



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 17549- 17562

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Metode Pengendalian Risiko Operasional sebagai Pertimbangan Investasi pada Bank Digital di Indonesia: Studi Kualitatif pada Blu by BCA Digital

Rani Amalia¹, Diana Novita², Leni Herawati³, Anisa Putri Aulia⁴, Ai Esti⁵, Yusuf Maulana⁶, Palupi Permata Rahmi⁷, Eko Djoko Prabowo⁸

¹²³⁴⁵⁶⁷Program Studi Manajemen, Universitas Indonesia Membangun

⁸PT.Bank Rakyat Indonesia Kantor Wilayah Bandung

¹raniamalia@student.inaba.ac.id, ²diana.novita@student.inaba.ac.id, ³leniherawati@student.inaba.ac.id,

⁴anisaputri@student.inaba.ac.id, ⁵aiesti@student.inaba.ac.id, ⁶yusufmaulana@student.inaba.ac.id,

⁷palupi.permata@inaba.ac.id, ⁸eko.djoko.prabowo@corp.bri.co.id

Abstrak

Transformasi digital pada sektor perbankan telah meningkatkan efisiensi layanan sekaligus memunculkan berbagai risiko operasional yang dapat memengaruhi kinerja perusahaan dan kepercayaan investor. Penelitian ini bertujuan menganalisis metode pengendalian risiko operasional pada layanan blu by BCA Digital serta relevansinya sebagai pertimbangan investasi pada bank digital di Indonesia. Penelitian menggunakan metode kualitatif dengan pendekatan deskriptif dan desain studi kasus. Data dikumpulkan melalui observasi non-partisipan terhadap layanan blu by BCA Digital serta dokumentasi yang bersumber dari laporan tahunan perusahaan, publikasi resmi, regulasi Otoritas Jasa Keuangan (OJK), dan berbagai literatur ilmiah. Analisis data dilakukan menggunakan model Miles, Huberman, dan Saldaña yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan, sedangkan keabsahan data diuji melalui triangulasi sumber. Hasil penelitian menunjukkan bahwa risiko operasional utama yang dihadapi blu by BCA Digital meliputi gangguan sistem, ancaman keamanan siber, phishing dan fraud digital, kebocoran data, serta kesalahan proses operasional. Untuk mengendalikan risiko tersebut, perusahaan menerapkan berbagai mekanisme, antara lain Risk Control Self-Assessment (RCSA), Operational Risk Management Information System (ORMIS), IT Risk Register, Whistleblowing System (WBS), serta standar keamanan informasi berbasis ISO. Meskipun sistem pengendalian risiko telah diterapkan secara komprehensif, perusahaan masih menghadapi tantangan berupa perkembangan ancaman siber, tingginya ketergantungan pada teknologi, dan meningkatnya ekspektasi nasabah terhadap kualitas layanan. Penelitian ini menyimpulkan bahwa efektivitas pengendalian risiko operasional berperan penting dalam menjaga stabilitas operasional, meningkatkan kepercayaan nasabah, serta menjadi salah satu indikator yang dipertimbangkan investor dalam menilai prospek bank digital.

Kata Kunci: Pengendalian Risiko Operasional, Bank Digital, Blu by BCA Digital, Investasi, Manajemen Risiko.

1. Latar Belakang

Sektor perbankan Indonesia mengalami perubahan struktural yang signifikan seiring dengan meningkatnya penetrasi teknologi digital. Perubahan perilaku konsumen yang semakin terbiasa menggunakan perangkat smartphone untuk kebutuhan sehari-hari mendorong pergeseran preferensi keuangan dari model konvensional menuju model berbasis aplikasi. Hal ini diperkuat oleh meningkatnya jumlah pengguna internet dan pertumbuhan ekosistem pembayaran digital di Indonesia. Menurut data Bank Indonesia, nilai transaksi digital banking terus mengalami kenaikan dari tahun ke tahun, mencerminkan tingginya ketergantungan masyarakat terhadap layanan keuangan berbasis teknologi.

Transformasi digital dalam perbankan tidak hanya membuka peluang bisnis yang lebih luas, tetapi juga menghadirkan risiko yang lebih kompleks. Salah satu risiko yang paling signifikan adalah risiko operasional, yaitu risiko yang timbul akibat kegagalan proses internal, kesalahan manusia, gangguan sistem teknologi informasi, atau kejadian eksternal yang merugikan (OJK, 2021). Pada bank digital, risiko ini menjadi lebih kritis karena seluruh operasional bergantung pada infrastruktur teknologi mulai dari autentikasi pengguna hingga pemrosesan transaksi sehingga satu gangguan teknis saja dapat berdampak langsung pada ratusan ribu bahkan jutaan nasabah sekaligus.

Berbeda dengan bank konvensional yang memiliki lapisan layanan tatap muka sebagai cadangan, bank digital sepenuhnya bertumpu pada aplikasi, jaringan internet, dan pengelolaan data secara elektronik. Risiko operasional pada lingkungan ini mencakup ancaman serangan siber, kebocoran data pribadi nasabah, downtime sistem, kegagalan integrasi teknologi pihak ketiga, serta potensi fraud digital yang semakin canggih (Satrya I.Z, 2024). Oleh karena itu, pengendalian risiko operasional pada bank digital perlu dilakukan dengan pendekatan yang lebih komprehensif dan adaptif dibandingkan pengelolaan risiko pada bank tradisional.

Menyadari urgensi tersebut, Otoritas Jasa Keuangan (OJK) telah menerbitkan Cetak Biru Transformasi Digital Perbankan yang menekankan pentingnya lima elemen kunci dalam digitalisasi layanan keuangan, yaitu: data, teknologi, manajemen risiko, kolaborasi, dan tata kelola institusi (OJK, 2021). Regulasi ini secara tegas menempatkan manajemen risiko sebagai salah satu pilar utama dalam transformasi digital, bukan sekadar pelengkap. Selain itu, POJK Nomor 12/POJK.03/2021 tentang Bank Umum juga mengatur kewajiban bank untuk menerapkan prinsip kehati-hatian dalam penggunaan teknologi informasi sebagai bagian dari pengendalian risiko operasional secara menyeluruh (OJK, 2021).

Dalam konteks persaingan industri perbankan digital di Indonesia yang semakin ketat, kepercayaan nasabah menjadi aset yang sangat berharga. Riset (Kirana & Fasa, 2024) menunjukkan bahwa loyalitas nasabah terhadap layanan bank digital dipengaruhi secara langsung oleh kualitas layanan dan persepsi risiko yang mereka rasakan. Artinya, risiko operasional yang tidak dikelola dengan baik dapat menurunkan kepercayaan pengguna, merusak reputasi bank, dan pada akhirnya mengancam keberlanjutan bisnis. Fenomena ini semakin relevan mengingat nasabah bank digital cenderung lebih peka terhadap gangguan layanan dibandingkan nasabah bank konvensional, karena mereka tidak memiliki alternatif kanal layanan fisik.

Dalam perspektif analisis investasi, kemampuan bank digital dalam mengendalikan risiko operasional menjadi salah satu pertimbangan penting bagi investor. Risiko seperti gangguan sistem, serangan siber, kebocoran data, dan fraud digital dapat memengaruhi reputasi perusahaan, kepercayaan nasabah, stabilitas layanan, serta prospek keberlanjutan usaha bank digital.

Salah satu bank digital yang menunjukkan pertumbuhan cukup pesat di Indonesia adalah Blu by BCA Digital, layanan digital banking dari PT Bank Digital BCA. Blu beroperasi sepenuhnya melalui aplikasi mobile tanpa jaringan kantor cabang fisik, menyasar segmen digital-savvy terutama generasi muda dan profesional urban yang mengutamakan kemudahan dan kecepatan transaksi. Sebagai bagian dari ekosistem BCA Group salah satu kelompok perbankan terbesar di Indonesia, Blu memiliki keunggulan dari sisi infrastruktur teknologi dan kepercayaan merek induk. Berdasarkan laporan tahunan PT Bank Digital BCA (2024), Blu terus mengembangkan fitur layanan dan memperluas basis penggunaannya secara signifikan dalam beberapa tahun terakhir.

Pemilihan Blu by BCA Digital sebagai objek penelitian didasarkan pada beberapa pertimbangan. Pertama, Blu merupakan representasi bank digital yang beroperasi tanpa infrastruktur fisik sehingga seluruh risiko operasionalnya berpusat pada sistem teknologi. Kedua, posisi Blu dalam ekosistem BCA Group memberikan karakteristik unik dalam hal tata kelola dan manajemen risiko yang berbeda dari bank digital yang berdiri sendiri. Ketiga, pertumbuhan pengguna yang pesat membuat pengelolaan risiko operasional menjadi isu yang semakin krusial bagi keberlangsungan layanan (Tanic & Atahau, 2021). Penelitian ini menjadi relevan untuk memahami bagaimana praktik pengendalian risiko operasional diterapkan pada model bisnis bank digital semacam ini.

Meskipun literatur tentang digital banking di Indonesia telah berkembang mencakup topik seperti kualitas layanan elektronik, kepuasan pengguna, dan niat penggunaan berkelanjutan penelitian yang secara spesifik mengkaji mekanisme pengendalian risiko operasional pada bank digital masih sangat terbatas (Wijayanti, 2024). Sebagian besar studi yang ada berfokus pada perspektif nasabah atau aspek pemasaran digital, bukan pada dimensi manajerial dan operasional internal bank. Kesenjangan penelitian ini menjadi landasan urgensi studi kualitatif yang mendalam mengenai bagaimana risiko operasional diidentifikasi, dikendalikan, dan dimitigasi dalam praktik nyata operasional Blu by BCA Digital.

Tabel 1 Potensi Risiko Operasional pada Bank Digital

Jenis Risiko Operasional	Contoh pada Bank Digital	Dampak Potensial	Bentuk Pengendalian Risiko
Gangguan Sistem Aplikasi	Server down, bug pada pembaruan aplikasi, respon lambat saat transaksi	Transaksi gagal, nasabah tidak dapat mengakses layanan, potensi kerugian finansial	Pemeliharaan rutin, uji coba pra-rilis, sistem redundansi dan failover
Serangan Siber	Phishing, DDoS, brute-force attack, injeksi malware	Kebocoran data nasabah, gangguan layanan masif, kerugian reputasi	Enkripsi end-to-end, firewall berlapis, pemantauan anomali real-time
Kebocoran Data Nasabah	Akses tidak sah ke basis data, kerentanan API, kebocoran informasi pribadi	Pelanggaran privasi, sanksi regulasi, penurunan kepercayaan nasabah	Penerapan ISO 27001, audit keamanan berkala, kebijakan perlindungan data
Kesalahan Proses Internal	Kesalahan konfigurasi sistem, human error pada operasi back-end, keliru alur kerja	Transaksi tidak terbukukan, dana salah arah, laporan tidak akurat	SOP yang ketat, pelatihan SDM, kontrol empat mata (dual control)
Fraud Digital	Pembobolan akun nasabah, transaksi tidak sah, penipuan identitas	Kerugian finansial nasabah, tuntutan hukum, kerusakan brand	Autentikasi dua faktor (2FA), deteksi anomali berbasis AI, notifikasi real-time
Kegagalan Integrasi Pihak Ketiga	Gangguan pada API payment gateway, mitra fintech, atau layanan cloud	Layanan pembayaran terganggu, proses transfer tertunda, pengalaman pengguna buruk	Seleksi vendor ketat, SLA yang jelas, uji beban integrasi secara berkala

Sumber: Diolah dari berbagai sumber (OJK, 2021; Sartya I.Z., 2024)

Tabel 1 di atas merangkum enam kategori risiko operasional yang relevan dengan lingkungan bank digital. Keenam kategori tersebut menggambarkan bahwa risiko operasional pada layanan berbasis teknologi mencakup dimensi yang sangat luas dari ancaman eksternal seperti serangan siber hingga kerentanan internal seperti kegagalan proses dan kesalahan konfigurasi. Setiap jenis risiko memiliki dampak yang tidak hanya bersifat finansial, tetapi juga memengaruhi kepercayaan nasabah dan kelangsungan operasional secara keseluruhan.

Dalam konteks Blu by BCA Digital, seluruh enam jenis risiko dalam tabel tersebut berpotensi terjadi mengingat operasional Blu yang sepenuhnya digital dan bergantung pada ekosistem teknologi yang kompleks. Penelitian ini akan mengkaji lebih lanjut bagaimana manajemen Blu mengenali, merespons, dan mengendalikan risiko-risiko tersebut dalam praktik nyata, sehingga temuan penelitian dapat memberikan gambaran komprehensif tentang tata kelola risiko operasional pada bank digital di Indonesia. Dengan demikian, pengendalian risiko operasional tidak hanya penting untuk menjaga kualitas layanan dan keamanan nasabah, tetapi juga dapat menjadi dasar pertimbangan dalam menilai prospek investasi pada bank digital.

2. Metode Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif dan desain studi kasus untuk menganalisis pengendalian risiko operasional pada layanan blu by BCA Digital serta relevansinya terhadap pertimbangan investasi. Objek penelitian berfokus pada penerapan pengendalian risiko operasional, meliputi

DOI: <https://doi.org/10.31004/riggs.v5i2.11852>

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

identifikasi, pengelolaan, dan mitigasi risiko seperti gangguan sistem, keamanan siber, kebocoran data, kegagalan transaksi, dan kesalahan operasional. Data penelitian terdiri atas data primer yang diperoleh melalui observasi non-partisipan terhadap layanan blu by BCA Digital serta data sekunder yang berasal dari buku, jurnal ilmiah, laporan tahunan perusahaan, publikasi resmi PT Bank Digital BCA Tbk, dan regulasi OJK. Teknik pengumpulan data dilakukan melalui observasi dan dokumentasi. Analisis data menggunakan model Miles, Huberman, dan Saldaña (2014) yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan. Keabsahan data dijaga melalui triangulasi sumber dengan membandingkan hasil observasi dengan berbagai dokumen dan literatur yang relevan.

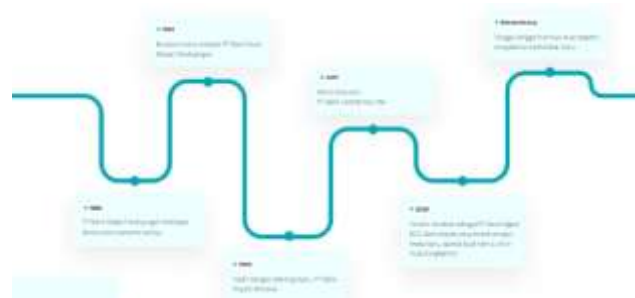
3. Hasil dan Diskusi

Sejarah Berdirinya PT Bank Digital BCA Tbk

PT Bank Digital BCA Tbk merupakan hasil transformasi dari bank konvensional menjadi bank digital yang berada dalam ekosistem Grup BCA. Cikal bakal perusahaan ini bermula pada tahun 1965 di Bandung dengan nama PT Bank Rakjat Parahyangan. Pada masa awal operasionalnya, bank tersebut melayani kebutuhan perbankan masyarakat setempat dalam skala yang masih terbatas.

Seiring perkembangan industri perbankan, perusahaan mengalami beberapa perubahan, baik dari sisi nama maupun model bisnis, hingga kemudian dikenal sebagai Bank Royal Indonesia. Perubahan paling signifikan terjadi pada tahun 2019 ketika PT Bank Central Asia Tbk mengakuisisi Bank Royal sebagai bagian dari langkah ekspansi ke sektor perbankan digital.

Setelah akuisisi tersebut, perusahaan menjalani proses transformasi bisnis secara bertahap dan pada tahun 2020 resmi berganti nama menjadi PT Bank Digital BCA Tbk. Transformasi ini menandai perubahan arah perusahaan dari bank konvensional menuju bank yang mengandalkan layanan berbasis teknologi digital.

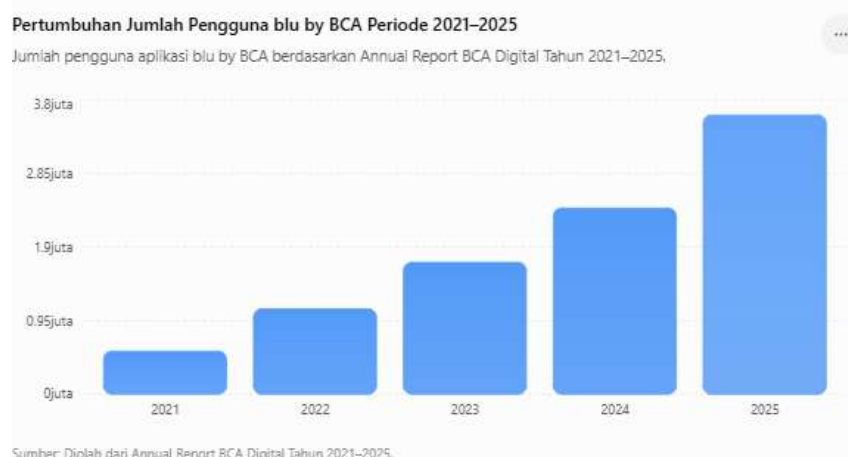


Gambar 4.1 Timeline Transformasi PT Bank Digital BCA Tbk

Sumber: Website resmi PT Bank Digital BCA, diakses 2026

Peluncuran dan Perkembangan blu by BCA Digital

Produk unggulan yang dimiliki oleh BCA Digital adalah blu by BCA Digital, yaitu aplikasi layanan perbankan digital yang mulai diperkenalkan kepada masyarakat pada Juli 2021. Aplikasi ini dirancang untuk memberikan kemudahan bagi nasabah dalam mengakses berbagai layanan perbankan secara daring, mulai dari pembukaan rekening, transfer dana, pembayaran, hingga pengelolaan tabungan. Dengan konsep layanan yang sepenuhnya berbasis digital, nasabah dapat melakukan hampir seluruh aktivitas perbankan tanpa harus mendatangi kantor cabang. Peluncuran blu merupakan bagian dari upaya BCA Digital dalam mendukung transformasi digital di sektor perbankan sekaligus menjawab perubahan perilaku masyarakat yang semakin mengutamakan layanan keuangan yang praktis, cepat, dan fleksibel.



Gambar 4 1.2 Pertumbuhan Jumlah Pengguna blu by BCA Periode 2021-2025
Sumber : Diolah dari Annual Report BCA Digital Tahun 2021-2025

Sejak resmi diluncurkan, blu by BCA Digital menunjukkan perkembangan yang cukup pesat. Berdasarkan Gambar 4.1, jumlah pengguna terus mengalami peningkatan dari tahun ke tahun. Pada akhir tahun 2021, jumlah pengguna tercatat sekitar 552 ribu. Selanjutnya, angka tersebut meningkat menjadi sekitar 1,1 juta pada tahun 2022, kemudian bertambah menjadi 1,7 juta pada tahun 2023. Tren pertumbuhan tersebut berlanjut hingga mencapai sekitar 2,4 juta pengguna pada tahun 2024 dan meningkat lagi menjadi sekitar 3,6 juta pada tahun 2025. Perkembangan tersebut mencerminkan semakin tingginya tingkat penerimaan masyarakat terhadap layanan perbankan digital serta menunjukkan bahwa blu berhasil memperluas jangkauan layanannya melalui pemanfaatan inovasi teknologi.

Di balik pertumbuhan tersebut, terdapat konsekuensi berupa meningkatnya kompleksitas operasional yang harus dihadapi perusahaan. Bertambahnya jumlah pengguna menyebabkan intensitas transaksi digital, volume pengelolaan data nasabah, serta kebutuhan akan ketersediaan dan keandalan sistem teknologi informasi ikut meningkat. Situasi ini dapat memperbesar peluang munculnya berbagai risiko operasional, seperti gangguan pada sistem (*system downtime*), kegagalan dalam pemrosesan transaksi, ancaman serangan siber, kebocoran informasi nasabah, maupun kesalahan operasional yang berasal dari faktor manusia (*human error*). Oleh sebab itu, pertumbuhan jumlah pengguna tidak hanya menjadi indikator keberhasilan perusahaan dalam mengembangkan bisnis digitalnya, tetapi juga menjadi tantangan dalam menjaga efektivitas proses operasional.

Sejalan dengan perkembangan tersebut, penerapan pengendalian risiko operasional menjadi aspek yang tidak dapat diabaikan oleh BCA Digital. Sistem pengendalian risiko yang efektif diperlukan untuk memastikan keberlangsungan operasional perusahaan, menjaga keamanan data dan transaksi nasabah, serta mempertahankan kualitas layanan yang diberikan. Dari perspektif investasi, kemampuan perusahaan dalam mengelola risiko operasional menjadi salah satu faktor yang dapat memengaruhi tingkat kepercayaan investor terhadap prospek perusahaan. Dengan demikian, pertumbuhan jumlah pengguna blu by BCA Digital tidak hanya mencerminkan keberhasilan ekspansi bisnis, tetapi juga menjadi dasar yang relevan untuk menilai efektivitas metode pengendalian risiko operasional sebagai salah satu pertimbangan dalam pengambilan keputusan investasi pada industri perbankan digital di Indonesia.

Strategi dan Komitmen Bisnis BCA Digital

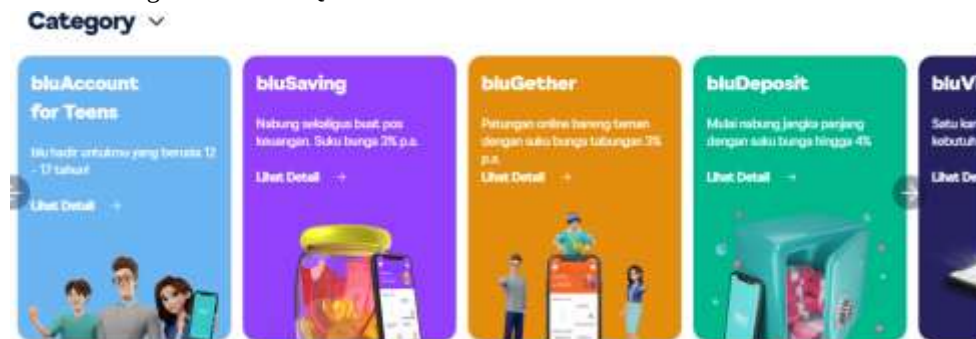
Dalam menjalankan bisnisnya, BCA Digital berupaya menghadirkan layanan keuangan yang selaras dengan perubahan kebutuhan masyarakat digital. Perusahaan tidak hanya berfokus pada pertumbuhan bisnis, tetapi juga pada penguatan pengalaman pengguna melalui inovasi layanan yang relevan, mudah digunakan, dan aman. Komitmen tersebut juga terlihat dari berbagai program edukasi keuangan yang dilakukan untuk meningkatkan literasi finansial masyarakat. Melalui pendekatan ini, BCA Digital berusaha membangun hubungan jangka panjang dengan nasabah sekaligus memperkuat kepercayaan terhadap layanan digital yang ditawarkan.

Model Bisnis Bank Digital

BCA Digital menerapkan model bisnis branchless banking, yaitu model operasional perbankan yang mengandalkan platform digital sebagai sarana utama pelayanan. Dengan model ini, sebagian besar layanan perbankan dapat diakses melalui aplikasi tanpa ketergantungan pada jaringan kantor cabang fisik. Fokus utama perusahaan berada pada segmen nasabah retail, khususnya masyarakat yang telah terbiasa menggunakan teknologi digital dalam aktivitas sehari-hari. Selain itu, dukungan ekosistem Grup BCA juga menjadi salah satu keunggulan kompetitif yang memperkuat operasional perusahaan. Ketergantungan yang tinggi terhadap sistem digital menyebabkan stabilitas teknologi menjadi aspek yang sangat penting. Oleh karena itu, potensi risiko operasional seperti gangguan sistem, ancaman keamanan siber, dan fraud digital menjadi tantangan yang perlu dikelola secara optimal.

Fitur Utama Aplikasi blu by BCA Digital

Aplikasi blu menyediakan berbagai fitur yang mendukung kebutuhan transaksi dan pengelolaan keuangan pengguna secara digital. Beberapa fitur utama yang tersedia meliputi bluSaving sebagai tabungan digital, bluGether untuk pengelolaan dana bersama, bluDeposit untuk deposito digital, serta layanan transfer dan pembayaran berbasis digital termasuk QRIS.



Gambar 4.1.2 Fitur-fitur pelayanan blu by BCA Digital
Sumber : Website Resmi blu by BCA Digital, 2026

Selain fitur transaksi utama, blu juga menyediakan layanan pendukung lain yang membantu pengguna mengatur keuangan secara lebih fleksibel. Kehadiran berbagai fitur tersebut menunjukkan bahwa blu tidak hanya berfungsi sebagai sarana transaksi, tetapi juga sebagai platform pengelolaan finansial yang terintegrasi.

Analisis Risiko Operasional pada Layanan blu by BCA Digital

Risiko operasional merupakan salah satu risiko utama yang dihadapi oleh bank digital karena seluruh aktivitas layanan sangat bergantung pada sistem teknologi informasi. Berbeda dengan bank konvensional yang masih memiliki layanan fisik melalui kantor cabang, operasional bank digital hampir sepenuhnya dilakukan melalui aplikasi dan jaringan digital. Kondisi ini menyebabkan gangguan kecil pada sistem maupun proses operasional dapat langsung memengaruhi kualitas layanan dan pengalaman nasabah.

Pada layanan blu by BCA Digital, risiko operasional dapat muncul dari berbagai faktor, baik internal maupun eksternal. Faktor internal meliputi kesalahan proses operasional, kegagalan sistem, serta human error, sedangkan faktor eksternal mencakup ancaman keamanan siber, penipuan digital, hingga perubahan pola perilaku pengguna dalam memanfaatkan layanan perbankan digital. Berdasarkan hasil analisis data dari laporan tahunan perusahaan, observasi terhadap aplikasi, serta berbagai sumber pendukung lainnya, terdapat beberapa bentuk risiko operasional utama yang berpotensi memengaruhi keberlangsungan layanan blu by BCA Digital.

Risiko Gangguan Sistem dan Downtime

Gangguan sistem atau *system downtime* merupakan salah satu bentuk risiko operasional yang paling nyata dalam operasional bank digital. Risiko ini muncul ketika aplikasi atau infrastruktur sistem mengalami gangguan sehingga layanan tidak dapat diakses secara normal oleh nasabah. Dampak dari gangguan tersebut dapat berupa kegagalan login, keterlambatan transaksi, kesalahan proses pembayaran, hingga terhentinya aktivitas layanan

secara sementara. Salah satu contoh nyata terjadi pada 29 September 2025 ketika layanan digital BCA Group, termasuk blu by BCA Digital, mengalami gangguan secara serentak. Gangguan tersebut menyebabkan sejumlah nasabah kesulitan mengakses aplikasi, melakukan transfer, mengecek saldo, hingga melakukan transaksi pembayaran. Insiden ini menunjukkan bahwa stabilitas sistem merupakan faktor yang sangat krusial dalam menjaga keandalan layanan bank digital.

Hasil observasi melalui ulasan pengguna pada App Store juga menunjukkan adanya keluhan terkait performa aplikasi blu. Beberapa pengguna mengeluhkan masalah koneksi, kesulitan login, hingga transaksi QRIS yang mengalami *lag* atau gagal diproses. Temuan ini mengindikasikan bahwa risiko downtime tidak hanya muncul dalam insiden besar, tetapi juga dapat terjadi dalam aktivitas operasional sehari-hari akibat bug aplikasi, pembaruan sistem, atau ketidakstabilan jaringan. Bagi bank digital, gangguan sistem dapat menurunkan tingkat kepercayaan nasabah karena akses layanan yang cepat dan stabil merupakan ekspektasi utama pengguna. Oleh sebab itu, pengelolaan infrastruktur teknologi yang andal menjadi kebutuhan penting untuk meminimalkan risiko ini.

Risiko Phishing, Scam, dan Fraud Digital

Selain gangguan sistem, risiko operasional lain yang cukup signifikan adalah risiko penipuan digital atau *fraud*. Risiko ini umumnya berasal dari pihak eksternal yang memanfaatkan celah keamanan maupun kelalaian pengguna untuk memperoleh akses terhadap data atau dana nasabah. Salah satu modus yang sering terjadi adalah *phishing*, yaitu upaya pencurian informasi sensitif seperti OTP, PIN, dan password melalui tautan atau media komunikasi palsu. Pada Maret 2025, blu by BCA Digital mengeluarkan peringatan resmi kepada nasabah terkait maraknya penipuan melalui SMS yang mengatasnamakan BCA Digital. Modus yang digunakan antara lain pemberian hadiah palsu, notifikasi transaksi fiktif, serta informasi perubahan biaya administrasi yang disertai tautan mencurigakan.

Ancaman phishing menunjukkan bahwa risiko operasional pada bank digital tidak selalu berasal dari kegagalan internal perusahaan, tetapi juga dapat muncul akibat serangan eksternal yang menargetkan nasabah. Dalam konteks ini, rendahnya literasi keamanan digital pengguna dapat memperbesar potensi kerugian yang ditimbulkan. Risiko fraud menjadi tantangan serius karena selain menyebabkan kerugian finansial, insiden semacam ini juga dapat merusak reputasi perusahaan dan menurunkan kepercayaan publik terhadap layanan bank digital.

Risiko Keamanan Siber dan Kebocoran Data

Ketergantungan tinggi terhadap teknologi menjadikan bank digital sangat rentan terhadap ancaman keamanan siber. Risiko ini mencakup serangan *malware*, *ransomware*, peretasan sistem, hingga kebocoran data pribadi nasabah. Bagi bank digital seperti blu by BCA Digital, perlindungan data nasabah merupakan aspek yang sangat penting karena hampir seluruh aktivitas layanan melibatkan pertukaran informasi sensitif secara digital. Kebocoran data tidak hanya berpotensi menyebabkan kerugian bagi nasabah, tetapi juga dapat menimbulkan konsekuensi hukum dan reputasi bagi perusahaan.

Pentingnya pengelolaan keamanan data juga diperkuat oleh pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menuntut perusahaan untuk memastikan keamanan, kerahasiaan, serta integritas data pengguna. Dalam konteks ini, ancaman keamanan siber menjadi salah satu risiko operasional yang harus diprioritaskan dalam sistem manajemen risiko bank digital. Semakin berkembangnya teknologi digital juga diikuti oleh semakin kompleksnya metode serangan siber. Oleh karena itu, perusahaan dituntut untuk terus memperbarui sistem keamanan agar tetap adaptif terhadap ancaman yang terus berkembang.

Risiko Human Error dan Kegagalan Proses Internal

Risiko operasional juga dapat muncul akibat kesalahan manusia (*human error*) maupun kegagalan proses internal. Risiko ini mencakup kesalahan input data, miskomunikasi antartim, kesalahan konfigurasi sistem, hingga ketidaktepatan prosedur operasional saat melakukan pembaruan aplikasi. Pada layanan bank digital, kesalahan kecil dalam pengelolaan sistem dapat berdampak besar terhadap kualitas layanan. Misalnya, kesalahan saat pembaruan sistem dapat memicu bug aplikasi, error transaksi, atau gangguan fitur tertentu yang memengaruhi pengalaman pengguna.

Human error sering kali sulit dihindari sepenuhnya karena berkaitan dengan faktor sumber daya manusia dan kompleksitas operasional teknologi. Oleh sebab itu, perusahaan perlu menerapkan standar operasional yang jelas, pengawasan yang ketat, serta evaluasi berkala untuk meminimalkan potensi kesalahan internal. Berdasarkan analisis tersebut, dapat disimpulkan bahwa risiko operasional pada blu by BCA Digital terdiri atas empat risiko

utama, yaitu gangguan sistem, fraud digital, ancaman keamanan siber, serta human error. Keempat risiko tersebut saling berkaitan dan dapat memengaruhi stabilitas operasional maupun tingkat kepercayaan nasabah terhadap layanan bank digital. Temuan ini menunjukkan bahwa pengelolaan risiko operasional yang efektif menjadi aspek penting dalam menjaga keberlangsungan bisnis dan daya saing bank digital di tengah perkembangan teknologi yang semakin pesat.

Mekanisme Pengendalian Risiko Operasional pada blu by BCA Digital

Sebagai bank yang beroperasi secara digital, blu by BCA Digital memiliki tingkat ketergantungan yang sangat tinggi terhadap sistem teknologi informasi. Kondisi tersebut membuat pengendalian risiko operasional menjadi aspek yang sangat penting untuk menjaga stabilitas layanan dan kepercayaan nasabah. Risiko operasional pada bank digital dapat muncul akibat proses internal yang kurang optimal, kesalahan manusia (*human error*), gangguan sistem, maupun faktor eksternal seperti serangan siber dan tindakan penipuan digital. Oleh karena itu, BCA Digital menerapkan berbagai mekanisme pengendalian risiko agar operasional layanan tetap berjalan dengan aman dan efektif.

Identifikasi dan Pemetaan Risiko Operasional

Langkah awal dalam pengendalian risiko operasional dilakukan melalui proses identifikasi dan pemetaan risiko. Tahapan ini bertujuan untuk mengenali berbagai potensi risiko yang dapat menghambat aktivitas operasional perusahaan, sekaligus menilai seberapa besar dampak yang mungkin ditimbulkan. Dalam praktiknya, BCA Digital menggunakan metode *Risk Control Self-Assessment* (RCSA). Metode ini memungkinkan setiap unit kerja melakukan penilaian secara mandiri terhadap risiko yang berpotensi muncul dari aktivitas operasional sehari-hari. Melalui pendekatan tersebut, potensi risiko dapat dideteksi lebih awal sehingga tindakan pencegahan dapat segera dilakukan.

Selain itu, pada divisi teknologi informasi, perusahaan juga menerapkan *IT Risk Register* sebagai alat untuk memetakan risiko yang berkaitan dengan sistem digital. Pemetaan ini mencakup risiko seperti gangguan server, kesalahan sistem aplikasi, hingga kerentanan keamanan yang dapat memengaruhi layanan kepada nasabah. Untuk mendukung proses pengawasan yang lebih terintegrasi, BCA Digital juga menggunakan *Operational Risk Management Information System* (ORMIS). Sistem ini membantu perusahaan dalam mencatat, memantau, serta mengevaluasi risiko operasional secara berkelanjutan sehingga pengelolaan risiko dapat dilakukan secara lebih terstruktur.

Pengendalian Risiko melalui Sistem dan Keamanan Teknologi

Karena seluruh layanan blu dijalankan melalui aplikasi digital, pengendalian risiko operasional sangat bergantung pada keamanan dan keandalan sistem teknologi yang digunakan. Oleh sebab itu, BCA Digital melakukan berbagai upaya untuk memperkuat infrastruktur teknologi agar mampu meminimalkan gangguan operasional. Salah satu bentuk pengendalian yang dilakukan adalah pemeliharaan sistem secara berkala dan pembaruan teknologi untuk menjaga stabilitas layanan. Langkah ini penting untuk mengurangi kemungkinan terjadinya *error*, *downtime*, maupun gangguan teknis lainnya yang dapat menghambat aktivitas transaksi nasabah.

Dalam aspek keamanan informasi, BCA Digital juga telah menerapkan standar keamanan yang mengacu pada sertifikasi ISO 27001:2013 mengenai Sistem Manajemen Keamanan Informasi. Penerapan standar tersebut menunjukkan komitmen perusahaan dalam melindungi data nasabah dan menjaga kerahasiaan informasi yang tersimpan dalam sistem. Pengendalian risiko teknologi juga mencakup antisipasi terhadap ancaman keamanan siber. Ancaman seperti *phishing*, malware, peretasan akun, dan pencurian data menjadi risiko yang terus berkembang seiring meningkatnya penggunaan layanan digital. Oleh karena itu, penguatan sistem keamanan menjadi bagian penting dalam menjaga keberlangsungan operasional bank digital.

Pengendalian Risiko melalui Tata Kelola Internal

Selain penguatan dari sisi teknologi, pengendalian risiko operasional juga dilakukan melalui tata kelola internal perusahaan. Tata kelola ini bertujuan memastikan bahwa seluruh aktivitas operasional berjalan sesuai dengan kebijakan, prosedur, dan prinsip manajemen risiko yang telah ditetapkan. BCA Digital menerapkan sistem pengawasan internal melalui Satuan Kerja Audit Intern (SKAI). Unit ini berperan dalam mengevaluasi efektivitas pengendalian internal dan menilai apakah proses operasional telah berjalan sesuai standar perusahaan. Melalui audit internal, kelemahan dalam proses kerja dapat diidentifikasi sehingga perusahaan dapat segera melakukan perbaikan.

Perusahaan juga menerapkan mekanisme pencegahan kecurangan melalui *Whistleblowing System* (WBS). Sistem ini memberikan sarana bagi pihak internal untuk melaporkan dugaan penyimpangan, pelanggaran etika, maupun tindakan fraud yang dapat menimbulkan risiko operasional. Selain itu, koordinasi antardivisi juga

dilakukan secara berkala untuk mengevaluasi efektivitas kontrol yang telah diterapkan. Upaya ini penting untuk membangun budaya sadar risiko di lingkungan perusahaan, sehingga setiap unit memiliki pemahaman yang sama mengenai pentingnya pengendalian risiko.

Evaluasi Efektivitas Pengendalian Risiko Operasional

Berdasarkan hasil analisis, mekanisme pengendalian risiko operasional yang diterapkan oleh BCA Digital dapat dikatakan cukup komprehensif. Pengendalian tidak hanya dilakukan melalui identifikasi risiko, tetapi juga diperkuat dengan penggunaan sistem digital, pengawasan internal, serta peningkatan kesadaran terhadap risiko keamanan. Meskipun demikian, masih terdapat beberapa tantangan dalam implementasinya. Gangguan layanan yang sesekali terjadi, termasuk keluhan pengguna terkait kendala aplikasi, menunjukkan bahwa pengendalian risiko operasional tetap memerlukan evaluasi dan pengembangan secara berkelanjutan.

Secara keseluruhan, mekanisme pengendalian risiko operasional pada blu by BCA Digital menunjukkan bahwa perusahaan telah memiliki sistem pengelolaan risiko yang memadai. Namun, di tengah perkembangan teknologi yang sangat cepat dan meningkatnya ancaman digital, perusahaan tetap perlu melakukan penyempurnaan agar kualitas layanan, keamanan transaksi, dan kepercayaan nasabah dapat terus terjaga.

Tantangan dalam Pengendalian Risiko Operasional pada blu by BCA Digital

Walaupun blu by BCA Digital telah menerapkan berbagai mekanisme pengendalian risiko operasional, pelaksanaannya di lapangan tetap menghadapi sejumlah tantangan. Hal ini tidak terlepas dari karakteristik bank digital yang hampir seluruh aktivitas operasionalnya bergantung pada teknologi dan sistem digital. Semakin berkembangnya teknologi juga membuat risiko yang dihadapi semakin beragam dan terus berubah. Oleh karena itu, pengendalian risiko operasional pada bank digital tidak bisa dilakukan secara statis, melainkan harus terus menyesuaikan diri dengan perkembangan kondisi yang ada.

Ancaman Keamanan Siber yang Terus Berkembang

Salah satu tantangan terbesar yang dihadapi bank digital adalah ancaman keamanan siber. Seiring meningkatnya penggunaan layanan perbankan digital, berbagai bentuk kejahatan siber juga ikut berkembang dengan metode yang semakin beragam. Ancaman yang sering muncul antara lain *phishing*, *social engineering*, pencurian data pribadi, hingga penyalahgunaan akun nasabah.

Dalam praktiknya, BCA Digital juga menghadapi tantangan serupa. Perusahaan beberapa kali memberikan edukasi kepada nasabah mengenai pentingnya menjaga keamanan data pribadi melalui kampanye #JagaDataJagaHarta. Selain itu, blu by BCA Digital juga pernah mengeluarkan peringatan terkait modus penipuan melalui SMS yang mengatasnamakan pihak bank. Modus semacam ini biasanya bertujuan memancing nasabah agar memberikan data penting seperti PIN, OTP, atau password.

Tantangan utama dalam aspek ini bukan hanya terletak pada sistem keamanan perusahaan, tetapi juga pada tingkat kewaspadaan pengguna. Meskipun sistem keamanan terus diperkuat, risiko tetap dapat muncul apabila nasabah kurang memahami cara melindungi data pribadinya.

Ketergantungan Tinggi terhadap Sistem Teknologi

Sebagai bank digital, blu menjalankan hampir seluruh layanannya melalui aplikasi dan jaringan internet. Kondisi ini membuat operasional perusahaan sangat bergantung pada kestabilan sistem teknologi yang digunakan. Ketergantungan yang tinggi terhadap teknologi menjadi tantangan tersendiri karena gangguan kecil sekalipun dapat langsung berdampak pada layanan. Contohnya terlihat pada gangguan sistem yang terjadi pada 29 September 2025, ketika layanan digital BCA Group, termasuk blu by BCA Digital, sempat mengalami kendala. Akibat gangguan tersebut, sejumlah nasabah kesulitan mengakses aplikasi, login, maupun melakukan transaksi.

Selain gangguan besar seperti itu, tantangan ini juga terlihat dari ulasan beberapa pengguna aplikasi blu yang masih mengeluhkan *lag*, error saat transaksi, atau kendala koneksi. Hal ini menunjukkan bahwa menjaga performa sistem agar tetap stabil bukan perkara mudah, terutama ketika jumlah pengguna terus bertambah dan volume transaksi semakin tinggi.

Perubahan Kebutuhan dan Ekspektasi Nasabah

Tantangan berikutnya berasal dari perubahan kebutuhan nasabah yang terus berkembang. Pengguna bank digital saat ini cenderung memiliki ekspektasi yang tinggi terhadap kualitas layanan. Mereka menginginkan aplikasi yang cepat, mudah digunakan, minim gangguan, dan mampu memenuhi berbagai kebutuhan transaksi

dalam satu platform. Kondisi tersebut mendorong bank digital untuk terus berinovasi dan menghadirkan fitur-fitur baru. Namun, di sisi lain, penambahan fitur juga dapat meningkatkan kompleksitas sistem operasional. Semakin kompleks suatu sistem, semakin besar pula potensi munculnya risiko operasional apabila pengelolaannya tidak dilakukan dengan baik. Pada blu by BCA Digital, tantangan ini terlihat dari kebutuhan perusahaan untuk terus menyesuaikan layanan dengan gaya hidup digital masyarakat, tanpa mengorbankan keamanan dan stabilitas sistem.

Tuntutan Kepatuhan terhadap Regulasi

Selain faktor teknologi dan pengguna, pengendalian risiko operasional juga dipengaruhi oleh regulasi yang berlaku di industri perbankan. Sebagai lembaga jasa keuangan, bank digital harus mematuhi berbagai ketentuan yang ditetapkan oleh regulator seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia. Tantangannya adalah regulasi di sektor digital terus berkembang mengikuti perubahan teknologi. Artinya, perusahaan harus mampu beradaptasi dengan cepat terhadap kebijakan baru, terutama yang berkaitan dengan perlindungan data, keamanan sistem, dan perlindungan konsumen. Bagi BCA Digital, kepatuhan terhadap regulasi menjadi hal yang sangat penting. Ketidaksiapan terhadap aturan tidak hanya berpotensi menimbulkan risiko operasional, tetapi juga dapat memengaruhi reputasi perusahaan di mata publik.

Menjaga Keseimbangan antara Inovasi dan Pengendalian Risiko

Tantangan lain yang tidak kalah penting adalah menjaga keseimbangan antara inovasi dan pengendalian risiko. Dalam persaingan bank digital yang semakin ketat, perusahaan dituntut untuk terus berkembang dan menghadirkan layanan yang relevan bagi nasabah. Namun, inovasi yang terlalu cepat tanpa pengelolaan risiko yang matang justru dapat membuka peluang munculnya gangguan operasional. Sebaliknya, apabila perusahaan terlalu berhati-hati dalam berinovasi, daya saing bisnis bisa menurun.

Berdasarkan hasil analisis, blu by BCA Digital menghadapi tantangan untuk menyeimbangkan dua hal tersebut. Perusahaan perlu memastikan bahwa setiap inovasi yang dilakukan tidak hanya meningkatkan kenyamanan nasabah, tetapi juga tetap berada dalam batas pengendalian risiko yang memadai. Secara keseluruhan, tantangan pengendalian risiko operasional pada blu by BCA Digital menunjukkan bahwa pengelolaan risiko dalam bank digital merupakan proses yang dinamis. Risiko tidak hanya berasal dari dalam perusahaan, tetapi juga dari perkembangan teknologi, perubahan perilaku pengguna, dan lingkungan bisnis yang terus berubah. Oleh karena itu, pengendalian risiko perlu terus diperbarui agar tetap relevan dengan tantangan yang dihadapi.

Strategi Mitigasi Risiko Operasional untuk Menjaga Kepercayaan Nasabah dan Keberlanjutan Layanan

Berdasarkan hasil analisis mengenai risiko operasional, mekanisme pengendalian, serta berbagai tantangan yang dihadapi, diperlukan strategi mitigasi yang berkelanjutan untuk meminimalkan potensi gangguan operasional pada layanan blu by BCA Digital. Strategi mitigasi menjadi aspek yang penting dalam operasional bank digital karena keberlangsungan layanan sangat bergantung pada kestabilan sistem, keamanan data, serta tingkat kepercayaan nasabah. Dalam konteks perbankan digital, gangguan operasional yang terjadi secara berulang dapat menurunkan reputasi perusahaan dan memengaruhi loyalitas pengguna. Upaya mitigasi risiko operasional pada blu by BCA Digital tidak hanya berfokus pada penguatan teknologi, tetapi juga mencakup peningkatan keamanan siber, edukasi nasabah, serta pengembangan inovasi layanan yang tetap memperhatikan prinsip manajemen risiko.

Penguatan Infrastruktur Teknologi dan Stabilitas Sistem

Salah satu strategi mitigasi yang perlu terus diperkuat adalah peningkatan infrastruktur teknologi untuk menjaga stabilitas operasional layanan digital. Sebagai bank digital, hampir seluruh aktivitas transaksi blu dilakukan melalui aplikasi dan jaringan internet, sehingga kualitas sistem teknologi menjadi faktor utama dalam menjaga kelancaran layanan. Pentingnya penguatan infrastruktur ini terlihat dari insiden gangguan layanan yang terjadi pada tahun 2025, ketika layanan digital BCA Group, termasuk blu by BCA Digital, mengalami kendala akses. Gangguan tersebut menyebabkan sebagian nasabah tidak dapat login, melakukan transfer, maupun mengakses fitur transaksi lainnya. Kondisi ini menunjukkan bahwa meskipun sistem pengendalian telah diterapkan, potensi gangguan operasional tetap dapat terjadi akibat kompleksitas sistem digital yang digunakan (CNBC Indonesia, 2025).

Sebagai langkah mitigasi, perusahaan perlu terus meningkatkan kapasitas server, memperkuat sistem *backup*, serta mengoptimalkan *disaster recovery plan* agar proses pemulihan layanan dapat berlangsung lebih cepat ketika terjadi gangguan. Selain itu, pemantauan sistem secara *real-time* juga penting untuk mendeteksi

potensi masalah sejak dini sehingga risiko downtime dapat diminimalkan (PT Bank Digital BCA Tbk, 2025).

Peningkatan Keamanan Siber dan Pencegahan Fraud Digital

Strategi mitigasi berikutnya adalah penguatan keamanan siber dan pencegahan fraud digital. Risiko keamanan siber merupakan salah satu ancaman terbesar bagi bank digital karena meningkatnya aktivitas kejahatan digital seperti *phishing*, penipuan berbasis SMS, pencurian data, serta *social engineering*. Pada Maret 2025, blu by BCA Digital mengeluarkan peringatan resmi terkait modus penipuan SMS yang mengatasnamakan pihak bank. Pelaku umumnya menggunakan pesan palsu yang menawarkan hadiah, notifikasi transaksi, atau informasi perubahan biaya administrasi untuk memancing nasabah memberikan data rahasia seperti OTP, PIN, dan password (BCA Digital, 2025). Hal ini menunjukkan bahwa ancaman risiko tidak hanya berasal dari kelemahan sistem internal, tetapi juga dari pihak eksternal yang memanfaatkan kurangnya kewaspadaan pengguna. Untuk memitigasi risiko tersebut, perusahaan perlu terus memperkuat autentikasi berlapis, sistem deteksi aktivitas mencurigakan (*fraud detection*), serta pemantauan transaksi secara otomatis. Pembaruan sistem keamanan secara berkala juga penting agar perusahaan mampu beradaptasi terhadap pola ancaman siber yang terus berkembang.

Peningkatan Literasi dan Kesadaran Nasabah

Pengendalian risiko operasional pada bank digital tidak dapat sepenuhnya bergantung pada sistem teknologi. Faktor manusia, khususnya tingkat pemahaman nasabah terhadap keamanan digital, juga memiliki peran yang sangat penting dalam menentukan efektivitas mitigasi risiko. BCA Digital telah menjalankan berbagai program edukasi kepada nasabah, termasuk kampanye #JagaDataJagaHarta, yang bertujuan meningkatkan kesadaran mengenai pentingnya menjaga kerahasiaan data pribadi dan keamanan transaksi digital. Selain itu, perusahaan juga aktif dalam kegiatan literasi keuangan melalui berbagai program edukasi dan publikasi yang ditujukan kepada masyarakat.

Peningkatan literasi digital diperlukan agar nasabah mampu mengenali berbagai modus penipuan, memahami pentingnya menjaga kredensial akun, serta lebih berhati-hati saat menerima informasi dari sumber yang tidak resmi. Dengan meningkatnya kesadaran pengguna, potensi fraud akibat kesalahan pengguna (*human error*) dapat ditekan secara lebih efektif.

Pengembangan Inovasi Layanan yang Seimbang dengan Manajemen Risiko

Sebagai bank digital yang beroperasi dalam industri yang kompetitif, blu by BCA Digital dituntut untuk terus menghadirkan inovasi layanan yang sesuai dengan kebutuhan nasabah. Pengembangan layanan seperti pembaruan aplikasi blu 2.0 merupakan salah satu bentuk upaya perusahaan dalam meningkatkan pengalaman pengguna dan relevansi layanan digital (PT Bank Digital BCA Tbk, 2025). Namun, inovasi yang dilakukan perlu tetap diimbangi dengan pengelolaan risiko yang matang. Penambahan fitur baru dapat meningkatkan kompleksitas sistem, sehingga berpotensi menimbulkan risiko operasional baru apabila tidak diikuti dengan pengujian dan evaluasi yang memadai.

Hal ini juga tercermin dari hasil observasi peneliti terhadap ulasan pengguna di App Store, yang masih menunjukkan adanya keluhan terkait kendala login, gangguan aplikasi, maupun error saat pembaruan sistem. Temuan tersebut menunjukkan bahwa inovasi layanan perlu disertai evaluasi teknis secara berkelanjutan agar kualitas pengalaman pengguna tetap terjaga.

Penguatan Kepercayaan Nasabah untuk Menjaga Keberlanjutan Layanan

Pada akhirnya, seluruh strategi mitigasi risiko operasional bermuara pada upaya menjaga kepercayaan nasabah. Dalam industri perbankan digital, kepercayaan merupakan aset yang sangat penting karena nasabah mempercayakan data pribadi maupun dana mereka sepenuhnya kepada sistem digital. Apabila gangguan operasional terjadi secara berulang, tingkat kepercayaan nasabah dapat menurun dan berdampak pada reputasi perusahaan. Sebaliknya, kemampuan perusahaan dalam mengelola risiko secara efektif akan meningkatkan persepsi positif masyarakat terhadap keamanan dan keandalan layanan.

Berdasarkan hasil analisis, strategi mitigasi risiko operasional pada blu by BCA Digital perlu dilakukan secara menyeluruh melalui penguatan teknologi, peningkatan keamanan siber, edukasi nasabah, serta inovasi layanan yang terukur. Dengan mitigasi yang efektif, perusahaan tidak hanya mampu menjaga kelancaran operasional, tetapi juga dapat memperkuat keberlanjutan bisnis di tengah persaingan industri perbankan digital yang semakin kompetitif.

Metode Pengendalian Risiko Operasional sebagai Pertimbangan Investasi pada *blu by BCA Digital*

Risiko Operasional sebagai Indikator Kesehatan Perusahaan

Dalam industri perbankan digital, risiko operasional menjadi salah satu indikator penting dalam menilai kesehatan dan stabilitas perusahaan. Hal ini disebabkan karena operasional bank digital hampir sepenuhnya bergantung pada teknologi informasi, mulai dari pembukaan rekening, transaksi keuangan, hingga pengelolaan data nasabah. Oleh karena itu, gangguan pada sistem, ancaman keamanan siber, maupun kegagalan proses operasional dapat memberikan dampak langsung terhadap kinerja perusahaan. Bagi investor, kemampuan perusahaan dalam mengelola risiko operasional dapat mencerminkan kualitas manajemen serta kesiapan perusahaan dalam menghadapi ketidakpastian bisnis. Semakin baik sistem pengendalian risiko yang diterapkan, semakin kecil kemungkinan perusahaan mengalami kerugian operasional yang dapat mengganggu pertumbuhan bisnis dalam jangka panjang.

Pada *blu by BCA Digital*, risiko operasional termasuk salah satu risiko utama yang menjadi perhatian perusahaan. Berdasarkan Laporan Tahunan 2025, risiko operasional dipahami sebagai potensi kerugian yang timbul akibat ketidakcukupan proses internal, kesalahan manusia, kegagalan sistem, maupun kejadian eksternal yang memengaruhi aktivitas operasional bank (**BCA Digital Tbk., 2025**). Definisi tersebut menunjukkan bahwa pengendalian risiko operasional bukan hanya berkaitan dengan aspek teknis, tetapi juga berkaitan dengan stabilitas fundamental perusahaan secara keseluruhan. Dengan demikian, dalam perspektif investasi, risiko operasional dapat digunakan sebagai salah satu indikator untuk menilai apakah suatu bank digital memiliki fondasi bisnis yang sehat dan mampu bertahan di tengah persaingan industri yang semakin dinamis.

Pengaruh Pengendalian Risiko terhadap Kepercayaan Investor

Pengendalian risiko operasional yang efektif dapat meningkatkan kepercayaan investor terhadap prospek perusahaan. Investor pada umumnya tidak hanya menilai potensi pertumbuhan laba, tetapi juga memperhatikan bagaimana perusahaan mengelola berbagai risiko yang dapat memengaruhi keberlangsungan usaha. *BCA Digital* telah menerapkan berbagai mekanisme pengendalian risiko operasional, seperti *Risk Control Self-Assessment (RCSA)*, *Operational Risk Management Information System (ORMIS)*, *Loss Event Database (LED)*, serta *IT Risk Register* untuk memantau dan mengevaluasi potensi risiko secara berkelanjutan (PT Bank Digital BCA Tbk, 2025). Penerapan berbagai sistem tersebut menunjukkan adanya komitmen perusahaan dalam membangun tata kelola risiko yang terstruktur.

Selain itu, *BCA Digital* juga memperkuat pengendalian melalui sertifikasi ISO 27001:2013 terkait manajemen keamanan informasi dan ISO 37001:2016 terkait sistem manajemen anti penyuapan. Keberadaan standar internasional ini memberikan sinyal positif kepada investor bahwa perusahaan berupaya menerapkan praktik tata kelola yang sesuai dengan standar keamanan dan kepatuhan yang baik. Meskipun demikian, insiden gangguan layanan pada tahun 2025 lalu menunjukkan bahwa sistem pengendalian risiko tetap menghadapi tantangan dalam implementasinya. Gangguan yang menyebabkan nasabah kesulitan mengakses layanan digital menjadi bukti bahwa kompleksitas operasional bank digital tetap menyimpan potensi risiko yang signifikan (Z. Aprilia, 2025). Dari sudut pandang investor, kemampuan perusahaan dalam merespons dan memulihkan gangguan seperti ini menjadi faktor penting dalam membangun kepercayaan pasar. Dengan kata lain, investor cenderung menilai bukan hanya dari ada atau tidaknya risiko, tetapi juga dari seberapa cepat dan efektif perusahaan merespons risiko yang muncul.

Analisis Prospek Investasi *blu by BCA Digital*

Prospek investasi pada bank digital umumnya dipengaruhi oleh pertumbuhan industri, kemampuan inovasi, kualitas tata kelola, serta efektivitas pengelolaan risiko. Sebagai bagian dari ekosistem *BCA Group*, *blu by BCA Digital* memiliki keunggulan berupa dukungan infrastruktur teknologi, reputasi merek, dan akses terhadap ekosistem layanan keuangan yang luas. Berdasarkan Laporan Tahunan 2024, pertumbuhan *BCA Digital* didukung oleh penerapan prinsip kehati-hatian (*prudential principle*), penguatan manajemen risiko, serta tata kelola perusahaan yang semakin baik. Hal ini menunjukkan bahwa pertumbuhan perusahaan tidak hanya didorong oleh ekspansi bisnis, tetapi juga oleh kemampuan perusahaan dalam menjaga kualitas operasional.

Dari sisi bisnis, pertumbuhan jumlah pengguna *blu* yang terus meningkat juga menunjukkan adanya potensi pasar yang besar bagi layanan bank digital. Pertumbuhan basis nasabah ini dapat menjadi indikator positif bagi investor karena menunjukkan adanya peningkatan penerimaan pasar terhadap layanan yang ditawarkan perusahaan. Namun demikian, prospek investasi tetap perlu dilihat secara objektif dengan mempertimbangkan

risiko yang ada. Ancaman phishing, fraud digital, gangguan sistem, serta tingginya ekspektasi pengguna terhadap layanan digital dapat menjadi faktor yang berpotensi memengaruhi reputasi dan kinerja perusahaan. Selain itu, hasil observasi peneliti terhadap ulasan pengguna di App Store menunjukkan bahwa masih terdapat beberapa keluhan terkait kendala login, error aplikasi, dan stabilitas sistem. Kondisi tersebut menunjukkan bahwa meskipun prospek pertumbuhan bank digital cukup menjanjikan, kualitas pengendalian risiko tetap menjadi faktor penentu dalam menjaga keberlanjutan pertumbuhan tersebut.

Implikasi Pengendalian Risiko terhadap Keputusan Investasi

Berdasarkan hasil analisis, metode pengendalian risiko operasional pada blu by BCA Digital memiliki keterkaitan yang erat dengan pertimbangan investasi. Dalam perspektif investor, pengendalian risiko operasional yang efektif dapat menjadi sinyal bahwa perusahaan memiliki tata kelola yang baik, stabilitas operasional yang terjaga, serta kapasitas untuk menghadapi tantangan bisnis di masa depan. Sebaliknya, apabila risiko operasional tidak dikelola secara optimal, potensi kerugian finansial, penurunan reputasi, dan berkurangnya kepercayaan nasabah dapat meningkatkan persepsi risiko investasi. Hal ini dapat memengaruhi keputusan investor dalam menilai kelayakan investasi pada bank digital. Berdasarkan temuan penelitian, blu by BCA Digital menunjukkan bahwa perusahaan telah memiliki sistem pengendalian risiko yang cukup komprehensif. Namun, berbagai tantangan operasional yang masih muncul menandakan bahwa penguatan mitigasi risiko tetap perlu dilakukan secara berkelanjutan.

Dengan demikian, dapat disimpulkan bahwa metode pengendalian risiko operasional pada blu by BCA Digital merupakan salah satu faktor penting dalam menilai prospek investasi perusahaan. Semakin efektif perusahaan dalam mengelola risiko operasional, semakin besar pula tingkat kepercayaan investor terhadap stabilitas dan keberlanjutan bisnis bank digital di masa mendatang. Berdasarkan hasil analisis terhadap bentuk risiko operasional, mekanisme pengendalian, tantangan, strategi mitigasi, serta kaitannya dengan pertimbangan investasi, dapat dipahami bahwa BCA Digital telah memiliki sistem pengendalian risiko yang relatif komprehensif. Meskipun demikian, perusahaan masih menghadapi berbagai tantangan yang memerlukan penguatan secara berkelanjutan agar stabilitas layanan dan kepercayaan investor tetap terjaga. Temuan tersebut menjadi dasar dalam penyusunan kesimpulan penelitian pada bab berikutnya.

4. Kesimpulan

Hasil penelitian menunjukkan bahwa layanan blu by BCA Digital memiliki beberapa potensi risiko operasional yang perlu mendapat perhatian, antara lain gangguan sistem (system downtime), ancaman keamanan siber, phishing, scam, fraud digital, serta risiko yang berkaitan dengan kelancaran transaksi dan perlindungan data nasabah. Risiko-risiko tersebut merupakan konsekuensi dari tingginya ketergantungan bank digital terhadap sistem teknologi informasi. Apabila tidak dikelola dengan baik, kondisi tersebut dapat memengaruhi kualitas layanan sekaligus menurunkan kepercayaan nasabah. BCA Digital telah menerapkan berbagai mekanisme pengendalian risiko operasional sebagai bagian dari upaya menjaga stabilitas layanan. Pengendalian tersebut dilakukan melalui penerapan Risk Control Self-Assessment (RCSA), Operational Risk Management Information System (ORMIS), Loss Event Database (LED), IT Risk Register, Whistleblowing System (WBS), serta penerapan standar keamanan informasi dan tata kelola yang didukung oleh sertifikasi ISO. Berbagai mekanisme tersebut menunjukkan bahwa perusahaan telah memiliki sistem pengelolaan risiko yang terstruktur dalam mendukung operasional bank digital. Meskipun telah memiliki sistem pengendalian yang memadai, BCA Digital masih menghadapi sejumlah tantangan dalam mengelola risiko operasional. Tantangan tersebut antara lain perkembangan ancaman kejahatan siber yang semakin kompleks, tingginya ekspektasi masyarakat terhadap layanan digital yang selalu tersedia, serta kebutuhan untuk terus menyesuaikan teknologi dan proses operasional dengan perkembangan lingkungan bisnis maupun regulasi. Kondisi tersebut menunjukkan bahwa pengendalian risiko operasional perlu terus dikembangkan agar mampu mengikuti perubahan yang terjadi. Berdasarkan hasil penelitian, strategi mitigasi risiko yang diterapkan maupun yang masih perlu diperkuat meliputi peningkatan keamanan sistem informasi, penguatan infrastruktur teknologi, edukasi kepada nasabah mengenai keamanan transaksi digital, serta optimalisasi pengawasan terhadap aktivitas operasional. Upaya tersebut menjadi bagian penting dalam menjaga kualitas layanan sekaligus mengurangi potensi terjadinya gangguan operasional di masa mendatang. Hasil penelitian juga menunjukkan bahwa metode pengendalian risiko operasional dapat menjadi salah satu pertimbangan dalam menilai prospek investasi pada bank digital. Bagi investor, efektivitas pengendalian risiko tidak hanya mencerminkan kemampuan perusahaan dalam mengelola potensi kerugian, tetapi juga menggambarkan kualitas tata kelola, stabilitas operasional, dan kesiapan perusahaan dalam menghadapi berbagai tantangan bisnis. Dengan demikian, semakin baik pengendalian risiko yang diterapkan, semakin besar pula peluang perusahaan untuk mempertahankan kepercayaan nasabah dan meningkatkan keyakinan investor terhadap prospek bisnisnya.

Referensi

1. Aprilia, Y., Khilmia, A., & Ilma Ahmad, Z. (2022). MANAJEMEN RISIKO OPERASIONAL PADA PERBANKAN SYARIAH: BIBLIOMETRIK. *IQTISHADIA Jurnal Ekonomi & Perbankan Syariah*, 9(2), 192–203. <https://doi.org/10.19105/iqtishadia.v9i2.6729>
2. Aprilia, Z. (2025). Netizen Teriak BCA Mobile & MyBCA Kompak Error, Ini Kata Manajemen. *CNBC Indonesia*. <https://www.cnbcindonesia.com/market/20250929084732-17-670940/netizen-teriak-bca-mobile-mybca-kompak-error-ini-kata-manajemen>
3. Atasyadila, H., & Muchlis, M. (2024). Pengaruh Digital Banking Terhadap Profitabilitas Dan Efisiensi Operasional Perbankan. *Journal of Accounting, Management and Islamic Economics*, 2(2), 469–478.
4. Bafera, J., & Kleinert, S. (2023). Signaling Theory in Entrepreneurship Research: A Systematic Review and Research Agenda. *Entrepreneurship Theory and Practice*, 47(6), 2419–2464. <https://doi.org/10.1177/10422587221138489>
5. Basel Committee & on Banking Supervision. (2021). Operational Risk—Supervisory Guidelines for the Advanced measurement Approaches. <https://www.bis.org/publ/bcbs196.pdf>
6. BCA Digital Tbk. (2025). BCA Digital | Laporan Perusahaan. BCA Digital. <https://bcdigital.co.id>
7. Kirana, M. S., & Fasa, M. I. (2024). Strategi Pemasaran dalam Peningkatan Produk Bank Syariah pada Era Digital. *Jurnal Media Akademik (JMA)*, 2(12).
8. Kurniawan, D., & Yuspin, W. (2023). Menggagas Pendirian Bank Digital di Indonesia: Sebuah Telaah Yuridis. *Jurnal Supremasi*, 1–14. <https://doi.org/10.35457/supremasi.v13i1.2158>
9. Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis*. sage.
10. Putra, I. G. W. S. C., & Ginting, J. A. (2022). Analisa Faktor-faktor yang mempengaruhi minat generasi Z dalam menggunakan Aplikasi Bank Digital di Indonesia. *Ekuitas: Jurnal Pendidikan Ekonomi*, 10(2), 306–318.
11. Satrya I.Z. (2024). SERANGAN SIBER DALAM PERKEMBANGAN PERBANKAN DIGITAL DI INDONESIA. *Syntax Literate ; Jurnal Ilmiah Indonesia*, 9(10). <https://doi.org/https://doi.org/10.36418/syntax-literate.v9i10>
12. Sugiyono, D. (2022). *Metode penelitian kualitatif*.
13. Tanic, R. H., & Atahau, A. D. R. (2021). DIGITAL BANKING DAN RISIKO OPERASIONAL (STUDI KASUS PADA NASABAH BANK CENTRAL ASIA DAN BANK RAKYAT INDONESIA). *IDEI: Jurnal Ekonomi & Bisnis*, 2(1), 1–20. <https://doi.org/10.38076/ideijeb.v2i1.55>
14. Apriani, D., & Fadillah, R. (2021). Digital banking dan risiko operasional: Studi kasus pada nasabah Bank Central Asia dan Bank Rakyat Indonesia. *Jurnal Manajemen dan Keuangan*, 10(2), 145–162.
15. Kirana, A., & Fasa, M. I. (2024). Transformasi digital perbankan: Implikasi layanan terhadap loyalitas nasabah. *Jurnal Ekonomi dan Bisnis Islam*, 9(1), 78–96.
16. Otoritas Jasa Keuangan. (2021). *Cetak biru transformasi digital perbankan*. OJK.
17. Otoritas Jasa Keuangan. (2021). Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum. OJK.
18. PT Bank Digital BCA. (2024). *Annual report 2024*. PT Bank Digital BCA.
19. Purba, J. H., Situmeang, C., Siagian, H., & Harianja, A. (2024). Serangan siber dalam perkembangan perbankan digital di Indonesia. *Jurnal Teknologi dan Sistem Informasi Keuangan*, 5(1), 33–49.
20. Wijayanti, Y. (2024). *Manajemen risiko perbankan dan transformasi digital*. Penerbit Akademik Keuangan Indonesia.
21. Hartanto Tanic, R., & Atahau, A. D. R. (2020). Digital Banking dan Risiko Operasional (Studi Kasus pada Nasabah Bank Central Asia dan Bank Rakyat Indonesia). *IDEI: Jurnal Ekonomi & Bisnis*, 2(1).
22. Ngamal, Y., & Perajaka, M. A. (2022). Penerapan Model Manajemen Risiko Teknologi Digital di Lembaga Perbankan Berkaca pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*,
23. Gusli, R. A., & Puteri, H. E. (2023). Kajian Risiko Operasional Pada Profitabilitas Bank Umum Syariah Periode 2018–2021. *Jurnal Manajemen dan Perbankan (JUMPA)*, 10(1).
24. Ngamal, Y., & Perajaka, M. A. (2021). Penerapan Model Manajemen Risiko Teknologi Digital di Lembaga Perbankan Berkaca pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, 3(1), 59–74
25. Pratiwi, D., & Nugraha, R. (2024). Manajemen Risiko Operasional pada Perbankan Digital di Era Transformasi Teknologi. *Jurnal Manajemen dan Teknologi Keuangan*, 6(1), 21–30.
26. Ramadani, N., & Wahyuni, S. (2022). Analisis Risiko Operasional pada Digital Banking di Indonesia. *Jurnal Ekonomi Digital*, 4(2), 55–63.
27. Shabri, H. (2022). Transformasi Digital Industri Perbankan Syariah Indonesia. *El-Kahfi: Journal of Islamic Economics*, 3(2), 228–234.