dari pihak eksternal.

Perkembangan teknologi digital yang sangat cepat juga menjadi tantangan tersendiri bagi industri perbankan. Teknologi keamanan yang diterapkan saat ini dapat menjadi kurang efektif apabila tidak diperbarui secara berkala. Pelaku kejahatan siber terus mengembangkan metode serangan baru dengan memanfaatkan teknologi modern seperti *artificial intelligence*, otomatisasi serangan, dan *deepfake*. Oleh karena itu, bank harus terus melakukan inovasi dan pembaruan sistem keamanan agar tidak tertinggal dari perkembangan ancaman siber.

Di sisi lain, implementasi keamanan siber membutuhkan biaya yang cukup besar. Pengadaan teknologi keamanan modern, pelatihan sumber daya manusia, audit keamanan, serta pemeliharaan sistem memerlukan investasi yang tidak sedikit. Hal ini menjadi tantangan khusus bagi institusi perbankan yang memiliki keterbatasan sumber daya dan infrastruktur teknologi.

Tantangan lain yang tidak kalah penting adalah menjaga keseimbangan antara keamanan dan kenyamanan pengguna. Sistem keamanan yang terlalu ketat dapat menyebabkan proses transaksi menjadi lebih rumit dan mengurangi kenyamanan nasabah dalam menggunakan layanan digital. Sebaliknya, sistem yang terlalu sederhana dapat meningkatkan risiko penyalahgunaan dan serangan siber. Oleh karena itu, bank perlu merancang sistem keamanan yang efektif namun tetap memberikan pengalaman pengguna yang baik.

Berdasarkan berbagai tantangan tersebut, dapat diketahui bahwa keamanan sistem informasi perbankan memerlukan pendekatan yang menyeluruh dan berkelanjutan. Penguatan teknologi keamanan harus diimbangi dengan peningkatan kesadaran pengguna, pengawasan internal yang baik, serta pembaruan strategi keamanan secara berkala agar sistem mampu menghadapi evolusi ancaman siber yang terus berkembang.

3.4. Strategi Peningkatan Keamanan Siber Perbankan

Untuk menghadapi perkembangan ancaman siber yang semakin kompleks, industri perbankan perlu menerapkan strategi keamanan yang lebih adaptif, proaktif, dan berkelanjutan. Strategi tersebut tidak hanya berfokus pada penggunaan teknologi

keamanan, tetapi juga mencakup penguatan tata kelola, peningkatan sumber daya manusia, serta pengelolaan risiko secara menyeluruh. Dengan strategi yang tepat, institusi perbankan dapat meningkatkan ketahanan sistem informasi dan meminimalkan dampak yang ditimbulkan oleh serangan siber.

Salah satu strategi yang banyak diterapkan saat ini adalah pendekatan *Zero Trust Security*. Konsep ini menekankan bahwa tidak ada pengguna atau perangkat yang secara otomatis dapat dipercaya, baik dari dalam maupun luar jaringan organisasi. Setiap akses terhadap sistem harus melalui proses verifikasi dan autentikasi yang ketat. Pendekatan *Zero Trust* dinilai lebih efektif dalam menghadapi ancaman modern karena mampu membatasi akses pengguna sesuai kebutuhan dan mengurangi risiko penyalahgunaan hak akses.

Selain itu, penerapan *artificial intelligence* (AI) dan *machine learning* menjadi strategi penting dalam meningkatkan kemampuan deteksi ancaman siber(Setiawan & Rahmadsyah, 2025). Teknologi ini memungkinkan sistem keamanan menganalisis pola aktivitas pengguna dan mendeteksi anomali secara otomatis dalam waktu singkat. Dengan kemampuan analisis *real-time*, sistem dapat memberikan peringatan dini terhadap aktivitas mencurigakan sehingga proses penanganan ancaman dapat dilakukan lebih cepat dan efektif.

Strategi peningkatan keamanan juga perlu didukung dengan penguatan sistem autentikasi pengguna. Penggunaan *multi-factor authentication* (MFA), biometrik, serta token keamanan dapat membantu mengurangi risiko pencurian akun dan akses ilegal terhadap sistem perbankan. Selain itu, bank juga perlu menerapkan kebijakan pengelolaan *password* yang lebih kuat untuk meningkatkan keamanan akun pengguna.

Di samping penguatan teknologi, peningkatan kesadaran keamanan siber bagi pegawai dan nasabah menjadi langkah yang sangat penting. Edukasi mengenai phishing, social engineering, keamanan data pribadi, serta cara mengenali ancaman digital perlu dilakukan secara berkala. Dengan meningkatnya literasi keamanan digital, risiko keberhasilan serangan yang memanfaatkan kelemahan manusia dapat diminimalkan.

Bank juga perlu melakukan audit keamanan dan *penetration testing* secara rutin untuk mengidentifikasi potensi kelemahan pada sistem informasi. Melalui pengujian

keamanan secara berkala, organisasi dapat mengetahui celah keamanan yang perlu diperbaiki sebelum dimanfaatkan oleh pelaku kejahatan siber. Selain itu, evaluasi rutin terhadap kebijakan dan prosedur keamanan juga diperlukan agar sistem tetap relevan dengan perkembangan ancaman digital.

Strategi lain yang penting adalah penyusunan *disaster recovery plan* dan *business continuity plan*. Kedua strategi tersebut bertujuan memastikan bahwa layanan perbankan tetap dapat berjalan meskipun terjadi gangguan akibat serangan siber atau bencana tertentu. Dengan adanya prosedur pemulihan yang jelas, proses pemulihan sistem dapat dilakukan lebih cepat sehingga dampak kerugian dapat diminimalkan.

Kolaborasi antara institusi perbankan, pemerintah, regulator, dan lembaga keamanan siber juga menjadi bagian penting dalam meningkatkan ketahanan keamanan digital. Pertukaran informasi mengenai ancaman siber, pola serangan, dan strategi mitigasi dapat membantu organisasi lebih siap dalam menghadapi potensi ancaman yang muncul. Dengan penerapan strategi yang terintegrasi dan berkelanjutan, sektor perbankan dapat memperkuat keamanan sistem informasi serta meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital.

3.5. Analisis *Framework* dan Standar Keamanan Informasi

Dalam meningkatkan keamanan sistem informasi, industri perbankan memerlukan pedoman dan standar yang dapat digunakan untuk mengelola risiko keamanan secara sistematis. *Framework* dan standar keamanan informasi berfungsi sebagai acuan dalam merancang kebijakan, prosedur, serta mekanisme pengendalian keamanan yang sesuai dengan kebutuhan organisasi. Penerapan *framework* keamanan juga membantu institusi perbankan dalam meningkatkan konsistensi pengelolaan keamanan informasi dan memastikan bahwa sistem yang digunakan memenuhi standar keamanan yang berlaku.

Salah satu standar keamanan informasi yang banyak diterapkan adalah ISO/IEC 27001. Standar ini berfokus pada penerapan *Information Security Management System* (ISMS) yang bertujuan melindungi kerahasiaan, integritas, dan ketersediaan informasi. ISO 27001 menyediakan pendekatan berbasis manajemen risiko dalam pengelolaan keamanan informasi sehingga organisasi dapat mengidentifikasi ancaman, mengevaluasi risiko, dan menentukan kontrol keamanan yang sesuai(M. N. H. Siregar & Mardiah,

2025). Dalam sektor perbankan, penerapan ISO 27001 membantu meningkatkan tata kelola keamanan informasi dan memperkuat perlindungan terhadap data nasabah.

Selain ISO 27001, *framework* yang sering digunakan dalam keamanan siber adalah NIST *Cybersecurity Framework*. *Framework* yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) ini menyediakan panduan keamanan berbasis lima fungsi utama, yaitu *identify, protect, detect, respond*, dan *recover*. Melalui pendekatan tersebut, organisasi dapat membangun sistem keamanan yang lebih terstruktur dan mampu merespons ancaman siber secara efektif. *Framework* NIST dinilai fleksibel karena dapat diterapkan pada berbagai jenis organisasi, termasuk institusi perbankan.

Framework lain yang memiliki peran penting dalam tata kelola teknologi informasi adalah COBIT (*Control Objectives for Information and Related Technologies*). COBIT membantu organisasi dalam mengelola dan mengawasi penggunaan teknologi informasi agar selaras dengan tujuan bisnis perusahaan. Dalam konteks keamanan sistem informasi, COBIT berperan dalam memastikan bahwa pengelolaan risiko TI dilakukan secara efektif dan terintegrasi dengan proses bisnis organisasi.

Pada sektor perbankan, standar PCI DSS (*Payment Card Industry Data Security Standard*) juga menjadi *framework* penting dalam melindungi data transaksi pembayaran. Standar ini dirancang untuk menjaga keamanan data kartu pembayaran dan mencegah terjadinya pencurian informasi transaksi. PCI DSS mengatur berbagai aspek keamanan seperti pengelolaan akses, perlindungan jaringan, pemantauan aktivitas sistem, dan pengujian keamanan secara berkala.

Penerapan *framework* dan standar keamanan informasi memberikan banyak manfaat bagi institusi perbankan. Dengan adanya standar keamanan yang jelas, organisasi dapat memiliki prosedur penanganan risiko yang lebih terstruktur dan terukur.

Namun demikian, implementasi *framework* keamanan juga memiliki tantangan tersendiri. Proses penerapan standar membutuhkan sumber daya, biaya, dan komitmen organisasi yang cukup besar. Selain itu, *framework* keamanan perlu disesuaikan dengan kebutuhan dan karakteristik masing-masing institusi agar implementasinya berjalan efektif. Oleh karena itu, keberhasilan penerapan *framework* keamanan tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada dukungan manajemen,

budaya organisasi, serta kesiapan sumber daya manusia dalam menjalankan kebijakan keamanan informasi secara konsisten.

4. KESIMPULAN DAN SARAN

Transformasi digital dalam industri perbankan telah menghadirkan efisiensi layanan yang signifikan, namun di sisi lain memicu evolusi kejahatan siber yang semakin kompleks dan terorganisasi. Berdasarkan analisis yang telah dilakukan, dapat disimpulkan bahwa sektor perbankan merupakan target utama serangan siber karena memiliki nilai ekonomi tinggi dan menyimpan data sensitif nasabah. Ancaman utama yang teridentifikasi meliputi *phishing, malware* (khususnya *ransomware*), serangan *Distributed Denial of Service* (DDoS), serta teknik *social engineering* yang mengeksploitasi celah psikologis manusia.

Kapabilitas keamanan sistem informasi perbankan saat ini telah diperkuat melalui integrasi teknologi modern seperti *multi-factor authentication* (MFA), penggunaan *firewall*, sistem deteksi intrusi, hingga pemanfaatan kecerdasan buatan (AI) untuk analisis ancaman secara real-time. Penerapan standar internasional seperti ISO 27001, NIST *Cybersecurity Framework*, dan COBIT juga menjadi pilar krusial dalam mengelola risiko keamanan secara sistematis dan terstruktur.

Meskipun teknologi keamanan terus berkembang, faktor manusia (*human error*) dan kompleksitas infrastruktur teknologi tetap menjadi tantangan utama yang dapat menimbulkan celah keamanan. Oleh karena itu, strategi peningkatan ketahanan siber di masa depan tidak boleh hanya bertumpu pada aspek teknis, tetapi harus melibatkan pendekatan komprehensif melalui penerapan *konsep Zero Trust Security*, penguatan tata kelola TI, peningkatan literasi keamanan bagi pegawai dan nasabah, serta kolaborasi lintas sektor antara institusi perbankan dengan pemerintah. Keberhasilan dalam menghadapi evolusi kejahatan siber sangat bergantung pada kemampuan bank untuk bersikap adaptif, proaktif, dan berkelanjutan dalam memperbarui strategi keamanan mereka di era digital

DAFTAR REFERENSI

Anjheli, D. (2025). Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi

Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023. *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(1), 165–189. https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3964

Cantika Sarma Seicilia Silalahi, Agni Maria Veronika Manullang, Nazira Maulidia Nasution, Lia Oktafriani Pandiangan, G. N. B. B. (2024). *Analisis Keamanan Siber Perbankan dan Peran OJK: Studi Kasus Serangan Ransomware pada Bank Syariah Indonesia Tahun 2023 Cantika*. *2*(5), 524–532.

Diny, W. E. S., Eka, F. N. afifah, & Nafiza, S. F. (2024). Keamanan Siber Dalam Perbankan Serta TantanganDan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42.

Evy Nurmiati, Anugrah, S., Muhammad Zaky Himawan, & Qalby, N. R. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *11*(2), 106–112. https://doi.org/10.34010/jtk3ti.v11i2.17033

Fauziah, H. N. (n.d.). *Analisis Computer Crime dalam Ranah TIK : Bahaya Phising , Malware , dan Data Breach*.

Guntara, A. R. (n.d.). *KEJAHATAN KOMPUTER DAN PENTINGNYA ETIKA PROFESI TIK DALAM ERA DIGITAL INDONESIA Ahmad*.

Nur, F. (2023). Penegakan Hukum terhadap Kejahatan Digital Perbankan. *Innovative: Journal Of Social Science Research*, *3*(6), 3234–3249. https://j-innovative.org/index.php/Innovative/article/view/6617

Setiawan, R., & Rahmadsyah. (2025). Digitalisasi Perbankan dan Ancaman Keamanan Siber: Tantangan dan Strategi Mitigasi Risiko Operasional. *ASEFBA: Advanced Studies in Economic, Finance and Banking*, *1*(1), 1–15. https://doi.org/10.123456/asefba.v1i1.xxxx

Siregar, M. N. H., & Mardiah. (2025). Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001. *Jurnal Ilmu Komputer Dan Teknik Informatika*, *1*(2), 58–64. https://doi.org/10.64803/juikti.v1i2.52

Siregar, S. (2020). Analisis Risiko dalam Perbankan Syariah : tantangan dan solusi. *Jurnal Ekonomi Dan Bisnis Islam*, *12*(1), 56–72.

Sya, R., Razzaq, D., & Nurmiati, E. (2026). *Tantangan Etika dan Privasi terhadap Cyber Crime Big Data (Studi Literatur)*. *3*(2), 604–608.

Rahmatullah Rizki (2023). *IMPLEMENTASI AVG ANTIVIRUS DALAM MENJAGA KEAMANAN SISTEM DAN INFORMASI PADA KOMPUTER Rahmatullah*. (November 2023), 1–3