

ANALISIS RISIKO OPERASIONAL PADA BANK SYARIAH DI ERA DIGITAL BANKING

Marsyah¹, Nurwahyuni², Angraeni³, Kamaruddin Arsyad⁴

marsyahm245@gmail.com¹, uniqueen180305@gmail.com², angraenisapitri6@gmail.com³,
dr.kamaruddin46@gmail.com⁴

Universitas Islam Negeri Alauddin Makassar

ABSTRAK

Evolusi perbankan digital telah menghasilkan perubahan yang berarti dalam cara operasional perbankan syariah di Indonesia. Namun, di balik perkembangan teknologi itu, terdapat sejumlah risiko operasional yang harus diidentifikasi dan diatasi dengan cara yang menyeluruh. Studi ini bertujuan untuk menganalisis risiko operasional yang dihadapi oleh bank syariah dalam era perbankan digital, mengidentifikasi faktor-faktor penyebabnya, serta merumuskan strategi mitigasi yang sesuai dengan prinsip syariah. Metodologi yang diterapkan adalah pendekatan deskriptif kualitatif melalui teknik telaah pustaka dan analisis dokumen peraturan. Hasil penelitian mengungkapkan bahwa risiko operasional di bank syariah pada zaman digital mencakup risiko keamanan siber, risiko sistem teknologi informasi yang gagal, risiko kepatuhan syariah di platform digital, risiko penipuan digital, dan risiko kesalahan dari sumber daya manusia. Hasil ini menunjukkan pentingnya penguatan pengelolaan risiko yang terintegrasi antara teknologi, regulasi, dan nilai-nilai syariah.

Kata Kunci: Risiko Operasional, Bank Syariah, Digital Banking, Manajemen Risiko, Keamanan Siber.

ABSTRACT

The evolution of digital banking has resulted in significant changes in the way Islamic banks operate in Indonesia. However, behind these technological developments, there are a number of operational risks that must be identified and addressed comprehensively. This study aims to analyze the operational risks faced by Islamic banks in the digital banking era, identify their causal factors, and formulate mitigation strategies in accordance with Sharia principles. The methodology applied is a qualitative descriptive approach through literature review techniques and regulatory document analysis. The study results reveal that operational risks in Islamic banks in the digital age include cybersecurity risks, risks of failed information technology systems, risks of Sharia compliance on digital platforms, risks of digital fraud, and risks of human resource errors. These results demonstrate the importance of strengthening integrated risk management between technology, regulations, and Sharia values.

Keywords: Operational Risk, Islamic Bank, Digital Banking, Risk Management, Cybersecurity.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah memicu transformasi besar dalam industri perbankan global, termasuk perbankan syariah di Indonesia. Era digital banking ditandai dengan hadirnya layanan perbankan berbasis internet, mobile banking, aplikasi finansial (fintech), dan ekosistem pembayaran digital yang semakin kompleks. Bank syariah, sebagai lembaga keuangan yang beroperasi sesuai dengan prinsip-prinsip Islam, dituntut untuk beradaptasi dengan perkembangan teknologi guna mempertahankan daya saing dan memenuhi harapan nasabah yang semakin melek digital.

Namun, transformasi digital ini tidak datang tanpa konsekuensi. Di balik kemudahan dan efisiensi yang ditawarkan oleh layanan perbankan digital, terdapat berbagai risiko operasional yang semakin kompleks dan beragam. Risiko operasional dalam perbankan didefinisikan sebagai risiko kerugian yang muncul akibat ketidakcukupan atau kegagalan dalam proses internal, faktor manusia, sistem, atau kejadian eksternal (Basel Committee

on Banking Supervision, 2006). Dalam konteks digital banking, risiko ini mengalami peningkatan signifikan seiring dengan bertambahnya ketergantungan pada infrastruktur teknologi.

Urgensi kajian ini semakin diperkuat oleh temuan kajian bibliometrik dan systematic literature review yang dilakukan Nuzulia dan Kasanah (2024) terhadap 372 artikel internasional mengenai manajemen risiko perbankan syariah pada rentang 2002–2022. Studi tersebut menunjukkan bahwa penelitian mengenai risiko finansial, seperti risiko kredit dan likuiditas, jauh lebih mendominasi dibandingkan risiko operasional dan praktik manajemen risiko, yang justru menjadi kata kunci dengan kemunculan paling sedikit dalam pemetaan literatur. Kesenjangan ini menegaskan bahwa kajian mendalam mengenai risiko operasional bank syariah, terlebih dalam konteks transformasi digital yang relatif baru, masih sangat diperlukan.

Bank syariah menghadapi tantangan yang lebih kompleks dibandingkan bank konvensional dalam mengelola risiko operasional di era digital. Selain menghadapi risiko teknologi yang sama dengan bank konvensional, bank syariah juga harus memastikan bahwa semua produk dan layanan digital yang ditawarkan tidak bertentangan dengan prinsip-prinsip syariah, seperti larangan riba, gharar (ketidakpastian), dan maysir (spekulasi). Hal ini menambah dimensi risiko kepatuhan syariah yang perlu dikelola secara khusus dalam setiap inovasi digital yang diimplementasikan.

Data dari Otoritas Jasa Keuangan (OJK) menunjukkan bahwa jumlah pengguna mobile banking dan internet banking di bank syariah Indonesia meningkat signifikan sebesar 45% dalam periode 2021-2023 (OJK, 2023). Pertumbuhan yang pesat ini juga diikuti oleh peningkatan insiden siber dan kejadian operasional yang dilaporkan oleh industri perbankan syariah. Berdasarkan laporan Indonesia Cyber Security Incident (BSSN, 2023), sektor keuangan menjadi salah satu target utama serangan siber di Indonesia. Menariknya, studi persepsi nasabah yang dilakukan Laksana, Shaferi, dan Naznii (2023) terhadap 240 pengguna internet banking di Banyumas justru menemukan bahwa mayoritas nasabah tidak menganggap layanan internet banking berisiko tinggi. Perbedaan antara eksposur risiko riil yang meningkat dengan persepsi risiko nasabah yang relatif rendah ini menjadi salah satu justifikasi penting mengapa kajian mendalam mengenai risiko operasional bank syariah di era digital, dari sisi lembaga maupun nasabah, perlu terus dilakukan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk: (1) mengidentifikasi jenis-jenis risiko operasional yang dihadapi bank syariah di era digital banking; (2) menganalisis faktor-faktor penyebab dan dampak dari risiko operasional tersebut; (3) merumuskan strategi mitigasi risiko yang sesuai dengan prinsip syariah dan regulasi yang berlaku; (4) memberikan rekomendasi kebijakan bagi pemangku kepentingan dalam industri perbankan syariah.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif, yang bertujuan untuk memahami dan mendeskripsikan fenomena risiko operasional pada bank syariah di era digital banking secara mendalam. Pendekatan kualitatif dipilih karena penelitian ini berusaha mengeksplorasi kompleksitas risiko operasional yang tidak dapat diukur sepenuhnya secara kuantitatif.

Teknik pengumpulan data yang digunakan mencakup: (1) Studi pustaka, yang melibatkan pengkajian literatur ilmiah, jurnal internasional bereputasi, laporan regulasi, dan dokumen kebijakan yang relevan dengan topik penelitian; (2) Analisis dokumen regulasi, yang berfokus pada kajian berbagai peraturan yang mengatur manajemen risiko

operasional dan digital banking di Indonesia, seperti regulasi dari OJK, POJK, dan Peraturan Bank Indonesia; (3) Analisis laporan tahunan bank syariah, khususnya laporan manajemen risiko yang dipublikasikan oleh Bank Syariah Indonesia (BSI) dan beberapa bank umum syariah lainnya.

Untuk memperkaya interpretasi, hasil telaah kualitatif tersebut turut dibandingkan dengan temuan studi bibliometrik (Nuzulia & Kasanah, 2024), studi pengukuran kuantitatif berbasis Loss Distribution Approach (Yudiana, Hafidhuiddin, & Ismal, 2018), studi persepsi nasabah (Laksana, Shaferi, & Naznii, 2023), serta studi determinan pengungkapan risiko operasional (Putri & Filianti, 2021). Perbandingan lintas metode ini dimaksudkan untuk memberikan gambaran yang lebih komprehensif mengenai risiko operasional bank syariah, baik dari sisi identifikasi kualitatif, besaran kerugian kuantitatif, persepsi nasabah, maupun tingkat transparansi pengungkapannya.

Data yang telah dikumpulkan dianalisis dengan menggunakan teknik analisis isi (content analysis) dan analisis tematik. Analisis isi digunakan untuk mengidentifikasi tema-tema utama yang berkaitan dengan risiko operasional dalam literatur dan dokumen yang dikaji. Sementara itu, analisis tematik digunakan untuk mengelompokkan temuan ke dalam kategori risiko yang relevan.

Untuk menjaga validitas dan reliabilitas penelitian, dilakukan triangulasi sumber data dengan membandingkan informasi dari berbagai sumber, termasuk literatur akademis, dokumen regulasi, dan laporan industri. Proses triangulasi ini memastikan bahwa temuan penelitian memiliki dasar yang kuat dan dapat dipertanggungjawabkan secara ilmiah.

HASIL DAN PEMBAHASAN

1. Identifikasi Risiko Operasional Bank Syariah di Era Digital

Berdasarkan kajian literatur dan analisis dokumen yang dilakukan, penelitian ini mengidentifikasi lima kategori utama risiko operasional yang dihadapi bank syariah di era digital banking:

a) Risiko Keamanan Siber (Cybersecurity Risk)

Risiko keamanan siber merupakan ancaman terbesar yang dihadapi bank syariah dalam era digital. Serangan siber seperti phishing, ransomware, serangan distributed denial-of-service (DDoS), dan pencurian data nasabah dapat mengakibatkan kerugian finansial yang besar serta kerusakan reputasi yang serius. Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, sektor keuangan Indonesia mengalami lebih dari 1,2 miliar serangan siber sepanjang tahun 2022, dengan bank-bank syariah menjadi salah satu target yang semakin sering disasar oleh pelaku kejahatan siber.

Secara lebih rinci, risiko keamanan siber pada bank syariah dapat diuraikan ke dalam beberapa bentuk. Pertama, kebocoran data (data breach) yang terjadi akibat peretasan basis data nasabah, baik melalui celah pada aplikasi mobile banking maupun pada sistem penyimpanan cadangan (backup) yang tidak terenkripsi dengan baik. Kedua, akses tidak sah (unauthorized access) terhadap sistem inti perbankan (core banking system) melalui celah keamanan pada Application Programming Interface (API) yang menghubungkan bank dengan mitra fintech maupun penyedia layanan pembayaran pihak ketiga. Ketiga, serangan malware dan ransomware yang menyasar perangkat mobile nasabah maupun server internal bank, yang berpotensi melumpuhkan layanan transaksi digital dalam waktu tertentu. Keempat, risiko keamanan pada skema open banking dan Quick Response Code Indonesian Standard (QRIS) yang melibatkan banyak pihak eksternal, sehingga memperluas permukaan serangan (attack surface) yang harus diawasi bank.

Bank syariah menghadapi kerentanan yang lebih tinggi terhadap serangan siber disebabkan beberapa faktor, antara lain: pertama, terbatasnya investasi dalam infrastruktur keamanan siber jika dibandingkan dengan bank konvensional besar; kedua, tingkat literasi digital nasabah yang bervariasi, sehingga lebih rentan terhadap serangan social engineering; ketiga, integrasi sistem dengan berbagai mitra fintech yang dapat menjadi celah keamanan. Kerentanan ini juga tercermin pada indikator risiko sistem yang digunakan Laksana, Shaferi, dan Naznii (2023), seperti data yang tidak lengkap (data corruption), kesalahan input data, dan lemahnya kontrol atas perubahan data, yang seluruhnya berpotensi menjadi pintu masuk bagi eksploitasi keamanan siber apabila tidak dikelola dengan baik.

b) Risiko Kegagalan Sistem Teknologi Informasi

Kegagalan sistem teknologi informasi mencakup downtime layanan, gangguan aplikasi mobile banking, kegagalan pemrosesan transaksi, dan ketidakmampuan sistem untuk menangani volume transaksi yang tinggi. Dalam konteks bank syariah, kegagalan sistem ini tidak hanya menimbulkan kerugian finansial dan ketidaknyamanan bagi nasabah, tetapi juga dapat menyebabkan terjadinya transaksi yang tidak sesuai dengan prinsip syariah jika sistem tidak mampu memvalidasi kepatuhan syariah secara real-time.

Penelitian yang dilakukan oleh Karyani dan Komarudin (2023) menunjukkan bahwa bank-bank syariah di Indonesia rata-rata mengalami 12-18 kali gangguan layanan digital dalam setahun, dengan durasi gangguan rata-rata 2-4 jam per kejadian. Gangguan-gangguan ini mengakibatkan hilangnya transaksi dan kepercayaan nasabah. Temuan ini sejalan dengan hasil pengukuran kuantitatif Yudiana, Hafidhuddin, dan Ismal (2018), yang menemukan bahwa kontribusi kerugian operasional terbesar pada salah satu bank syariah di Indonesia justru berasal dari kejadian business disruption and system failure serta execution, delivery and process management, dengan penyebab utama berupa ketidakstabilan penggantian core banking system dan tingginya kerentanan sistem terhadap serangan virus. Kesamaan pola ini menegaskan bahwa risiko kegagalan sistem bukan sekadar potensi teoretis, melainkan kontributor kerugian operasional riil yang signifikan bagi bank syariah di Indonesia, baik sebelum maupun sesudah akselerasi digitalisasi layanan.

Secara lebih spesifik, kegagalan sistem teknologi informasi dapat dipilah menjadi beberapa jenis kejadian. Pertama, gangguan menyeluruh (full outage) yang menyebabkan seluruh layanan digital, termasuk core banking, payment system, dan e-channel, tidak dapat diakses sama sekali; Yudiana, Hafidhuddin, dan Ismal (2018) mengategorikan gangguan dengan durasi empat jam atau lebih sebagai gangguan berkategori tinggi (high). Kedua, gangguan parsial (partial outage) yang hanya memengaruhi sebagian fitur, misalnya kegagalan notifikasi transaksi melalui SMS atau surel meskipun dana telah berpindah, sebagaimana turut menjadi salah satu indikator risiko proses dalam studi Laksana, Shaferi, dan Naznii (2023). Ketiga, kerentanan sistem terhadap ancaman virus dan malware; sebagai gambaran, Yudiana, Hafidhuddin, dan Ismal (2018) mencatat ribuan varian serangan virus yang berhasil ditangani (cleaned), dikarantina (quarantined), maupun yang masih menunggu penanganan (pending repair) pada satu periode pelaporan bulanan bank syariah yang diteliti. Keempat, kegagalan proses transaksi (execution delivery and process management) akibat kompleksitas integrasi antara core banking system dengan branch delivery system, financing origination system, dan sistem pendukung lainnya, yang berpotensi menimbulkan kesalahan pencatatan maupun keterlambatan penyelesaian transaksi nasabah.

c) Risiko Kepatuhan Syariah dalam Platform Digital

Risiko ini muncul ketika produk atau layanan digital yang ditawarkan oleh bank syariah tidak memenuhi syarat-syarat syariah yang telah ditetapkan oleh Dewan Pengawas Syariah (DPS) dan Majelis Ulama Indonesia (MUI). Dalam konteks perbankan digital, risiko ini menjadi semakin kompleks karena kecepatan inovasi produk digital seringkali melebihi kecepatan proses tinjauan dan validasi syariah yang diperlukan.

Contoh nyata dari risiko ini adalah penggunaan algoritma untuk penetapan harga dinamis dalam pembiayaan digital yang dapat mengandung unsur riba atau penggunaan akad yang tidak tepat dalam layanan dompet digital syariah. Muttaqin dan Khasanah (2023) menekankan bahwa setiap inovasi produk digital di bank syariah harus menjalani proses validasi kepatuhan syariah dengan perspektif maqashid syariah yang ketat sebelum diluncurkan ke publik. Hal ini relevan dengan peran DPS yang, menurut Putri dan Filianti (2021), semakin aktif melakukan rapat pengawasan akan mendorong pengungkapan informasi kepatuhan syariah yang lebih transparan kepada publik, termasuk terkait produk-produk digital baru.

Beberapa bentuk konkret risiko kepatuhan syariah digital dapat diuraikan sebagai berikut. Pertama, ketidaksesuaian akad pada fitur *paylater* atau pembiayaan instan berbasis aplikasi, di mana skema denda keterlambatan atau biaya administrasi berpotensi menyerupai riba jika tidak dirancang menggunakan akad yang sesuai, misalnya *ta'widh* (ganti rugi) yang dibatasi hanya pada kerugian riil. Kedua, potensi unsur *gharar* pada fitur *robo-advisory* atau investasi digital syariah apabila mekanisme bagi hasil dan risiko investasi tidak dijelaskan secara transparan kepada nasabah. Ketiga, keterlambatan pembaruan opini atau ketetapan Dewan Pengawas Syariah terhadap fitur digital baru yang diluncurkan secara cepat mengikuti siklus pengembangan produk teknologi (*agile development*), sehingga berpotensi terjadi jeda waktu antara peluncuran fitur dan validasi kepatuhan syariahnya. Keempat, risiko pengungkapan pendapatan non halal dari produk digital, misalnya bunga mengambang yang secara tidak sengaja diterima dari mitra pembayaran pihak ketiga, yang menurut kerangka *Operational Risk Disclosure Index* milik Putri dan Filianti (2021) semestinya diungkapkan secara eksplisit dalam laporan tahunan bank syariah.

d) Risiko Penipuan Digital (Digital Fraud Risk)

Penipuan digital merupakan salah satu risiko operasional yang paling umum terjadi dalam industri perbankan syariah. Bentuk-bentuk penipuan digital yang sering terjadi meliputi rekayasa sosial (*social engineering*), pengambilalihan akun (*account takeover*), transaksi tidak sah yang menggunakan identitas nasabah yang dicuri, serta penipuan investasi berbasis platform digital yang mengatasnamakan bank syariah.

Data dari OJK (2023) menunjukkan bahwa pengaduan terkait penipuan digital pada bank syariah meningkat sebesar 67% dalam periode 2020-2022, sejalan dengan bertambahnya penetrasi layanan digital. Tingginya tingkat penipuan ini disebabkan oleh rendahnya literasi digital nasabah dan kelemahan dalam sistem autentikasi. Sebagai perbandingan, Yudiana, Hafidhuddin, dan Ismal (2018) mencatat bahwa kejadian internal fraud berkontribusi lebih dari 90% terhadap total kerugian operasional bank syariah yang diteliti pada tahun 2015. Temuan ini memperkuat urgensi pengendalian risiko penipuan secara menyeluruh, baik yang berasal dari pihak eksternal maupun dari kolusi internal pegawai, dalam konteks layanan digital yang semakin luas jangkauannya.

Merujuk pada pemetaan jenis risiko operasional digital banking yang disusun Laksana, Shaferi, dan Nazni (2023), penipuan digital pada bank syariah dapat

berupa: pencurian informasi atau kredensial nasabah oleh pihak internal maupun eksternal; pengambilalihan akun oleh pelaku yang berpura-pura menjadi nasabah untuk mengakses rekening tanpa izin; pihak eksternal yang menyamar sebagai petugas bank guna meminta kata sandi atau user ID nasabah; kerja sama antara pelaku dengan oknum pegawai bank untuk menghubungkan mesin ATM dengan rekening pribadi atau rekening lain; penggunaan domain palsu yang menyerupai laman resmi bank untuk mengelabui nasabah (phishing); serta pembukaan rekening fiktif oleh oknum pegawai atas nama nasabah demi memperoleh insentif. Ragam modus tersebut menegaskan bahwa penipuan digital pada bank syariah tidak hanya bersumber dari faktor eksternal, tetapi juga dapat melibatkan kelemahan pengendalian internal, sehingga memerlukan pengawasan berlapis pada kedua sisi.

e) Risiko Sumber Daya Manusia

Risiko sumber daya manusia (SDM) dalam konteks perbankan digital mencakup kurangnya kompetensi tenaga kerja dalam mengelola teknologi baru, kesalahan operasional dalam pengelolaan sistem digital, hingga ancaman dari dalam (insider threat) di mana karyawan bank menyalahgunakan akses mereka terhadap sistem digital. Bank syariah menghadapi tantangan tambahan terkait kebutuhan akan sumber daya manusia yang tidak hanya memiliki kompetensi teknologi, tetapi juga pemahaman mendalam tentang prinsip-prinsip syariah.

Temuan ini relevan dengan hasil studi persepsi nasabah oleh Laksana, Shaferi, dan Naznii (2023), yang menemukan bahwa sebagian besar responden bersikap netral terhadap kemungkinan tingginya turnover karyawan dan potensi kecurangan internal (internal fraud) pada bank tempat mereka bertransaksi. Sikap netral ini mengindikasikan minimnya informasi atau transparansi yang diterima nasabah terkait pengelolaan risiko SDM oleh bank, sehingga nasabah tidak dapat menilai secara pasti tinggi-rendahnya risiko tersebut.

Studi tersebut secara rinci mengukur risiko SDM melalui tujuh indikator, yaitu masalah keselamatan dan kesehatan kerja, tingkat perputaran karyawan (turnover), potensi kecurangan internal, perselisihan antarkaryawan, praktik manajemen yang kurang baik, pelatihan yang tidak memadai, serta ketergantungan berlebihan pada karyawan tertentu (key person dependency). Ketergantungan pada karyawan tertentu perlu mendapat perhatian khusus pada bank syariah era digital, mengingat terbatasnya jumlah tenaga ahli yang menguasai baik aspek teknologi maupun kepatuhan syariah secara bersamaan; ketiadaan salah satu karyawan kunci tersebut, misalnya karena resign atau cuti panjang, berpotensi menghambat proses validasi syariah terhadap produk digital baru maupun penanganan insiden teknis yang bersifat mendesak.

Untuk memperjelas keterkaitan antara kelima kategori risiko tersebut dengan sumber literatur pendukung, ringkasan disajikan pada Tabel 1 berikut.

No	Kategori Risiko	Deskripsi Singkat	Contoh kejadian	Referensi pendukung
----	-----------------	-------------------	-----------------	---------------------

1	Keamanan Siber	Ancaman terhadap kerahasiaan, integritas dan ketersediaan data serta sistem digital bank.	Kebocoran data, akses tidak sah via API, serangan malware/ransomware, celah pada skema open banking/QRIS.	BSSN (2023); Laksana dkk. (2023)
---	----------------	---	---	----------------------------------

2. Faktor-Faktor yang Mempengaruhi Risiko Operasional

Analisis menunjukkan beberapa faktor utama yang mempengaruhi tingkat risiko operasional bank syariah di era digital. Pertama, faktor infrastruktur teknologi yang mencakup kualitas dan keandalan sistem IT, kapasitas keamanan siber, dan tingkat integrasi sistem. Kedua, faktor regulasi yang meliputi kompleksitas kepatuhan terhadap regulasi perbankan digital dan ketentuan syariah secara bersamaan. Ketiga, faktor sumber daya manusia yang mencakup tingkat kompetensi digital karyawan serta pemahaman tentang syariah. Keempat, faktor lingkungan eksternal yang meliputi tingkat ancaman siber, dinamika kompetisi dengan fintech, dan ekspektasi nasabah yang terus berkembang.

Luthfiatussa'dyah (2023) dalam penelitiannya menemukan bahwa faktor infrastruktur teknologi dan kompetensi sumber daya manusia adalah dua faktor yang paling signifikan mempengaruhi tingkat risiko operasional bank syariah di Indonesia. Temuan ini konsisten dengan hasil penelitian Oktaviani dan Basyariah (2022) mengenai layanan mobile banking syariah, serta Azzahra (2024) yang menegaskan pentingnya kesiapan infrastruktur teknologi dalam mengurangi risiko operasional bank syariah di era transformasi digital.

Sejalan dengan hal tersebut, kajian bibliometrik Nuzulia dan Kasanah (2024) menegaskan bahwa topik risiko operasional dan praktik manajemen risiko pada perbankan syariah relatif kurang diteliti dibandingkan risiko kredit dan likuiditas dalam literatur internasional selama dua dekade terakhir. Kesenjangan penelitian ini semakin menguatkan urgensi kajian mengenai faktor-faktor risiko operasional di era digital sebagaimana dilakukan dalam penelitian ini, sekaligus mengisi celah literatur yang selama ini lebih berfokus pada risiko finansial bank syariah.

3. Strategi Mitigasi Risiko Operasional

Berdasarkan hasil identifikasi dan analisis risiko yang telah dilakukan, penelitian ini merumuskan beberapa strategi mitigasi risiko yang komprehensif dan sesuai dengan prinsip syariah:

1) Penguatan Infrastruktur Keamanan Siber

Terjadi melalui implementasi sistem keamanan berlapis (defense in depth), penggunaan enkripsi data end-to-end, penerapan multi-factor authentication (MFA), serta pengembangan Security Operations Center (SOC) yang beroperasi 24 jam sehari, 7 hari seminggu. Investasi dalam keamanan siber seharusnya dipandang bukan sebagai beban operasional, melainkan sebagai tanggung jawab amanah terhadap nasabah sesuai dengan prinsip syariah.

2) Pengembangan Rencana Keberlangsungan Bisnis (BCP) dan Rencana Pemulihan Bencana (DRP)

Rencana ini perlu komprehensif untuk memastikan ketersediaan layanan secara berkelanjutan. Hal ini meliputi skenario berbagai jenis gangguan sistem dan mekanisme pemulihan yang cepat, mengingat temuan Yudiana, Hafidhuddin, dan Ismal (2018) bahwa gangguan sistem dan kegagalan proses eksekusi transaksi merupakan salah satu kontributor kerugian operasional terbesar pada bank syariah.

3) Penguatan Tata Kelola Kepatuhan Syariah Digital

Ini dilakukan melalui pembentukan unit khusus yang bertugas untuk memvalidasi kepatuhan syariah dari setiap produk digital sebelum diluncurkan, serta melakukan pemantauan kepatuhan syariah secara berkelanjutan terhadap layanan digital yang sudah beroperasi.

4) Peningkatan Kapasitas Sumber Daya Manusia

Diperlukan program pelatihan berkelanjutan yang mencakup kompetensi teknologi digital, keamanan siber, dan pengetahuan syariah. Bank syariah perlu mengembangkan tenaga ahli dengan keahlian gabungan di bidang teknologi dan keuangan syariah.

5) Edukasi dan Literasi Digital Nasabah

Ini merupakan bagian dari strategi mitigasi risiko eksternal. Bank syariah harus aktif mengedukasi nasabah tentang keamanan transaksi digital, cara mengenali penipuan digital, serta pentingnya menjaga kerahasiaan data pribadi. Sebagaimana ditunjukkan oleh Laksana, Shaferi, dan Naznii (2023), sikap netral nasabah terhadap sejumlah indikator risiko operasional mengindikasikan perlunya edukasi yang lebih intensif agar nasabah dapat menilai risiko secara lebih tepat, bukan sekadar merasa aman tanpa dasar informasi yang memadai.

6) Peningkatan Transparansi Pengungkapan Risiko Operasional

Merujuk pada temuan Putri dan Filianti (2021), bank syariah dengan ukuran aset yang lebih besar dan frekuensi rapat Dewan Pengawas Syariah yang lebih tinggi cenderung mengungkapkan informasi risiko operasional secara lebih transparan, sementara bank dengan efisiensi biaya yang rendah justru cenderung mengurangi pengungkapan risikonya, kemungkinan sebagai upaya menjaga reputasi. Bank syariah di era digital disarankan menjadikan pengungkapan risiko siber, risiko sistem teknologi informasi, dan risikokepatuhan syariah digital sebagai bagian rutin dari laporan tahunan, tidak sekadar memenuhi standar minimum regulasi, guna menjaga kepercayaan dan legitimasi di mata nasabah dan otoritas.

4. Kerangka Regulasi dan Peran OJK

Otoritas Jasa Keuangan (OJK) sebagai regulator perbankan di Indonesia telah menerbitkan berbagai regulasi yang mengatur manajemen risiko operasional di era digital. POJK No. 38/POJK.03/2016 mengharuskan bank umum, termasuk bank syariah, untuk menerapkan manajemen risiko teknologi informasi yang komprehensif. Di sisi lain, POJK No. 12/POJK.03/2018 secara khusus mengatur penyelenggaraan layanan perbankan digital.

Selain itu, Surat Edaran OJK No. 10/SEOJK.03/2014 turut menjadi acuan standar pengungkapan risiko perbankan secara umum, yang oleh Putri dan Filianti (2021) dipadukan dengan standar IFSB dan Basel II untuk membangun indeks pengungkapan risiko operasional yang lebih komprehensif bagi bank umum syariah. Dalam tahap perkembangan ini, OJK juga telah menerbitkan Roadmap Pengembangan Perbankan Syariah Indonesia 2020-2025. Roadmap ini mencakup aspek transformasi digital dan penguatan manajemen risiko operasional sebagai salah satu prioritas utama. Dengan

demikian, roadmap ini memberikan arah kebijakan yang jelas bagi bank syariah dalam mengembangkan kapabilitas digital, sambil tetap menjaga kepatuhan syariah dan pengelolaan risiko yang prudent (OJK, 2020).

5. Pengukuran Kuantitatif dan Pengungkapan sebagai Pelengkap Mitigasi

Identifikasi risiko secara kualitatif sebagaimana dilakukan dalam penelitian ini perlu dilengkapi dengan pengukuran kuantitatif untuk memberikan gambaran yang lebih presisi mengenai besaran eksposur risiko. Pendekatan Loss Distribution Approach (LDA) Aggregate yang digunakan Yudiana, Hafidhuddin, dan Ismal (2018) menunjukkan bahwa model internal semacam ini dapat menghasilkan beban modal risiko operasional yang lebih efisien dan lebih sensitif terhadap profil kerugian riil dibandingkan pendekatan indikator dasar. Bank syariah di era digital berpotensi mengadaptasi pendekatan serupa untuk mengukur kerugian yang bersumber dari kanal digital secara spesifik, seperti kerugian akibat downtime sistem, serangan siber, maupun penipuan digital.

Di sisi lain, indeks pengungkapan risiko operasional yang dikembangkan Putri dan Filianti (2021) dapat menjadi instrumen evaluasi bagi regulator maupun akademisi untuk menilai sejauh mana bank syariah telah transparan dalam mengomunikasikan risiko operasional era digital kepada publik. Kombinasi antara identifikasi risiko kualitatif, pengukuran kuantitatif, dan evaluasi pengungkapan ini diharapkan dapat memberikan kerangka manajemen risiko operasional yang lebih holistik bagi industri perbankan syariah di Indonesia.

KESIMPULAN

Penelitian ini berhasil mengidentifikasi lima kategori utama risiko operasional yang dihadapi bank syariah di era digital banking, yaitu: risiko keamanan siber, risiko kegagalan sistem teknologi informasi, risiko kepatuhan syariah dalam platform digital, risiko penipuan digital, dan risiko sumber daya manusia. Setiap kategori risiko ini memiliki karakteristik dan dampak yang berbeda, namun semuanya memerlukan pendekatan manajemen risiko yang terintegrasi dan komprehensif.

Temuan penelitian juga menunjukkan bahwa bank syariah menghadapi tantangan unik dalam mengelola risiko operasional digital, yaitu keharusan untuk menyeimbangkan antara inovasi teknologi, keamanan operasional, kepatuhan regulasi, dan kepatuhan syariah secara bersamaan. Hal ini menuntut pendekatan manajemen risiko yang tidak hanya mempertimbangkan dimensi teknis dan finansial, tetapi juga dimensi spiritual dan etis sesuai nilai-nilai Islam.

Perbandingan dengan penelitian terdahulu memperkuat validitas temuan ini: kajian bibliometrik Nuzulia dan Kasanah (2024) menegaskan bahwa risiko operasional masih menjadi topik yang kurang diteliti dibandingkan risiko finansial; pengukuran kuantitatif Yudiana, Hafidhuddin, dan Ismal (2018) membuktikan bahwa kegagalan sistem dan penipuan internal merupakan kontributor kerugian operasional riil yang besar; studi persepsi nasabah oleh Laksana, Shaferi, dan Naznii (2023) mengungkap kesenjangan antara eksposur risiko dan tingkat kesadaran nasabah; serta studi pengungkapan oleh Putri dan Filianti (2021) menunjukkan bahwa ukuran bank dan tata kelola syariah memengaruhi transparansi informasi risiko operasional. Secara keseluruhan, keempat perspektif ini saling melengkapi dan memperkuat argumen bahwa pengelolaan risiko operasional bank syariah di era digital memerlukan pendekatan kualitatif, kuantitatif, edukatif, dan tata kelola yang berjalan secara simultan.

Strategi mitigasi yang dirumuskan dalam penelitian ini menekankan pentingnya pendekatan holistik yang mengintegrasikan penguatan infrastruktur teknologi,

pengembangan SDM, tata kelola kepatuhan syariah yang kuat, edukasi nasabah, serta transparansi pengungkapan risiko. Implementasi strategi ini harus didukung oleh komitmen manajemen puncak dan kolaborasi yang erat antara unit teknologi, unit risiko, unit syariah, dan unit bisnis bank.

Saran

Berdasarkan kesimpulan di atas, penelitian ini merumuskan beberapa saran sebagai berikut:

- 1) Bagi bank syariah, disarankan untuk meningkatkan investasi dalam infrastruktur keamanan siber dan pengembangan SDM yang memiliki kompetensi ganda di bidang teknologi dan syariah, serta memperluas pengungkapan risiko operasional digital dalam laporan tahunan sebagaimana direkomendasikan oleh Putri dan Filianti (2021).
- 2) Bagi OJK, disarankan untuk memperkuat kerangka regulasi manajemen risiko digital khusus untuk bank syariah yang mempertimbangkan dimensi kepatuhan syariah, termasuk memperbarui standar indeks pengungkapan risiko operasional agar mengakomodasi risiko-risiko spesifik era digital.
- 3) Bagi akademisi dan peneliti, disarankan untuk melakukan penelitian empiris lebih lanjut dengan menggunakan data primer dari bank syariah untuk mengkuantifikasi dampak finansial dari masing-masing jenis risiko operasional digital, misalnya dengan mengadaptasi pendekatan Loss Distribution Approach (Yudiana, Hafidhuddin, & Ismal, 2018) secara khusus pada data kerugian kanal digital.
- 4) Bagi Dewan Pengawas Syariah, disarankan untuk mengembangkan pedoman khusus yang memberikan panduan teknis tentang kepatuhan syariah dalam konteks inovasi produk digital, mengingat frekuensi rapat DPS terbukti berpengaruh signifikan terhadap transparansi pengungkapan risiko operasional (Putri & Filianti, 2021).
- 5) Bagi peneliti selanjutnya, disarankan untuk melakukan studi persepsi nasabah bank syariah pengguna layanan digital secara lebih luas, mengikuti pendekatan Laksana, Shaferi, dan Naznii (2023), guna memetakan kesenjangan antara persepsi nasabah dan eksposur risiko operasional riil di berbagai wilayah di Indonesia.

DAFTAR PUSTAKA

- Akbar, C. E., Abdullah, E. M. W., & Awaluddin, M. (2022). Manajemen Risiko di Perbankan Syariah. *Milkiyah: Jurnal Hukum Ekonomi Syariah*, 1(2), 51–56.
- Azzahra, N. (2024). Analisis Efisiensi Bank Syariah Pasca Transformasi Digital. *Jurnal Ekonomi Syariah Indonesia*, 9(1), 12–25.
- Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Keamanan Siber Indonesia 2022. BSSN.
- Budianto, E. W. H. (2023). Pemetaan Penelitian Risiko Operasional pada Industri Keuangan Syariah dan Konvensional: Studi Bibliometrik VOSviewer dan Literature Review. *Jurnal Ekonomi Islam*, 14(2), 158–174.
- Farid, M., & Azizah, W. (2021). Manajemen Risiko dalam Perbankan Syariah. *Muhasabatuna: Jurnal Akuntansi dan Keuangan Islam*, 3(2), 67–80.
- Ilyas, R. (2021). Peran Dewan Pengawas Syariah dalam Perbankan Syariah. *JPS (Jurnal Perbankan Syariah)*, 2(1), 42–53.
- Karyani, E., & Komarudin, M. (2023). Analisis risiko operasional perbankan syariah di Indonesia: Studi kasus Bank Syariah Indonesia. *Jurnal Keuangan dan Perbankan Syariah*, 9(2), 112–135.
- Laksana, R. D., Shaferi, I., & Naznii, H. (2023). The Effect of Operational Risks for Digital Banking Services at Banks. *Jurnal Manajemen Bisnis*, 14(2), 451–468. <https://doi.org/10.18196/mb.v14i2.19302>
- Luthfiatussa'dyah, N. (2023). Pengaruh Digitalisasi terhadap Risiko Operasional Bank Syariah di Indonesia. *Jurnal Perbankan Syariah*, 8(3), 144–159.

- Muhlis, M., & Sudirman, S. (2021). Tantangan dan Pengelolaan Sejumlah Risiko Perbankan Syariah Era Digital. *Al-Buhuts*, 17(2), 253–275.
- Muttaqin, Q., & Khasanah, U. (2023). Analisis kepatuhan prinsip syariah dalam layanan e-money perspektif Maqashid Syariah. *Jurnal Ilmiah Ekonomi Islam*, 9(2), 1806–1811.
- Nuzulia, & Kasanah, R. (2024). Islamic Banking Risk Management: Trends and Insights from a Bibliometric and SLR Approach. *Journal of Islamic Finance and Accounting*, 7(2), 115–128. <https://doi.org/10.22515/jifa.v7i2.9851>
- Oktaviani, S., & Basyariah, N. (2022). Analisis manajemen risiko layanan mobile banking pada bank syariah. *Jurnal Manajemen dan Penelitian Akuntansi*, 15(1), 29–34.
- Otoritas Jasa Keuangan (OJK). (2016). Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. OJK.
- Otoritas Jasa Keuangan (OJK). (2018). Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum. OJK.
- Otoritas Jasa Keuangan (OJK). (2020). Roadmap Pengembangan Perbankan Syariah Indonesia 2020-2025. OJK.
- Otoritas Jasa Keuangan (OJK). (2023). Statistik Perbankan Syariah Indonesia Desember 2022. OJK.
- Putri, R. R., & Filianti, D. (2021). Analisis Tingkat Pengungkapan Risiko Operasional Bank Umum Syariah Periode 2015-2019. *Jurnal Ekonomi Syariah Teori dan Terapan*, 8(5), 655–668. <https://doi.org/10.20473/vol8iss20215pp655-668>
- Sudarmanto, E., Yusuf, S. R., Yuliana, I., Wahyuni, N., & Zaki, A. (2024). Transformasi digital dalam keuangan Islam: Peluang dan tantangan. *Jurnal Ilmiah Ekonomi Islam*, 10(1), 645–655.
- Yudiana, Y., Hafidhuddin, D., & Ismal, R. (2018). Pengukuran Risiko Operasional pada Bank Syariah Indonesia (Studi Kasus Bank Syariah XYZ). *Jurnal Aplikasi Bisnis dan Manajemen*, 4(2), 179–190. <https://doi.org/10.17358/jabm.4.2.179>