Madani: Jurnal Ilmiah Multidisiplin
Volume 4, Nomor 8, September, P. 171-176
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.22870766

Konsep Dasar Manajemen Risiko dalam Pengelolaan Organisasi

Basic Concepts of Risk Management in Organizational Management

Anugerah[1], Dila Sri Handayani[2], Febri Lestari[3], Fitriani Pulungan[4], Emelia Rahmadany Putri Gami[5]
[1-5]Manajemen, Universitas Muslim Nusantara Al Washliyah, Indonesia
Email korespondensi: ameliagamie@gmail.com

Abstrak

Transformasi digital telah memperluas kemampuan bank dalam menyediakan layanan yang cepat, terintegrasi, dan berbasis data, tetapi pada saat yang sama memperluas eksposur terhadap risiko teknologi, siber, operasional, pihak ketiga, data, serta risiko keberlanjutan. Artikel ini bertujuan mengidentifikasi kelompok risiko utama pada perbankan digital dan menyusun prioritas risiko sebagai dasar penguatan mitigasi. Penelitian menggunakan pendekatan deskriptif-kualitatif berbasis studi dokumen dengan menelaah ketentuan Otoritas Jasa Keuangan, kerangka Basel Committee on Banking Supervision, serta literatur ilmiah mutakhir mengenai digitalisasi perbankan, FinTech, keamanan siber, dan risiko operasional. Identifikasi dilakukan melalui pemetaan sumber risiko, kemungkinan kejadian, dampak terhadap operasi dan nasabah, serta kebutuhan pengendalian. Hasil analisis menunjukkan lima kelompok risiko utama, yaitu risiko siber dan keamanan informasi, risiko data dan privasi, risiko gangguan teknologi dan operasional, risiko pihak ketiga/ketergantungan teknologi, dan risiko iklim/ESG. Dalam matriks prioritas konseptual, risiko siber dan keamanan informasi serta gangguan teknologi memperoleh perhatian tertinggi karena berpotensi mengganggu layanan kritis, menimbulkan kerugian finansial, dan menurunkan kepercayaan nasabah. Artikel menghasilkan kerangka identifikasi yang menghubungkan identifikasi risiko, penilaian, prioritas, mitigasi, monitoring, dan resiliensi operasional. Kerangka tersebut dapat digunakan sebagai dasar pengembangan penelitian empiris dan penyusunan indikator manajemen risiko pada bank yang sedang melakukan transformasi digital.
Kata kunci: identifikasi risiko; perbankan digital; risiko siber; risiko operasional; resiliensi

Abstract

Digital transformation has expanded banks' capabilities to provide fast, integrated, and data-driven services, but at the same time, it has increased their exposure to technology, cyber, operational, third-party, data, and sustainability risks. This article aims to identify the major risk groups in digital banking and establish risk priorities as a basis for strengthening risk mitigation. The study employs a descriptive-qualitative approach based on document analysis by reviewing regulations issued by the Financial Services Authority (Otoritas Jasa Keuangan/OJK), the framework of the Basel Committee on Banking Supervision (BCBS), and recent scholarly literature on banking digitalization, FinTech, cybersecurity, and operational risk. Risk identification was conducted by mapping risk sources, the likelihood of occurrence, impacts on operations and customers, and control requirements. The analysis identifies five major risk groups: cybersecurity and information security risk, data and privacy risk, technology and operational disruption risk, third-party risk/technology dependency, and climate/ESG risk. In the conceptual priority matrix, cybersecurity and information security risks, as well as technology disruption risks, receive the highest level of attention because they have the potential to disrupt critical services, cause financial losses, and undermine customer trust. This article develops an identification framework that links risk identification, assessment, prioritization, mitigation, monitoring, and operational resilience. The framework can serve as a basis for further empirical research and the development of risk management indicators for banks undergoing digital transformation.
Keywords: *risk identification; digital banking; cyber risk; operational risk; resilience*

Article Info
Received date: 20 August 2026 Revised date: 28 August 2026 Accepted date: 17 September 2026

PENDAHULUAN

Digitalisasi telah mengubah cara bank mengembangkan produk, berinteraksi dengan nasabah, memproses transaksi, dan mengelola informasi. Perbankan semakin bergantung pada aplikasi mobile,

komputasi awan, analitik data, kecerdasan artifisial, antarmuka pemrograman aplikasi, serta integrasi dengan penyedia teknologi. Perubahan tersebut meningkatkan efisiensi dan akses layanan, tetapi juga memperluas titik masuk risiko. Literatur menunjukkan bahwa digitalisasi perbankan dapat memengaruhi profil risiko secara berbeda: pada satu sisi dapat meningkatkan efisiensi dan kapasitas pengelolaan risiko, sedangkan pada sisi lain dapat memperbesar kompleksitas operasional dan ketergantungan terhadap teknologi (Uddin et al., 2023; Zhang et al., 2024).

Konteks risiko menjadi semakin penting karena layanan digital bersifat real time, saling terhubung, dan sangat bergantung pada ketersediaan sistem. Basel Committee on Banking Supervision menempatkan identifikasi dan penilaian risiko operasional sebagai elemen fundamental dalam manajemen risiko, dengan cakupan ancaman internal maupun eksternal pada produk, aktivitas, proses, dan sistem bank (BCBS, 2021). Kerangka resiliensi operasional juga menekankan tata kelola, kesinambungan bisnis, pengelolaan ketergantungan pihak ketiga, manajemen insiden, serta teknologi informasi yang tangguh dan keamanan siber.

Di Indonesia, kebutuhan tersebut sejalan dengan POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Regulasi tersebut mengharuskan manajemen risiko teknologi informasi dilakukan secara terintegrasi melalui proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko. Pengamanan informasi juga harus mempertimbangkan sumber daya manusia, proses, teknologi, dan aspek fisik atau lingkungan. Dengan demikian, identifikasi risiko bukan sekadar kegiatan administratif, tetapi menjadi dasar bagi pengendalian dan ketahanan operasional bank.

Ancaman siber menjadi salah satu isu yang menonjol. Tinjauan sistematis terhadap 74 publikasi menunjukkan bahwa ekosistem FinTech menghadapi beragam ancaman yang bersumber dari teknologi, manusia, dan prosedur, sementara strategi pertahanan perlu dibangun secara berlapis (Javaheri et al., 2024). Studi lain mengenai transformasi digital perbankan menunjukkan bahwa privasi data dan keamanan siber menjadi tantangan penting ketika bank mengadopsi cloud computing, big data analytics, artificial intelligence, dan blockchain (2024). Bank Indonesia juga menegaskan bahwa peningkatan digitalisasi meningkatkan eksposur risiko siber dan karena itu memerlukan penguatan keamanan sistem informasi dan ketahanan siber.

Selain risiko digital, bank menghadapi risiko yang berkembang dari aspek keberlanjutan. Perubahan iklim dapat memengaruhi kualitas aset, model bisnis, pembiayaan, dan ketahanan bank. OJK pada 2024 menerbitkan Climate Risk Management & Scenario Analysis (CRMS) sebagai kerangka untuk menilai ketahanan model bisnis dan strategi bank terhadap risiko iklim dalam jangka pendek, menengah, dan panjang. Perkembangan berikutnya pada 2026 melalui Climate Risk and Banking Resilience Assessment menunjukkan semakin kuatnya integrasi risiko iklim ke dalam pendekatan ketahanan perbankan.

Berdasarkan kondisi tersebut, artikel ini memfokuskan perhatian pada identifikasi dan pemetaan risiko yang muncul dalam transformasi digital perbankan. Tujuan penelitian adalah: (1) mengidentifikasi kelompok risiko utama; (2) memetakan sumber, dampak, dan pengendalian risiko; dan (3) menyusun prioritas konseptual risiko sebagai dasar penguatan mitigasi dan resiliensi operasional. Kontribusi artikel terletak pada penggabungan risiko digital, operasional, pihak ketiga, dan keberlanjutan dalam satu kerangka identifikasi.

METODE

Penelitian menggunakan pendekatan deskriptif-kualitatif melalui studi dokumen. Sumber utama terdiri atas regulasi Otoritas Jasa Keuangan dan Bank Indonesia, prinsip Basel Committee on Banking Supervision, serta artikel ilmiah yang membahas digital transformation, FinTech, cybersecurity, operational risk, dan sustainable banking. Pemilihan sumber mempertimbangkan relevansi langsung dengan risiko perbankan dan publikasi mutakhir, terutama periode 2023–2026.

Tahapan analisis meliputi empat langkah. Pertama, dilakukan identifikasi sumber risiko berdasarkan karakteristik transformasi digital bank. Kedua, risiko dikelompokkan ke dalam kategori yang memiliki kesamaan sumber dan dampak. Ketiga, setiap kategori dipetakan berdasarkan kemungkinan kejadian dan besarnya dampak menggunakan skala konseptual 1–5. Skor prioritas dihitung dengan rumus sederhana: Risk Priority Score (RPS) = Likelihood × Impact. Keempat, hasil pemetaan digunakan untuk merumuskan kebutuhan mitigasi dan indikator monitoring. Skor pada artikel ini merupakan hasil penilaian analitis berbasis dokumen, bukan hasil survei responden atau data insiden aktual, sehingga tidak boleh ditafsirkan sebagai estimasi probabilitas statistik.

HASIL DAN PEMBAHASAN

Hasil identifikasi menunjukkan bahwa risiko transformasi digital perbankan bersifat multidimensional. Risiko tidak hanya berada pada lapisan teknologi, tetapi juga pada manusia, proses, tata kelola, hubungan dengan pihak ketiga, dan keberlanjutan. Tabel 1 merangkum kelompok risiko, sumber utama, dampak potensial, serta bentuk pengendalian yang relevan.

Tabel 1. Identifikasi risiko utama dalam transformasi digital perbankan

No	Kelompok risiko	Sumber risiko	Dampak potensial	Pengendalian utama
1	Siber & keamanan informasi	Malware, phishing, credential theft, ransomware, kelemahan sistem	Gangguan layanan, kebocoran data, kerugian finansial, reputasi	MFA, encryption, SOC, penetration test, incident response
2	Data & privasi	Akses tidak sah, kualitas data, penyalahgunaan data, kesalahan konfigurasi cloud	Pelanggaran privasi, keputusan keliru, sanksi, hilangnya kepercayaan	Data governance, access control, data classification, audit trail
3	Teknologi & operasional	System failure, downtime, integrasi gagal, human error	Transaksi terganggu, biaya pemulihan, kegagalan layanan kritis	BCP/DRP, redundancy, testing, change management
4	Pihak ketiga	Vendor cloud, FinTech, outsourcing, API dan konsentrasi layanan	Vendor failure, lock-in, gangguan berantai, risiko konsentrasi	Due diligence, SLA, exit plan, monitoring vendor
5	Iklim & ESG	Risiko fisik, risiko transisi, kualitas pembiayaan, tuntutan stakeholder	Penurunan kualitas aset, biaya, risiko reputasi dan strategi	CRMS, ESG due diligence, scenario analysis, disclosure

Risiko siber dan keamanan informasi menempati posisi penting karena model layanan digital memperluas ketergantungan bank pada jaringan, aplikasi, identitas digital, dan data. Temuan Javaheri et al. (2024) menunjukkan bahwa ancaman FinTech mencakup kategori berbasis teknologi, manusia,

dan prosedur. Temuan tersebut memperkuat argumentasi bahwa pengendalian tidak cukup hanya berupa perangkat keamanan, tetapi harus mencakup kompetensi pegawai, prosedur, dan tata kelola. Dalam konteks Indonesia, Bank Indonesia menempatkan identifikasi dan asesmen risiko siber sebagai bagian dari kerangka keamanan sistem informasi dan ketahanan siber.

Risiko data dan privasi memiliki hubungan erat dengan risiko siber, tetapi perlu dibedakan. Risiko siber berfokus pada ancaman dan serangan terhadap sistem, sedangkan risiko data juga mencakup kualitas, integritas, ketersediaan, penggunaan, dan tata kelola data. Ketika bank menggunakan big data dan artificial intelligence, kualitas data menjadi semakin penting karena keputusan bisnis dapat dipengaruhi oleh data yang tidak lengkap atau tidak akurat. Karena itu, data governance perlu ditempatkan sebagai bagian dari arsitektur manajemen risiko digital.

Risiko teknologi dan operasional muncul ketika sistem gagal, terjadi downtime, integrasi antarsistem tidak berjalan, atau perubahan sistem menghasilkan gangguan. Uddin et al. (2023) menunjukkan bahwa digitalisasi dapat berkaitan dengan eksposur risiko operasional karena peningkatan volume bisnis dan ketergantungan pada teknologi. Temuan tersebut tidak berarti digitalisasi selalu meningkatkan risiko, tetapi menunjukkan bahwa pertumbuhan aktivitas digital harus diimbangi dengan kontrol, kapasitas sistem, pengujian, dan perencanaan pemulihan. Basel Committee menekankan business continuity, pemetaan interdependensi, dan kemampuan respons serta pemulihan sebagai bagian dari operational resilience.

Risiko pihak ketiga juga menjadi semakin relevan ketika bank menggunakan cloud, vendor keamanan, FinTech, data center, dan penyedia layanan lainnya. Ketergantungan tersebut dapat menciptakan risiko konsentrasi dan risiko berantai. Gangguan pada satu penyedia dapat memengaruhi banyak proses sekaligus. Oleh sebab itu, due diligence, service level agreement, pemantauan kinerja, hak audit, rencana keluar, dan alternatif penyedia perlu menjadi bagian dari identifikasi risiko sejak tahap pengadaan.

Risiko iklim dan ESG memperluas cakupan identifikasi risiko dari aspek operasional menuju keberlanjutan. OJK melalui CRMS mengarahkan bank untuk mempertimbangkan tata kelola, strategi, manajemen risiko, dan pengungkapan dalam menilai ketahanan terhadap perubahan iklim. Risiko iklim dapat bersifat fisik maupun transisi dan berpotensi memengaruhi debitur, nilai agunan, kualitas kredit, serta model bisnis bank. Karena itu, integrasi ESG risk management dengan proses risiko konvensional dapat membantu bank mengidentifikasi risiko jangka panjang yang tidak selalu terlihat dari indikator keuangan historis.

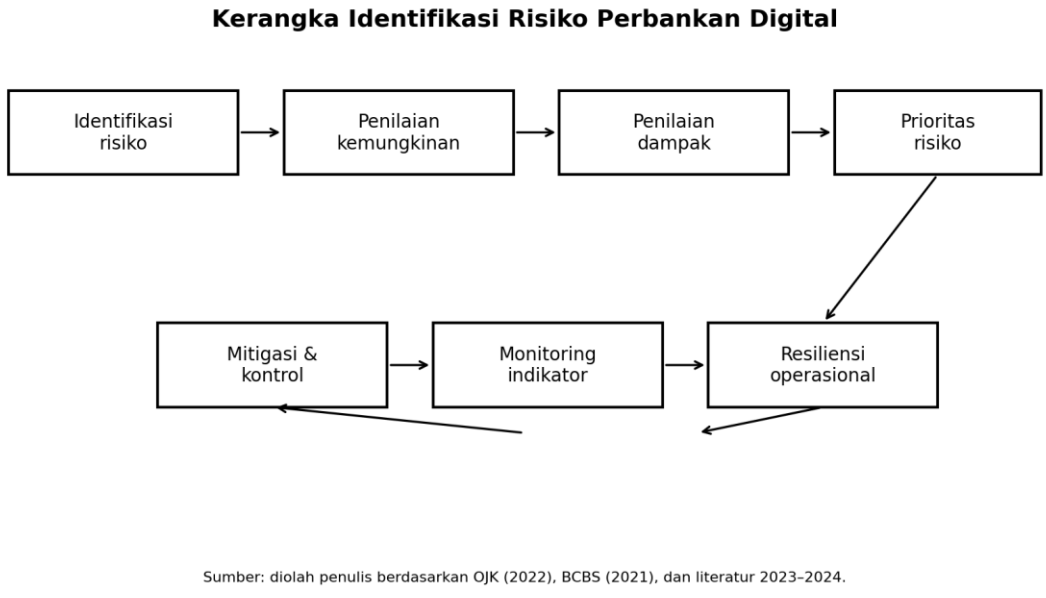
Tabel 2. Matriks prioritas konseptual risiko

Risiko	Likelihood (1–5)	Impact (1–5)	RPS	Prioritas konseptual	Fokus mitigasi
Siber & keamanan informasi	5	5	25	Sangat tinggi	Deteksi, pencegahan, respons insiden
Teknologi & operasional	4	5	20	Tinggi	Resiliensi, BCP/DRP, redundancy
Data & privasi	4	5	20	Tinggi	Data governance dan access control
Pihak ketiga	4	4	16	Tinggi	Vendor risk management

Iklim & ESG	3	4	12	Menengah	Scenario analysis dan ESG integration

Tabel 2 menunjukkan prioritas konseptual yang menempatkan risiko siber dan keamanan informasi pada skor tertinggi. Penempatan tersebut merupakan hasil analisis berbasis karakteristik risiko, bukan pemeringkatan empiris antarbank. Risiko teknologi-operasional dan data-privasi juga berada pada prioritas tinggi karena gangguan terhadap sistem atau data dapat langsung memengaruhi layanan kritis. Sementara itu, risiko pihak ketiga perlu mendapat perhatian tinggi karena keterhubungan antarsistem dapat memperbesar dampak insiden. Risiko iklim dan ESG memperoleh prioritas menengah dalam matriks ini, tetapi sifatnya strategis dan berjangka panjang sehingga tidak tepat diabaikan.

Kerangka identifikasi yang dihasilkan disajikan pada Gambar 1. Kerangka tersebut menempatkan identifikasi risiko sebagai proses berkelanjutan. Setelah risiko ditemukan, bank perlu menilai kemungkinan dan dampaknya, menentukan prioritas, menetapkan mitigasi, memantau indikator risiko, dan menggunakan hasil monitoring untuk meningkatkan resiliensi. Pendekatan ini sejalan dengan prinsip Basel bahwa identifikasi, penilaian, mitigasi, dan pemantauan efektivitas kontrol saling terkait dalam membangun operational resilience.



Gambar 1. Kerangka identifikasi risiko perbankan digital

Implikasinya bagi manajemen bank adalah perlunya perubahan dari pendekatan yang reaktif menuju pendekatan risk-informed. Indikator risiko utama dapat mencakup jumlah insiden siber, waktu deteksi, waktu pemulihan, tingkat kegagalan transaksi, downtime, jumlah temuan kontrol, ketergantungan pada vendor kritis, serta indikator risiko iklim pada portofolio pembiayaan. Dengan indikator tersebut, identifikasi risiko tidak berhenti pada daftar risiko, tetapi berkembang menjadi sistem monitoring yang dapat mendukung pengambilan keputusan.

Temuan ini juga memberikan ruang bagi penelitian berikutnya. Kerangka konseptual dapat diuji menggunakan data sekunder bank melalui pengungkapan risiko, sustainability report, annual report, indikator teknologi, dan ukuran kinerja keuangan. Pengujian empiris dapat diarahkan untuk melihat apakah digital governance, digital finance capability, dan green finance berhubungan dengan

kemampuan manajemen risiko dan kinerja keuangan berkelanjutan. Dengan demikian, identifikasi risiko menjadi tahap awal untuk mengembangkan model risk-adjusted digital sustainable finance.

SIMPULAN

Identifikasi risiko pada transformasi digital perbankan menunjukkan bahwa risiko bersifat saling terhubung dan tidak terbatas pada risiko teknologi. Lima kelompok utama yang teridentifikasi adalah risiko siber dan keamanan informasi, data dan privasi, teknologi dan operasional, pihak ketiga, serta iklim dan ESG. Matriks konseptual menempatkan risiko siber sebagai perhatian tertinggi, diikuti risiko teknologi-operasional, data-privasi, dan pihak ketiga, sedangkan risiko iklim dan ESG perlu dikelola sebagai risiko strategis jangka panjang. Kerangka yang dihasilkan menekankan siklus identifikasi, penilaian, prioritas, mitigasi, monitoring, dan resiliensi. Penelitian lanjutan disarankan menggunakan data empiris perbankan untuk menguji validitas indikator dan hubungan antarvariabel secara kuantitatif.

REFERENSI

Bank for International Settlements. (2021). Principles for operational resilience. Basel Committee on Banking Supervision.

Bank Indonesia. (2024). Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications, 241, 122697.

Otoritas Jasa Keuangan. (2022). Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Otoritas Jasa Keuangan. (2024). Panduan Climate Risk Management & Scenario Analysis (CRMS) Perbankan 2024.

Otoritas Jasa Keuangan. (2026). Climate Risk and Banking Resilience Assessment (CBRA) 2026.

Papathomas, A., & Konteos, G. (2024). Financial institutions digital transformation: The stages of the journey and business metrics to follow. Journal of Financial Services Marketing, 29, 590–606.

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? Technological Forecasting and Social Change, 197, 122919.

Zhang, Y. et al. (2024). Research on the impact of digital transformation on the systemic risk of banks. Procedia Computer Science, 242, 364–371.