**Maliki Interdisciplinary Journal (MIJ)** eISSN: 3024-8140
Volume 3, Issue Mei, 2025 pp. 771-775 http://urj.uin-malang.ac.id/index.php/mij/index

# Implementasi Manajemen Risiko Teknologi Informasi dalam Proses Transformasi Digital Bank Syariah Indonesia

**Zulaikhatul Khuluddiyah**
*Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang*
*e-mail: zulaikhatulkhuluddiyah12@gmail.com*

***Kata Kunci:***
*Transformasi; Risiko; Teknologi; Bank Syariah; Keamanan.*

**Keywords:**
Transformation; Risk; Technology; Islamic Bank; Security.

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

*Transformasi digital di sektor perbankan syariah menghadirkan tantangan baru dalam pengelolaan risiko teknologi informasi. Bank Syariah Indonesia (BSI) sebagai institusi syariah terbesar di Indonesia mengalami insiden kebocoran data pada tahun 2023 akibat serangan ransomware, yang menyoroti pentingnya sistem keamanan TI yang tangguh dan terstruktur. Penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko teknologi informasi di BSI dalam menghadapi insiden tersebut. Metode yang digunakan adalah studi pustaka kualitatif dengan mengkaji literatur terkait manajemen risiko TI, keamanan siber, serta studi kasus kebocoran data di sektor perbankan syariah. Hasil kajian menunjukkan bahwa BSI telah memperkuat struktur organisasi, membentuk unit-unit strategis seperti CISO dan SOC, serta menerapkan pengujian sistem yang komprehensif. Selain itu, tata kelola operasional dan kolaborasi dengan pihak ketiga juga dilakukan berdasarkan prinsip kepatuhan dan perlindungan data. Penelitian ini merekomendasikan peningkatan literasi keamanan siber, evaluasi berkala teknologi, serta sinergi antarlembaga sebagai langkah strategis untuk memperkuat ketahanan digital bank syariah ke depan.*

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

Digital transformation in the Islamic banking sector brings new challenges in managing information technology (IT) risks. Bank Syariah Indonesia (BSI), the largest Islamic bank in Indonesia, experienced a major data breach in 2023 due to a ransomware attack, highlighting the urgency of robust and structured IT security systems. This study aims to analyze the implementation of IT risk management at BSI in response to the incident. The method used is qualitative literature review by examining references on IT risk management, cybersecurity, and case studies of data breaches in Islamic banking. The results show that BSI has strengthened its organizational structure, established strategic units such as the CISO and SOC, and implemented comprehensive system testing. In addition, operational governance and third-party collaborations are managed based on compliance principles and data protection. This study recommends enhancing cybersecurity awareness, conducting regular technology evaluations, and fostering inter-institutional synergy as strategic measures to strengthen the digital resilience of Islamic banking in the future.

## Pendahuluan

Dalam perkembangan era digital saat ini, industri perbankan, termasuk bank syariah, menghadapi tantangan baru dalam mengelola risiko teknologi informasi. Peran teknologi sangat krusial dalam mendukung layanan operasional, mulai dari sistem perbankan daring hingga aplikasi berbasis seluler. Kemajuan teknologi juga meningkatkan potensi risiko, terutama terkait dengan keamanan, privasi, dan integritas data nasabah (Faizal et al., 2023). Perbankan syariah perlu terus mengembangkan layanannya dengan menghadirkan keunikan nilai (value proposition) yang

membedakannya dari perbankan konvensional, serta merumuskan kebijakan-kebijakan khusus yang mendukung pemanfaatan teknologi informasi secara inovatif (Widiya & Safitri, 2022). Selain itu, penting bagi bank syariah untuk memastikan bahwa kualitas layanan digital yang diberikan selaras dengan nilai-nilai ekonomi Islam dan hukum syariah yang menjadi landasan operasionalnya (Kartika & Segaf, 2022). Pengamanan sistem teknologi informasi merupakan bagian penting dari manajemen risiko operasional dalam perbankan. Sistem ini memegang peran kunci dalam menjalankan aktivitas perbankan, sehingga pengamanannya sangat krusial untuk meminimalkan risiko operasional. Bank perlu melakukan uji penetrasi secara berkala guna memastikan bahwa sistem tetap aman dan memiliki kemampuan mendeteksi serta mengatasi potensi serangan. Hal ini membantu bank memahami tingkat kerentanan sistem dan mengambil tindakan yang tepat sebelum terjadi insiden nyata (Budianto, 2023).

Salah satu contoh nyata dari risiko tersebut adalah insiden kebocoran data yang dialami oleh Bank Syariah Indonesia (BSI) pada tahun 2023. Pada Mei 2023, BSI mengalami gangguan akses sistem yang diduga sebagai dampak dari serangan ransomware oleh kelompok peretas bernama LockBit 3.0. Serangan ini memungkinkan pihak peretas memperoleh berbagai data penting nasabah, seperti nama, konfigurasi host, informasi domain, pengaturan local drive, sistem berbagi jarak jauh, hingga perangkat penyimpanan eksternal. Meskipun BSI merupakan bank syariah terbesar di Indonesia, kasus ini menunjukkan bahwa institusi syariah tidak terlepas dari risiko yang sama seperti bank konvensional, terutama dalam hal keamanan data pribadi (Antoine et al., 2025). Insiden pembobolan data yang menimpa Bank Syariah Indonesia membawa dampak yang besar, tidak hanya terhadap kondisi keuangan dan reputasi lembaga, tetapi juga memperbesar potensi kerentanan bagi nasabah terhadap berbagai modus penipuan dan pencurian identitas. Kejadian ini mempertegas kompleksitas tantangan dalam bidang keamanan siber yang harus ditangani secara serius. Di dalamnya termasuk perlindungan terhadap data pribadi dan informasi keuangan, peningkatan sistem keamanan secara berkala, serta upaya berkelanjutan untuk menumbuhkan kesadaran akan pentingnya menjaga keamanan siber di kalangan seluruh pemangku kepentingan (Hutagalung et al., 2024).

Berdasarkan berbagai temuan yang telah dijelaskan sebelumnya, jelas bahwa analisis dan manajemen risiko memiliki peran yang sangat penting bagi institusi perbankan, termasuk bank syariah, dalam menghadapi tantangan yang muncul akibat pemanfaatan teknologi informasi. Dengan melakukan kajian mendalam dan menerapkan pendekatan yang tepat dalam pengelolaan risiko, bank dapat memitigasi potensi ancaman secara efektif, menjaga kelancaran operasional, dan memastikan perlindungan optimal terhadap data nasabah. Kasus kebocoran data yang menimpa Bank Syariah Indonesia pada tahun 2023 menegaskan bahwa manajemen risiko bukan sekadar pelengkap, melainkan kebutuhan strategis untuk menghadapi serangan siber yang semakin canggih. Risiko seperti kegagalan sistem, serangan ransomware, hingga akses ilegal terhadap data sensitif dapat menyebabkan gangguan besar terhadap layanan perbankan dan menimbulkan kerugian baik dari sisi keuangan maupun kepercayaan nasabah. Oleh karena itu, penerapan manajemen risiko yang terstruktur dan menyeluruh sangat diperlukan guna memastikan keberlangsungan operasional sistem

digital dan meminimalkan dampak negatif yang mungkin timbul akibat kebocoran data atau insiden keamanan lainnya (Putra & Hendrawan, 2024).

Tujuan dari penelitian ini adalah untuk mengetahui bagaimana penerapan manajemen risiko teknologi informasi di Bank Syariah Indonesia, khususnya dalam merespons insiden kebocoran data yang terjadi pada tahun 2023. Penelitian ini dilakukan dengan menggunakan metode kualitatif melalui studi pustaka, yang melibatkan penelusuran dan analisis berbagai sumber literatur terkait manajemen risiko TI, keamanan siber, serta studi kasus serangan siber pada sektor perbankan syariah. Melalui pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai efektivitas penerapan manajemen risiko TI di BSI, serta rekomendasi perbaikan untuk menghadapi ancaman siber di masa mendatang.

## Pembahasan

### Penguatan Struktur Organisasi dalam Pengelolaan Risiko TI

Menurut Laporan Tahunan BSI (2024), BSI memiliki Komite Pengarah Teknologi Informasi (IT Steering Committee) yang berperan dalam mengarahkan kebijakan strategis TI agar sejalan dengan rencana bisnis bank. Selain itu, bank juga menetapkan rencana strategis TI yang terintegrasi dengan visi dan misi institusi. Guna memastikan pengamanan terhadap penerapan teknologi informasi, BSI membentuk Group Chief Information Security Officer (CISO) yang bertanggung jawab penuh atas keamanan sistem, termasuk pada layanan digital banking.Selanjutnya, BSI membentuk unit kerja seperti IT & Product Delivery Risk yang fokus pada pelaksanaan *risk assessment* sejak tahap perencanaan hingga pengawasan pasca peluncuran sistem. Untuk memperkuat fungsi pengawasan, juga dibentuk Internal Audit IT, serta Security Operation Center (SOC) yang bekerja 24/7 untuk memantau potensi serangan siber. BSI juga memiliki Security Incident Response Team untuk menangani insiden keamanan siber, serta Senior Operational Risk Officer yang langsung disupervisi oleh Direktur IT.Struktur ini mencerminkan bahwa BSI telah mengambil pendekatan proaktif dan terstruktur dalam membangun fondasi tata kelola risiko TI yang kuat selama proses transformasi digital.

### Strategi Keamanan Siber dalam Menangkal Ancaman Digital

Sebagai respons terhadap meningkatnya serangan siber dan kompleksitas teknologi, BSI memperkuat sistem keamanan informasi dan infrastruktur digitalnya melalui serangkaian mekanisme perlindungan dan pengujian sistem. Strategi ini dilakukan melalui identifikasi aset teknologi, analisis ancaman dan kerentanan, serta pemantauan insiden secara real time.BSI secara berkala melaksanakan penetration testing oleh pihak independen guna menguji ketahanan sistem terhadap serangan siber. Selain itu, dilakukan standarisasi perangkat jaringan, pengelolaan hak akses, serta pengujian menyeluruh pada setiap aplikasi atau layanan digital yang dikembangkan. Proses ini mencakup System Integration Test (SIT), User Acceptance Test (UAT), serta evaluasi akhir oleh Release Control Board (RCB) untuk memastikan kesiapan sistem dari segi infrastruktur, keamanan, dan proses bisnis.

Dalam hal keamanan jaringan, BSI juga menguji keandalan perangkat keras dan perangkat lunak, termasuk infrastruktur pendukung seperti cadangan daya, server, dan

sistem enkripsi. Langkah-langkah ini menunjukkan komitmen BSI dalam membangun sistem TI yang tidak hanya efisien, namun juga tangguh terhadap potensi gangguan dan ancaman eksternal.

**Tata Kelola Operasional dan Mitigasi Risiko TI Berbasis Kepatuhan dan Kolaborasi**

Penerapan manajemen risiko TI oleh BSI juga menyentuh aspek pengelolaan operasional sehari-hari. Hal ini mencakup pengelolaan pusat data (data center), manajemen kapasitas dan konfigurasi perangkat, serta pengelolaan perubahan sistem (change management). BSI secara konsisten melaksanakan risk assessment dalam proses pengadaan dan pengembangan teknologi, dimulai dari perencanaan hingga pengawasan pasca implementasi.Dalam kolaborasi eksternal, BSI menetapkan syarat ketat dalam kerja sama dengan pihak ketiga untuk menjamin keamanan dan kerahasiaan data. Hal ini penting terutama dalam penggunaan layanan berbasis cloud dan outsourcing TI. Setiap kerja sama harus memenuhi standar pengamanan data, baik dalam kondisi normal maupun ketika terjadi insiden.Selain itu, layanan digital yang dikembangkan oleh BSI dirancang agar sesuai dengan prinsip keamanan transaksi elektronik dan perlindungan data nasabah, termasuk aspek kerahasiaan, akurasi, dan validitas akses. Komitmen ini menunjukkan bahwa transformasi digital di BSI dijalankan dengan mengedepankan prinsip kehati-hatian dan kepatuhan terhadap regulasi syariah serta otoritas perbankan nasional (Astuti, 2024).

## Kesimpulan dan Saran

Transformasi digital yang dijalankan oleh Bank Syariah Indonesia (BSI) menuntut penerapan manajemen risiko teknologi informasi yang menyeluruh dan terintegrasi. Insiden kebocoran data pada tahun 2023 menjadi pelajaran berharga mengenai pentingnya sistem keamanan TI yang kuat serta perlunya pendekatan proaktif dalam mengidentifikasi, mengevaluasi, dan mengatasi berbagai risiko digital. BSI telah menunjukkan keseriusan dalam hal ini melalui penguatan struktur tata kelola, pembentukan unit-unit strategis seperti CISO, SOC, dan tim respons insiden, serta pelaksanaan pengujian sistem yang konsisten dan terstandar. Upaya tersebut mencerminkan komitmen BSI dalam menjaga integritas, kerahasiaan, dan ketersediaan data nasabah di tengah tantangan era digital.

Pada sisi operasional, BSI telah menerapkan prinsip pengelolaan teknologi informasi yang mengedepankan kepatuhan terhadap regulasi, perlindungan data, dan selektivitas kerja sama dengan pihak ketiga. Tata kelola ini tidak hanya menjamin keberlangsungan layanan digital secara optimal, tetapi juga memperkuat kepercayaan nasabah terhadap bank syariah yang berbasis nilai-nilai Islam.Guna memperkuat pencapaian tersebut, disarankan agar BSI terus meningkatkan literasi keamanan siber di seluruh lini organisasi, memperluas program pelatihan karyawan, serta mengembangkan sistem pemantauan yang adaptif terhadap ancaman-ancaman baru. Evaluasi berkala terhadap teknologi dan kebijakan yang digunakan juga penting untuk memastikan kesiapan menghadapi dinamika lanskap digital. Di samping itu, membangun sinergi dengan regulator, institusi teknologi, serta komunitas keamanan siber akan semakin

memperkuat posisi BSI sebagai pelopor transformasi digital dalam industri perbankan syariah yang aman, terpercaya, dan relevan secara global.

## Daftar Pustaka

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 316–327.

ASTUTI, A. N. I. (2024). *PENGARUH CITRA PERUSAHAAN DAN PERLINDUNGAN NASABAH TERHADAP KEPERCAYAAN PENGGUNA MOBILE BANKING (Studi kasus pada pengguna BRImo dan BSI Mobile di Kabupaten Pemalang)*.

BSI. (2024). *Laporan tahunan 2023: Ekspansi dan akselerasi bisnis untuk pertumbuhan berkelanjutan*. https://www.bankbsi.co.id/

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. http://repository.uin-malang.ac.id/17264/

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis risiko teknologi informasi pada bank syariah: Identifikasi ancaman dan tantangan terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100.

Hutagalung, A. M. C., Marendra, N. R., & Hosnah, A. U. (2024). Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *2*(1), 156–165.

Kartika, G., & Segaf, S. (2022). Kombinasi peran model TAM dan CARTER terhadap optimalisasi kepuasan nasabah mobile syariah banking di masa pandemi Covid-19. *Jurnal Manajerial*, *9*(02), 152–167. http://repository.uin-malang.ac.id/17283/

Putra, I. P. A. S., & Hendrawan, I. K. R. (2024). Analisis Manajemen Risiko SIMRS pada Rumah Sakit Ganesha Menggunakan ISO 31000. *Jurnal Teknologi Dan Informasi*, *14*(1), 88–98.

Widiya, T. N., & Safitri, R. (2022). … Layanan Digital Banking: the Effect of Sharia Compliance on Customer Satisfaction At Bsi Kc Malang Soetta Mediated By Digital …. *NISBAH: Jurnal Perbanka Syariah*, *96*(2), 93–102. http://repository.uin-malang.ac.id/15052/