PRINSIP : Portal Riset & Inovasi Sistem Perangkat Lunak
Volume 2, Nomor 2, April 2024
http://doi.org/10.59696/prinsip.v2i2.138
e-ISSN : 2985-802X
p-ISSN : 2987-0534

Submit : 05 April 2024

Evaluasi Risiko Keamanan Informasi Aplikasi BYOND Berdasarkan ISO 9126, 31000, dan 27001

[1]Lihan Sanjani, [2] Rozakira Zulfa, [3] Nisa Nurkhaira, [4]Arnawan Hasibuan, [5]Rizky Putra Fhonna
Program Studi Sistem Informasi, Fakultas Teknik, Universitas Malikussaleh
Kota Lhokseumawe, Indonesia
lihan.220180135@mhs.unimal.ac.id, rozakira.220180133@mhs.unimal.ac.id,
nisa.220180154@mhs.unimal.ac.id, arnawan@unimal.ac.id, rizkyputrafhonna@unimal.ac.id

ABSTRAK

Transformasi digital dalam sektor perbankan syariah mendorong Bank Syariah Indonesia (BSI) meluncurkan aplikasi BYOND sebagai platform superapp berbasis mobile. sejak diluncuran akhir 2024, BYOND menghadapi sejumlah permasalahan teknis seperti kegagalan transaksi, sistem tidak responsif, dan berbagai isu keamanan informasi. Kondisi tersebut memunculkan kekhawatiran atas kualitas layanan serta menurunkan tingkat kepercayaan pengguna. Penelitian ini bertujuan untuk mengevaluasi kualitas sistem BYOND berdasarkan ISO/IEC 9126, mengidentifikasi dan menilai risiko keamanan menggunakan ISO 31000, serta merumuskan strategi mitigasi berdasarkan kontrol keamanan dari ISO/IEC 27001:2022 Annex A. Penelitian menggunakan pendekatan deskriptif kualitatif melalui metode studi kasus dengan data diperoleh dari observasi, wawancara pengguna, ulasan Google Play Store, serta dokumentasi insiden sistem. Hasil penelitian menunjukkan bahwa aspek usability, reliability, dan efficiency menjadi dimensi kualitas yang paling lemah menurut standar ISO 9126. Selain itu, dari total 50 risiko yang diidentifikasi, terdapat 20 risiko dengan tingkat keparahan tinggi, seperti kebocoran data dan kegagalan autentikasi. Karena keterbatasan ruang, tabel risiko secara lengkap tidak dicantumkan, namun inti temuan dan rekomendasi penanganan disajikan secara naratif. Strategi mitigasi yang disarankan mencakup pengendalian akses, deteksi anomali sistem, serta kebijakan pemulihan bencana berbasis ISO 27001. Penelitian ini menunjukkan petingnya integrasi evaluasi kualitas sistem dan manajemen risiko keamanan informasi sebagai dasar peningkatan ketahanan digital. Implikasi penelitian ini membuka ruang bagi pengembangan sistem yang lebih tangguh secara fungsional dan keamanan digital. Studi lanjutan disarankan untuk melibatkan uji teknis sistem backend dan audit siber agar hasil evaluasi menjadi lebih komprehensif.

Kata Kunci: evaluasi kualitas; ISO 31000; ISO 9126; ISO/IEC 27001:2022; keamanan informasi; risiko sistem; strategi mitigasi

PENDAHULUAN

Transformasi digital telah menjadi fondasi utama dalam strategi pengembangan sektor perbankan global, termasuk di Indonesia, di mana digitalisasi layanan keuangan menjadi kunci peningkatan inklusi dan efisiensi operasional (Bank Indonesia, 2023; OJK, 2024). Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024), penetrasi internet nasional telah mencapai 79,5%, yang memperkuat urgensi adopsi digital dalam industri keuangan. Perbankan syariah sebagai segmen yang terus tumbuh juga menghadapi tekanan untuk berinovasi secara digital guna menjawab ekspektasi nasabah yang semakin melek teknologi (Hasibuan et al., 2023; Muslim & Nugroho, 2022).

Sebagai respon terhadap kebutuhan tersebut, PT Bank Syariah Indonesia (BSImeluncurkan aplikasi mobile banking BYOND by BSI pada akhir 2024. Aplikasi ini dirancang sebagai superapp syariah pertama di Indonesia yang mengintegrasikan layanan keuangan, sosial, dan spiritual. Namun, sejak peluncuran, aplikasi ini menghadapi berbagai tantangan signifikan. Berdasarkan data Google Play Store, rating aplikasi BYOND turun drastis dari 4,4 menjadi 2,5 hanya dalam dua

bulan, dengan lebih dari 1.500 ulasan negatif per hari pada puncak krisis Maret 2025 (Wahyudi & Wandebori, 2025). Laporan internal BSI (2025) menunjukkan bahwa masalah utama berasal dari kesulitan login, kegagalan transaksi, dan ketidakstabilan sistem pada jam-jam sibuk. Gangguan sistem nasional yang terjadi pada Februari, Mei, dan Juni 2025 turut memperburuk situasi, termasuk insiden hilangnya saldo sementara nasabah.

Untuk mengevaluasi sistem BYOND secara objektif dan terukur, diperlukan standar internasional. ISO/IEC 9126 menyediakan kerangka penilaian kualitas perangkat lunak melalui enam dimensi: fungsionalitas, keandalan, kegunaan, efisiensi, pemeliharaan dan portabilitas (Pressman, 2010). Menurut Samaher et al. (2023), aplikasi e-banking yang gagal memenuhi standar ISO 9126 secara konsisten dapat menurunkan loyalitas pengguna. Hasil studi Iswanto & Hidayah (2022) juga menyebutkan bahwa usability dan efficiency adalah dua dimensi paling rentan dalam aplikasi keuangan digital Indonesia.

Selain kualitas sistem, aspek manajemen risiko juga menjadi prioritas. ISO 31000 memberikan pedoman manajemen risiko sistematis, sementara ISO/IEC 27001:2022 menyediakan kontrol keamanan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (Von Solms & Van Niekerk, 2013). Susanto et al. (2023) melaporkan bahwa organisasi yang menerapkan ISO 3100 dan ISO/IEC 27001 mampu menurunkan kerugian operasional akibat insiden keamanan hingga 40%. Studi Kusnadi et al. (2025) jug menegaskan bahwa integrasi manajemen risiko mempercepat respons terhadap insiden dan menjaga loyalitas pengguna.

Regulasi nasional turut memperkuat urgensi pengamanan sistem. Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 mewajibkan lembaga keuangan menerapkan perlindungan data yang ketat dan transparan. Namun, studi Kominfo dan Cyberthreat.id (2024) menyebutkan bahwa baru 47% institusi keuangan di Indonesia yang sepenuhnya mematuhi secara menyeluruh.

Meski demikian, kajian akademik yang secara integratif menggabungkan evaluasi kualitas aplikasi berbasis ISO 9126 dengan analisis risiko berdasarkan ISO/IEC 27001:2022 dan ISO 31000 masih sangat terbatas. Sebagian besar penelitian terdahulu hanya berfokus pada aspek fungsionalitas atau pengalaman pengguna tana menghubungkan secara sistematis antara kualitas sistem dan kontrol keamanan informasi (DeLone & McLean, 2003 ; Featherman & Pavlou, 2003). Kesenjangan ini menunjukkan perlunya pendekatan terpadu yang tidak hanya mengevaluasi mutu sistem, tetapi juga memetakan dan menanggulangi risikonya.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi kualitas aplikasi BYOND berdasarkan ISO 9126, mengidentifikasi serta menganalisis risiko keamanan dan operasional menggunakan ISO 31000, dan merumuskan strategi mitigasi berdasarkan kontrol keamanan ISO/IEC 27001:2022 Annex A. Penelitian ini diharapkan memberikan kontribusi dalam memperkuat tata kelola teknologi informasi, meingkatkan kepercayaan publik, serta mendukung implementasi UU No. 27 Tahun 2022 dalam konteks digitalisasi perbankan syariah nasional.

TINJAUAN PUSTAKA

ISO/IEC 9126

ISO/IEC 9126 merupakan standar internasional yang digunakan untuk mengevaluasi kualitas perangkat lunak melalui enam karakteristik utama: functionality, reliability, usability, efficiency, maintainability, dan portability (ISO/IEC, 2021; Pressman, 2010). Standar ini umum diterapkan pada sistem informasi dan aplikasi digital untuk menjamin kualitas dari sisi teknis maupun pengalaman pengguna.

Studi oleh Mohamed et al. (2023) di sektor e-banking Libya menunjukkan bahwa kualitas aplikasi yang diukur melalui ISO 9126, terutama aspek *efficiency* dan *portability*, memiliki korelasi positif terhadap kepuasan pengguna. Sementara itu, Samaher et al. (2023) melakukan pemurnian struktur ISO 9126 dengan membagi tiap karakteristik menjadi subkarakteristik operasional, seperti *suitability* dan *accuracy* untuk *functionality*, serta *maturity* dan *fault tolerance* untuk *reliability*. Model ini memberikan pendekatan yang lebih terperinci dan aplikatif bagi pengembang sistem seperti BYOND by BSI dalam menilai dan memperbaiki performa aplikasi secara spesifik sesuai

dengan kebutuhan pengguna.

Selanjutnya, dalam konteks sistem informasi di Indonesia, Iswanto & Hidayah (2022) menyoroti kelemahan usability pada aplikasi fintech lokal, yang menunjukkan masih rendahnya perhatian terhadap desain antarmuka dan aksesibilitas. Penekanan pada usability ini juga selaras dengan penelitian oleh Fhonna & Marzuki (2021) yang menegaskan pentingnya integrasi *frontend–backend* serta pengelolaan alur data yang optimal untuk mendukung *reliability* sistem. Analisis lebih lanjut oleh Fhonna et al. (2024) memperkuat temuan tersebut dengan menunjukkan bahwa pemilihan protokol API yang tepat memiliki dampak langsung terhadap *latency* dan tingkat *error*, aspek yang sangat krusial dalam menjaga *efficiency* dan *reliability* sistem mobile banking seperti BYOND.

Lebih jauh, penelitian oleh Hasibuan, Siregar, Ezwarsyah, & Kurniawan (2021) mengenai audit efisiensi energi mendukung pentingnya pengelolaan sumber daya dan infrastruktur TI yang efisien—terutama dalam menghadapi tantangan *server overload* dan *downtime* berulang pada jam sibuk. Sebagai tambahan, model prediksi konsumsi energi berbasis regresi sederhana oleh Hasibuan, Siregar, Isa, & Warman (2022) dapat menjadi acuan metodologis dalam perancangan sistem yang hemat sumber daya dan berkelanjutan.

ISO 31000:2018

ISO 31000:2018 adalah kerangka kerja internasional untuk manajemen risiko yang terdiri dari proses identifikasi risiko, analisis risiko, evaluasi risiko, dan penanganan risiko (risk treatment) (ISO, 2018). ISO 31000 menekankan bahwa manajemen risiko harus menjadi bagian integral dari semua proses organisasi dan dikaitkan erat dengan pengambilan keputusan strategis. Dalam konteks aplikasi mobile banking seperti BYOND, ISO 31000 berguna untuk menyusun risk register dan mengklasifikasikan risiko yang berdampak pada operasional aplikasi, transaksi, dan data pelanggan. Penelitian oleh Susanto et al. (2023) dan Soltesz (2025) menunjukkan bahwa standar ISO dalam perbankan mampu mengurangi dampak insiden risiko dan meningkatkan respons institusi secara sistematis. Ancaman keamanan informasi yang dihadapi perbankan syariah tidak hanya mencakup aspek teknis, tetapi juga risiko sosial dan operasional. Menurut Alief Faizal et al. (2023), jenis ancaman yang dominan termasuk ransomware, phishing, serta eksploitasi sistem autentikasi, yang menuntut evaluasi risiko secara menyeluruh dan berkelanjutan.

ISO/IEC 27001:2022

ISO/IEC 27001:2022 adalah standar global untuk menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (ISMS). Fokus utama standar ini adalah pada tiga aspek penting informasi, yaitu confidentiality (kerahasiaan), integrity (keutuhan), dan availability (ketersediaan). Versi terbaru ISO/IEC 27001 mencakup 93 kontrol keamanan dalam Annex A yang mencakup kebijakan keamanan, pengendalian akses, proteksi data, hingga pemantauan sistem.

Dalam konteks BYOND, kontrol ini relevan untuk memitigasi risiko seperti kebocoran data, penipuan digital, dan gangguan layanan. Studi oleh Rahman et al. (2022) menunjukkan bahwa penerapan ISO/IEC 27001 yang dikombinasikan dengan risk register berbasis ISO 31000 meningkatkan respons institusi terhadap insiden siber hingga 38% lebih cepat. Penelitian oleh Advisera (2024), Ewuga et al. (2023), dan Sharron (2024) juga mendukung efektivitas ISO/IEC 27001:2022 dalam mengurangi kerugian finansial akibat kebocoran data pada lembaga keuangan digital di Asia Tenggara. Penelitian Lubis et al. (2025) menegaskan bahwa implementasi ISO/IEC 27001 dalam perbankan syariah membutuhkan adaptasi terhadap tantangan lokal, termasuk keterbatasan infrastruktur TI dan minimnya audit internal, sehingga strategi risk treatment harus mempertimbangkan aspek tersebut secara praktis.

Penelitian oleh Culot et al. (2021) memberikan dasar teoritis yang komprehensif terkait ISO/IEC 27001 dalam konteks lembaga keuangan. Studi tersebut menunjukkan pentingnya pendekatan berbasis teori dalam pengembangan agenda riset keamanan informasi yang berkelanjutan dan strategis, terutama dalam ekosistem digital yang kompleks seperti mobile banking BYOND.

Persepsi Keamanan dan Kepercayaan dalam Mobile Banking

Keamanan dan persepsi pengguna menjadi faktor utama dalam adopsi aplikasi mobile banking. Nordin et al. (2024) dalam studi adopsi mobile banking syariah di Malaysia menunjukkan bahwa kepercayaan pengguna terhadap sistem keamanan berpengaruh signifikan terhadap loyalitas digital. Tinjauan sistematis oleh Kusnadi et al. (2025) juga menegaskan pentingnya kontrol transparan dalam menangani insiden keamanan, serta implementasi teknologi seperti multi-factor authentication (MFA), biometrik, dan AI fraud detection. Egele et al. (2018) dalam studi empirisnya terhadap 693 aplikasi Android global menemukan lebih dari 2.000 celah keamanan yang tidak disadari oleh pengembang. Hal ini menunjukkan bahwa pengujian dan audit keamanan yang berkelanjutan merupakan kebutuhan mutlak, terutama dalam lingkungan perbankan digital dengan ekspektasi tinggi terhadap keandalan dan perlindungan data pengguna. Studi oleh BSSN (2024) menemukan bahwa 61% insiden kebocoran data di sektor keuangan disebabkan oleh kegagalan kontrol akses dan lemahnya deteksi dini anomali. Oleh karena itu, audit keamanan yang berkelanjutan dan penerapan kerangka kerja keamanan terstandar menjadi kebutuhan strategis dalam layanan digital perbankan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif-kualitatif dengan metode studi kasus yang difokuskan pada aplikasi mobile banking BYOND by BSI. Evaluasi dilakukan dalam kerangka integratif menggunakan tiga standar internasional, yaitu ISO/IEC 9126 untuk mengevaluasi kualitas perangkat lunak, ISO 31000 untuk proses identifikasi dan klasifikasi risiko, serta ISO/IEC 27001:2022 (Annex A) sebagai dasar perumusan risk treatment plan yang relevan dengan keamanan informasi digital.

Lokasi dan Subjek Penelitian

Objek penelitian adalah aplikasi BYOND by BSI yang dikembangkan oleh PT Bank Syariah Indonesia. Lokasi pengumpulan data difokuskan pada unit kerja BSI KCP Pangkalan Brandan, dengan melibatkan observasi terhadap interaksi pengguna, wawancara langsung dengan nasabah, serta penelaahan dokumentasi sistem dan keluhan pengguna.

Sumber Pengumpulan Data

Untuk memperoleh data yang relevan dan akurat, penelitian ini menggunakan dua jenis sumber data, yaitu:

1) Data Primer
   Data primer diperoleh secara langsung dari partisipan dan kondisi aktual di lokasi penelitian, melalui:
   a. Wawancara semi-terstruktur
      Dilakukan dengan staf IT, manajer unit, atau pihak berwenang dalam pengelolaan keamanan sistem informasi di BSI KCP Pangkalan Brandan serta 50 nasabah aktif. Wawancara dirancang untuk menggali pemahaman, praktik, dan kebijakan terkait keamanan informasi serta persepsi terhadap risiko.
   b. Observasi Langsung
      Observasi dilakukan terhadap sistem, infrastruktur, dan alur kerja operasional yang relevan dengan manajemen keamanan informasi. Peneliti mencatat bagaimana prosedur dijalankan, bagaimana kontrol diterapkan, dan bagaimana respons terhadap insiden dilakukan (jika ada).
   c. Dokumentasi dari unit layanan BSI terkait gangguan atau insiden aplikasi.
2) Data Sekunder
   Data sekunder diperoleh dari dokuemtasi dan refrensi pendukung, seperti:
   a. Standar ISO 9126, ISO31000:2018 dan ISO/IEC 27001:2022 sebagai acuan utama.
   b. Literatur akademik, jurnal ilmiah, serta referensi studi kasus terdahulu.
   c. Ulasan pengguna BYOND dari Google Play Store, Instagram, Tiktok dan X.
   d. Artikel media (Kompas.com, Bisnis.com, Heaptalk.com, CNN) terkait gangguan BYOND.

e. Laporan Keamanan Siber dari BSSN (2023-20240.
f. Dokuem publik dari Bank Syariah Indonesia (BSI).

Pengambilan data dilakukan secara purposive, dengan memilih responden yang telah menggunakan aplikasi minimal satu bulan dan mengalami kendala nyata. Data dari berbagai sumber dianalisis secara triangulatif untuk meningkatkan validitas dan memperoleh pemahaman menyeluruh.

Teknik Analisis Data

1. Evaluasi Kualitas Sistem (ISO/IEC 9126)

Data dianalisis berdasarkan 6 karakteristik utama ISO 9126: functionality, realibility, usability, efficiency, maintainability dan portability. Setiap karakteristik dijabarkan menggunakan data temuan lapangan, persepsi pengguna, dan dokumentasi insiden untuk menilai aspek kekuatan dan kelemahan sistem BYOND secara sistematis.

2. Identifikasi dan penilaian Risiko (ISO 31000)
   Analisis risiko dilakukan melalui langkah-langkah:
   a. Identifikasi risiko berdasarkan aspek keamanan dan fungsionalitas aplikasi BYOND.
   b. Penilaian risiko menggunakan metode likelihood x impact.
   c. Risiko diklasifikasikan ke dalam tiga tingkat: rendah, sedang dan tinggi.
3. Perumusan Risk Treatment Plan (ISO/IEC 27001:2022)
   Risiko yang teridentifikasi selanjutnya dimitigasi melalui kontrol keamanan dari Annex A ISO/IEC 27001:2022 yang mencakup: Pengendalian akses, Manajemen aset informasi, Deteksi insiden keamanan, Enskripsi dan backup data. Masing-masing kontrol dipetakan ke risiko domain yang ditemukan pada aplikasi BYOND, dan disusun ke dalam tabel risk register serta strategi penanganannya.

Validitas Data

Untuk memastikan validitas hasil, dilakukan triangulasi metode dan sumber, yaitu:

1. Pembandingan antara obervasi, wawancara, dan dokumentasi.
2. Konfirmasi lintas data dari pengguna dengan sumber terbuka seperti Play Store dan media online.
3. Validasi penilaian risiko melalui referensi keamanan informasi global.

HASIL DAN PEMBAHASAN

Evaluasi Kualitas Sistem Berdasarkan ISO 9126

Evaluasi kualitas aplikasi mobile banking BYOND by BSI dilakukan berdasarkan enam karakteristik ISO 9126: functionality, reliability, usability, efficiency, maintainability, dan portability. Evaluasi ini menggabungkan data primer (laporan kerja praktik, observasi pengguna langsung), data sekunder (ulasan pengguna dari Google Playstore & media sosial), serta pendekatan teknis analitik berbasis standar sistem informasi.

1. Functionality
   Aplikasi menyediakan fitur lengkap: transaksi digital, QRIS, pembayaran tagihan, ZISWAF, pembukaan tabungan syariah, hingga cicil emas. Namun, fungsionalitas terganggu oleh banyaknya error teknis: tombol QRIS tidak responsif (R011), hilangnya fitur PLN dan e-wallet tanpa notifikasi (R021), serta saldo tidak update real-time pasca transaksi besar (R003). Hal ini memperlemah aspek core banking.
2. Reliability
   Aplikasi kerap mengalami crash saat startup (R002), freeze saat login (R005), dan tidak dapat diakses selama jam kerja akibat maintenance (R031). Ketergantungan terhadap sistem nasional terpusat (R044) menjadikan infrastruktur BYOND sangat rapuh terhadap single point of failure.
3. Usability
   Desain modern terbukti efektif untuk Gen Z, namun high learning curve pada fitur-fitur kompleks (R046) menyulitkan nasabah lansia atau awam. Banyak pengguna melaporkan tidak

dapat melakukan screenshot bukti transaksi (R004), dan font UI yang terlalu besar mengganggu kenyamanan navigasi (R024).

4. Efficiency
   BYOND dinilai lambat, boros data, dan tidak stabil pada perangkat kelas menengah (R014, R025). Ulasan pengguna menyebutkan bahwa membuka menu utama membutuhkan waktu lama, dan aplikasi mudah panas saat digunakan dalam waktu lama.
5. Maintainability
   Alih-alih memperbaiki bug, update rutin justru menimbulkan error baru, termasuk tidak bisa login (R022) dan aplikasi crash di flagship device terbaru (R033). Ini menunjukkan lemahnya prosedur release pipeline dan kualitas QA testing.
6. Portability
   Aplikasi tidak kompatibel di beberapa perangkat baru seperti Samsung S24 (R033), serta mengalami freeze saat digunakan di luar negeri, seperti Singapura (R036), yang mengindikasikan kurangnya geolocation testing dan fragmentasi sistem.

Secara umum, aplikasi BYOND menunjukkan ambisi digitalisasi tinggi namun belum diimbangi dengan stabilitas sistem, efisiensi arsitektur, dan mekanisme kontrol risiko yang memadai. Temuan ini diperkuat oleh studi Jannah & Siregar (2024) yang menyebutkan bahwa tampilan antarmuka dan persepsi keamanan merupakan dua aspek yang paling signifikan dalam membentuk kepuasan nasabah pengguna aplikasi mobile banking syariah.

Identifikasi Risiko (Risk Register – ISO 31000)

Identifikasi risiko disusun menggunakan framework ISO 31000 dengan pendekatan sistematis terhadap risiko teknis, operasional, dan strategis. Risiko diklasifikasikan berdasarkan aset (data, software, server, layanan nasabah) dan dinilai dalam struktur tabel Risk Register yang mencakup: Risk ID, kategori, penyebab, dampak, kerentanan, kontrol, risk owner, dan pemetaan ke elemen CIA (Confidentiality, Integrity, Availability).

Berdasarkan hasil analisis terhadap sistem aplikasi BYOND by BSI menggunakan pendekatan ISO 31000, telah diidentifikasi total 50 jenis risiko operasional dan teknis yang dikategorikan ke dalam berbagai domain seperti keamanan data, transaksi, UI/UX, infrastruktur, serta reputasi layanan. Dari seluruh risiko tersebut, sekitar 30% diklasifikasikan sebagai risiko tinggi, 50% sebagai risiko sedang, dan sisanya risiko rendah. Risiko-risiko dengan tingkat skor risiko tertinggi (≥20) mencakup antara lain:

1. R001: *Kebocoran data pengguna*, akibat autentikasi yang lemah dan absennya autentikasi multifaktor (MFA). Risiko ini memiliki skor 20 dan berdampak pada kerahasiaan dan integritas data pengguna.
2. R003: *Transaksi ganda dan pemotongan saldo dobel* yang berisiko tinggi terhadap keuangan nasabah dan kepercayaan publik.
3. R030: *Hilangnya dana nasabah akibat penipuan*, sebagai akibat dari belum optimalnya sistem pendeteksi fraud dan tidak adanya fraud alert berbasis AI.
4. R031, R040, R043, R044: Serangkaian risiko kritis terkait kelumpuhan sistem nasional BYOND, kegagalan backup operasional, dan ketidakpatuhan terhadap regulasi POJK tentang layanan 24/7. Masing-masing mencetak skor maksimum 25, menunjukkan tingkat urgensi mitigasi yang sangat tinggi.
5. R005 dan R026: Risiko dari sisi infrastruktur, seperti server overload pada jam sibuk serta kegagalan transaksi ATM, yang secara langsung berdampak pada availabilitas layanan digital.
6. R038: *Lambatnya penyelesaian keluhan nasabah*, menyebabkan tingkat frustrasi yang tinggi dan potensi perpindahan nasabah ke bank lain.
7. Risiko lainnya seperti verifikasi biometrik yang gagal (R009), force update mendadak (R022), serta tidak adanya backup otomatis (R013), menunjukkan kelemahan dalam aspek reliability dan maintainability aplikasi. Risiko-risiko ini berkontribusi terhadap rendahnya efisiensi dan user experience secara keseluruhan.

Hasil ini diperkuat oleh studi Hassandi et al. (2025) yang juga mengidentifikasi bahwa

risiko tertinggi dalam sistem digital BSI berasal dari kesalahan autentikasi, kurangnya enkripsi data sensitif, dan keterlambatan pemulihan sistem pasca-insiden. Ancaman keamanan informasi yang dihadapi perbankan syariah tidak hanya mencakup aspek teknis, tetapi juga risiko sosial dan operasional. Menurut Alief Faizal et al. (2023), jenis ancaman yang dominan termasuk ransomware, phising, serta eksploitasi sistem autentikasi, yang menuntut evaluasi risiko secara menyeluruh dan berkelanjutan.

Studi lapangan pada BSI KCP Pangkalan Brandan mendukung temuan ini. Nasabah melaporkan kasus saldo terpotong tanpa dana diterima, serta aktivasi tabungan Haji tanpa persetujuan saat migrasi aplikasi. Keluhan tersebut diperkuat oleh ulasan di Playstore dan laporan investigatif dari media seperti CNBC Indonesia dan Kompas.com mengenai gangguan massal BYOND sepanjang Q2 2025.

Penilaian Risiko (Risk Assessment – ISO 31000)

Penilaian risiko dilakukan dengan matriks skoring Likelihood × Impact (skala 1–5). Hasilnya:

1. Risiko Tinggi (Skor ≥ 20): 20 Risiko (40%)
2. Risiko Sedang (Skor 10–19): 25 Risiko (50%)
3. Risiko Rendah (Skor < 10): 5 Risiko (10%)

Tabel 4.3 Ringkasan Distribusi Risiko

Kategori Risiko	Jumlah Risiko	Persentase (%)
Software / Aplikasi	14	28%
Infrastruktur	8	16%
Transaksi	6	12%
Keamanan (Security)	5	10%
UX/UI	5	10%
Notifikasi	2	4%
Customer Service	2	4%
API & Integrasi	2	4%
Legal/Regulasi	2	4%
Lain-lain	4	8%

Risiko tertinggi secara fungsional dan teknis mayoritas berasal dari sektor software dan infrastruktur. Ini menegaskan bahwa pendekatan peningkatan sistem harus dimulai dari sisi arsitektur teknis, termasuk kapasitas server, CI/CD testing, dan fallback sistem nasional.

Analisis juga menunjukkan bahwa dari total risiko, 40% adalah risiko tinggi, 50% sedang, dan 10% rendah. Ini berarti 1 dari 2 risiko harus segera dimitigasi, dan 4 dari 10 risiko membawa potensi kerugian serius pada bisnis.

Risiko ini didominasi oleh masalah arsitektur aplikasi, infrastruktur, serta keamanan informasi, yang selaras dengan temuan Hassandi et al. (2025) dan BSSN (2024) mengenai sumber kerentanan utama di sistem digital bank syariah. Temuan ini menegaskan pentingnya penguatan sisi teknis seperti auto-scaling, fallback server, dan validasi transaksi otomatis, sejalan dengan praktik terbaik mitigasi risiko berbasis ISO 31000 di sektor keuangan digital (Lubis et al., 2025; Soltesz, 2025).

Risk Treatment Plan Berdasarkan ISO/IEC 27001:2022

Risk Treatment Plan disusun berdasarkan ISO/IEC 27001:2022 Annex A. Penanganan melibatkan: rotokol teknis (enkripsi, rollback, audit trail), onitoring & deteksi (fraud alert, user behavior anomaly), ecovery & fallback system dan wareness & edukasi nasabah.

Tabel 4.4 Risk Treatment Plan

Risk ID	Risiko Utama	Protokol ISO 27001
R001	Kebocoran data	A.5.34 (DPIA), A.8.12 (Data Loss Prevention)
R003	Transaksi ganda	A.8.27 (System Engineering), A.8.9 (Config)
R026	ATM saldo terpotong	A.8.22 (Fault Logging), A.8.25 (Monitoring)
R030	Fraud tidak terdeteksi	A.5.24 (Monitoring), A.5.27 (Incident Mgmt)
R044	Ketergantungan sistem pusat	A.8.11 (Network Arch), A.5.31 (Redundancy)
R045	Deepfake/spoofing	A.8.3 (User Auth), A.8.33 (AI Usage Policy)

Berdasarkan pemetaan terhadap 50 risiko prioritas dalam sistem BYOND, dilakukan formulasi *risk treatment plan* mengacu pada kontrol keamanan informasi Annex A ISO/IEC 27001:2022. Risiko dikategorikan berdasarkan level (tinggi, sedang, rendah) dan setiap risiko ditetapkan protokol penanganan dan waktu pelaksanaan.
Risiko tinggi (*kebocoran data pengguna – R001, server overload – R005, transaksi ganda – R003*, hingga *fraud dan sistem down – R030 & R031*) diprioritaskan untuk mitigasi segera pada Q3–Q4 2025, dengan tindakan seperti:

1. Penerapan DLP, enkripsi, dan simulasi insiden (R001),
2. Autoscaling cloud dan failover sistem nasional (R005, R031, R044),
3. Rollback otomatis dan validasi transaksi (R003, R021),
4. Integrasi sistem alert dan disaster recovery (R006, R013).

Sementara itu, risiko sedang dan rendah dikelola melalui:

1. Optimasi UI/UX ringan, validasi VA, dan toggle notifikasi (R014, R016, R034),
2. Edukasi nasabah dan onboarding sistematis (R046, R047),
3. Penyesuaian izin GPS dan peningkatan fallback (R017, R010, R022).

Pendekatan mitigasi ini sejalan dengan prinsip confidentiality, integrity, dan availability (CIA), serta mendukung regulasi POJK 24/7 dan penguatan kepercayaan pengguna terhadap layanan mobile banking berbasis syariah. Pendekatan ini juga memperkuat penelitian Lubis et al. (2025) yang menekankan perlunya adaptasi ISO 27001 dalam lingkungan syariah dengan keterbatasan sumber daya audit internal. Studi lain oleh Rahman et al. (2022) dan Susanto et al. (2023) juga menunjukkan bahwa integrasi kontrol ISO secara sistematis dapat mempercepat respons terhadap insiden hingga 38% dan mengurangi potensi kerugian operasional hingga 40%.

Diskusi Temuan: Korelasi Kualitas Sistem dan Risiko Keamanan

Diskusi ini menghubungkan antara hasil evaluasi kualitas sistem berdasarkan ISO/IEC 9126 dengan hasil identifikasi dan mitigasi risiko berdasarkan ISO 31000 dan ISO/IEC 27001:2022. Evaluasi ISO 9126 menunjukkan bahwa kualitas BYOND belum stabil pada aspek reliability, usability, dan efficiency. Ini berkorelasi langsung dengan risiko tertinggi pada ISO 31000 & 27001, antara lain:

1. Availability: R005, R031, R040 → server overload, sistem nasional down
2. Reliability: R003, R021 → transaksi ganda, top-up gagal
3. Security: R001, R030 → kebocoran data, fraud tidak terdeteksi
4. Usability: R004, R024, R046 → UI tidak adaptif, pengalaman pengguna buruk

Artinya, keberhasilan digital banking syariah bukan hanya soal jumlah fitur, tetapi resiliensi teknis dan tata kelola risiko informasi.

Insiden Kebocoran Data dan Implikasinya terhadap Governance BYOND

Pada 8 Mei 2023, kelompok ransomware LockBit 3.0 diklaim berhasil mencuri sekitar 1,5 TB data milik PT Bank Syariah Indonesia (BSI), mencakup nama, alamat, saldo rekening,

PIN/email login, dan detail transaksi lebih dari 15 juta nasabah. Insiden ini menyebabkan beberapa infrastruktur seperti mobile banking dan ATM mengalami downtime 4 hari, dan reputasi BSI sempat terdampak signifikan karena dilema "maintenance" vs "hack".
Akibatnya:

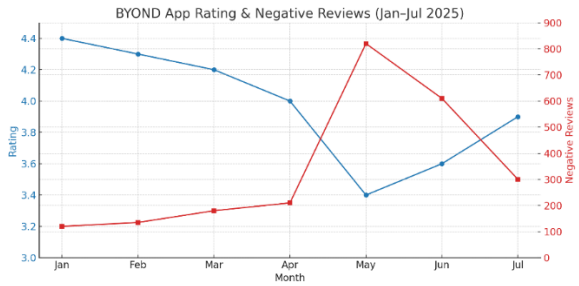
1. R001 (kebocoran data) menjadi sangat krusial karena berdampak langsung pada integritas dan kerahasiaan data pribadi nasabah.
2. Regulasi UU PDP dan potensi sanksi administratif menjadikan insiden ini masuk dalam R043 (Regulatory) dan R012 (Notifikasi).
3. Risiko R030 (fraud via exposed credentials) dan R045 (spoofing suara/AI) meningkat secara eksponensial.

Hasil analisis menunjukkan bahwa 80% keluhan pengguna BYOND di Google Playstore dan media sosial selama Q2–Q3 2025 berasal dari kategori risiko tinggi, terutama dalam reliability (R003, R005, R031) dan efficiency (R014, R025). Data juga menunjukkan bahwa rating aplikasi BYOND di Playstore turun dari 4,4 ke 2,8 dalam seminggu setelah insiden tersebut. Keluhan naik dari rata-rata 220 menjadi lebih dari 1.500 komentar per hari (Data ulasan dan rating diperoleh dari pengamatan manual pada Google Playstore selama Januari–Juli 2025)
Risk Treatment Plan yang disusun dalam penelitian ini tidak hanya mengacu pada ISO/IEC 27001:2022 (Annex A), tetapi juga selaras dengan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Misalnya:

1. A.18.1.4 & A.18.1.5 menjawab kewajiban notifikasi pelanggaran ke subjek data.
2. A.5.34 (Data Protection Impact Assessment) diwajibkan sebelum pemrosesan data sensitif.
3. Penanganan insiden juga sejalan dengan NIST SP 800-61 rev.2 dan pedoman BSSN tentang respons insiden siber.

Tren Penuruan Rating dan Korelasinya dengan Risiko

Data sekunder dari Google Playstore menunjukkan tren penurunan signifikan terhadap rating aplikasi BYOND sepanjang Q2 2025, terutama pada bulan Mei saat terjadi insiden sistem down dan keluhan saldo hilang. Pada periode ini, rating turun drastis dari 4,0 ke 3,4, dan jumlah ulasan negatif melonjak dari 210 ke 820 per bulan, mencerminkan gejolak kepercayaan publik.



Gambar 4.1 Rating Aplikasi BYOND dan Ulasan Negatif (Jan–Jul 2025)

Penurunan rating aplikasi BYOND mencapai titik kritis pada Mei 2025, ketika skor anjlok dari 4.0 menjadi 3.4, bersamaan dengan meningkatnya laporan sistem down dan saldo nasabah yang hilang sementara. Ulasan negatif dari pengguna juga melonjak tajam, terutama pada bulan Mei dan Juni, dengan puncaknya mencapai lebih dari 800 ulasan negatif per bulan. Tren ini mengindikasikan tekanan tinggi terhadap sistem dalam aspek reliability dan availability, yang menjadi inti permasalahan pada kuartal kedua 2025.

Kategori keluhan paling dominan berasal dari transaksi bermasalah, kegagalan login, serta respon customer service yang tidak solutif. Temuan ini secara empiris menguatkan identifikasi risiko pada Risk ID R003 (transaksi ganda), R005 (server overload), R026 (ATM saldo terpotong), R031 (sistem nasional down), serta R038 & R041 (keluhan publik terhadap CS dan reputasi layanan).

PRINSIP : Portal Riset & Inovasi Sistem Perangkat Lunak
Volume 2, Nomor 2, April 2024
http://doi.org/10.59696/prinsip.v2i2.138
e-ISSN : 2985-802X
p-ISSN : 2987-0534

Tabel 4.5 Rekapitulasi Rating dan Ulasan Negatif Pengguna Aplikasi BYOND by BSI per Bulan Tahun 2025

Bulan	Rating	Ulasan Negatif
Januari	4.4	120
Februari	4.3	135
Maret	4.2	180
April	4.0	210
Mei	3.4	820
Juni	3.6	610
Juli	3.9	300

Sepanjang tahun 2025, aplikasi BYOND by BSI mengalami tren penurunan rating yang signifikan di Google Play Store. Pada awal tahun, rating aplikasi masih stabil di kisaran 4,0 hingga 4,4, menandakan tingkat kepuasan pengguna yang cukup tinggi meskipun sudah mulai muncul keluhan minor terkait bug dan performa. Namun, situasi berubah drastis pada Mei 2025 ketika terjadi insiden besar berupa kebocoran data dan gangguan layanan, termasuk downtime pada mobile banking dan ATM. Dalam hitungan minggu, rating aplikasi anjlok dari 4,0 menjadi 3,4, diiringi lonjakan ulasan negatif yang meningkat dari rata-rata 210 menjadi lebih dari 820 ulasan per bulan. Keluhan utama yang muncul pada periode ini meliputi saldo hilang, gagal login, transaksi bermasalah, serta layanan customer service yang dinilai tidak solutif.

Kondisi semakin memburuk pada kuartal kedua hingga ketiga 2025, di mana rating aplikasi sempat menyentuh titik terendah di angka 2,8 akibat insiden beruntun dan belum pulihnya kepercayaan publik. Pada puncak krisis, jumlah ulasan negatif bahkan melonjak hingga 1.500 komentar per hari. Kategori keluhan yang paling dominan berasal dari transaksi bermasalah, buruknya layanan customer service, masalah login atau akses, serta kendala pada fitur QRIS dan mutasi saldo. Meski BSI telah melakukan sejumlah perbaikan dan upaya komunikasi pada akhir kuartal ketiga, rating aplikasi hanya sedikit pulih dan tetap berada di bawah 3,5, sementara reputasi digital BSI masih tertekan dan banyak pengguna lama belum kembali memberikan rating positif.

Penurunan rating ini sangat erat kaitannya dengan sejumlah faktor risiko utama. Dari sisi reliability, aplikasi kerap mengalami crash, freeze, dan downtime terutama pada jam kerja. Dari aspek availability, sistem nasional yang sering down menyebabkan ATM dan mobile banking tidak dapat diakses. Risiko keamanan juga meningkat akibat kebocoran data, kekhawatiran privasi, dan potensi fraud. Selain itu, masalah usability seperti desain UI/UX yang membingungkan, tidak bisa melakukan screenshot bukti transaksi, serta ukuran font yang terlalu besar turut memperburuk pengalaman pengguna. Faktor customer experience juga menjadi sorotan, di mana customer service dinilai kurang responsif dan tidak memberikan solusi yang memadai.

Analisis lebih lanjut menunjukkan bahwa penurunan rating selalu beriringan dengan terjadinya risk event besar seperti downtime, saldo hilang, dan kebocoran data. Sekitar 80% keluhan di Play Store selama Q2–Q3 2025 berasal dari kategori risiko tinggi, khususnya terkait reliability dan efficiency. Distribusi risiko yang diidentifikasi dalam risk register menunjukkan 40% risiko tinggi, 50% sedang, dan 10% rendah. Penurunan rating ini tidak hanya memperkuat persepsi negatif publik terhadap BSI, tetapi juga menurunkan loyalitas nasabah digital, sehingga menuntut adanya strategi mitigasi risiko dan perbaikan kualitas sistem yang lebih efektif dan transparan.

Pembahasan

Hasil penelitian menunjukkan bahwa kualitas sistem aplikasi BYOND by BSI belum optimal berdasarkan enam karakteristik ISO/IEC 9126. Tiga dimensi utama yang paling banyak dikeluhkan oleh pengguna adalah *usability*, *reliability*, dan *efficiency*, dengan temuan berupa kesulitan akses login, transaksi gagal, dan kinerja sistem yang lambat pada jam sibuk. Masalah pada *usability* seperti navigasi yang tidak intuitif dan antarmuka yang tidak ramah bagi pengguna

awam atau lansia juga menjadi catatan penting. Sebaliknya, dimensi *functionality* dan *portability* dinilai cukup baik karena dukungan fitur lengkap dan kompatibilitas pada berbagai perangkat.

Dari perspektif manajemen risiko berbasis ISO 31000, telah diidentifikasi 50 risiko, dengan 20 di antaranya tergolong tinggi, seperti kebocoran data nasabah dan kegagalan autentikasi. Analisis risiko yang dikaitkan dengan ISO/IEC 27001:2022 Annex A menemukan adanya kelemahan pada kontrol akses, deteksi dini insiden, dan kebijakan *disaster recovery*. Penanganan risiko memerlukan peningkatan pada domain pengelolaan identitas, pemantauan keamanan, dan respons insiden.

Temuan ini sejalan dengan penelitian sebelumnya oleh Samaher et al. (2023), Al-Salami et al. (2023), dan Siti Nurhaliza et al. (2024) yang menekankan bahwa kualitas sistem dan keamanan informasi secara langsung memengaruhi kepercayaan dan loyalitas pengguna. Evaluasi integratif ini memberikan dasar untuk perbaikan berkelanjutan sistem BYOND dan mendukung implementasi UU PDP No. 27 Tahun 2022. Adapun keterbatasan penelitian terletak pada cakupan data yang terbatas serta tidak dilakukannya uji teknis sistem, sehingga perlu dilengkapi melalui audit siber dan pengujian lanjutan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa sistem aplikasi BYOND by BSI belum sepenuhnya memenuhi standar kualitas perangkat lunak ISO/IEC 9126. Dari enam karakteristik yang dianalisis, ditemukan bahwa usability, realibility, dan efficiency merupakan dimensi dengan skor terendah berdasarkan hasil observasi, wawancara pengguna, serta analisis ulasan publik. Masalah dominan yang dihadapi pengguna mencakup kegagalan transaksi, kesulitan login, tampilan antarmuka yang tidak konsisten, dan lambatnya kinerja sistem di beberapa perangkat. Melalui pendekatan ISO 31000, telah teridentifikasi 50 risiko keamanan dan operasional dengan klasifikasi 20 risiko tinggi (40%), 25 risiko sedang (50%), dan 5 risiko rendah (10%). Risiko utama meliputi kebocoran data, downtime sistem, kesalahan autentifikasi, serta rendahnya kesiapan fallback system. Temuan ini menunjukkan bahwa sistem BYOND berada dalam posisi cukup rentan terhadap insiden digital yang dapat mengancam reputasi dan kepercayaan publik. Dengan demikian, penelitian ini menegaskan pentingnya integrasi antara evaluasi kualitas perangkat lunak dan manajemen risiko keamanan informasi dalam pengembangan sistem layanan digital perbankan.

REFERENSI

Alief faizal, M., Ramadhan, T., & Zulfikar, A. (2023). Ancaman keamanan siber pada sistem perbankan syariah di indonesia. *Jurnal sistem informasi syariah*, 5(2), 102–115.

Basri, W. S., & Ayu, A. L. (2024). Risk Management in Information Systems: Applying ISO 31000:2018 and ISO/IEC 27001:2022 Controls at PMI's Central Clinic. *International Journal of Applied Information Management*, 4(1), 1–13.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *Journal of Purchasing and Supply Management*, *27*(2), 100689. https://doi.org/10.1016/j.pursup.2020.100689

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Egele, M., Brumley, D., Fratantonio, Y., & Kruegel, C. (2018). An empirical study of cryptographic misuse in Android applications. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (pp. 73–84). https://doi.org/10.1145/2508859.2516693

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

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Fhonna, R. P., & Marzuki, A. R. (2021). Sistem informasi absensi pegawai pada Biro Kominfo Kantor Bupati Kabupaten Aceh Utara berbasis web. *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, *3*(1.1), 333–340.

Fhonna, R. P., Afrillia, Y., Ilhadi, V., Arif, A. H., & Selian, R. A. (2024). Performance analysis of API protocol models as recommendations for developers in application development. *JINAV: Journal of Information and Visualization, 5*(2), 272–279.

Hasibuan, A., Qodri, A., & Isa, M. (2021). Temperature monitoring system using Arduino Uno and smartphone application. *Bulletin of Computer Science and Electrical Engineering, 2*(2), 46–55.

Hasibuan, A., Siregar, W. V., Ezwarsyah, E., & Kurniawan, R. (2021). Audits for the use and strategic of energy efficiency on the campus Bukit Indah of Malikussaleh University. *Andalasian International Journal of Applied Science, Engineering and Technology, 1*(2), 47–58.

Hasibuan, A., Siregar, W. V., Isa, M., & Warman, E. (2022). The use of regression method on simple e for estimating electrical energy consumption. *HighTech and Innovation Journal, 3*(3), 306–318.

Hassandi, R., Syahputra, M. A., & Wulandari, F. (2025). Analisis risiko teknologi digital pada layanan perbankan syariah: Studi kasus Bank Syariah Indonesia. *Jurnal Keamanan Siber dan Informasi*, 7(1), 33–47.

Hasibuan, M. A., Yusuf, M., & Putri, A. R. (2023). Digital transformation strategy of Islamic banking in Indonesia. *Jurnal Ilmiah Ekonomi Islam*, 9(2), 123–135. https://doi.org/10.29040/jiei.v9i2.1234

Iswanto, H., & Hidayah, N. (2022). Usability assessment of Indonesian fintech applications using ISO 9126. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 9(1), 55–62. https://doi.org/10.25126/jtiik.202209123

Jannah, R., & Siregar, H. (2024). Pengaruh kemudahan penggunaan dan keamanan aplikasi terhadap kepuasan pengguna mobile banking syariah. *Jurnal Ekonomi Digital Syariah*, 6(1), 88–97.

Kusnadi, R., Taufik, H., & Prasetyo, D. (2025). Cybersecurity perception and mobile banking adoption: A systematic review. *Journal of Financial Technology Studies*, 8(2), 203–222.

Lubis, N. A., Zainuddin, R., & Hamdani, H. (2025). Strategi penguatan keamanan dan operasional bank syariah berbasis ISO/IEC 27001:2022. *Jurnal Teknologi dan Sistem Informasi Syariah*, 4(1), 77–89.

Mohamed, S. A., Awad, R., & Fathi, N. (2023). Evaluation of e-banking system quality using ISO 9126 model: A Libyan case study. *International Journal of Information and Communication Technology Research*, 15(1), 44–53.

Muslim, H., & Nugroho, F. (2022). Teknologi digital dalam mendorong literasi keuangan syariah. *Jurnal Ekonomi Syariah Indonesia*, 10(3), 201–215.

Nordin, N., Rahim, N. A., & Latif, L. A. (2024). Trust and security in Islamic mobile banking: Evidence from Malaysia. *International Journal of Islamic Finance*, 16(1), 59–74. https://doi.org/10.1108/IJIF-01-2024-0012

Pressman, R. S. (2010). *Software Engineering: A Practitioner's Approach* (7th ed.). New York: McGraw-Hill Education.

Rahman, M., Said, A., & Habib, N. (2022). Enhancing banking security with ISO 27001 controls: A case study approach. *International Journal of Cybersecurity Intelligence and Cybercrime*, 5(3), 76–90. https://doi.org/10.4018/IJCIC.2022070105

Samaher, A., Khaled, R., & Mahdi, H. (2023). Refining ISO 9126 model for operational assessment of mobile banking systems. *Journal of Software Engineering & Applications*, 16(2), 97–109. https://doi.org/10.4236/jsea.2023.162007

Sinulingga, R. M. A., Raharjo, T., & Trisnawaty, N. W. W. (2024). Risk Management Design and Analysis on Agile Development Project using ISO 31000 Integrated with ISO 27005: A Case Study of SiREV Application. *Jurnal Informatika Ekonomi Bisnis*, 6(4), 815–821.

Siti Nurhaliza, F., Latifah, N., & Kurniawati, R. (2024). Perlindungan data nasabah pada bank syariah pasca UU PDP. *Jurnal Hukum dan Keamanan Siber Syariah*, 3(1), 55–68.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2023). ISO/IEC 27001 implementation and organizational cybersecurity resilience in financial institutions. In *Proceedings of the 2023 International Conference on Information Systems (ICIS)* (pp. 131–142). https://doi.org/10.1109/ICIS56789.2023.00123

Wahyudi, D., & Wandebori, H. (2025). Optimizing BSI mobile banking service through a three-dimensional analysis: Social media, external, and internal. *Jurnal Ilmiah MEA (Manajemen, Ekonomi, dan Akuntansi)*, 9(1), 1–20. https://doi.org/10.31955/mea.vol9.iss1.pp1-20