JKAM Jurnal Kajian Akademik Multidisiplin
Yayasan Paramarta Akademika Indonesia
P-ISSN XXXX, E-ISSN XXXX

Tata Kelola Keamanan Siber Pada Perbankan Syariah Menggunakan Prinsip Maqashid Syariah Di Era Digital

ABSTRACT *- This study aims to examine how cybersecurity governance is integrated with the principles of *Maqashid Sharia* at PT Bank Syariah Indonesia, Tbk. (BSI). A descriptive qualitative method was employed, involving the collection and analysis of data from literature reviews, regulatory documents, and annual reports covering the 2022–2023 period. The findings indicate that cybersecurity management in Islamic banking must encompass technical aspects, applicable regulations, ethical values, and *Maqashid Sharia* principles. This integration is achieved by protecting data and customer assets (*hifz al-mal*), demonstrating transparency during crises as an act of fulfilling trust (*amanah*), and providing digital literacy education as a means of safeguarding the intellect (*hifz al-'aql*). The study emphasizes that cybersecurity is not merely a matter of adhering to administrative rules but also constitutes a form of moral responsibility and a Sharia-compliant approach to maintaining customer trust.*

ABSTRAK - Penelitian ini bertujuan untuk melihat bagaimana tata kelola keamanan siber diintegrasikan dengan prinsip-prinsip Maqashid Syariah di PT Bank Syariah Indonesia, Tbk.(BSI). Metode yang digunakan adalah kualitatif deskriptif dengan cara mengumpulkan dan menganalisis data dari studi literatur serta dokumen regulasi dan laporan tahunan periode 2022 hingga 2023. Temuan penelitian menunjukkan bahwa pengelolaan keamanan siber di bank syariah perlu mencakup aspek teknis, aturan yang berlaku, nilai-nilai etika, serta prinsip Maqashid Syariah. Integrasi ini dilakukan dengan melindungi data, melindungi harta nasabah (hifz al-mal), memperlihatkan transparansi dalam krisis sebagai bentuk amanah, serta memberikan pendidikan literasi digital sebagai cara menjaga akal (hifz al-'aql). Penelitian ini menekankan bahwa keamanan siber bukan hanya soal mengikuti aturan administratif, tetapi juga merupakan bentuk tanggung jawab moral dan sesuai dengan syariah dalam mempertahankan kepercayaan nasabah.

Author
[1] **Farah Salsabila**, Universitas Al-Azhar Medan, Indonesia
[2] **Euis Kanersih**, Universitas Al-Azhar Medan, Indonesia
[3] **Tengku Widia Marsanda Iriyantika**, Universitas Al-Azhar Medan, Indonesia
[4] **Muhammad Putra Yoga**, Universitas Al-Azhar Medan, Indonesia

*[*1]Corresponding email:* salsabilafarrah01@gmail.com

Article History
Submitted: 22 Juli 2026
Revised: 23 Juli 2026
Accepted: 24 Juli 2026
Published: 24 Juli 2026

Keywords
Tata kelola;
Keamanan siber;
Perbankan syariah;
Maqashid syariah;
Bank Syariah Indonesia

PENDAHULUAN

Perkembangan teknologi digital telah mengubah cara perbankan memberikan layanan kepada masyarakat. Perbankan syariah kini memanfaatkan berbagai layanan digital seperti mobile banking, internet banking, pembayaran digital, dan sistem informasi berbasis teknologi untuk meningkatkan kualitas pelayanan serta efisiensi operasional.

Transisi digital tersebut memberikan kemudahan bagi nasabah dalam melakukan transaksi kapan saja dan di mana saja.

Namun, di balik berbagai manfaat tersebut, penggunaan teknologi juga memiliki risiko berupa keamanan siber yang dapat mengancam kerahasiaan data, integritas sistem, dan keamanan transaksi keuangan. Kini keamanan siber tidak lagi dipandang hanya sebagai persoalan teknis, tetapi juga sebagai bagian penting dari tata kelola perusahaan yang bertujuan menjaga keberlangsungan operasional, melindungi kepentingan nasabah, dan memenuhi tuntutan regulasi di era digital.

Dalam perbankan syariah, tata kelola keamanan siber tidak hanya berorientasi pada efektivitas pengendalian risiko, tetapi juga harus sejalan dengan nilai-nilai syariah. Salah satu prinsip yang dapat dijadikan landasan adalah maqashid syariah, yaitu tujuan utama syariat Islam yang bertujuan mewujudkan kemaslahatan dan mencegah kemudaratan. Penerapan keamanan siber yang baik dapat dikaitkan dengan upaya menjaga harta (hifz al-mal), menjaga akal (hifz al-‘aql) melalui edukasi literasi digital, serta menjaga kemaslahatan masyarakat dengan memberikan layanan keuangan yang aman, terpercaya, dan bertanggung jawab.

Kebaruan artikel ini terdapat pada kesadaran dan pemahaman dengan pendekatan bahwa keamanan siber tidak hanya dipahami sebagai kewajiban teknis dan regulatif, tetapi juga sebagai tanggung jawab moral dan syariah dalam menjaga kepercayaan nasabah. Penelitian ini bertujuan untuk merumuskan model tata kelola keamanan siber yang tidak hanya patuh pada regulasi, tetapi juga sesuai hukum Islam.

Perbankan Syariah

Perbankan syariah adalah sistem perbankan yang menjalankan kegiatan usahanya sesuai dengan ajaran Islam, yaitu tidak menggunakan riba (bunga) , gharar (ketidakpastian), dan maisir (perjudian). Perbankan syariah lebih mengutamakan keadilan, keterbukaan, serta kerja sama melalui sistem bagi hasil. Sesuai Undang-Undang No.21 tahun 2008 tentang Perbankan Syariah, bank syariah juga menjalankan fungsi sosial dengan menjalankan fungsi seperti lembaga baitul mal, yaitu menerima dana yang berasal dari zakat, infak, sedekah, hibah, atau dana sosial lainnya dan menyalurkannya kepada pengelola wakaf (nazhir) sesuai kehendak pemberi wakaf (wakif) (Andrianto & Firmansyah, 2019).

Maqashid Syariah

Secara etimologi, Maqasid Syariah terdiri dari dua kata, yaitu maqasid yang berarti tujuan-tujuan dan syariah yang merujuk pada aturan hukum Islam. Dalam pengertian terminologis, Maqasid Syariah adalah tujuan yang ingin dicapai oleh hukum Islam agar manusia bisa mendapatkan kebaikan dan manfaat (Algifari & Andrini, 2024). Prinsip Maqashid Syariah sangat dibutuhkan pada sistem perbankan syari'ah, dalam perbankan syariah Maqashid Syariah berfungsi sebagai kompas moral sekaligus fondasi operasional.

Sistem perbankan syariah di Indonesia didasarkan pada prinsip-prinsip Maqashid Syariah, terutama prinsip Hifz al-Mal (pelindung harta) dan Hifz al-Din (pelindung agama). Bank-bank syariah di Indonesia menawarkan produk-produk yang sesuai dengan prinsip-prinsip syariah, seperti mudharabah (bagi hasil), musyarakah (kerjasama), dan murabahah (jual beli dengan markup) (Jauhari, 2024). Prinsip maqashid syariah ini

bertujuan untuk selalu menjaga segala aturan sesuai dengan ajaran Islam, sehingga prosedur yang dijalankan tidak akan mengalami perubahan arah dan tujuan yang tidak sesuai dengan ajaran Islam.

Tata Kelola (Governance)

Tata kelola perusahaan adalah cara atau proses yang mengatur dan mengendalikan perusahaan untuk mencapai tujuan secara efisien dan transparan. Pendapat ini sejalan dengan prinsip utama GCG dari Forum for Corporate Governance in Indonesia (FCGI), prinsip utama GCG meliputi: transparansi, akuntabilitas, tanggung jawab, independensi, dan kewajaran (Erni et al., 2025). Berikut adalah penjelasan mengenai pembahasan prinsip GCG:

a. Transparansi mengharuskan perusahaan menyediakan informasi yang jelas dan benar kepada para pemegang saham serta pihak-pihak yang berkepentingan. Hal ini mencakup penerbitan laporan keuangan yang jelas, informasi mengenai kebijakan bisnis, serta keputusan strategis perusahaan.
b. Akuntabilitas adalah prinsip GCG yang menyatakan bahwa setiap orang dalam perusahaan harus bertanggung jawab atas semua tindakan dan keputusan yang diambil. Akuntabilitas merupakan fondasi dari sistem pengambilan keputusan yang baik dan membantu menghindari konflik kepentingan.
c. Tanggung Jawab adalah kewajiban perusahaan untuk mematuhi peraturan perundang-undangan dan melaksanakan tanggung jawab kepada masyarakat dan lingkungan sekitar.
d. Idependensi adalah prinsip GCG yang menuntut perusahaan dikelola secara profesional tanpa pengaruh atau tekanan dari pihak manapun.
e. Kewajaran adalah perlakuan yang adil dan setara kepada seluruh stakeholder perusahaan sesuai hak dan kewajibannya tanpa diskriminasi.

Tata Kelola Pada Perbankan Syariah

Penerapan tata kelola perusahaan dalam perbankan syariah ialah sebagai upaya mendasar dalam menjaga jati diri bank sebagai lembaga yang berlandaskan ajaran Islam. Tata kelola ini berfungsi sebagai petunjuk yang memastikan seluruh kegiatan operasional, mulai dari penghimpunan dana hingga penyaluran pembiayaan tetap berada dalam koridor syariah yang melarang praktik riba, gharar, dan maisir. Oleh karena itu, kerangka tata kelola di bank syariah memiliki tanggung jawab ganda, yaitu memenuhi standar profesional perbankan sekaligus memastikan setiap keputusan tidak melanggar prinsip-prinsip hukum Islam yang diawasi oleh Dewan Pengawas Syariah (DPS).

Prinsip-prinsip GCG seperti transparansi dan akuntabilitas sebenarnya merupakan cerminan dari etika Islam yaitu Shiddiq (jujur) dan Amanah (dapat dipercaya). Dalam perbankan syariah, transparansi mewajibkan bank untuk memberikan informasi yang jujur terkait skema akad dan nisbah bagi hasil agar nasabah benar-benar memahami risiko serta keuntungan yang ada, yang secara langsung mencegah terjadinya ketidakpastian atau gharar. Selain itu, akuntabilitas menjadi fondasi penting karena bank syariah mengelola dana titipan nasabah yang posisinya adalah mitra, sehingga setiap langkah dalam mengelola dana tersebut harus dapat dipertanggungjawabkan demi menjaga kepercayaan publik.

Keamanan Siber

Keamanan siber atau pertahanan siber adalah cara-cara dan mekanisme yang digunakan untuk melindungi serta mengurangi gangguan terhadap kerahasiaan, integritas, dan ketersediaan informasi (Rizki, 2022). Keamanan siber merupakan upaya untuk membangun kepastian dan kepercayaan bagi para penggunanya. Dengan memastikan bahwa informasi hanya bisa diakses oleh pihak yang berhak, data tidak dimanipulasi oleh tangan yang tidak bertanggung jawab, dan sistem selalu siap diakses saat dibutuhkan, keamanan siber berfungsi sebagai garda terdepan dalam menjaga integritas perusahaan.

Keamanan Siber Pada Perbankan Syariah

Keamanan siber saat ini menjadi pilar utama dalam menjaga stabilitas keuangan perbankan syariah. Keamanan siber bukan hanya masalah teknis, tetapi juga elemen penting untuk menjaga kepercayaan publik terhadap lembaga keuangan (Restika & Sonita, 2023). Hal ini menunjukkan bahwa keamanan data nasabah berbanding lurus dengan stabilitas likuiditas. Jika nasabah kehilangan kepercayaan akibat kebocoran data, risiko penarikan dana massal akan mengancam ketersediaan kas bank.

Bank syariah wajib mematuhi standar keamanan hukum sekaligus memastikan kepatuhan terhadap prinsip syariah, seperti transparansi dan perlindungan nasabah (Restika & Sonita, 2023). Artinya, sistem keamanan siber di bank syariah tidak boleh hanya canggih, tetapi juga harus mencerminkan prinsip kehati-hatian dan amanah. Pelanggaran siber di bank syariah bukan hanya sekedar kerugian materi, tetapi juga bentuk pelanggaran terhadap etika islam yang merusak reputasi bank. Beberapa tantangan keamanan siber utama yang dihadapi oleh bank syariah (Restika & Sonita, 2023):

a. Serangan phising dan social engineering: Bank syariah mudah menjadi target serangan phishing yang memanfaatkan cara-cara psikologis untuk mendapatkan informasi sensitif dari nasabah atau pegawai. Serangan phishing yang berhasil dapat merusak nama baik bank syariah dan menyebabkan nasabah kehilangan uangnya.

b. Malware dan ransomware: Bisa menyebabkan data bocor, informasi keuangan dicuri, atau sistem terkunci yang mengganggu jalannya operasional bank. Tidak bisa mengontrol sistem dan data sensitif, serta bisa terkena tebusan dalam serangan ransomware.

c. Tantangan kepatuhan syariah: Memastikan keamanan siber sekaligus mematuhi prinsip-prinsip syariah menjadi tantangan yang unik bagi bank syariah, karena mereka harus tetap menjaga kepatuhan terhadap norma dan etika Islam. Pelanggaran terhadap prinsip syariah bisa merusak reputasi bank syariah dan mengganggu keseimbangan keuangan yang bergantung pada kepercayaan nasabah

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur sistematis untuk menganalisis bagaimana tata kelola keamanan siber diintegrasikan dengan Maqashid Syariah. Data diambil dari 20 sumber referensi yang dipilih, yaitu berbagai dokumen, termasuk peraturan OJK (POJK 11/2022 dan SEOJK 21/2023), Laporan Tahunan BSI, serta artikel akademik dari Google Scholar, Garuda, dan

Sinta. Kriteria inklusi difokuskan pada dokumen yang membahas tata kelola teknologi informasi, perbankan syariah, dan perlindungan data, sedangkan sumber yang tidak terkait dengan kebijakan perbankan atau prinsip syariah tidak dimasukkan.

Teknik analisis dilakukan dengan metode analisis konten dalam tiga tahap, yaitu reduksi data, penyajian data, dan penarikan kesimpulan. Proses ini dilakukan dengan mengidentifikasi aspek-aspek teknis keamanan siber dalam mengacu pada tiga dimensi maqashid syariah, yaitu melindungi harta (Hifz al-Mal), melindungi akal (Hifz al-'aql), dan melindungi martabat (Hifz al-'Ird). Hasil dari analisis tersebut kemudian digunakan untuk menyusun model manajemen keamanan siber yang didasarkan pada Maqashid Syariah yang diusulkan dalam penelitian ini.

HASIL DAN PEMBAHASAN

Tata Kelola Kemanan Siber dalam Regulasi Perbankan

Dalam dunia perbankan syariah, keamanan siber bukan lagi pilihan, melainkan kewajiban. Otoritas Jasa Keuangan (OJK) melalui (POJK 11/2022, 2022) menetapkan bahwa bank wajib memiliki sistem TI yang aman dan bertanggung jawab untuk melindungi data nasabah. Standar ini dipertegas oleh SEOJK Nomor 24/SEOJK.03/2023 ((OJK), 2024) yang mewajibkan bank melakukan dua hal penting, yaitu rutin mengecek tingkat keamanan (maturitas) dan rutin melakukan simulasi serangan siber. Aturan ini mewajibkan unit keamanan siber bekerja secara independen agar pengawasan terhadap risiko siber tetap objektif dan tidak terganggu oleh kepentingan operasional.

Respons Krisis Siber BSI Tahun 2023

Pada Mei 2023, BSI diduga mengalami serangan ransomware Lockbit 3.0 yang sempat menganggu layanan digital mereka. Dalam merespon hal ini, BSI melakukan beberapa tindakan (Maulana, B. R., & Nasrulloh, 2024), berikut penjelasannya:

Tabel 1: Respons Kasus Bank Syariah Indonesia (2023)

No	Kategori	Tindakan yang Diambil BSI	Tujuan
1	Komunikasi	Penggunaan narasi *maintenance* (awal) dan penjelasan bertahap (lanjutan) berbasis SCCT (*Situational Crisis Communication Theory*)	*Diminish & Rebuilding*, mengurangi kepanikan publik dan memulihkan reputasi.
2	Teknis	Restorasi sistem, konsolidasi *gateaway*, enkripsi data, dan *multi-factor authentication*.	Menjamin keberlangsungan operasional
3	Manajerial	Kolaborasi dengan BSSN dan OJK, serta layanan *weekend banking*.	Mendapatkan legitimasi eksternal dan membuktikan pemulihan layanan.
4	Komersial	Program Loyalitas nasabah dan insentif (Pesta Hadiah)	Kompensasi untuk meredam kekecewaan dan mempertahankan loyalitas.

Sumber : Diolah dari (Nasrulloh & Maulana), (Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber), (2024).

Merujuk pada BSI Annual Report 2023 Hal 225, BSI menyatakan komitmennya pada pengawasan keamanan yang memadai dalam setiap pengembangan atau modifikasi sistem TI dan memastikan ketahanan dan keamanan siber Bank secara independen terhadap fungsi pengelolaan operasional TI. Selain aspek teknis, komunikasi saat krisis juga menjadi faktor kunci. Nasabah sangat membutuhkan transparansi informasi di saat layanan terganggu. Menurut (Liddiana et al., 2026), keterbukaan informasi terbukti mampu meredam kekhawatiran publik. Selain komunikasi krisis, reputasi perusahaan berperan sebagai aset strategis, nasabah dengan persepsi positif cenderung memberikan toleransi lebih tinggi terhadap gangguan layanan (Liddiana et al., 2026). Sejalan dengan itu, (Julianto & Prasetiyo, 2025) menambahkan bahwa strategi public relations menjadi instrumen penting bagi BSI dalam membangun kembali reputasi dan kepercayaan publik. Mengingat bahwa kepercayaan berpengaruh signifikan terhadap loyalitas nasabah, peningkatan kepercayaan tersebut menjadi kunci untuk memastikan retensi nasabah jangka panjang (Azizah & Udayana, 2023).

Setelah melewati fase krisis yang menguji stabilitas operasional, BSI tidak hanya berhenti pada pemulihan layanan. Krisis itu menjadi pemicu bagi BSI untuk melakukan evaluasi yang mendalam dan memperkuat dasar teknologinya. Setelah krisis, fokus utamanya adalah memperkuat pertahanan agar kejadian serupa tidak terjadi lagi, dengan mengacu pada “Kebijakan Teknologi Informasi PT Bank Syariah Indonesia, Tbk” sebagai dasar utama yang kini lebih terintegrasi dengan nilai-nilai syariah (PT Bank Syariah Indonesia tbk, 2023).

Kebijakan Teknologi Informasi & Keamanan Siber

Penyelenggaraan Teknologi Informasi (TI) di BSI diatur melalui struktur tata kelola yang jelas untuk menjamin efektivitas operasional dan keamanan data:

a. Dewan Komisaris, bertanggung jawab melakukan evaluasi, pengarahan, dan pemantauan strategi dan tata kelola TI, termasuk aspek manajemen risiko dan audit.

b. Direksi, memiliki wewenang penuh dalam pengaturan strategi TI, kebijakan, manajemen risiko, juga memastikan kompetensi SDM dan perlindungan kepentingan bank dalam kontrak pihak ketiga.

c. Komite Pengarah TI, bertugas memberikan rekomendasi kepada direksi dan memastikan setiap proyek TI selaras dengan rencana strategis bank.

d. Satuan Kerja TI, bertanggung jawab operasional atas seluruh siklus hidup TI, mulai dari perencanaan, pengembangan, hingga pemantauan.

Ketahanan dan Keamanan Siber (KKS)

BSI menggabungkan pengelolaan risiko siber ke dalam manajemen risiko perusahaan dengan fokus pada:

a. Proses utama meliputi pengenalan aset dan ancaman, perlindungan (seperti pengembangan kode yang aman dan pengelolaan akses), mendeteksi dan melakukan pengawasan berkelanjutan.

b. Bank harus membuat fungsi keamanan siber yang berdiri sendiri, terpisah dari bagian teknologi informasi, agar kontrol keamanan bisa lebih objektif dan tidak dipengaruhi oleh kepentingan operasional lainnya.

c. Diwajibkan melakukan penilaian mandiri tahunan terkait tingkat kesiapan keamanan siber yang dilaporkan ke OJK, dan melakukan pengujian keamanan secara berkala dengan metode analisis kerentanan dan simulasi skenario.

Integrasi Keamanan Siber dengan Hifz al-Mal (Pelindung Harta)

Dalam prinsip ekonomi Islam, dana nasabah adalah titipan yang harus dijaga dengan sungguh-sungguh. Pasca-krisis, BSI memperkuat sistem keamanan siber bukan hanya untuk kepentingan teknis, tetapi sebagai bentuk tanggung jawab agama dalam melindungi harta nasabah dari pencurian atau manipulasi data. Selain itu, sistem audit syariah digital yang terintegrasi dengan core banking system juga memastikan transparansi transaksi, memastikan kepatuhan terhadap prinsip syariah, sekaligus memitigasi risiko spekulasi atau penyalahgunaan dana yang tidak sesuai dengan hukum Islam (Amhar Maulana Harahap, 2022).

Integrasi Keamanan Siber dengan Hifz al-‘aql dan Literasi Digital

Hifz al-‘aql (menjaga akal) di era digital berarti menjaga nasabah dari informasi yang menyesatkan. Banyak nasabah yang terjebak penipuan (seperti phising) karena kurangnya informasi. BSI berperan aktif memberikan literasi digital agar nasabah tetap rasional dan waspada saat bertransaksi. Selain itu, nasabah juga harus berhati-hati dengan segala aktivitas yang mencurigakan seperti pengiriman file anonim yang dapat meretas akun mereka. Dengan nasabah yang berhati-hati serta literasi digital yang aktif dari BSI, risiko kejahatan siber dapat ditekan secara signifikan.

Integrasi Keamanan Siber dengan Hifz al-‘Ird dan Perlindungan Privasi

Privasi adalah bagian dari kehormatan atau Hifz al-‘Ird. Kebocoran data bukan hanya masalah sistem, tetapi pelanggaran martabat nasabah. Dengan kebijakan kontrol akses yang lebih ketat, BSI berupaya melindungi privasi nasabah. Sistem yang aman memastikan bahwa kepercayaan nasabah yang telah dibangun tidak rusak, karena akses terhadap data pribadi dibatasi hanya untuk pihak yang berwenang.

Model Tata Kelola Keamanan Siber Berbasis Maqashid Syariah

Tata kelola keamanan siber perbankan syariah saat ini telah melampaui paradigma administratif kepatuhan regulatif menuju paradigma berbasis nilai yang mengintegrasikan maqashid syariah. Model ini menempatkan keamanan siber bukan hanya sebagai tanggung jawab teknis, tetapi juga sebagai bentuk ibadah dalam menjalankan amanah nasabah. Model tata kelola ini beroperasi melalui tiga pilar utama yang didukung oleh berbagai literatur akademis:

Tabel 2: Model Tata Kelola Keamanan Siber Berbasis Maqashid Syariah

Pilar Utama	Dimensi Maqashid Syariah	Fokus Strategis	Referensi
Antisipatif	Amanah	Manajemen risiko siber komprehensif	(Amalina & Sari, 2025)
Stabilitas	*Hifz al-Nafs & Mal*	Penguatan *core banking* & likuiditas	(Nurhasim et al., 2026); (Putra et al., 2025)
Akuntabilitas	*Maslahah*	Audit sistem oleh Dewan Pengawas Syariah	(Regin Aeros Fidiyah, 2025)

Sumber : Hasil sintesis penulis berdasarkan literatur terkait (2026).

Tabel di atas menyajikan model tata kelola keamanan siber yang mengintegrasikan aspek teknis dengan nilia-nilai maqashid syariah. Secara operasional, model ini mengubah cara pandang bank terhadap keamanan informasi. Model tata kelola keamanan siber berbasis maqashid syariah yang diusulkan dalam penelitian ini merupakan bentuk sintesis dari pemikiran Amalina & Sari (2025), Nurhasim et al., (2026), Putra et al., (2025), serta Regin Aeros Fidiyah (2025), yang kemudian diadaptasi untuk memenuhi kebutuhan strategis perbankan syariah di Indonesia.

Pertama, melalui pilar antisipatif, bank tidak lagi sekedar bereaksi terhadap serangan, melainkan membangun sistem pertahanan proaktif sebagai wujud menjaga amanah. Kedua, melalui pilar stabilitas, keamanan siber diposisikan sebagai fondasi untuk menjaga keberlangsungan institusi dan harta nasabah, yang secara langsung berdampak pada kemaslahatan ekonomi. . Selain itu, stabilitas lembaga keuangan adalah perwujudan dari Maslahah. Ariyanto, 2024 menjelaskan bahwa transparansi dalam krisis menjadi kunci untuk menjaga kepercayaan publik. Stabilitas ini memerlukan manajemen aset dan liabilitas yang adaptif. Ketiga, melalui pilar akuntabilitas, peran Dewan Pengawas Syariah (DPS) menjadi penting untuk memastikan bahwa seluruh infrastruktur TI berjalan selaras dengan prinsip syariah.

Dengan pendekatan ini, keamanan siber bertransformasi dari sekadar bagian operasioanl menjadi indikator kerja utama. Pendekatan ini memastikan bahwa setiap inovasi digital yang diterapkan tetap berada dalam koridor perlindungan nasabah dan sesuai syariah Islam.

KESIMPULAN

Berdasarkan hasil analisis, cara mengelola keamanan siber di PT Bank Syariah Indonesia Tbk sudah berubah dari pendekatan yang reaktif menjadi sebuah kerangka kerja yang terpadu dan didasarkan pada nilai-nilai Maqashid Syariah. Penerapan aturan dari OJK (POJK Nomor 11/POJK.03/2022 dan SEOJK Nomor 21/SEOJK.03/2023) memberikan dasar struktur yang kuat. Lebih lanjut, perlindungan data nasabah kini dianggap sebagai bentuk nyata dari hifz al-mal (mengamankan harta), hifz al-'aql (mengamankan akal melalui pendidikan digital), dan hifz al-'ird (mengawal martabat privasi). Penelitian ini menemukan tiga hal penting. Pertama, keamanan siber di bank syariah berperan sebagai alat perlindungan bagi tujuan pokok syariah, yaitu melindungi harta nasabah dari tindak kejahatan digital, menjaga pemahaman dan kesadaran nasabah tentang teknologi digital, serta menjaga kehormatan nasabah dengan memastikan data pribadi tidak disalahgunakan. Kedua, cara BSI merespons krisis setelah insiden 2023 menunjukkan bahwa transparan dan komunikasi yang baik saat menghadapi krisis sangat penting untuk menjaga kepercayaan dan tanggung jawab terhadap publik. Ketiga, model pengelolaan keamanan siber yang didasarkan pada maqashid syariah terbukti mampu menjadikan aspek teknis perlindungan data sebagai tolak ukur utama yang sesuai dengan tujuan besar dari ekonomi Islam.

Untuk memperkuat ketahanan siber dan implementasi nilai syariah di masa depan, penelitian ini mengajukan beberapa rekomendasi: Bagi Manajemen Bank Syariah: Disarankan untuk terus memperkuat mekanisme pelaporan insiden yang transparan serta mengadopsi teknologi keamanan siber yang mutakhir. Meningkatkan pemahaman keamanan bagi nasabah juga penting untuk memperkuat ketahanan terhadap kejahatan digital. Bagi Otoritas Jasa Keuangan (OJK): Diharapkan untuk terus memperbarui standar teknis keamanan siber dengan menggabungkan nilai-nilai syariah, sehingga perbankan syariah memiliki standar pengelolaan teknologi informasi yang tetap bisa bersaing.

Bagi Dewan Pengawas Syariah: Perlu memperkuat peran dalam meninjau sistem informasi sebagai bagian dari audit syariah tahunan, untuk memastikan bahwa infrastruktur teknologi informasi memenuhi prinsip kehati-hatian dan transparansi. Bagi Peneliti Berikutnya: Diharapkan untuk memperluas cakupan penelitian melalui pendekatan empiris atau studi komparatif antar lembaga keuangan syariah untuk mengukur efektivitas model tata kelola keamanan siber perbankan syariah secara lebih luas.

REFERENSI

Algifari, M. A., & Andrini, R. (2024). Maqasid Syariah Dalam Pengembangan Ekonomi Islam (Analisis Komprehensif dan Implementasi). JoSES: Journal of Sharia Economics Scholar, 2(3), 95–100. https://doi.org/10.5281/zenodo.14522804

Amalina, N., & Sari, V. F. (2025). Karakteristik Dewan Dan Cybersecurity Disclosure (CSD) Pada Perusahaan Perbankan Indonesia. E-Jurnal Akuntansi, 35(10), 2063–2077. https://doi.org/10.24843/EJA.2025.v35.i10.p03

Amhar Maulana Harahap. (2022). Kebijakan Dan Implementasi Digitalisasi Perbankan Syariah di Indonesia Dalam Sistem Informasi Perbankan. Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah, 11(204), 543–559. https://journal.um-surabaya.ac.id/Mas/article/view/30723/10620

Andrianto, & Firmansyah, A. (2019). Buku Manajemen Syariah: Implementasi dan Praktek (Q. Media, Ed.). CV. Penerbit Qiara Media.

Ariyanto, S. (2024). Analisis Framing Model Robert N. Entman tentang Serangan Ransomware Pada PT Bank Syariah Indonesia Tbk. CommLine, 9(1), 59. https://doi.org/10.36722/cl.v9i1.2899

Azizah, B. P., & Udayana, I. B. N. (2023). Pengaruh Kepercayaan Dan Kepuasan Pelanggan Terhadap Loyalitas Nasabah Bank Syariah. Jurnal Ilmiah Manajemen EMOR (Ekonomi Manajemen Orientasi Riset), 2(1), 306–312.

Erni, Rehani, N., & Ilham Ilham. (2025). Tata Kelola Perbankan Syariah. Jurnal Bisnis, Ekonomi Syariah, Dan Pajak, 2(2), 01–12. https://doi.org/10.61132/jbep.v2i2.965

Jauhari, J. (2024). Penerapan Prinsip Maqashid Syariah Dalam Perundang-Undangan Di Indonesia. Karimiyah (Journal Of Islamic Literature and Muslim Society), 4(1), 1–14. https://doi.org/10.59623/karimiyah.v4i1.49

Julianto, P. R., & Prasetiyo, L. (2025). Economics And Digital Business Review Strategi Public Relations BSI Dalam Membangun Reputasi Pasca Insiden Gangguan Sistem Analisis Konten Berbasis Pemberitaan. Economics and Digital Business Review, 6(2), 1543–1556.

Liddiana, A., Aminullah, M., & Andrean, R. (2026). Pemulihan Kepercayaan Nasabah Bank Syariah Pasca Kegagalan Layanan Digital : Analisis Komunikasi Krisis Dan Reputasi Perusahaan Pada Byond By BSI. JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin, 3(1), 1–13.

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. Politeia: Jurnal Ilmu Politik, 14(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. EKSISBANK (Ekonomi Syariah Dan Bisnis Perbankan), 8, 76–91.

Nurhasim, Nofal, I., & Aguspriyani, Y. (2026). Optimalisasi Manajemen Aset Dan Liabilitas Dalam Meningkatkan Ketahanan Likuiditas Bank Syariah Di Era Digital Banking. Jurnal Ekonomi Bisnis, Manajemen Dan Akuntansi (JEBMAK), 5(2).

POJK 11/2022. (2022). Penyelenggaraan Teknologi Informasi Oleh Bank Umum.

PT Bank Syariah Indonesia tbk. (2023). Kebijakan Teknologi Informasi PT Bank Syariah Indonesia tbk (Vol. 2, Number 29). https://ir.bankbsi.co.id

Putra, K. P. D., Sutopo, J., & Suhirman. (2025). Studi Literatur Audit ISO 27001 , COBIT , Dan ITIL Pada Layanan Sistem Informasi JURNAL MEDIA INFORMATIKA [JUMIN]. Jurnal Media Informatika (JUMIN), 6(6), 2911–2920.

Regin Aeros Fidiyah. (2025). Penerapan Prinsip Maqashid Syariah Dalam Tata Kelola Internal Perseroan Syariah: Analisis Terhadap Mekanisme Eksekusi Dan Perlindungan Konsumen. Sighat: Jurnal Hukum Ekonomi Syariah, 3(2), 23–33. https://doi.org/10.35905/shighat_hes.v3i2.14668

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. Krigan: Journal of Management and Sharia Business, 1(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

(OJK), O. J. K. (2024). SEOJK 24-SEOJK.03-2023. Penilaian Tingkat Maturitas Digital Bank Umum. In Otoritas Jasa Keuangan (Vol. 235).