Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi (JEBMAK)
p–ISSN: 2964-8858 e-ISSN: 2963-3087
Vol. 5, No. 2, Juli 2026

Optimalisasi Manajemen Risiko Siber Pada Perbankan Syariah di Indonesia dalam Menghadapi Era Fintech

Siti Nurul Aisyah[1] Fitri Wulandari[2] Tursina[3], Joni Hendra K[4]
[1,2,3,4] Program Studi Perbankan Syariah Jurusan Syariah dan Ekonomi Islam,
Sekolah Tinggi Agama Islam Negeri Bengkalis, Indonesia
Email: sitinrlaissyah@gmail.com[1.] fwulandariii@gmail.com[2.] Tursina03062005@gmail.com
joniqizel77@gmail.com[4]

Abstrak

Transformasi digital yang didorong oleh perkembangan financial technology (fintech) telah membawa perubahan signifikan dalam industri perbankan, termasuk perbankan syariah di Indonesia. Digitalisasi tidak hanya meningkatkan efisiensi dan aksesibilitas layanan keuangan, tetapi juga memperluas potensi risiko siber yang semakin kompleks, seperti kebocoran data, serangan siber, dan gangguan sistem informasi. Kondisi ini menuntut adanya penguatan dan optimalisasi manajemen risiko siber yang tidak hanya berbasis teknologi, tetapi juga selaras dengan prinsip-prinsip syariah. Penelitian ini bertujuan untuk menganalisis secara kritis optimalisasi manajemen risiko siber pada perbankan syariah di Indonesia dalam menghadapi era fintech. Metode yang digunakan adalah pendekatan kualitatif melalui studi literatur dengan analisis deskriptif-kritis terhadap berbagai sumber, seperti regulasi, jurnal ilmiah, dan laporan industri. Fokus penelitian meliputi identifikasi jenis risiko siber, evaluasi penerapan manajemen risiko, serta tingkat kesiapan perbankan syariah dalam menghadapi ancaman digital. Hasil penelitian menunjukkan bahwa perbankan syariah telah mengimplementasikan berbagai upaya mitigasi risiko, seperti peningkatan sistem keamanan informasi, penerapan tata kelola teknologi informasi, serta penguatan kapasitas sumber daya manusia. Namun demikian, masih terdapat sejumlah tantangan, antara lain keterbatasan infrastruktur teknologi, rendahnya literasi keamanan siber, serta belum optimalnya integrasi antara prinsip syariah dan praktik manajemen risiko modern. Oleh karena itu, optimalisasi manajemen risiko siber perlu dilakukan secara komprehensif melalui penguatan regulasi, peningkatan kolaborasi antara regulator, industri perbankan, dan penyedia fintech, serta pengembangan sistem keamanan yang adaptif dan berbasis nilai syariah. Dengan demikian, perbankan syariah di Indonesia diharapkan mampu membangun sistem yang lebih tangguh, aman, dan berdaya saing dalam ekosistem keuangan digital.

Kata Kunci: *Manajemen Risiko Siber, Perbankan Syariah, Fintech, Keamanan Informasi, Tata Kelola Teknologi*

Abstract

The digital transformation driven by the development of financial technology (fintech) has brought significant changes to the banking industry, including Islamic banking in Indonesia. Digitalization not only increases the efficiency and accessibility of financial services but also expands the potential for increasingly complex cyber risks, such as data breaches, cyberattacks, and information system disruptions. This situation demands the strengthening and optimization of cyber risk management that is not only technology-based but also aligned with Sharia

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

principles. This study aims to critically analyze the optimization of cyber risk management in Islamic banking in Indonesia in facing the fintech era. The method used is a qualitative approach through literature review with descriptive-critical analysis of various sources, such as regulations, scientific journals, and industry reports. The research focuses on identifying types of cyber risks, evaluating risk management implementation, and the level of preparedness of Islamic banking in facing digital threats. The results show that Islamic banking has implemented various risk mitigation efforts, such as improving information security systems, implementing information technology governance, and strengthening human resource capacity. However, several challenges remain, including limited technological infrastructure, low cybersecurity literacy, and the suboptimal integration of Sharia principles and modern risk management practices. Therefore, comprehensive optimization of cyber risk management requires strengthening regulations, increasing collaboration between regulators, the banking industry, and fintech providers, and developing adaptive security systems based on Sharia values. This way, Islamic banking in Indonesia is expected to be able to build a more resilient, secure, and competitive system within the digital financial ecosystem.

Keywords: *Cyber Risk Management, Islamic Banking, Fintech, Information Security, Technology Governance*

Pendahuluan

Transformasi digital yang terjadi secara masif dalam beberapa dekade terakhir telah mengubah lanskap industri keuangan global, termasuk di Indonesia. Perkembangan teknologi informasi yang pesat mendorong lahirnya inovasi di sektor jasa keuangan, khususnya melalui kehadiran financial technology (fintech) yang menawarkan kemudahan, kecepatan, serta efisiensi dalam berbagai layanan keuangan (Arner, Barberis, & Buckley, 2016). Fenomena ini tidak hanya memengaruhi perbankan konvensional, tetapi juga memberikan dampak signifikan terhadap perbankan syariah yang dituntut untuk beradaptasi dengan dinamika digital guna mempertahankan daya saingnya (Otoritas Jasa Keuangan, 2023).

Perbankan syariah sebagai bagian dari sistem keuangan nasional memiliki karakteristik yang berbeda dibandingkan dengan perbankan konvensional, terutama dalam hal prinsip operasional yang berlandaskan pada nilai-nilai syariah seperti keadilan (adl), transparansi (transparency), serta larangan terhadap praktik riba, gharar, dan maysir (Antonio, 2011). Dalam konteks ini, digitalisasi layanan perbankan syariah tidak hanya berorientasi pada efisiensi operasional, tetapi juga harus tetap menjaga kepatuhan terhadap prinsip-prinsip syariah (sharia compliance) (Ascarya, 2015). Oleh karena itu, integrasi teknologi dalam perbankan syariah memerlukan pengelolaan yang cermat, khususnya dalam aspek risiko.

Seiring dengan meningkatnya adopsi teknologi digital dan integrasi dengan ekosistem fintech, risiko yang dihadapi oleh perbankan syariah menjadi semakin kompleks, salah satunya adalah risiko siber (cyber risk). Risiko siber mencakup berbagai potensi ancaman seperti serangan malware, phishing, ransomware, pencurian data (data breach), hingga gangguan terhadap sistem informasi yang dapat menghambat operasional perbankan (Kaspersky, 2022). Ancaman ini tidak hanya berdampak pada kerugian finansial, tetapi juga dapat merusak reputasi lembaga serta menurunkan tingkat kepercayaan masyarakat, yang merupakan aspek fundamental dalam industri perbankan (Bank Indonesia, 2022).

Dalam era fintech, kolaborasi antara perbankan dan perusahaan teknologi keuangan menjadi semakin intensif. Di satu sisi, kolaborasi ini memberikan peluang besar dalam memperluas inklusi keuangan, meningkatkan efisiensi layanan, serta menciptakan inovasi produk berbasis digital. Namun di sisi lain, keterhubungan sistem yang semakin luas juga meningkatkan potensi kerentanan terhadap serangan siber (Gomber et al., 2018). Hal ini menuntut perbankan syariah untuk memiliki sistem manajemen risiko siber yang tidak hanya responsif, tetapi juga proaktif dan adaptif terhadap perkembangan ancaman yang terus berubah.

Regulator di Indonesia, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia, telah mengeluarkan berbagai kebijakan terkait manajemen risiko teknologi informasi dan keamanan siber dalam sektor jasa keuangan (OJK, 2022). Meskipun demikian, implementasi kebijakan tersebut pada perbankan syariah masih menghadapi sejumlah tantangan, antara lain keterbatasan infrastruktur teknologi, kurangnya sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, serta rendahnya tingkat literasi digital dan kesadaran akan pentingnya keamanan informasi (Susanto, 2021). Selain itu, kompleksitas dalam menjaga keseimbangan antara inovasi teknologi dan kepatuhan terhadap prinsip syariah juga menjadi tantangan tersendiri.

Optimalisasi manajemen risiko siber menjadi suatu keniscayaan bagi perbankan syariah dalam menghadapi era fintech. Optimalisasi ini tidak hanya mencakup penguatan sistem keamanan teknologi informasi, tetapi juga melibatkan aspek tata kelola (governance), budaya organisasi, peningkatan kapasitas sumber daya manusia, serta integrasi kebijakan yang selaras dengan prinsip-prinsip syariah

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

(ISO, 2018). Dengan pendekatan yang komprehensif, diharapkan perbankan syariah mampu meminimalkan potensi risiko siber sekaligus memanfaatkan peluang yang ditawarkan oleh perkembangan teknologi digital.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis mengenai bagaimana optimalisasi manajemen risiko siber dapat diterapkan secara efektif pada perbankan syariah di Indonesia dalam menghadapi era fintech. Penelitian ini juga bertujuan untuk mengidentifikasi tantangan yang dihadapi serta merumuskan strategi yang relevan dan aplikatif dalam meningkatkan ketahanan siber (cyber resilience) perbankan syariah. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi teoritis maupun praktis dalam pengembangan sistem manajemen risiko yang lebih adaptif, inovatif, dan sesuai dengan prinsip syariah.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian deskriptif-analitis yang bertujuan untuk menganalisis optimalisasi manajemen risiko siber pada perbankan syariah di Indonesia dalam menghadapi era financial technology (fintech). Pendekatan ini dipilih untuk memperoleh pemahaman yang komprehensif terkait aspek kebijakan, konsep, dan praktik manajemen risiko siber (Creswell, 2014).

Penelitian ini menggunakan pendekatan normatif dan konseptual, dengan menelaah regulasi yang berlaku serta teori-teori yang relevan, seperti manajemen risiko dan keamanan siber dalam konteks perbankan syariah (ISO, 2018; Otoritas Jasa Keuangan, 2022). Data yang digunakan merupakan data sekunder yang diperoleh dari laporan perbankan syariah, publikasi resmi regulator, serta literatur ilmiah yang relevan (Sugiyono, 2019). Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research), sedangkan teknik analisis data menggunakan analisis kualitatif deskriptif melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan (Miles & Huberman, 2014). Untuk menjaga keabsahan data, digunakan teknik triangulasi sumber guna meningkatkan validitas hasil penelitian (Moleong, 2018).

Hasil Dan Pembahasan

Perkembangan financial technology (*fintech*) telah membawa perubahan yang signifikan terhadap operasional perbankan syariah di Indonesia, terutama dalam aspek digitalisasi layanan keuangan. Transformasi ini mendorong peningkatan efisiensi, kecepatan, dan aksesibilitas layanan, namun di sisi lain juga memperluas spektrum risiko yang dihadapi, khususnya risiko siber. Berdasarkan hasil kajian literatur yang dilakukan, dapat dipahami bahwa risiko siber dalam perbankan syariah tidak hanya bersifat teknis, melainkan juga mencakup dimensi kelembagaan, sumber daya manusia, serta kepatuhan terhadap prinsip-prinsip syariah.

Dalam konteks operasional perbankan syariah, risiko siber muncul seiring dengan meningkatnya ketergantungan terhadap sistem teknologi informasi. Layanan seperti mobile banking, internet banking, serta integrasi dengan platform fintech telah membuka peluang terjadinya berbagai jenis serangan siber. Ancaman tersebut mencakup serangan malware yang dapat merusak sistem, ransomware yang mengunci akses terhadap data penting, serta phishing yang menargetkan kelemahan pengguna dalam menjaga informasi pribadi. Fenomena ini menunjukkan bahwa digitalisasi tidak hanya menciptakan efisiensi, tetapi juga meningkatkan kompleksitas risiko yang harus dikelola secara sistematis.(Arifin dan Fasa, 2024a)

Lebih lanjut, kebocoran data menjadi salah satu risiko yang paling krusial dalam sektor perbankan syariah. Data nasabah yang bersifat sensitif, seperti informasi keuangan dan identitas pribadi, menjadi target utama bagi pelaku kejahatan siber. Kebocoran data tidak hanya berdampak pada kerugian finansial, tetapi juga berpotensi merusak reputasi lembaga perbankan. Dalam konteks perbankan syariah, kepercayaan (trust) merupakan aspek fundamental yang harus dijaga, sehingga setiap insiden keamanan dapat memiliki implikasi yang lebih luas terhadap keberlangsungan institusi.

Selain itu, integrasi antara perbankan syariah dan perusahaan fintech juga menjadi faktor yang memperbesar potensi risiko siber. Kolaborasi ini memang memberikan manfaat dalam hal inovasi dan inklusi keuangan, namun juga menciptakan ketergantungan terhadap sistem pihak ketiga. Keterhubungan sistem yang semakin kompleks membuka peluang bagi terjadinya serangan melalui celah keamanan yang mungkin tidak sepenuhnya berada dalam kendali bank. Oleh karena

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

itu, manajemen risiko siber tidak lagi dapat dipandang sebagai tanggung jawab internal semata, melainkan memerlukan pendekatan yang lebih luas dan kolaboratif.

Dalam menghadapi berbagai ancaman tersebut, perbankan syariah di Indonesia telah menunjukkan upaya dalam mengimplementasikan manajemen risiko siber. Upaya ini mencakup penguatan sistem keamanan teknologi informasi melalui penerapan berbagai perangkat keamanan seperti firewall, enkripsi data, serta sistem deteksi dan pencegahan intrusi. Implementasi teknologi ini bertujuan untuk melindungi sistem dari akses yang tidak sah serta memastikan integritas dan kerahasiaan data.(Syafitri *dkk.*, 2026)

Di samping itu, penerapan tata kelola teknologi informasi menjadi aspek penting dalam mendukung efektivitas manajemen risiko siber. Tata kelola ini mencakup kebijakan, prosedur, serta mekanisme pengawasan yang dirancang untuk memastikan bahwa seluruh aktivitas teknologi informasi berjalan sesuai dengan standar yang telah ditetapkan. Dengan adanya tata kelola yang baik, perbankan syariah dapat mengidentifikasi, mengukur, dan mengendalikan risiko secara lebih terstruktur.

Namun demikian, hasil analisis menunjukkan bahwa penerapan manajemen risiko siber pada perbankan syariah masih menghadapi berbagai kendala. Salah satu kendala utama adalah keterbatasan infrastruktur teknologi, terutama pada bank syariah yang memiliki skala operasional lebih kecil. Keterbatasan ini berdampak pada kemampuan bank dalam mengadopsi teknologi keamanan yang canggih, sehingga meningkatkan kerentanan terhadap serangan siber.

Selain faktor teknologi, aspek sumber daya manusia juga menjadi tantangan yang signifikan. Rendahnya literasi keamanan siber di kalangan pegawai maupun nasabah menyebabkan meningkatnya risiko yang berasal dari faktor manusia. Banyak kasus serangan siber yang berhasil terjadi bukan karena kelemahan sistem, melainkan karena kurangnya kesadaran dalam menjaga keamanan informasi. Oleh karena itu, peningkatan kapasitas sumber daya manusia menjadi bagian yang tidak terpisahkan dari upaya optimalisasi manajemen risiko siber.(Hasanah, Sayuti dan Lisnawati, 2024)

Dalam perspektif perbankan syariah, pengelolaan risiko siber juga harus mempertimbangkan aspek kepatuhan terhadap prinsip-prinsip syariah. Prinsip

seperti keadilan, transparansi, dan amanah harus tercermin dalam setiap kebijakan dan praktik yang diterapkan. Hal ini menambah kompleksitas dalam pengelolaan risiko, karena bank tidak hanya dituntut untuk efektif secara teknis, tetapi juga harus memastikan bahwa seluruh aktivitasnya sesuai dengan nilai-nilai syariah.

Lebih jauh lagi, perkembangan ancaman siber yang semakin dinamis menuntut perbankan syariah untuk memiliki pendekatan yang adaptif dan proaktif. Ancaman tidak lagi bersifat statis, melainkan terus berkembang seiring dengan kemajuan teknologi. Oleh karena itu, sistem keamanan yang diterapkan harus mampu beradaptasi dengan perubahan tersebut. Pendekatan berbasis risiko (risk-based approach) menjadi penting dalam menentukan prioritas pengelolaan risiko serta alokasi sumber daya yang efektif.

Dalam upaya mengoptimalkan manajemen risiko siber, diperlukan strategi yang komprehensif dan berkelanjutan. Salah satu strategi yang dapat dilakukan adalah peningkatan investasi dalam teknologi keamanan informasi. Penggunaan teknologi berbasis kecerdasan buatan (artificial intelligence) dan machine learning dapat membantu dalam mendeteksi pola serangan serta memberikan respons yang lebih cepat terhadap ancaman.(Fajri dan Violita, 2023)

Selain itu, peningkatan kolaborasi antara berbagai pihak juga menjadi faktor penting dalam menciptakan ekosistem keuangan yang aman. Kolaborasi antara perbankan, regulator, dan perusahaan fintech memungkinkan terjadinya pertukaran informasi mengenai ancaman siber serta pengembangan standar keamanan yang lebih baik. Dengan adanya kerja sama yang solid, risiko yang dihadapi dapat dikelola secara lebih efektif.

Peran regulator dalam hal ini juga sangat krusial. Kebijakan yang dikeluarkan oleh otoritas seperti Otoritas Jasa Keuangan dan Bank Indonesia menjadi landasan dalam penerapan manajemen risiko siber. Namun, efektivitas kebijakan tersebut sangat bergantung pada implementasi di tingkat institusi. Oleh karena itu, diperlukan pengawasan yang lebih ketat serta evaluasi yang berkelanjutan untuk memastikan bahwa kebijakan yang telah ditetapkan dapat dijalankan secara optimal.

Di sisi lain, edukasi kepada masyarakat juga menjadi bagian penting dalam pengelolaan risiko siber. Nasabah sebagai pengguna layanan digital memiliki peran dalam menjaga keamanan informasi pribadi. Peningkatan kesadaran mengenai

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

praktik keamanan, seperti tidak membagikan informasi sensitif dan berhati-hati terhadap pesan mencurigakan, dapat membantu mengurangi risiko serangan yang berasal dari faktor eksternal.

Dalam konteks jangka panjang, optimalisasi manajemen risiko siber pada perbankan syariah memerlukan integrasi antara teknologi, manusia, dan nilai-nilai syariah. Pendekatan ini tidak hanya bertujuan untuk melindungi sistem dari ancaman, tetapi juga untuk membangun kepercayaan masyarakat terhadap layanan perbankan syariah. Kepercayaan ini menjadi modal utama dalam menghadapi persaingan di era digital yang semakin kompetitif.

Dengan demikian, dapat disimpulkan bahwa perbankan syariah di Indonesia telah menunjukkan upaya dalam mengelola risiko siber, namun masih diperlukan peningkatan dalam berbagai aspek untuk mencapai optimalisasi yang diharapkan. Penguatan infrastruktur teknologi, peningkatan kapasitas sumber daya manusia, serta integrasi prinsip syariah dalam manajemen risiko menjadi kunci dalam menciptakan sistem yang tangguh dan berkelanjutan. Pendekatan yang komprehensif dan kolaboratif akan memungkinkan perbankan syariah untuk tidak hanya bertahan, tetapi juga berkembang dalam menghadapi tantangan di era fintech.(Nusantari dan Suryani, 2025)

Lebih lanjut, dinamika perkembangan teknologi digital juga menuntut adanya perubahan paradigma dalam pengelolaan risiko pada perbankan syariah. Jika sebelumnya pendekatan manajemen risiko lebih bersifat reaktif, yaitu merespons setelah terjadinya insiden, maka dalam konteks risiko siber diperlukan pendekatan yang lebih proaktif dan preventif. Hal ini disebabkan oleh karakteristik ancaman siber yang sulit diprediksi serta memiliki dampak yang dapat terjadi secara cepat dan luas. Oleh karena itu, perbankan syariah perlu mengembangkan sistem deteksi dini (early warning system) yang mampu mengidentifikasi potensi ancaman sebelum berkembang menjadi insiden yang merugikan.

Penguatan sistem deteksi dini ini dapat dilakukan melalui pemanfaatan teknologi analitik data yang mampu memantau aktivitas sistem secara real-time. Dengan adanya pemantauan yang berkelanjutan, setiap anomali yang terjadi dalam sistem dapat segera diidentifikasi dan ditindaklanjuti. Pendekatan ini tidak hanya meningkatkan efektivitas pengelolaan risiko, tetapi juga mempercepat proses

respons terhadap insiden siber. Dalam hal ini, kecepatan respons menjadi faktor kunci dalam meminimalkan dampak yang ditimbulkan oleh serangan siber.

Di samping itu, penting bagi perbankan syariah untuk mengembangkan budaya keamanan siber (cybersecurity culture) di dalam organisasi. Budaya ini mencerminkan tingkat kesadaran dan kepedulian seluruh elemen organisasi terhadap pentingnya menjaga keamanan informasi. Pengembangan budaya keamanan tidak hanya dilakukan melalui pelatihan formal, tetapi juga melalui internalisasi nilai-nilai yang mendorong perilaku aman dalam penggunaan teknologi. Dengan terbentuknya budaya yang kuat, setiap individu dalam organisasi akan memiliki tanggung jawab dalam menjaga keamanan sistem.(Putro dan Sifa, 2025)

Budaya keamanan siber juga harus diintegrasikan dengan nilai-nilai syariah yang menjadi landasan operasional perbankan syariah. Nilai amanah, misalnya, dapat diimplementasikan dalam bentuk tanggung jawab untuk menjaga kerahasiaan data nasabah. Sementara itu, prinsip transparansi dapat diwujudkan melalui penyampaian informasi yang jelas kepada nasabah terkait potensi risiko dalam penggunaan layanan digital. Integrasi ini menunjukkan bahwa pengelolaan risiko siber tidak hanya berorientasi pada aspek teknis, tetapi juga pada pembentukan etika dan nilai dalam organisasi.

Selain aspek internal, pengelolaan risiko siber juga memerlukan perhatian terhadap faktor eksternal yang memengaruhi keamanan sistem perbankan. Salah satu faktor tersebut adalah perkembangan regulasi yang terus berubah mengikuti dinamika teknologi. Perbankan syariah perlu memastikan bahwa setiap kebijakan yang diterapkan selaras dengan regulasi yang berlaku, sekaligus mampu mengantisipasi perubahan yang mungkin terjadi di masa depan. Hal ini menuntut adanya fleksibilitas dalam penyusunan kebijakan serta kemampuan untuk melakukan penyesuaian secara cepat.

Lebih lanjut, kompleksitas ekosistem fintech yang melibatkan berbagai pihak juga menuntut adanya standar keamanan yang terintegrasi. Tanpa adanya standar yang seragam, setiap pihak dalam ekosistem akan memiliki tingkat keamanan yang berbeda, sehingga menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. Oleh karena itu, diperlukan upaya untuk menyusun standar

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

keamanan bersama yang dapat diterapkan oleh seluruh pihak yang terlibat dalam ekosistem keuangan digital.

Dalam konteks ini, perbankan syariah dapat mengambil peran aktif dalam mendorong terbentuknya standar tersebut, baik melalui kerja sama dengan regulator maupun melalui partisipasi dalam forum industri. Keterlibatan aktif ini tidak hanya meningkatkan keamanan sistem, tetapi juga memperkuat posisi perbankan syariah dalam ekosistem keuangan digital yang semakin kompetitif. (Arifin dan Fasa, 2024b)

Di sisi lain, penting untuk mempertimbangkan aspek keberlanjutan dalam pengelolaan risiko siber. Penguatan sistem keamanan tidak dapat dilakukan secara sekali waktu, melainkan harus menjadi proses yang berkelanjutan. Hal ini disebabkan oleh sifat ancaman siber yang terus berkembang, sehingga sistem yang dianggap aman saat ini belum tentu mampu menghadapi ancaman di masa depan. Oleh karena itu, perbankan syariah perlu melakukan evaluasi dan pembaruan sistem keamanan secara berkala.

Evaluasi ini dapat dilakukan melalui audit keamanan, pengujian penetrasi (penetration testing), serta simulasi serangan siber untuk menguji ketahanan sistem. Melalui evaluasi yang berkelanjutan, perbankan syariah dapat mengidentifikasi kelemahan yang ada serta melakukan perbaikan sebelum kelemahan tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pendekatan ini menunjukkan bahwa pengelolaan risiko siber merupakan proses dinamis yang memerlukan perhatian secara terus-menerus.

Selain itu, pengembangan sistem manajemen risiko yang terintegrasi juga menjadi faktor penting dalam optimalisasi pengelolaan risiko siber. Sistem ini harus mampu menghubungkan berbagai aspek risiko, baik risiko operasional, risiko teknologi, maupun risiko kepatuhan. Dengan adanya integrasi, perbankan syariah dapat memperoleh gambaran yang lebih komprehensif mengenai profil risiko yang dihadapi, sehingga pengambilan keputusan dapat dilakukan secara lebih tepat.

Integrasi ini juga memungkinkan adanya sinergi antara berbagai unit dalam organisasi, sehingga pengelolaan risiko tidak berjalan secara terpisah-pisah. Setiap unit memiliki peran dalam menjaga keamanan sistem, dan koordinasi yang baik antar unit akan meningkatkan efektivitas pengelolaan risiko secara keseluruhan. Dalam

konteks ini, peran manajemen puncak menjadi sangat penting dalam memberikan arah dan dukungan terhadap implementasi manajemen risiko yang terintegrasi.

Lebih jauh, perbankan syariah juga perlu memperhatikan aspek perlindungan konsumen dalam pengelolaan risiko siber. Nasabah sebagai pengguna layanan digital memiliki hak untuk mendapatkan perlindungan terhadap data dan transaksi yang dilakukan. Oleh karena itu, perbankan syariah harus memastikan bahwa sistem yang digunakan mampu memberikan perlindungan yang memadai serta memiliki mekanisme penanganan keluhan yang efektif.

Perlindungan konsumen ini tidak hanya berkaitan dengan aspek teknis, tetapi juga dengan aspek komunikasi. Penyampaian informasi yang jelas dan transparan kepada nasabah mengenai risiko dan cara mitigasinya akan meningkatkan kepercayaan serta mendorong perilaku yang lebih aman dalam penggunaan layanan digital. Dengan demikian, nasabah tidak hanya menjadi objek perlindungan, tetapi juga menjadi bagian dari sistem keamanan itu sendiri.

Pada akhirnya, optimalisasi manajemen risiko siber dalam perbankan syariah merupakan proses yang kompleks dan multidimensional. Proses ini melibatkan interaksi antara teknologi, manusia, regulasi, dan nilai-nilai syariah yang saling memengaruhi satu sama lain. Keberhasilan dalam mengelola risiko siber tidak hanya ditentukan oleh kecanggihan teknologi yang digunakan, tetapi juga oleh kemampuan organisasi dalam mengelola seluruh aspek tersebut secara terpadu.

Dengan pendekatan yang holistik dan berkelanjutan, perbankan syariah di Indonesia memiliki peluang untuk membangun sistem yang tidak hanya aman, tetapi juga resilient terhadap berbagai ancaman yang mungkin muncul di masa depan. Ketahanan ini menjadi kunci dalam menjaga stabilitas operasional serta meningkatkan daya saing dalam industri keuangan yang semakin terdigitalisasi. Oleh karena itu, penguatan manajemen risiko siber harus menjadi prioritas strategis dalam pengembangan perbankan syariah ke depan, seiring dengan terus berkembangnya inovasi dalam ekosistem fintech.(Syafitri *dkk.*, 2026)

Kesimpulan

Optimalisasi manajemen risiko siber pada perbankan syariah di Indonesia merupakan suatu kebutuhan yang bersifat strategis dan tidak dapat ditunda,

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550

terutama dalam menghadapi perkembangan pesat teknologi finansial (fintech). Transformasi digital yang terjadi telah memperluas akses layanan keuangan, namun pada saat yang sama juga meningkatkan kompleksitas serta potensi ancaman siber yang dapat mengganggu stabilitas operasional dan kepercayaan nasabah. Oleh karena itu, perbankan syariah dituntut untuk mengintegrasikan kerangka manajemen risiko siber yang komprehensif, adaptif, dan berbasis prinsip kehati-hatian, dengan tetap berlandaskan nilai-nilai syariah seperti transparansi, keadilan, dan tanggung jawab.

Dalam konteks implementasi, optimalisasi tersebut perlu didukung oleh penguatan infrastruktur teknologi informasi, peningkatan kapasitas sumber daya manusia, serta penerapan kebijakan dan prosedur keamanan yang sesuai dengan standar nasional maupun internasional. Selain itu, kolaborasi antara regulator, industri perbankan, dan penyedia layanan fintech menjadi faktor penting dalam menciptakan ekosistem keuangan digital yang aman dan berkelanjutan. Dengan demikian, perbankan syariah di Indonesia tidak hanya mampu memitigasi risiko siber secara efektif, tetapi juga dapat meningkatkan daya saing dan kepercayaan publik di tengah dinamika industri keuangan digital yang semakin kompetitif.

Daftar Pustaka

Arifin, B.D. dan Fasa, M.I. (2024a) "Transformasi Digital Era Industri 4.0 Revolusi Layanan Yang Mengubah Lanskap Perbankan Syariah Di Indonesia," *Jurnal Manajemen, Akuntansi dan Logistik (JUMATI)*, 2(4). Tersedia pada: https://ciptakind-publisher.com/jumati/index.php/ojs/article/view/208 (Diakses: 29 April 2026).

Arifin, B.D. dan Fasa, M.I. (2024b) "Transformasi Digital Era Industri 4.0 Revolusi Layanan Yang Mengubah Lanskap Perbankan Syariah Di Indonesia," *Jurnal Manajemen, Akuntansi dan Logistik (JUMATI)*, 2(4). Tersedia pada: https://ciptakind-publisher.com/jumati/index.php/ojs/article/view/208 (Diakses: 29 April 2026).

Fajri, A.M. dan Violita, E.S. (2023) "Analisis manajemen risiko bank syariah dalam melakukan transformasi digital (Studi kasus pada Bank AS)," *Owner: Riset dan Jurnal Akuntansi*, 7(2), hlm. 1249–1258.

Hasanah, N., Sayuti, M.N. dan Lisnawati, L. (2024) "Optimalisasi regulasi perbankan syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam akselerasi transformasi digital," *Jurnal Manajemen Terapan Dan Keuangan*, 13(03), hlm. 709–723.

Nusantari, F.A.A. dan Suryani, S. (2025) "Akselerasi Layanan Bank Syariah melalui Fintech: Strategi Operasional, Inovasi Produk, dan Perlindungan Konsumen," *Revenue: Lentera Bisnis Manajemen*, 3(04), hlm. 182–192.

Putro, H.K. dan Sifa, M.A. (2025) "Manajemen Resiko Pembiayaan Bank Syariah Indonesia: Tantangan dan Solusi," *Journal of Islamic Banking*, 6(1), hlm. 20–36.

Syafitri, F. *dkk.* (2026) "Optimalisasi Sumber Daya Data Untuk Inovasi Layanan Bank Syariah Di Era Digital," *Jurnal Ekonomi Bisnis dan Kewirausahaan*, 3(1), hlm. 37–44.

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1550