**Maliki Interdisciplinary Journal (MIJ)** eISSN: 3024-8140
Volume 4, Issue June, 2026 pp. 62-71 http://urj.uin-malang.ac.id/index.php/mij/index

# *Human error* dan kelemahan kontrol internal sebagai pemicu risiko operasional: Studi kasus gangguan sistem Bank Syariah Indonesia

**Ahmad Rizqi Romadhoni**
*Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang*
*e-mail: ahmadrizqi8788@gmail.com*

***Kata Kunci:***
*Risiko operasional; human error; kontrol internal; perbankan syariah; gangguan sistem.*

**Keywords:**
Operational risk; human error; internal control; islamic banking; system malfunction.

***A B S T R A K***

*Penelitian ini bertujuan menganalisis peran human error dan kelemahan kontrol internal sebagai pemicu risiko operasional pada perbankan syariah melalui studi kasus gangguan sistem Bank Syariah Indonesia (BSI) pada Mei 2023. Metode yang digunakan adalah pendekatan kualitatif deskriptif berbasis studi kasus konseptual dengan teknik analisis literatur, telaah kronologi insiden, serta pengaitan temuan dengan teori risiko operasional dan pengendalian internal. Hasil penelitian menunjukkan bahwa risiko operasional tidak hanya disebabkan oleh faktor eksternal seperti serangan siber, tetapi juga dipengaruhi secara signifikan oleh faktor internal. Dugaan penggunaan sistem yang usang, lemahnya pembatasan akses, rendahnya kesadaran pegawai terhadap keamanan siber, serta lambatnya monitoring dan respons insiden menjadi indikator belum optimalnya sistem pengendalian internal. Kombinasi faktor tersebut memperbesar dampak gangguan hingga mengakibatkan terganggunya layanan ATM, mobile banking, dan transaksi kantor cabang secara nasional. Dalam konteks perbankan syariah, insiden operasional juga berdampak pada menurunnya kepercayaan nasabah yang merupakan fondasi utama industri. Oleh karena itu, bank syariah perlu memperkuat kontrol internal berbasis kerangka COSO, meningkatkan kapasitas sumber daya manusia melalui pelatihan keamanan siber, menerapkan audit teknologi informasi secara berkala, serta menyusun disaster recovery plan dan business continuity plan yang efektif guna memitigasi risiko operasional di era digital.*

**A B S T R A C T**

This study aims to analyze the role of human error and weak internal controls as triggers of operational risk in Islamic banking through a case study of the Bank Syariah Indonesia (BSI) system disruption in May 2023. The research employed a descriptive qualitative approach based on a conceptual case study using literature review, incident chronology analysis, and linkage of findings with operational risk and internal control theories. The results indicate that operational risk is not solely caused by external factors such as cyberattacks, but is also significantly influenced by internal factors. The suspected use of outdated systems, weak access controls, low employee cybersecurity awareness, and slow monitoring and incident response were identified as indicators of ineffective internal control systems. The combination of these factors amplified the disruption, causing failures in ATM services, mobile banking, and branch transactions nationwide. In the context of Islamic banking, operational incidents also reduce customer trust, which is the main foundation of the industry. Therefore, Islamic banks need to strengthen COSO-based internal controls, enhance human resource capacity through cybersecurity training, conduct regular information technology audits, and establish effective disaster recovery plans and business continuity plans to mitigate operational risk in the digital era.

## Pendahuluan

Transformasi digital dalam industri perbankan global telah menjadi fenomena yang tidak terhindarkan seiring dengan perkembangan teknologi informasi seperti *artificial intelligence, big data*, dan *cloud computing*. Digitalisasi ini memungkinkan bank meningkatkan efisiensi operasional, mempercepat layanan, serta memperluas akses ke nasabah secara lebih fleksibel dan *real-time* (Sudarmanto et al., 2024). Namun demikian, di balik berbagai manfaat tersebut, transformasi digital juga membawa konsekuensi berupa meningkatnya kompleksitas risiko, khususnya risiko operasional dan keamanan data. Ketergantungan yang tinggi terhadap infrastruktur digital membuka peluang terjadinya berbagai ancaman siber seperti *phishing, malware, ransomware*, hingga kebocoran data yang dapat mengganggu stabilitas operasional perbankan (Nabbila et al., 2023; Wang et al., 2024). Selain itu, perluasan penggunaan teknologi digital juga memperbesar "*attack surface*" atau titik rentan terhadap serangan, sehingga meningkatkan eksposur risiko operasional yang sebelumnya tidak terlalu signifikan dalam sistem perbankan konvensional (Wati, 2024) Dengan demikian, meskipun transformasi digital mampu mendorong efisiensi dan inovasi dalam industri perbankan, hal tersebut sekaligus menuntut adanya penguatan manajemen risiko dan sistem keamanan yang lebih adaptif guna menjaga keberlanjutan dan kepercayaan nasabah.

Dalam konteks perbankan syariah, aspek kepercayaan (*trust*), amanah, serta perlindungan terhadap data nasabah memiliki peran yang sangat fundamental dalam menjaga keberlangsungan industri. Hal ini disebabkan karena bank syariah tidak hanya berfungsi sebagai lembaga intermediasi keuangan, tetapi juga sebagai institusi yang beroperasi berdasarkan prinsip-prinsip syariah yang menekankan nilai kejujuran, tanggung jawab, dan transparansi (Arfan et al., 2016). Sejumlah penelitian menunjukkan bahwa kepercayaan nasabah dan persepsi terhadap keamanan sistem menjadi faktor utama dalam mendorong penggunaan layanan perbankan syariah, khususnya dalam layanan digital seperti mobile banking (Kamila & Rahayu, 2024). Selain itu, keamanan data nasabah menjadi elemen krusial karena adanya potensi risiko kebocoran data dan penyalahgunaan informasi yang dapat menurunkan tingkat kepercayaan masyarakat terhadap bank syariah (Nurhaliza et al., 2025). Penelitian lain juga menegaskan bahwa persepsi keamanan dan kepercayaan memiliki pengaruh signifikan terhadap loyalitas nasabah, sehingga gangguan terhadap kedua aspek tersebut dapat berdampak langsung terhadap reputasi dan keberlanjutan bank syariah (Lubis & Lubis, 2024) . Oleh karena itu, dalam kerangka tata kelola (*governance*), perlindungan data nasabah dan penguatan kepercayaan tidak hanya menjadi kewajiban normatif, tetapi juga merupakan strategi utama dalam menghadapi risiko operasional di era digital yang semakin kompleks.

Fenomena meningkatnya risiko operasional dan keamanan data dalam transformasi digital perbankan juga tercermin pada kasus gangguan layanan yang dialami oleh Bank Syariah Indonesia pada periode 8–11 Mei 2023. Gangguan ini menyebabkan berbagai layanan perbankan seperti ATM, *mobile banking*, hingga transaksi di kantor cabang tidak dapat diakses secara normal oleh nasabah di seluruh Indonesia. Berdasarkan kronologi yang dilaporkan oleh media teknologi, gangguan awalnya disampaikan sebagai proses maintenance sistem, namun dalam

perkembangannya muncul indikasi kuat adanya serangan siber berupa *ransomware* yang dilakukan oleh kelompok peretas LockBit 3.0 (Puspaningtyas, 2023). Serangan tersebut bahkan dikaitkan dengan ancaman penyebaran data nasabah dalam jumlah besar jika tuntutan tebusan tidak dipenuhi, yang menunjukkan tingginya risiko kebocoran data dalam sistem perbankan digital (Azarine, 2023). Selain itu, lamanya proses pemulihan layanan serta dugaan adanya celah dalam infrastruktur teknologi informasi, termasuk kemungkinan penggunaan sistem yang belum sepenuhnya mutakhir, semakin memperkuat indikasi bahwa kompleksitas sistem digital perbankan dapat menjadi titik lemah yang dimanfaatkan oleh pelaku kejahatan siber. Oleh karena itu, kasus gangguan layanan BSI ini tidak hanya mencerminkan risiko operasional semata, tetapi juga menjadi bukti nyata bahwa ancaman keamanan data dan serangan siber dapat berdampak langsung terhadap kepercayaan nasabah serta stabilitas industri perbankan, khususnya dalam konteks perbankan syariah yang sangat bergantung pada prinsip amanah dan kepercayaan.

Penelitian-penelitian sebelumnya dalam bidang keamanan siber pada sektor perbankan umumnya lebih berfokus pada aspek teknis seperti jenis dan mekanisme *cyber attack*, termasuk *ransomware*, *malware*, dan eksploitasi sistem. Hal ini juga terlihat dalam berbagai studi kasus pada Bank Syariah Indonesia yang mengalami serangan siber pada Mei 2023, di mana penelitian lebih banyak menyoroti karakteristik serangan ransomware serta dampaknya terhadap sistem dan kepercayaan nasabah (Putri & Yusuf, 2025; Rizal & Ardhian, 2023). Serangan tersebut bahkan menyebabkan gangguan layanan operasional serta kebocoran data dalam skala besar, sehingga menegaskan dominasi kajian pada aspek teknis serangan dan dampaknya (Apriyadi, 2025). Namun demikian, pendekatan tersebut cenderung mengabaikan faktor non-teknis, khususnya human error dan kelemahan kontrol internal organisasi. Beberapa penelitian memang mulai menyoroti pentingnya manajemen risiko dan respons organisasi terhadap serangan siber, tetapi masih terbatas pada aspek mitigasi pasca-insiden dan belum mengkaji secara mendalam bagaimana kesalahan manusia dan lemahnya kontrol internal berkontribusi sebagai akar penyebab terjadinya serangan (Hassandi et al., 2025; Timur et al., 2024). Padahal, dalam konteks perbankan digital, interaksi antara pengguna, prosedur internal, dan sistem teknologi menjadi faktor krusial dalam menentukan tingkat kerentanan terhadap serangan siber. Oleh karena itu, masih terdapat celah penelitian yang signifikan dalam mengkaji hubungan antara human error, kontrol internal, dan risiko keamanan siber secara terintegrasi, khususnya pada kasus perbankan seperti insiden BSI tahun 2023.

Metode yang digunakan adalah pendekatan kualitatif deskriptif berbasis studi kasus konseptual, dengan teknik analisis literatur, telaah kronologi insiden, dan pengaitan temuan kasus dengan teori risiko operasional serta pengendalian internal pada perbankan syariah. Pendekatan ini dinilai relevan karena studi literatur dan analisis konseptual terbukti efektif dalam menjelaskan dinamika risiko operasional, terutama pada kasus kegagalan sistem dan pengawasan internal di bank syariah.

## Pembahasan

### Risiko Operasional dan Kronologi Gangguan Sistem BSI

Risiko operasional merupakan salah satu jenis risiko utama dalam industri perbankan yang timbul akibat ketidakcukupan atau kegagalan proses internal, sumber daya manusia, sistem, maupun akibat peristiwa eksternal. Menurut *Basel Committee on Banking Supervision*, risiko operasional mencakup potensi kerugian yang disebabkan oleh kesalahan manusia (*human error*), kegagalan sistem (*system failure*), serta kelemahan dalam prosedur internal (Committee, 2011). Dalam konteks perbankan modern yang telah terdigitalisasi, ketergantungan tinggi terhadap sistem teknologi informasi menjadikan risiko ini semakin kompleks dan krusial untuk dikelola (MOOSA, 2007).

Dalam praktiknya, dua sumber utama risiko operasional yang sering terjadi adalah human error dan system failure. Human error merujuk pada kesalahan yang dilakukan oleh individu dalam menjalankan tugas operasional, seperti kesalahan konfigurasi sistem atau kelalaian dalam prosedur keamanan. Sementara itu, system failure berkaitan dengan gangguan pada infrastruktur teknologi, seperti server, jaringan, atau aplikasi yang mendukung layanan perbankan (Robertson, 2015). Penelitian menunjukkan bahwa kombinasi antara kesalahan manusia dan kelemahan sistem dapat memperbesar dampak risiko operasional, terutama dalam sistem yang terintegrasi secara digital (Aven, 2016).

Dalam konteks perbankan nasional, risiko operasional menjadi perhatian utama karena meningkatnya kompleksitas aktivitas dan ketergantungan terhadap teknologi, sehingga diperlukan sistem pengendalian yang efektif untuk meminimalkan potensi kerugian. Dalam konteks bank syariah, risiko operasional memiliki dimensi tambahan karena tidak hanya berkaitan dengan efisiensi dan keberlangsungan layanan, tetapi juga menyangkut kepatuhan terhadap prinsip-prinsip syariah (*sharia compliance*) (Arfan, 2015). Menurut penelitian oleh Hassan (Hassan, 2009). Temuan ini sejalan dengan penelitian Yuniarti (Fahmi et al., 2023) yang menegaskan bahwa dinamika risiko pada bank umum syariah sangat dipengaruhi oleh kualitas tata kelola, siklus bisnis, dan respons kelembagaan terhadap perubahan lingkungan eksternal. kegagalan operasional dalam bank syariah dapat berdampak pada reputasi dan kepercayaan nasabah, yang merupakan faktor kunci dalam sistem keuangan berbasis syariah. Oleh karena itu, manajemen risiko operasional dalam bank syariah harus mempertimbangkan aspek teknologi sekaligus kepatuhan syariah secara simultan.

Kasus gangguan layanan pada Bank Syariah Indonesia (BSI) pada periode 8–11 Mei 2023 menjadi contoh nyata dari manifestasi risiko operasional. Gangguan ini menyebabkan hampir seluruh layanan perbankan, termasuk ATM, mobile banking, dan transaksi teller, tidak dapat diakses oleh nasabah selama beberapa hari. Berdasarkan laporan dan analisis berbagai sumber, kronologi kejadian dimulai pada 8 Mei 2023 ketika sistem BSI mengalami gangguan signifikan yang diduga berawal dari masalah pada salah satu perangkat komputer di kantor cabang. Gangguan tersebut kemudian menyebar ke sistem pusat akibat lemahnya kontrol internal dan kurangnya segmentasi sistem, sehingga mengakibatkan kegagalan sistem secara luas.

Selama periode 8 hingga 11 Mei 2023, layanan BSI mengalami kelumpuhan total atau sebagian besar tidak berfungsi, yang berdampak pada aktivitas transaksi nasabah di seluruh Indonesia. Insiden ini kemudian dikonfirmasi sebagai bagian dari serangan siber jenis ransomware, yang semakin memperparah kondisi sistem (Puspaningtyas, 2023). Kejadian ini menunjukkan bagaimana titik awal yang tampak sederhana, seperti gangguan pada perangkat cabang, dapat berkembang menjadi krisis sistemik apabila tidak didukung oleh sistem pengendalian internal yang kuat dan mekanisme deteksi dini yang efektif.

Kasus BSI tersebut menegaskan bahwa risiko operasional dalam perbankan tidak hanya bersumber dari faktor eksternal seperti serangan siber, tetapi juga dari kelemahan internal yang mencakup human error dan kegagalan sistem. Oleh karena itu, penting bagi institusi perbankan untuk memperkuat manajemen risiko operasional melalui peningkatan kualitas sumber daya manusia, penguatan sistem teknologi, serta implementasi kontrol internal yang komprehensif dan adaptif terhadap perkembangan ancaman digital.

***Human Error* dan Kelemahan Kontrol Internal sebagai Akar Masalah**

Dalam manajemen risiko operasional, *human error* dan kelemahan kontrol internal merupakan faktor dominan yang sering menjadi akar terjadinya gangguan sistem dan kerugian operasional. Berdasarkan kerangka *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*, sistem pengendalian internal terdiri dari lima komponen utama, yaitu lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan (monitoring) (*COSO Internal Control – Integrated Framework ( 2013 )*, 2013). Kelemahan pada salah satu atau beberapa komponen tersebut dapat membuka celah terhadap terjadinya kesalahan manusia maupun eksploitasi oleh pihak eksternal.

Dalam kasus gangguan sistem Bank Syariah Indonesia (BSI) pada Mei 2023, salah satu faktor yang diduga berkontribusi adalah penggunaan workstation atau perangkat kerja yang sudah usang (*outdated system*). Sistem yang tidak diperbarui secara berkala rentan terhadap kerentanan keamanan (*vulnerabilities*) yang dapat dimanfaatkan oleh pelaku serangan siber (Singer & Friedman, 2014). Kondisi ini menunjukkan adanya kelemahan dalam penerapan patch management, yaitu proses pembaruan sistem untuk menutup celah keamanan. Penelitian menunjukkan bahwa kegagalan dalam *patch management* merupakan salah satu penyebab utama terjadinya insiden keamanan informasi di sektor keuangan (Fund et al., 2017)

Selain aspek teknologi, faktor sumber daya manusia juga memainkan peran penting. Rendahnya tingkat kesadaran (*awareness*) pegawai terhadap keamanan siber dapat meningkatkan risiko phishing dan penyalahgunaan kredensial (*credential misuse*). Menurut studi oleh Parsons et al. (Parsons et al., 2014). perilaku pengguna merupakan salah satu titik terlemah dalam sistem keamanan informasi, di mana kurangnya pelatihan dan pemahaman terhadap ancaman digital dapat menyebabkan kebocoran akses yang berdampak luas. Dalam konteks ini, human error tidak hanya berupa kesalahan teknis, tetapi juga mencakup kelalaian dalam menjaga keamanan informasi. Penelitian pada bank syariah di Indonesia juga menunjukkan bahwa risiko operasional

sangat erat kaitannya dengan faktor human error dan kelemahan sistem informasi, sehingga diperlukan peningkatan kualitas SDM dan sistem pengawasan internal (Putra & Hasibuan, 2024).

Lebih lanjut, kelemahan dalam pembatasan akses (*access control*) juga menjadi indikator lemahnya kontrol internal. Prinsip least privilege yang seharusnya diterapkan—yaitu memberikan akses minimum sesuai kebutuhan kerja—sering kali tidak dijalankan secara optimal. Hal ini dapat menyebabkan penyebaran gangguan dari satu titik ke seluruh sistem, sebagaimana terlihat pada kasus BSI. Penelitian oleh Ahmad (Ahmad et al., 2014). menegaskan bahwa kontrol akses yang tidak memadai dapat memperbesar dampak serangan siber karena memungkinkan pergerakan lateral (*lateral movement*) dalam jaringan.

Kelemahan lain yang krusial adalah lambatnya proses monitoring dan incident response, termasuk dalam tahap pemulihan (*recovery*). Dalam kerangka COSO, aktivitas pemantauan berfungsi untuk memastikan bahwa sistem pengendalian internal berjalan secara efektif dan mampu mendeteksi anomali secara dini. Namun, dalam kasus BSI, proses pemulihan yang memakan waktu beberapa hari menunjukkan bahwa sistem deteksi dan respons belum optimal. Menurut penelitian oleh Herath dan Herath (2014), organisasi yang tidak memiliki sistem pemantauan yang kuat cenderung mengalami keterlambatan dalam merespons insiden, yang pada akhirnya memperbesar kerugian operasional.

Selain itu, prinsip dual control atau pemisahan fungsi (*segregation of duties*) juga tampaknya belum diterapkan secara maksimal. Prinsip ini bertujuan untuk mencegah terjadinya kesalahan atau kecurangan dengan memastikan bahwa tidak ada satu individu yang memiliki kendali penuh atas suatu proses. Kegagalan dalam menerapkan dual control dapat meningkatkan risiko kesalahan manusia yang tidak terdeteksi serta memperbesar peluang terjadinya pelanggaran keamanan (Gramling et al., 2004). Selain itu, penerapan sistem pengendalian risiko yang tidak optimal dapat meningkatkan potensi kerugian akibat fraud maupun kesalahan operasional, sebagaimana ditemukan pada studi perbankan nasional yang menekankan pentingnya kontrol internal dalam memitigasi risiko (Yuniarti & Sunarjo, 2017)

Dengan demikian, kasus gangguan sistem BSI mencerminkan bagaimana kombinasi antara human error dan kelemahan kontrol internal dapat menjadi akar masalah dalam risiko operasional. Kegagalan dalam memperbarui sistem, rendahnya kesadaran pegawai terhadap keamanan siber, lemahnya pembatasan akses, serta tidak optimalnya fungsi pemantauan dan dual control menunjukkan bahwa pengendalian internal belum berjalan secara efektif. Argumen tersebut diperkuat oleh penelitian Eka Wahyu Hestya Budianto (Budianto, 2023) yang menunjukkan bahwa pengendalian internal, system failure, dan human factor merupakan klaster dominan dalam kajian risiko operasional lembaga keuangan syariah, sehingga kelemahan pada aspek tersebut berpotensi memperbesar eskalasi gangguan layanan digital. Oleh karena itu, penguatan sistem kontrol internal berbasis kerangka COSO menjadi langkah penting untuk memitigasi risiko operasional di era digital, khususnya dalam industri perbankan yang sangat bergantung pada teknologi informasi.

**Strategi Mitigasi Risiko Operasional pada Perbankan Syariah**

Mitigasi risiko operasional dalam industri perbankan, khususnya perbankan syariah, memerlukan pendekatan yang komprehensif dengan mengintegrasikan aspek teknologi, sumber daya manusia, serta penguatan tata kelola berbasis prinsip syariah. Mengacu pada kerangka *Committee of Sponsoring Organizations of the Treadway Commission* dan *Basel Committee on Banking Supervision*, strategi mitigasi risiko operasional harus mencakup penguatan kontrol internal, peningkatan kesadaran keamanan, serta kesiapan menghadapi gangguan sistem melalui perencanaan keberlangsungan bisnis.

Langkah pertama yang krusial adalah penguatan sistem pengendalian internal (*internal control*). Hal ini mencakup perbaikan pada seluruh komponen COSO, termasuk aktivitas pengendalian, pemantauan, dan sistem informasi. Implementasi kontrol internal yang kuat terbukti mampu mengurangi probabilitas terjadinya kesalahan operasional maupun serangan siber (Aven, 2016). Hal ini sejalan dengan penelitian Mardiana (Mardiana, 2018) menegaskan bahwa efektivitas manajemen risiko dan penguatan pengendalian internal berkontribusi signifikan terhadap peningkatan kualitas kinerja perbankan syariah. Dalam konteks ini, bank perlu memastikan adanya kebijakan yang jelas terkait manajemen risiko, termasuk standar operasional prosedur (SOP) yang adaptif terhadap perkembangan ancaman digital.

Selain itu, peningkatan kapasitas sumber daya manusia melalui training cyber awareness menjadi strategi penting dalam mengurangi risiko human error. Pelatihan yang berkelanjutan dapat meningkatkan kemampuan pegawai dalam mengenali ancaman seperti phishing, malware, dan penyalahgunaan kredensial. Penelitian oleh Parsons (Parsons et al., 2014), menunjukkan bahwa program kesadaran keamanan informasi secara signifikan meningkatkan perilaku aman pengguna dalam organisasi, sehingga dapat meminimalkan potensi kebocoran sistem.

Dari sisi teknologi, penerapan endpoint security di seluruh cabang bank merupakan langkah strategis untuk melindungi perangkat pengguna (workstation) dari ancaman siber. Sistem ini mencakup penggunaan antivirus terkini, endpoint detection and response (EDR), serta pembaruan sistem secara berkala (*patch management*). Menurut Kopp (Fund et al., 2017), perlindungan pada level endpoint menjadi salah satu lini pertahanan utama dalam mencegah penyebaran serangan siber di sektor keuangan.

Selanjutnya, kesiapan menghadapi gangguan sistem perlu diperkuat melalui implementasi *disaster recovery plan (DRP)* dan *business continuity plan (BCP)*. DRP berfungsi untuk memulihkan sistem setelah terjadi gangguan, sementara BCP memastikan bahwa operasional bisnis tetap berjalan dalam kondisi krisis. Studi oleh Herbane (Herbane, 2010), menegaskan bahwa organisasi yang memiliki perencanaan keberlangsungan bisnis yang matang mampu meminimalkan dampak gangguan operasional dan mempercepat proses pemulihan layanan.

Audit teknologi informasi (IT audit) secara berkala juga menjadi elemen penting dalam mitigasi risiko operasional. Audit ini bertujuan untuk mengevaluasi efektivitas kontrol internal, mengidentifikasi celah keamanan, serta memastikan kepatuhan terhadap regulasi dan standar industri. Menurut Gramling et al. (2004), fungsi audit

internal memiliki peran strategis dalam meningkatkan kualitas tata kelola dan pengendalian risiko organisasi.

Dalam aspek operasional sehari-hari, penerapan prinsip *maker-checker* atau *dual control* menjadi mekanisme penting untuk mengurangi risiko kesalahan dan kecurangan. Prinsip ini memastikan bahwa setiap transaksi atau keputusan penting harus melalui proses verifikasi oleh pihak lain, sehingga dapat meminimalkan potensi human error maupun penyalahgunaan wewenang (*COSO Internal Control – Integrated Framework ( 2013 )*, 2013).

Lebih lanjut, dalam perspektif perbankan syariah, strategi mitigasi risiko operasional tidak hanya berorientasi pada efisiensi dan keamanan, tetapi juga harus berlandaskan prinsip amanah dan perlindungan nasabah. Konsep amanah menekankan tanggung jawab moral dan profesional dalam menjaga kepercayaan nasabah, termasuk dalam menjaga keamanan data dan dana. Menurut *Islamic Financial Services Board*, manajemen risiko dalam perbankan syariah harus mengedepankan transparansi, keadilan, dan perlindungan terhadap kepentingan nasabah (Rahman & Nasution, 2012). Dengan demikian, kegagalan dalam mengelola risiko operasional tidak hanya berdampak pada kerugian finansial, tetapi juga pada penurunan kepercayaan yang bertentangan dengan prinsip dasar syariah.

Secara keseluruhan, strategi mitigasi risiko operasional pada perbankan syariah harus dilakukan secara terintegrasi melalui penguatan kontrol internal, peningkatan kesadaran pegawai, perlindungan sistem teknologi, serta kesiapan menghadapi krisis. Pendekatan ini tidak hanya mampu mengurangi potensi gangguan operasional, tetapi juga memperkuat kepercayaan nasabah sebagai fondasi utama dalam industri perbankan syariah.

## Kesimpulan dan Saran

Penelitian ini menunjukkan bahwa risiko operasional dalam perbankan syariah tidak hanya dipicu oleh faktor eksternal seperti serangan siber, tetapi juga sangat dipengaruhi oleh faktor internal, khususnya *human error* dan kelemahan kontrol internal. Studi kasus gangguan sistem Bank Syariah Indonesia (BSI) pada Mei 2023 membuktikan bahwa kesalahan manusia, kurangnya pengawasan, serta lemahnya sistem pengendalian dapat memperbesar dampak gangguan hingga berkembang menjadi krisis sistemik yang mengganggu layanan secara luas.

Selain itu, dalam konteks perbankan syariah, gangguan operasional tidak hanya berdampak pada aspek teknis, tetapi juga berimplikasi pada menurunnya kepercayaan nasabah yang menjadi fondasi utama industri. Hal ini menegaskan bahwa pengelolaan risiko operasional harus dilakukan secara menyeluruh dengan mengintegrasikan aspek teknologi, sumber daya manusia, dan tata kelola internal. Oleh karena itu, bank syariah perlu memperkuat sistem kontrol internal, meningkatkan kualitas dan kesadaran SDM terhadap risiko, serta mengembangkan sistem keamanan yang adaptif terhadap ancaman digital.

## Daftar Pustaka


Ahmad, A., Maynard, S., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*. https://doi.org/10.1007/s10845-012-0683-0

Apriyadi, C. (2025). *Sentiment Analysis of Cyber Attacks in Bank Syariah Indonesia Using SVM and Indobert Method*. *6*(2), 819–838.

Arfan, A. (2015). Lima prinsip istinbat kontemporer sebagai konklusi pembaharuan dalam teori penetapan hukum Islam. *Al-Manahij*, *9*(2), 223–236. https://repository.uin-malang.ac.id/609/

Arfan, A., Saifullah, S., & Fakhruddin, F. (2016). Implementasi prinsip bagi hasil dan manajemen risiko dalam produk-produk pembiayaan perbankan syariah di Kota Malang. *INFERENSI: Jurnal Penelitian Sosial Keagamaan*, *10*(1), 213–238. https://repository.uin-malang.ac.id/622/

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Budianto, E. W. H. (2023). *Pemetaan Penelitian Risiko Operasional Pada Industri Keuangan Syariah Dan Konvensional: Studi Bibliometrik Vosviewer Dan Literature Review Eka*. *14*(November), 158–174.

Committee, B. (2011). *Principles for the Sound Management of Operational Risk*. (June).

*COSO Internal Control – Integrated Framework ( 2013 )*. (2013). 1–8.

Fahmi, M. M., Wahyuni, N., Hidayah, Y., & Putra, S. (2023). *The Business Cycle as a Moderator of Financing for Financing Risk of Islamic Commercial Banks in Indonesia Siklus Bisnis sebagai Pemoderator Pembiayaan terhadap Risiko Pembiayaan Bank Umum Syariah di Indonesia*. *10*(1), 27–40. https://doi.org/10.20473/vol10iss20231pp27-40

Fund, E., Fund, L., & Fund, C. (2017). Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers*, *17*, 1. https://doi.org/10.5089/9781484313787.001

Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature*, *23*, 194–244.

Hassan, A. (2009). Risk management practices of Islamic banks of Brunei Darussalam. *The Journal of Risk Finance*, *10*(1), 23–37. https://doi.org/10.1108/15265940910924472

Hassandi, I., Yossinomita, & Pangestu, M. G. (2025). *Identifikasi Resiko Dalam Era Digital: Studi Kasus Resiko Teknologi Pada PT Bank Syariah Indonesia*. *5*, 996–1004.

Herbane, B. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers. *Business History*, *52*, 978–1002. https://doi.org/10.1080/00076791.2010.511185

Kamila, T. P., & Rahayu, Y. S. (2024). *Pengaruh Keamanan,Kepercayaan,Dan Risiko Terhadap Penggunaan Layanan Mobile Banking Pada Mahasiswa Di Kota Malang*. *5*, 49–61.

Lubis, Z. A., & Lubis, F. A. (2024). *Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia*. *5*(10), 4215–4230.

Mardiana. (2018). *Pengaruh Manajemen Risiko Terhadap Kinerja Keuangan (Study Pada Perbankan Syariah Yang Terdaftar Di Bei)*. 151–166. https://repository.uin-malang.ac.id/7242/

MOOSA, I. A. (2007). *Operational Risk: A Survey*. (4).

Nabbila, F. L., Andriani, Putri, D. F., & Sari, W. R. (2023). Analisis Manajemen Risiko Operasional Pada Bank Syariah Indonesia (BSI) Pasca Merger. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 91–99.

Nurhaliza, S., Ningsih, A. S., Ismaini, D., & Nurbaiti. (2025). *Keamanan data nasabah bank syariah*. *2*(1), 651–662.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Putra, R., & Hasibuan, A. (2024). *Manajemen Risiko Operasional pada Bank Syariah Indonesia ( BSI ) KC Bengkulu*. *3*(4), 879–891.

Putri, A. A., & Yusuf, H. (2025). *Ransomware Di Sektor Keuangan : Studi Kasus Serangan Terhadap Bsi Pada Tahun 2023 Ransomware In The Financial Sector : A Case Study Of Attacks On Bsi In 2023*. 15649–15656.

Rahman, H. E. A., & Nasution, H. E. D. (2012). *Guiding Principles On Liquidity Risk Management For Institutions [ Excluding Islamic Insurance ( Tak Ā Ful ) Institutions And Islamic Collective Investment Schemes ]*. (March).

Rizal, I., & Ardhian, N. (2023). *Dampak serangan siber dan kebocoran data pada perbankan syariah terhadap tingkat kepercayaan nasabah*. *1*(3), 351–359.

Robertson, D. (2015). *Managing Operational Risk*.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know®What Everyone Needs to Know®*. https://doi.org/10.1093/wentk/9780199918096.001.0001

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. https://repository.uin-malang.ac.id/19648/

Timur, Y. P., Ridiwan, A. A., Fikriyah, K., Canggih, C., & Nurafini, F. (2024). *How should Bank Syariah Indonesia respond to cyber-attacks? Churn, sentiments, and emotions analysis with machine learning*. *10*(1), 439–470.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, *147*, 104051. https://doi.org/10.1016/j.cose.2024.104051

Wati, M. (2024). *Digital Transformation in Banking: Shielding Against Cyber Threats and Operational Risks*. *1*(3), 4–8.

Yuniarti, S., & Sunarjo. (2017). *Sistem Pengendalian Risiko Operasional Pada Bank Perkreditan Rakyat Dengan Pendekatan Indikator Dasar Dasar*. *21*(040), 96–104.