

Eskalasi risiko operasional dalam layanan perbankan digital: Tantangan pengendalian internal di tengah kompleksitas teknologi

Yuke Ivana Kusuma Wardani

Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: yukeivanao@gmail.com

Kata Kunci:

Risiko operasional;
perbankan digital;
pengendalian internal;
manajemen risiko; risiko siber.

Keywords:

Operational risk; digital banking; internal control; risk management; cyber risk.

ABSTRAK

Penelitian ini bertujuan untuk mengeksplorasi peningkatan risiko operasional di bidang layanan perbankan digital serta menilai seberapa efektif pengendalian internal dalam menangani kompleksitas teknologi yang semakin tinggi. Meskipun kemajuan digital banking telah membawa efisiensi dalam layanan, sisi gelapnya muncul risiko baru seperti kerusakan sistem, serangan dari dunia maya, dan gangguan dalam proses operasional. Penelitian ini mengadopsi metode kualitatif dengan melakukan kajian literatur pada publikasi internasional dan domestik yang relevan. Temuan menunjukkan bahwa pelaksanaan manajemen risiko operasional yang mencakup tahap identifikasi, pengukuran, pemantauan, dan pengendalian secara garis besar telah berpedoman pada kerangka Basel. Namun, pelaksanaannya masih jauh

dari ideal, terutama dalam memperkuat pengendalian internal serta mengurangi risiko yang berkaitan dengan teknologi. Ditemukan bahwa terdapat perbedaan antara teori dan praktik di lapangan, terutama dalam menghadapi risiko digital yang semakin rumit. Oleh karena itu, diperlukan penguatan pengendalian internal yang fleksibel, integrasi teknologi dalam manajemen risiko, serta peningkatan pengelolaan risiko untuk menjaga stabilitas dan keberlangsungan perbankan digital.

ABSTRACT

This research aims to explore the increasing operational risk in the field of digital banking services as well as to assess how effective internal controls are in handling the growing complexity of technology. Although advancements in digital banking have brought efficiency to services, the dark side emerges in the form of new risks such as system failures, cyber-attacks, and disruptions in operational processes. This research adopts a qualitative method by reviewing literature from relevant international and domestic publications. The findings indicate that the implementation of operational risk management, covering the stages of identification, measurement, monitoring, and control, has broadly followed the Basel framework. However, its execution is still far from ideal, especially in strengthening internal controls and reducing technology-related risks. It was found that there is a gap between theory and practice in the field, particularly in facing increasingly complex digital risks. Therefore, it is necessary to strengthen flexible internal controls, integrate technology into risk management, and improve risk management to maintain the stability and sustainability of digital banking.

Pendahuluan

Perkembangan teknologi informasi telah mendorong perubahan yang cukup signifikan dalam industri perbankan terutama melalui transformasi menuju layanan



digital banking (Danarhuda & Solekah, 2025). Digitalisasi ini memungkinkan bank untuk menyediakan layanan yang lebih cepat, efisien, dan fleksibel tanpa dibatasi oleh ruang dan waktu. Di Indonesia, pertumbuhan layanan perbankan digital menunjukkan peningkatan yang sangat pesat, yang dipengaruhi oleh tingginya penetrasi internet, penggunaan smartphone, serta perubahan perilaku masyarakat yang semakin mengutamakan kemudahan dalam bertransaksi (Laksana et al., 2023). Kondisi ini menjadikan digital banking sebagai salah satu elemen penting dalam sistem keuangan modern.

Di sisi lain, perkembangan tersebut juga membawa konsekuensi berupa meningkatnya kompleksitas risiko operasional. Risiko yang sebelumnya didominasi oleh kesalahan manusia kini berkembang menjadi lebih kompleks mencakup kegagalan sistem, gangguan jaringan, kesalahan algoritma, hingga ancaman serangan siber (*cyber risk*). Perubahan ini menunjukkan bahwa digitalisasi tidak hanya memberikan efisiensi, tetapi juga memperbesar potensi risiko yang dihadapi oleh perbankan (Management, 2018).

Dalam dunia perbankan, risiko operasional merupakan salah satu risiko utama yang perlu dikelola secara sistematis. (Cristea, 2021) mendefinisikan risiko operasional sebagai risiko yang timbul akibat kegagalan proses internal, manusia, sistem, maupun faktor eksternal. Risiko ini memiliki dampak yang signifikan terhadap kinerja keuangan, reputasi, serta tingkat kepercayaan nasabah. Oleh karena itu, penerapan manajemen risiko operasional menjadi sangat penting untuk menjaga keberlangsungan operasional bank.

Secara umum pengelolaan risiko operasional mengacu pada standar internasional seperti Basel II dan Basel III yang menekankan pentingnya proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko. Selain itu pengendalian internal juga memegang peranan penting dalam memastikan risiko dapat diminimalkan secara efektif. Sistem pengendalian internal yang baik memungkinkan organisasi untuk mendeteksi potensi risiko lebih awal serta mengambil langkah mitigasi yang tepat (*Humanities And Social Sciences*, 2022).

Namun penerapan manajemen risiko operasional di sektor perbankan digital di Indonesia masih menghadapi beragam masalah yang sulit (Arfan et al., 2016). Perubahan digital yang cepat tidak selalu sejalan dengan kesiapan pengendalian internal dan kerangka kerja manajemen risiko yang mampu beradaptasi terhadap kemajuan teknologi. (Mazayo et al., 2023) mengungkapkan bahwa digitalisasi perbankan di Indonesia meningkatkan paparan terhadap risiko operasional, khususnya yang berkaitan dengan pengintegrasian sistem, keamanan teknologi, dan kemungkinan kegagalan dalam proses digital.

Selain itu pertumbuhan penggunaan layanan perbankan digital juga berkontribusi pada peningkatan ancaman risiko siber yang semakin rumit. (Mujanah et al., 2025) menunjukkan bahwa kemajuan dalam sistem keuangan digital secara langsung membuat lebih rentan terhadap risiko siber, yang merupakan elemen dari risiko operasional modern dalam dunia perbankan. Risiko ini tidak hanya menyebabkan

gangguan sistem, tetapi juga dapat mengakibatkan kerugian finansial dan menurunkan tingkat kepercayaan nasabah terhadap layanan perbankan digital (Mardiana, 2018).

Meskipun penelitian mengenai manajemen risiko operasional telah banyak dilakukan, sebagian besar masih berfokus pada aspek umum dan belum secara mendalam mengkaji eskalasi risiko dalam konteks digital banking khususnya terkait efektivitas pengendalian internal. Padahal, dalam era digital pengendalian internal tidak hanya berfungsi sebagai alat pengawasan tetapi juga sebagai mekanisme adaptif dalam menghadapi perubahan risiko yang dinamis.

Berdasarkan hal tersebut, penelitian ini bertujuan untuk menganalisis peningkatan risiko operasional dalam layanan perbankan digital serta mengkaji peran pengendalian internal dalam mengelola kompleksitas teknologi. Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi berbagai tantangan dalam implementasi manajemen risiko operasional di Indonesia serta merumuskan strategi mitigasi yang relevan untuk menjaga stabilitas perbankan digital.

Pembahasan

Peningkatan Risiko Operasional dalam Perubahan Perbankan Digital

Pengelolaan risiko operasional pada dasarnya adalah mekanisme penting dalam memastikan kelangsungan fungsi intermediasi perbankan melalui pengenalan dan pengendalian berbagai kemungkinan kegagalan operasional. Risiko ini meliputi kesalahan manusia, kegagalan sistem, kelemahan prosedur, serta gangguan dari luar termasuk serangan siber (Cristea, 2021). Akan tetapi, sifat risiko operasional kini tidak lagi statis dalam lingkup perbankan digital, melainkan telah berevolusi menjadi risiko yang lebih rumit, terintegrasi, dan berbasis teknologi.

Di era digital, risiko operasional tidak hanya bertambah dalam jumlah, namun juga mengalami perubahan sifat secara kualitatif. (Management, 2018) menyatakan bahwa digitalisasi dalam sistem perbankan meningkatkan ketergantungan terhadap infrastruktur teknologi yang rumit, sehingga meningkatkan kemungkinan terjadinya gangguan sistemik yang berdampak luas pada operasional bank. Dengan kata lain, digitalisasi tidak hanya menghasilkan efisiensi, tetapi juga memperluas area risiko yang sebelumnya terbatas pada proses manual.

(Laksana et al., 2023) menunjukkan bahwa layanan perbankan digital di Indonesia memiliki tingkat paparan risiko operasional yang lebih tinggi dibandingkan layanan tradisional, terutama dalam aspek stabilitas sistem dan keamanan data. Temuan ini mendukung pandangan bahwa peningkatan risiko operasional tidak hanya disebabkan oleh kemajuan teknologi, tetapi juga oleh meningkatnya kompleksitas dalam integrasi sistem digital yang masih belum sepenuhnya matang secara institusional.

Ketidakesesuaian Kerangka Risiko dengan Realitas Digital Banking

Secara konseptual, manajemen risiko operasional masih mengacu pada kerangka Basel II dan Basel III yang menekankan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko. Namun, kerangka ini pada dasarnya dibangun dalam konteks perbankan tradisional yang belum sepenuhnya terdigitalisasi. Akibatnya,

terdapat kesenjangan struktural antara pendekatan normatif dengan dinamika risiko aktual dalam digital banking.

(*Humanities And Social Sciences*, 2022) menegaskan bahwa munculnya *cyber risk*, *data breach*, serta risiko berbasis algoritma menunjukkan perlunya redefinisi dalam konsep manajemen risiko operasional. Risiko tidak lagi bersifat linier dan terprediksi, tetapi berubah menjadi sistemik, real-time, dan adaptif terhadap perubahan teknologi. Kondisi ini menunjukkan bahwa pendekatan konvensional dalam manajemen risiko mulai kehilangan relevansinya dalam menghadapi kompleksitas digital.

Dengan demikian, permasalahan utama bukan hanya pada meningkatnya jenis risiko baru, tetapi pada ketidaksesuaian antara framework risiko yang digunakan dengan realitas operasional perbankan modern.

Kesenjangan antara Risiko Digital dan Pengendalian Internal

Dalam dunia perbankan digital, peningkatan risiko operasional tak bisa dipisahkan dari isu mendasar, yaitu keterbatasan sistem pengendalian internal dalam menghadapi teknologi yang terus berubah. Secara teori, pengendalian internal memiliki tujuan untuk memastikan bahwa proses operasional dilakukan sesuai dengan prosedur dan mengurangi risiko yang ada. Namun dalam praktiknya, banyak sistem pengendalian internal di lembaga perbankan masih berfungsi secara administratif, berkala, dan berfokus pada kepatuhan.

(*Humanities And Social Sciences*, 2022) menunjukkan bahwa perubahan digital memerlukan pengendalian internal yang harus bersifat adaptif, real-time, dan berbasis teknologi. (Mazayo et al., 2023) menemukan bahwa banyak bank di Indonesia masih dalam proses transisi untuk menggabungkan sistem pengendalian internal dengan infrastruktur digital. Situasi ini menciptakan kesenjangan antara laju perkembangan teknologi dan kemampuan kontrol internal untuk beradaptasi.

Oleh karena itu, peningkatan risiko operasional dalam perbankan digital pada dasarnya mencerminkan ketidakmampuan sistem pengendalian internal konvensional untuk menyesuaikan diri dengan kompleksitas teknologi yang semakin maju. Risiko ini tidak hanya meningkat, tetapi juga menjadi semakin sulit untuk dikendalikan karena alat pengendalian yang ada kini tidak lagi sesuai dengan karakteristik risiko digital.

Risiko Siber sebagai Wujud Kegagalan Integrasi Sistem Pengendalian

Di dalam dunia perbankan digital, risiko siber muncul sebagai bentuk yang paling mencolok dari risiko operasional masa kini. Jenis risiko ini mencakup peretasan, perangkat lunak berbahaya, pencurian identitas, dan kebocoran informasi yang berpengaruh tidak hanya pada aspek operasional tetapi juga pada citra dan kepercayaan nasabah.

(Mujanah et al., 2025) mengungkapkan bahwa digitalisasi dalam sektor keuangan secara langsung memperbesar paparan terhadap risiko siber yang bersifat kompleks dan tidak mudah diprediksi. Akan tetapi, tantangan utama bukan hanya seputar meningkatnya ancaman siber, melainkan juga terkait dengan pemisahan dalam pengelolaan risiko siber dari sistem manajemen risiko operasional secara menyeluruh.

Sering kali risiko siber dianggap sebagai masalah teknis semata sebagai elemen strategis dalam pengendalian risiko operasional. Namun di dalam konteks perbankan digital risiko siber menjadi indikator yang paling jelas dari kegagalan integrasi antara teknologi dan sistem pengendalian internal.

Kelemahan dalam Penerapan Manajemen Risiko di Indonesia

Di dalam Walaupun *Enterprise Risk Management* (ERM) telah diadopsi oleh sektor perbankan di Indonesia, efektivitasnya masih terhambat oleh berbagai keterbatasan struktural. (Laksana et al., 2023) mengungkapkan bahwa walaupun risiko operasional telah diakui secara resmi dalam sistem perbankan digital, pengelolaan terhadap risiko tersebut masih belum optimal.

Ada tiga isu utama yang menjadi hambatan dalam penerapan manajemen risiko di Indonesia:

Ketergantungan pada pendekatan yang berbasis kepatuhan, di mana manajemen risiko hanya berfungsi untuk memenuhi ketentuan hukum, alih-alih menjadi alat untuk pengambilan keputusan strategis.

Keterhubungan yang rendah antara sistem digital dan tata kelola risiko, yang mengakibatkan deteksi risiko tidak dapat dilakukan secara langsung.

Budaya risiko yang belum terbentuk dengan baik, sehingga kesadaran organisasi mengenai risiko digital masih terbatas.

Situasi ini menunjukkan bahwa masalah utamanya tidak pada ketiadaan sistem manajemen risiko, melainkan pada rendahnya kualitas penerapan dan integrasi sistem tersebut dalam operasi bank.

Berkembangnya kerumitan risiko operasional memerlukan pergeseran pengendalian internal dari metode konvensional ke sistem yang lebih responsif, mendahului, dan berbasis teknologi. Pengendalian internal kini harus lebih dari sekedar alat administrasi, tetapi wajib mampu mengidentifikasi risiko secara langsung. Penggabungan teknologi seperti kecerdasan buatan, analisis data besar, dan sistem monitoring digital menjadi hal yang krusial dalam meningkatkan efisiensi pengendalian internal.

Kesimpulan dan Saran

Berdasarkan ulasan yang telah dilakukan, dapat disimpulkan bahwa peningkatan risiko operasional dalam layanan perbankan digital tidak hanya disebabkan oleh pergeseran teknologi, tetapi juga mencerminkan adanya perubahan mendasar dalam sifat risiko yang semakin rumit, dinamis, dan didukung oleh sistem digital. Risiko operasional sekarang tidak lagi bersifat tradisional, tetapi telah berubah menjadi risiko sistemik yang melibatkan elemen teknologi, keamanan data, dan integrasi sistem digital yang saling berkaitan.

Secara teoritis kerangka kerja pengelolaan risiko yang berlandaskan pada Basel II dan Basel III belum sepenuhnya dapat memenuhi kebutuhan dinamika risiko di era digital. Ini menunjukkan adanya gap antara pendekatan normatif dan kondisi nyata

dalam operasional perbankan yang modern, terutama dalam menghadapi risiko siber, kegagalan sistem, serta risiko yang bergantung pada algoritma.

Temuan signifikan lainnya mengindikasikan bahwa isu utama dalam peningkatan risiko operasional bukan hanya terfokus pada penambahan jenis dan kekuatan risiko, tetapi juga pada keterbatasan sistem pengendalian internal yang masih berpola tradisional, administratif, dan hanya mengutamakan kepatuhan. Sistem pengendalian internal tersebut belum sepenuhnya beradaptasi dengan sifat risiko digital yang nyata dan berbasis teknologi.

Dengan demikian, peningkatan risiko operasional dalam perbankan digital pada dasarnya mencerminkan ketidakseimbangan antara kompleksitas teknologi dan kapasitas adaptasi pengendalian internal. Ketika pengendalian internal tidak dapat mengikuti laju perubahan teknologi digital, maka teknologi yang seharusnya meningkatkan efisiensi justru menjadi penyebab ketidakstabilan baru dalam sistem perbankan.

Berdasarkan analisis yang telah dilakukan, perlu adanya penguatan sistem pengendalian internal yang lebih responsif terhadap perubahan dalam perbankan digital melalui penerapan teknologi seperti kecerdasan buatan, analisis data besar, dan sistem pemantauan risiko secara langsung supaya dapat meningkatkan efektivitas dalam mendeteksi dan mengurangi risiko operasional. Selain itu, manajemen risiko operasional perlu diintegrasikan dengan baik bersama infrastruktur perbankan digital agar tidak terjadi jurang antara kemajuan teknologi dan kapabilitas pengendalian internal. Perbankan juga harus memperkuat budaya terkait risiko di semua tingkatan organisasi serta meningkatkan kemampuan SDM dalam menghadapi risiko yang berasal dari teknologi. Di sisi lain, pihak pengawas dan sektor perbankan perlu menilai kembali kerangka manajemen risiko yang ada agar lebih sesuai dengan karakteristik risiko digital yang bersifat dinamis, kompleks, dan sistemik, sehingga pengelolaan risiko tidak hanya bersifat untuk merespons, tetapi juga dapat bersifat prediktif dan strategis dalam menjaga kestabilan perbankan digital.

Daftar Pustaka

- Arfan, A., Saifullah, S., & Fakhruddin, F. (2016). Implementasi prinsip bagi hasil dan manajemen risiko dalam produk-produk pembiayaan perbankan syariah di Kota Malang. *INFERENSI: Jurnal Penelitian Sosial Keagamaan*, 10(1), 213–238. <https://repository.uin-malang.ac.id/622/>
- Cristea, M. (2021). *Operational Risk Management In Banking Activity*. 2021. <https://doi.org/10.5171/2021.969612>
- Danarhuda, A., & Solekah, N. A. (2025). Exploring the role of Islamic value proposition, digital customer experience, and trust on customer satisfaction in Islamic Banking: Evidence from Indonesia's emerging market. *IQTISHODUNA: Jurnal Ekonomi Islam*, 14(2), 413–428. <https://repository.uin-malang.ac.id/24568/>
- Humanities And Social Sciences*. (2022). 30.
- Laksana, R. D., Shaferi, I., & Naznii, H. (2023). *The Effect of Operational Risks for Digital Banking Services at Banks*. 14(2). <https://doi.org/10.18196/mb.v14i2.19302>

- Management, I. B. (2018). *Operational risk management in the digital era in the Swiss banking industry*. (June).
- Mardiana, M. (2018). Pengaruh manajemen risiko terhadap kinerja keuangan keuangan: Studi pada perbankan syariah yang terdaftar di BEI. *Iqtishoduna: Jurnal Ekonomi Dan Bisnis Islam*, 14(2), 151–166. <https://repository.uin-malang.ac.id/7242/>
- Mazayo, K., Agustina, S., Asri, R., Accounting, C., Batu, B., & Regency, B. (2023). *Application of Digital Technology Risk Management Models in Banking Institutions Reflecting The Digital Transformation of Indonesian Banking*. 3(2).
- Mujanah, S., Yanu, A., & Fianto, A. (2025). *Digital Modern Financial Systems In The Perspective of Cyber Risk Management: A Structural Equation Modelling Approach*. 18(3), 365–374.