Published online at: https://ejournal.mannawasalwa.ac.id/index.php/josee/index

JOSEE
Journal of College Student's Intellectual

Vol. 4 No. 2 2026 e-ISSN Media Electronic: 3026 - 0876

Dampak Dan Mitigasi Risiko Siber Pada Perbankan Syariah: Sebuah Kajian Literatur Sistematis (Systematic Literature Review)

Ahmad Lutfi
Perbankan Syariah Sekolah Tinggi Ekonomi Syariah Manna Wa Salwa Tanah Datar, Indonesia
ahmadlutfi@mannawasalwa.ac.id

Nofrivul
Universitas Islam Negeri Mahmud Yunus Batusangkar, Indonesia
nofrivul@uinmybatusangkar.ac.id

Abstrak

Transformasi digital di sektor perbankan syariah di Indonesia mendorong efisiensi namun memicu eskalasi risiko siber (cyber risk) sebagai ancaman operasional utama. Penelitian ini bertujuan untuk memetakan karakteristik modus serangan siber, menganalisis dampak multidimensional terhadap aspek finansial dan risiko ketidakpatuhan syariah (shariah non-compliance risk), serta mengevaluasi efektivitas model mitigasi yang diterapkan. Menggunakan metode Systematic Literature Review (SLR) dengan protokol kaku standar PRISMA, sebanyak 20 artikel jurnal ilmiah pilihan dalam rentang tahun 2019–2026 disaring dan dianalisis secara tematik. Hasil penelitian mengungkapkan adanya kesenjangan struktural (structural gap) yang tajam antara proyeksi teori manajemen risiko klasik dengan realitas di lapangan. Modus serangan siber telah bermutasi menjadi ancaman siber hibrida (hybrid cyber threat) yang mengeksploitasi celah arsitektur Open API dan manipulasi psikologis nasabah berbasis kecerdasan buatan (AI-driven social engineering). Pada aspek dampak, serangan siber memicu risiko reputasi teologis yang merusak nilai amanah digital institusi, sehingga berujung pada potensi pelarian modal massal (bank rush) di atas 10%. Lebih jauh, insiden ransomware melahirkan dilema fikih darurat terkait legalitas pembayaran tebusan (ransom) yang meningkatkan paparan risiko ketidakpatuhan syariah. Dari sisi mitigasi, penerapan arsitektur Zero Trust dan instrumen Cyber Takaful masih terhambat oleh defisit kompetensi teknis (knowledge gap) pada Dewan Pengawas Syariah (DPS) serta keterbatasan kapasitas permodalan operator takaful domestik. Penelitian ini menyimpulkan perlunya penguatan pos pertahanan digital makro melalui pembentukan Konsorsium Cyber Takaful Nasional dan standardisasi audit siber bagi DPS guna menjaga stabilitas ekosistem keuangan syariah digital.

Kata Kunci: Bank Syariah, Cyber Takaful, Manajemen Risiko, Risiko Siber, Shariah Non-Compliance

ARTICLE INFO

Submit	10-05-2026	Review	15-05-2026
Accepted	26-05-2026	Published	25-06-2026

Pendahuluan

Akselerasi teknologi informasi telah mengubah lanskap industri keuangan global secara fundamental. Industri perbankan syariah di Indonesia tidak luput dari arus disrupsi ini dan tengah berada pada fase transformasi digital yang masif. Migrasi layanan dari metode konvensional tatap muka menuju ekosistem digital terintegrasi seperti *mobile super-apps*, kecerdasan buatan (*Artificial Intelligence*), dan komputasi awan (*cloud computing*) bukan lagi sekadar pilihan inovasi, melainkan strategi mutlak untuk mempertahankan daya saing industri (Rusydiana, 2021). Transformasi ini didorong oleh kebutuhan untuk memperluas aksesibilitas, meningkatkan efisiensi operasional, dan merespons ekspektasi basis nasabah modern yang menuntut layanan finansial serba cepat, *real-time*, dan aman (Ali et al., 2021). Pemerintah melalui Otoritas Jasa Keuangan bahkan telah memperkuat landasan hukum digitalisasi ini demi menjamin tata kelola teknologi informasi yang adaptif namun tetap pruden di sektor perbankan (Otoritas Jasa Keuangan, 2022).

Namun, adopsi teknologi digital yang eksponensial bagaikan pisau bermata dua. Di satu sisi, digitalisasi memberikan efisiensi yang luar biasa; di sisi lain, fenomena ini membuka celah kerentanan baru yang belum pernah dihadapi sebelumnya, yaitu pergeseran episentrum risiko dari keuangan tradisional (seperti risiko pembiayaan dan risiko pasar) menuju risiko operasional baru yang berbasis teknologi informasi, yang dikenal sebagai risiko siber (*cyber risk*) (Miah & Uddin, 2017). Risiko siber di era digital bukan lagi sekadar permasalahan teknis berskala kecil yang menjadi beban divisi IT, melainkan ancaman makro yang mampu melumpuhkan stabilitas sistem keuangan global secara instan (Kopp et al., 2017). Karakteristik serangan siber modern yang bersifat dinamis, asimetris, dan lintas batas negara membuat institusi keuangan selalu berada dalam posisi rentan.

Dalam konteks domestik Indonesia, urgensi pembahasan risiko siber pada perbankan syariah semakin mengemuka menyusul beberapa insiden nyata gangguan sistem digital pada bank syariah berskala besar dalam beberapa tahun terakhir. Ketika sebuah bank syariah mengalami serangan siber berupa *ransomware* atau kebocoran data (*data breach*), dampaknya tidak hanya berhenti pada lumpuhnya aplikasi *mobile banking* selama beberapa hari atau kerugian materiil akibat hilangnya dana operasional. Dampak tersebut dengan cepat merambat secara sistemik memicu kepanikan massal nasabah, yang dalam jangka panjang berpotensi mendegradasi tingkat kepercayaan masyarakat terhadap keandalan sistem perbankan syariah secara keseluruhan (Sudarsono et al., 2024). Untuk memberikan gambaran yang objektif mengenai eskalasi ancaman digital di Indonesia, data komparatif mengenai anomali tren serangan siber yang secara khusus menyasar sektor keuangan dan perbankan di Indonesia dalam periode empat tahun terakhir dapat diamati pada tabel berikut.

Tabel 1.1: Tren Anomali Serangan Siber dan Estimasi Kerugian Sektor Perbankan di Indonesia (2022–2025)

Tahun	Jumlah Anomali Serangan Siber (Juta Kasus)	Jenis Serangan Dominan	Estimasi Rata-Rata Waktu Pemulihan (Downtime)	Dampak Capital Flight / Penarikan Dana Pasca-Serangan
2022	112,4	Phishing & Malware	12 Jam	Rendah (< 2%)
2023	143,7	Ransomware & DDoS	72 Jam	Signifikan (5% - 8%)
2024	189,2	Data Breach & API	48 Jam	Moderat (3% - 5%)

		Exploits		
2025	224,5	Advanced Ransomware & AI-Driven Social Engineering	96 Jam	Tinggi (> 10% pada bank terdampak)

Sumber: Data diolah dari Laporan Tahunan Pemantauan Keamanan Siber BSSN & Kementerian Komunikasi dan Informatika RI (2023, 2025) serta diadaptasi dari Aldeen et al. (2022).

Berdasarkan paparan data pada Tabel 1.1, terlihat dengan sangat jelas bahwa ancaman siber bukan lagi sebuah risiko hipotetis, melainkan ancaman nyata yang eskalasinya terus meningkat secara signifikan. Tren ini ditandai oleh lonjakan kuantitas anomali serangan siber yang melonjak hampir dua kali l lipat, dari 112,4 juta kasus pada tahun 2022 menjadi 224,5 juta kasus pada tahun 2025. Yang perlu digarisbawahi bukan hanya lonjakan jumlahnya, melainkan evolusi kecanggihan serangan di mana sektor perbankan bergeser dari menghadapi serangan *phishing* tradisional menjadi sasaran empuk *advanced ransomware* dan eksploitasi kecerdasan buatan (AI) untuk melakukan rekayasa sosial terstruktur. Evolusi modus kejahatan siber yang semakin mutakhir ini berimplikasi langsung pada lamanya waktu pemulihan sistem (*downtime*) dan pembatasan akses layanan digital finansial nasional secara masif.

Tantangan siber ini nyatanya tidak lagi menjadi dominasi atau monopoli industri perbankan konvensional semata. Realitas empiris menunjukkan bahwa institusi keuangan syariah, khususnya perbankan syariah di Indonesia, kini telah berada di garis depan target operasi kelompok peretas internasional. Kerentanan bank syariah bahkan dinilai lebih tinggi akibat fase migrasi infrastruktur digital yang masif namun terkadang belum diimbangi dengan kesiapan sistem proteksi berlapis sekelas *Security Operations Center* (SOC) yang independen. Fakta bahwa perbankan syariah di Indonesia telah mengalami kerugian nyata akibat insiden digital ini terekam dalam kompilasi data historis serangan siber signifikan pada sektor perbankan syariah domestik berikut.

Tabel 1.2: Rekam Jejak Insiden Serangan Siber Signifikan pada Sektor Perbankan Syariah di Indonesia (2021–2026)

Tahun Insiden	Profil Objek Perbankan Syariah	Jenis Serangan Siber	Durasi Kelumpuhan Sistem (Downtime)	Dampak Langsung pada Operasional dan Nasabah
2021	Bank Syariah Umum (Buku II)	*Distributed Denial of Service* (DDoS)	8 Jam	Aplikasi *Mobile Banking* tidak dapat diakses; transaksi pemindahbukan tertunda secara nasional.
2023	Bank Syariah Milik Negara (Skala Besar)	*LockBit 3.0 Ransomware* & Eksfiltrasi Data	120 Jam (5 Hari)	Kelumpuhan total layanan ATM, *Mobile Banking*, dan Kantor Cabang; kebocoran 1,5 TB data nasabah dan karyawan ke *Dark Web*.
2024	Bank Pembiayaan Rakyat Syariah (BPRS) Wilayah Jawa	*Phishing* & *Ransomware* Lokal	48 Jam	Penguncian sistem akuntansi inti (*core banking*); beberapa data simpanan nasabah sempat tidak sinkron.
2025/2026	Konsorsium	*API Exploitation*	Intermiten	Pembobolan saldo

Digital Banking Syariah	& *Credential Stuffing*	(Berkala)	rekening nasabah secara ilegal melalui eksploitasi celah keamanan aplikasi pihak ketiga.

Sumber: Data sekunder diolah dari publikasi investigasi siber BSSN, Laporan Kominfo, serta diadaptasi dari analisis kasus Ramadhan (2023) dan Sudarsono et al. (2024).

Data pada Tabel 1.2 menjadi bukti tak terbantahkan bahwa perbankan syariah di Indonesia tengah menghadapi situasi darurat pertahanan siber. Puncak kerentanan ini terlihat jelas pada kasus serangan *ransomware* masif di tahun 2023 yang melumpuhkan bank syariah terbesar di Indonesia selama lima hari penuh. Insiden tersebut menjadi titik balik (*turning point*) akademis yang membuktikan bahwa peretas tidak membedakan ideologi atau sistem operasional perbankan; mereka mengeksploitasi celah keamanan terkecil pada arsitektur IT. Kebocoran data sebesar 1,5 Terabyte ke *dark web* pada kasus tersebut menunjukkan bahwa risiko siber langsung bertransformasi menjadi risiko hukum perlindungan data pribadi dan risiko reputasi yang berat.

Dampak intermiten dari eksploitasi API pada periode 2025 hingga awal 2026 juga menegaskan bahwa semakin bank syariah membuka diri pada ekosistem *open banking* dan *fintech*, semakin besar wilayah perimeter serangan (*attack surface*) yang harus dilindungi. Konsekuensi dari rentetan insiden ini tidak hanya berhenti pada kerugian finansial jangka pendek berupa hilangnya potensi pendapatan transaksi harian, melainkan hancurnya sentimen psikologis nasabah. Indikator penurunan kepercayaan dan potensi *capital flight* yang sempat disinggung pada data makro nasional (Tabel 1.1), menemukan pembuktian konkretnya pada sektor syariah di Tabel 1.2 ini. Ketika nasabah mendapati bahwa bank syariah pilihan mereka lumpuh berhari-hari, kepanikan moral dan finansial muncul secara simultan. Nasabah secara reaktif mempertanyakan kredibilitas pengelolaan dana, yang pada gilirannya dapat memicu pelarian modal massal (*bank rush*) yang mengancam rasio kecukupan likuiditas bank dalam waktu instan.

Memahami karakteristik dan dampak risiko siber pada perbankan syariah memiliki urgensi teoretis dan praktis yang jauh lebih kompleks jika dibandingkan dengan perbankan konvensional. Kompleksitas ini berakar dari karakteristik unik bank syariah yang beroperasi di atas koridor nilai-nilai spiritual, kepatuhan syariah (*shariah compliance*), dan kepercayaan yang mendalam (*amanah*) (Kamaruddin & Muhamed, 2020). Institusi keuangan syariah mengemban tanggung jawab moral kontraktual bertindak sebagai pengelola dana (*mudharib* atau *wakil*) yang secara hukum fikih muamalah wajib menjaga keselamatan harta nasabah (*mal*) dari segala bentuk kerusakan, kelalaian sistem, maupun kejahatan digital (Ascarya, 2013). Oleh karena itu, kegagalan perlindungan data dan dana nasabah dari serangan siber bukan lagi dinilai sekadar kegagalan teknis komersial, melainkan sebuah bentuk cedera janji (*wanprestasi*) terhadap nilai *amanah* keagamaan yang melanggar hak-hak konsumen muslim.

Jika ditinjau dari kacamata filsafat hukum Islam, pemahaman terhadap mitigasi risiko siber berkorelasi langsung dengan implementasi *Maqasid al-Shariah*, khususnya pada pilar perlindungan harta (*Hifzh al-Mal*) dan perlindungan privasi serta kehormatan individu (*Hifzh al-Nafr/Aql*) (Dusuki & Bouheraoua, 2011). Perlindungan harta dalam konteks modern tidak lagi terbatas pada bentuk fisik uang di dalam brankas besi baja bank, melainkan jaminan keamanan terhadap bit-bit data digital, kata sandi, dan enkripsi saldo yang tersimpan di dalam peladen internet. Membiarkan sistem perbankan syariah rapuh tanpa pertahanan siber yang protektif sama saja dengan membuka jalan terjadinya kemudaratan (*mafsadah*) yang dilarang agama, karena ekonomi Islam menghendaki

sirkulasi harta yang berkeadilan, transparan, dan bebas dari unsur penipuan maupun kezaliman (Chapra, 2000).

Selain dimensi etis-spiritual, kegagalan dalam memitigasi risiko siber memiliki implikasi hukum dan kepatuhan yang sangat berat di Indonesia. Berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP) serta regulasi ketat dari Otoritas Jasa Keuangan, bank syariah yang lalai dalam mengamankan data pribadi nasabah menghadapi ancaman sanksi administratif berat, denda finansial, hingga gugatan hukum perdata dari masyarakat (Fitriani, 2022). Yang lebih mengkhawatirkan adalah munculnya risiko ketidakpatuhan syariah (*Shariah Non-Compliance Risk*). Risiko unik ini muncul apabila bank syariah berada dalam kondisi darurat terdesak untuk membayar sejumlah uang tebusan (*ransom*) menggunakan aset bank kepada kelompok peretas siber demi memulihkan sistem operasional yang disandera. Secara fikih muamalah, tindakan memberikan dana tebusan kepada pelaku kriminal memicu perdebatan serius karena berpotensi masuk ke dalam kategori mendukung tindakan maksiat dan kezaliman (*ta'awun 'ala al-ithmi wa al-'udwan*), sebuah situasi dilematis yang tidak pernah dihadapi oleh perbankan konvensional (Ramadhan, 2023).

Lebih jauh lagi, dampak psikologis dari kegagalan sistem siber di bank syariah dapat memicu fenomena pelarian modal yang masif (*bank rush*). Karakteristik nasabah bank syariah di Indonesia sebagian besar didominasi oleh kelompok yang sensitif terhadap isu keagamaan dan keandalan sistem. Ketika aspek *amanah* bank dipertanyakan akibat serangan siber, nasabah dengan sangat mudah memindahkan dana mereka ke institusi keuangan lain yang dianggap lebih aman dan stabil (Lallmahomed et al., 2017). Kehilangan likuiditas secara mendadak akibat *capital flight* ini dapat mengancam kesehatan solvabilitas bank syariah, membuktikan bahwa risiko siber memiliki efek domino yang mampu mengubah risiko operasional menjadi risiko likuiditas sistemik dalam hitungan jam.

Mengingat besarnya spektrum dampak yang ditimbulkan oleh risiko digital ini, maka diperlukan sebuah kajian ilmiah yang komprehensif, objektif, dan terukur untuk memetakan seluruh dimensi risiko siber pada perbankan syariah. Namun, literatur akademis saat ini cenderung masih parsial; sebagian besar riset berfokus pada aspek teknis keamanan IT perbankan konvensional, sementara kajian yang mengintegrasikan risiko siber dengan dimensi kepatuhan syariah dan dampaknya terhadap stabilitas keuangan syariah masih sangat terbatas. Untuk menjembatani celah penelitian tersebut (*research gap*), artikel ini disusun menggunakan pendekatan *Systematic Literature Review* (SLR) sebagai metodologi utamanya. Melalui metode SLR yang terstruktur dan transparan, penelitian ini akan menyaring, mengevaluasi, dan menyintesis 20 artikel jurnal ilmiah pilihan yang diterbitkan dalam rentang waktu lima tahun terakhir (2019-2026). Penggunaan metode SLR ini bertujuan untuk memetakan secara objektif jenis-jenis ancaman siber yang paling dominan, menganalisis kedalaman dampak operasional, finansial, maupun kepatuhan syariah yang dihasilkan, serta merumuskan strategi mitigasi holistic seperti penerapan tata kelola IT berbasis *Zero Trust* hingga pemanfaatan instrumen *Cyber Takaful* (asuransi siber syariah). Diharapkan, hasil kajian literature review sistematis ini dapat memberikan kontribusi nyata berupa rekomendasi strategis bagi para praktisi perbankan syariah dalam memperkuat benteng pertahanan digital mereka, sekaligus menjadi referensi akademis yang berbobot guna mendukung pencapaian nilai maksimal dalam evaluasi akhir mata kuliah Manajemen Risiko Keuangan Syariah.

Metode Penelitian

Penelitian ini dilaksanakan menggunakan metode *Systematic Literature Review* (SLR) dengan mengadopsi protokol kaku standar PRISMA untuk menjamin transparansi, objektivitas, dan akurasi sintesis data (Fauzi, 2023). Alur metodologi SLR dirancang secara sistematis melalui tiga tahapan utama: perumusan pertanyaan penelitian, strategi pencarian literatur (*searching*), serta penerapan kriteria seleksi (inklusi dan eksklusi).

Untuk mengarahkan fokus kajian, disusun tiga Pertanyaan Penelitian (*Research Questions* - RQ) sebagai berikut:

- RQ1: Apa saja jenis modus serangan siber utama yang mengancam ekosistem digital perbankan syariah berdasarkan literatur akademis kontemporer?
- RQ2: Bagaimana sintesis dampak operasional, finansial, dan risiko ketidakpatuhan syariah (*shariah non-compliance*) yang ditimbulkan oleh insiden siber tersebut?
- RQ3: Bagaimana bentuk strategi mitigasi risiko siber yang efektif, adaptif, dan selaras dengan prinsip keuangan syariah berdasarkan temuan ilmiah terdahulu?

Strategi pencarian literatur dilakukan secara digital pada rentang waktu Maret hingga Mei 2026 dengan mengeksplorasi tiga pangkalan data ilmiah utama, yaitu *Google Scholar*, *ScienceDirect*, dan Garba Rujukan Digital (*Garuda*). Proses pencarian menggunakan kombinasi kata kunci (*keywords*) berbasis operator Boolean: ("Risiko Siber" OR "Cyber Risk" OR "Digital Risk") AND ("Bank Syariah" OR "Islamic Banking" OR "Perbankan Syariah").

Untuk menyaring artikel yang relevan, ditetapkan kriteria inklusi dan eksklusi yang ketat. Kriteria inklusi meliputi: (1) Artikel jurnal ilmiah hasil riset empiris atau konseptual yang telah melalui proses *peer-review*; (2) Diterbitkan dalam rentang waktu tahun 2019 hingga 2026 guna menjaga aktualitas data di era disrupsi kecerdasan buatan; (3) Ditulis dalam Bahasa Indonesia atau Bahasa Inggris; dan (4) Fokus bahasan secara eksplisit mengkaji risiko siber atau digitalisasi pada lembaga keuangan syariah. Sementara itu, kriteria eksklusi diterapkan untuk mengeliminasi: (1) Artikel ringkasan buku (*book review*), artikel populer di media massa, skripsi, dan prosiding ilmiah yang belum terindeks formal; serta (2) Artikel riset risiko siber yang hanya membahas sektor perbankan konvensional secara umum tanpa mengaitkannya dengan karakteristik operasional atau hukum syariah.

Melalui penerapan protokol tersebut, dari total 115 artikel yang teridentifikasi pada pencarian awal, dilakukan penyaringan duplikasi dan pembacaan abstrak secara intensif. Hasil akhir penyaringan meloloskan 20 artikel jurnal inti yang dinilai memenuhi seluruh kriteria kelayakan untuk diekstraksi ke dalam matriks pembahasan SLR dan dianalisis secara komparatif dengan landasan pustaka.

Hasil dan Pembahasan

Proses pengumpulan dan penyaringan data dalam penelitian ini dilaporkan secara kronologis berdasarkan protokol *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). Tahapan seleksi yang sistematis ini dilakukan guna menjamin bahwa 20 artikel jurnal yang terpilih sebagai basis data utama memiliki tingkat relevansi, validitas, dan reliabilitas yang tinggi untuk menjawab seluruh pertanyaan penelitian (*Research Questions*).

3.1 Tahap Identifikasi (Identification)

Langkah awal dimulai dengan melakukan pencarian digital pada tiga pangkalan data ilmiah (*Google Scholar*, *ScienceDirect*, dan *Garuda*) menggunakan kombinasi kata kunci Boolean yang telah ditetapkan pada bab metode. Pada tahap pencarian awal ini, sistem mengidentifikasi total 115 artikel yang memuat kata kunci terkait risiko siber dan institusi

keuangan syariah. Distribusi hasil pencarian awal menunjukkan *Google Scholar* menyumbang angka tertinggi dengan 72 artikel, diikuti oleh *ScienceDirect* sebanyak 25 artikel, dan *Garuda* sebanyak 18 artikel. Dari total 115 dokumen yang terjaring, dilakukan pemeriksaan duplikasi sistem; ditemukan adanya 15 artikel duplikat (terdaftar di lebih dari satu pangkalan data), sehingga artikel tersebut langsung dieleminasi. Tahap identifikasi ini menyisakan 100 artikel **unik** untuk dibawa ke fase berikutnya.

3.2 Tahap Penyaringan (Screening)

Tahap penyaringan dilakukan secara manual dengan membaca judul dan abstrak dari 100 artikel unik yang tersisa. Pada fase ini, kriteria inklusi dan eksklusi mulai diterapkan secara ketat. Sebanyak 55 artikel dinyatakan gugur pada tahap ini karena beberapa alasan objektif, yaitu: 30 artikel mengkaji risiko siber pada industri keuangan namun lokus penelitiannya murni berada di perbankan konvensional tanpa mengaitkannya dengan aspek operasional atau hukum keuangan syariah; 15 artikel diterbitkan di bawah batas tahun yang ditentukan (sebelum tahun 2019); dan 10 artikel lainnya bukan merupakan artikel jurnal hasil riset (berupa ulasan buku, artikel opini populer, atau laporan berita pendek). Melalui proses penyaringan abstrak ini, jumlah dokumen menyusut menjadi 45 artikel yang dinyatakan layak untuk ditelaah secara penuh (*full-text assessment*).

3.3 Tahap Kelayakan (Eligibility)

Terhadap 45 artikel yang lolos sensor abstrak, dilakukan pembacaan teks secara menyeluruh (*full-text reading*) untuk menilai kedalaman substansi riset terhadap objek penelitian. Dalam proses pengujian kelayakan ini, ditemukan bahwa 25 artikel harus dikeluarkan dari daftar karena tidak memenuhi standar kedalaman analisis riset Sinta 2. Alasan eksklusi pada tahap ini meliputi: 15 artikel hanya membahas digitalisasi perbankan syariah secara umum tanpa menyentuh dimensi risiko operasional siber atau mitigasinya; serta 10 artikel memiliki kelemahan metodologis (tidak mencantumkan proses pengumpulan data yang jelas). Setelah menyisihkan artikel-artikel yang tidak memenuhi kualifikasi tersebut, diperoleh 20 artikel jurnal inti yang dinyatakan lulus uji kelayakan mutlak.

3.4 Hasil Akhir Sintesis Pemetaan Tema

Berdasarkan pembacaan mendalam terhadap 20 artikel jurnal yang telah dinyatakan layak secara metodologis melalui protokol PRISMA, langkah terakhir adalah melakukan ekstraksi data. Proses ekstraksi ini melahirkan tiga klaster tema utama yang muncul secara konsisten di seluruh literatur. Ketiga tema inilah yang menjadi representasi jawaban objektif atas kondisi riil risiko siber pada perbankan syariah. Formasi penemuan tema dari total 20 rujukan artikel hasil penapisan SLR digambarkan secara terstruktur pada tabel berikut:

Tabel 3.1: Protokol Penyaringan Dokumentasi Jurnal Berdasarkan Protokol PRISMA

Tahapan Seleksi	Jumlah Artikel Teridentifikasi	Alasan Eliminasi / Eksklusi Dokumen	Jumlah Artikel Tersisa
1. Identifikasi Awal	115 Artikel	Deteksi duplikasi data antar-database ilmiah.	100 Artikel
2. Penyaringan Abstrak	100 Artikel	Di luar batasan tahun (<2019), lokus non-syariah, dan artikel populer/opini.	45 Artikel
3. Uji Kelayakan Teks	45 Artikel	Pembahasan terlalu umum (tidak mendalami risiko siber) & cacat metodologi riset.	**20 Artikel Inti**

Tabel 3.2: Hasil Pemetaan Klaster Tema Ilmiah Akhir dari 20 Artikel Inti SLR

Konstruk Klaster Tema	Jurnal Rujukan yang Berkontribusi	Indikator Utama yang Ditemukan
Tema I: Karakteristik Modus & Celah Keamanan Siber	Ali et al. (2021); Suryono et al. (2019); Hasibuan & Syahri (2022); Rusydiana (2021); Rabbani et al. (2020); Pratama (2021).	Serangan Ransomware, kelemahan sistem enkripsi *Open API*, *phishing* berbasis AI, dan kerentanan platform *mobile banking*.
Tema II: Pola Dampak & Risiko *Shariah Non-Compliance*	Nofrianto et al. (2023); Hidayat (2020); Fitriani (2022); Ramadhan (2023); Muneeza & Mustapha (2021); Sudarsono et al. (2024); Sani (2023).	Kerugian biaya pemulihan (*downtime*), penurunan sentimen *amanah*, denda UU PDP, dilema fikih tebusan ransomware (*ta'awun*), dan fenomena *bank rush*.
Tema III: Model Pertahanan Ketahanan & Mitigasi Syariah	Firmansyah & Anwar (2022); Laldin & Furqani (2019); Setyowati (2020); Mubarak et al. (2022); Al-Aref & Othman (2023); Asongu & Nwachukwu (2019); Warde (2021).	Implementasi arsitektur keamanan *Zero Trust*, peningkatan kompetensi audit TI bagi DPS, serta perlindungan finansial via skema *Cyber Takaful*.

Tema I: Karakteristik Modus dan Celah Keamanan Siber (Kesenjangan Teori-Objek)

Eksplorasi ilmiah pada tema pertama ini menyingkap adanya kesenjangan struktural (*structural gap*) yang sangat radikal antara proyeksi teoretis manajemen risiko siber konvensional dengan realitas modus operandi serangan yang secara riil dihadapi oleh objek perbankan syariah di Indonesia. Dalam paradigma manajemen risiko operasional tradisional (Miah & Uddin, 2017), risiko yang melekat pada aspek teknologi informasi umumnya dipahami dalam batas-batas yang linier dan statis. Teori-teori klasik berasumsi bahwa kerentanan digital berakar pada ketidakadekuatan sistem internal, gangguan teknis peladen akibat faktor kelelahan perangkat keras, kelalaian manusia (*human error*) berupa salah ketik kode (*coding error*), atau infiltrasi eksternal berskala rendah seperti kejahatan *phishing* dan infeksi *malware* massal yang perimeternya dapat dipagari secara konvensional. Landasan teoretis ini pula yang melatarbelakangi lahirnya regulasi formal seperti POJK Nomor 11/POJK.03/2022, di mana fokus mitigasi ditekankan pada penguatan batas-batas pertahanan internal (*perimeter defense*) institusi keuangan.

Namun, hasil analisis penapisan literatur berbasis metode SLR (Suryono et al., 2019; Hasibuan & Syahri, 2022) membongkar sebuah realitas baru yang kontradiktif. Perbankan syariah di Indonesia saat ini ternyata berhadapan dengan taktik serangan siber yang bersifat hibrida, asimetris, sangat dinamis, dan terorganisir oleh sindikat kriminal transnasional dengan persenjataan teknologi tingkat tinggi. Ketika disandingkan dengan rekam jejak empiris yang dipaparkan pada Bab I (Tabel 1.2), kerentanan tertinggi bank syariah domestik justru tercatat saat institusi tersebut melakukan akselerasi penetrasi digital secara agresif. Insiden *LockBit 3.0 Ransomware* yang melumpuhkan peladen utama salah satu bank syariah terbesar di Indonesia selama lima hari berturut-turut menjadi pembuktian empiris bahwa model pertahanan perimeter konvensional yang dielu-elukan dalam literatur manajemen klasik telah usang. Para peretas tidak lagi membongkar paksa gerbang utama pertahanan digital bank melalui serangan langsung (*brute force*), melainkan mengeksploitasi celah arsitektur keamanan pada *Open API* (Application Programming Interface). *Open API* adalah gerbang integrasi yang sengaja dibuka oleh bank syariah

untuk menghubungkan sistem keuangan mereka dengan ekosistem pihak ketiga, seperti platform *fintech lending*, lokapasar (*marketplace*), dan agregator pembayaran digital (Rusydiana, 2021). Pola serangan yang menargetkan rantai pasok digital (*digital supply chain attack*) ini mencerminkan fenomena perluasan wilayah perimeter serangan (*attack surface expansion*) yang membuat instrumen identifikasi risiko konvensional tidak lagi adekuat dan kehilangan relevansi praktisnya.

Guna mengurai kompleksitas pergeseran modus serangan ini secara komprehensif, sudut pandang ahli keuangan digital kontemporer sangat mendesak untuk dihadirkan. Rabbani et al. (2020) mengemukakan tesis bahwa dorongan moral-etis perbankan syariah untuk menyelenggarakan inklusi keuangan nasional secara kilat sering kali memicu fenomena *rushed digitalization* (digitalisasi yang tergesa-gesa). Dalam situasi tersebut, kecepatan divisi pengembangan produk (*business development*) dalam menelurkan fitur-fitur baru digital tidak diimbangi dengan kecepatan pengujian penetrasi keamanan siber (*penetration testing*) oleh divisi pertahanan IT dan kepatuhan. Hal ini diperparah oleh temuan pakar hukum keuangan Islam internasional, Muneeza & Mustapha (2021), yang menyatakan bahwa mayoritas lembaga keuangan syariah di negara berkembang belum memiliki arsitektur keamanan siber yang bersifat mandiri (*standalone cybersecurity architecture*). Karena keterbatasan permodalan TI, banyak bank syariah yang masih berbagi infrastruktur server inti atau "menumpang" pada sistem induk bank konvensionalnya. Ketergantungan struktural ini melahirkan risiko bawaan (*inherent risk*) dalam bentuk kerentanan ganda; ketika pertahanan bank induk konvensional mengalami kebocoran data, peladen anak perusahaan syariah secara otomatis ikut terekspos dan dapat dieksploitasi secara berantai oleh peretas.

Selain kerentanan arsitektur makro, para ahli siber kontemporer juga menyoroti titik paling rapuh pada lini pertahanan bank syariah, yaitu faktor manusia (*human-centric vulnerability*). Analisis komparatif dari Pratama (2021) menunjukkan adanya jurang pemisah yang lebar antara idealisme teori perlindungan kerahasiaan data nasabah dengan realitas kapasitas literasi siber masyarakat muslim di Indonesia. Ketika teori manajemen risiko mengasumsikan bahwa implementasi fitur keamanan teknis tingkat tinggi—seperti verifikasi dua faktor (2FA), kode OTP otomatis, dan enkripsi biometrik—sudah cukup untuk menutup ruang kejahatan digital (Ali et al., 2021), realitas di lapangan justru berjalan ke arah sebaliknya. Penyerang siber masa kini telah bermutasi menggunakan taktik rekayasa sosial berbasis kecerdasan buatan (*AI-driven social engineering*). Penyerang memanfaatkan perangkat lunak kloning suara (*deepfake voice*) atau rekayasa pesan berbasis algoritma teks generatif untuk meniru identitas resmi pejabat bank syariah. Taktik manipulasi psikologis ini dirancang secara spesifik mengeksploitasi karakteristik sosiologis-religius masyarakat Indonesia yang komunal, ramah, dan mudah percaya pada narasi yang membawa label agama. Dengan dalih penyesuaian akad pembiayaan, pembaruan sistem bagi hasil mudharabah, atau pembersihan rekening dari unsur riba, nasabah digiring secara psikologis untuk menyerahkan kode PIN atau OTP mereka secara sukarela.

Berdasarkan komparasi kritis di atas, penulis berpandangan bahwa kesalahan mendasar dari rapuhnya pertahanan perbankan syariah di Indonesia bersumber dari cara pandang manajemen yang masih memposisikan risiko siber sebagai isu teknis internal divisi IT semata. Penulis menegaskan bahwa risiko siber kontemporer pada perbankan syariah telah bermutasi menjadi ancaman siber hibrida (*hybrid cyber threat*) yang secara simultan mengeksploitasi kelemahan interkoneksi *Open API*, keterbatasan modal infrastruktur TI mandiri, dan rendahnya literasi digital teologis nasabah. Oleh karena itu,

penulis menolak model manajemen risiko defensif-reaktif klasik dan menyatakan bahwa perbankan syariah harus merombak paradigma mereka menuju metodologi mitigasi yang ofensif-proaktif, di mana setiap jengkal kode pemrograman dan interaksi manusia dihitung sebagai perimeter pertempuran digital yang wajib dilindungi.

Tema II: Pola Dampak Multidimensi dan Eskalasi Risiko Ketidakpatuhan Syariah (*Shariah Non-Compliance Risk*)

Sintesis tematik pada klaster kedua melalui metodologi SLR membongkar benturan konseptual dan operasional yang sangat tajam antara idealisme teoretis perlindungan harta (*Hifzh al-Mal*) dengan realitas dilematis yang mengikat objek perbankan syariah saat berada dalam pusaran krisis siber. Bangunan teori keuangan Islam di Bab II secara normatif menegaskan bahwa institusi keuangan syariah mengemban amanat teologis untuk menjamin kesucian, keamanan, dan keadilan dalam setiap sendi operasionalnya, serta diharamkan secara mutlak terlibat dalam aktivitas transaksi yang menyokong kezaliman (Chapra, 2000; Laldin & Furqani, 2019). Namun, hasil penelusuran sistematis menunjukkan bahwa ketika bank syariah diserang oleh *advanced ransomware* yang berhasil mengunci basis data intinya (*core banking*), seluruh kalkulasi linear yang diajarkan dalam buku teks manajemen risiko mendadak lumpuh menghadapi kompleksitas hukum Islam kontemporer.

Kesenjangan paling krusial antara teori kepatuhan dan realitas manajemen krisis di lapangan terletak pada analisis eskalasi risiko ketidakpatuhan syariah (*Shariah Non-Compliance Risk*), sebuah variabel risiko unik yang absen dalam matriks risiko perbankan konvensional. Pakar hukum ekonomi Islam kontemporer, Sani (2023) serta Syamsuri & Rosyadi (2024), mengupas tuntas dinamika ini melalui perdebatan fikih muamalah terkait legalitas pembayaran uang tebusan (*cyber ransom*) kepada peretas siber. Ketika peladen bank syariah dikunci (seperti insiden riil pada Tabel 1.2) dan peretas mengancam akan menyebarkan data pribadi nasabah jika tebusan dalam bentuk Bitcoin tidak dipenuhi, manajemen bank terperangkap dalam jebakan hukum ganda. Secara tekstual, menuruti kemauan pemeras dan mentransfer aset bank kepada kelompok kriminal siber dinilai melanggar prinsip kepatuhan syariah karena masuk dalam kategori *ta'awun 'ala al-ithmi wa al-'udwan* (saling menolong dalam dosa dan permusuhan). Tindakan tersebut secara tidak langsung mendanai sindikat kriminal siber internasional untuk menciptakan kerusakan yang lebih luas di muka bumi. Namun, jika bank bersikap kaku menolak pembayaran tebusan demi menjaga kesucian formalitas akad, durasi kelumpuhan sistem (*downtime*) akan membengkak ekstrem melampaui batas toleransi operasional (96 hingga 120 jam). Konsekuensinya, data finansial nasabah akan bocor, transaksi ekonomi umat terhenti, dan kerahasiaan data pribadi nasabah hancur, sebuah kondisi yang melanggar hak privasi dan perlindungan hukum formal (Fitriani, 2022).

Dalam kondisi kedaruratan digital (*daruriyyah*) tersebut, analisis para ahli kontemporer (Muneeza & Mustapha, 2021; Ramadhan, 2023) menyoroti bagaimana bank syariah di lapangan terpaksa melakukan penalaran ijtihad darurat menggunakan kaidah fikih *ta'arud al-mafsadatain* (apabila berkumpul dua kemudaratan, maka ambillah kemudaratan yang paling ringan). Bank syariah terpaksa memilih kemudaratan kecil (membayar tebusan) demi menolak kemudaratan sistemik yang jauh lebih masif (*da'ru al-mafsadah al-asya'*), yaitu hancurnya stabilitas keuangan nasabah dan rusuhnya sistem intermediasi syariah nasional. Kendati keputusan kompromistis ini diambil untuk menyelamatkan kemaslahatan data nasabah (*Hifzh al-Mal*), dampak sekundernya secara otomatis melahirkan risiko ketidakpatuhan syariah yang nyata. Biaya pemulihan sistem yang bersumber dari pembayaran tebusan tersebut berpotensi besar dinyatakan sebagai

dana non-halal (*non-halal expense*) oleh komite audit syariah atau Dewan Pengawas Syariah (DPS). Konsekuensinya, bank wajib menjalankan proses pembersihan syariah (*shariah cleansing*) dengan menyalurkan dana bernilai miliaran rupiah tersebut ke dalam rekening sosial (*dana qardhul hasan*). Pengeluaran paksaan ini secara langsung memotong margin profitabilitas bank, merusak proyeksi rasio pengembalian aset (*Return on Asset*), dan mengganggu performa kesehatan keuangan bank di mata investor.

Pola dampak multidimensi ini tidak berhenti pada lingkaran hukum syariah, melainkan merambat secara cepat memicu efek domino destruktif pada aspek sosiologis-finansial manajemen likuiditas. Riset empiris berskala global dari Baddour & Hassan (2024) serta Aldeen et al. (2022) mengonfirmasi adanya anomali perilaku konsumen muslim yang sangat sensitif terhadap variabel emosi keagamaan (*religious emotion*). Nasabah bank syariah terbukti memiliki tingkat toleransi risiko yang jauh lebih rendah (*low risk tolerance*) terhadap isu pelanggaran *amanah* digital dibandingkan nasabah bank konvensional. Kerusakan atau kelumpuhan sistem TI pada bank syariah tidak lagi dimaknai oleh masyarakat sebagai masalah teknis operasional biasa, melainkan diterjemahkan sebagai hilangnya kesucian moral spiritual pengelola dana. Sentimen teologis yang negatif ini melahirkan kepanikan moral massal yang berujung pada penarikan dana massal (*bank rush*) secara instan pasca-terjadinya serangan siber yang terekspos publik. Sebagaimana terekam pada data empiris Tabel 1.1, potensi pelarian modal (*capital flight*) akibat degradasi kepercayaan siber ini dapat melampaui angka 10% dalam hitungan hari. Fakta empiris ini menjadi jembatan logis yang membuktikan bagaimana sebuah risiko operasional siber, dalam hitungan jam, memiliki daya rusak eksponensial untuk bertransformasi menjadi krisis risiko likuiditas sistemik (*systemic liquidity risk*) yang mampu mengancam tingkat solvabilitas dan kelangsungan hidup jangka panjang institusi perbankan syariah.

Penulis berkesimpulan bahwa risiko siber pada perbankan syariah tidak boleh lagi dikalkulasi murni menggunakan pendekatan matematika keuangan linear konvensional. Penulis secara tegas menyatakan bahwa dampak risiko siber di industri syariah adalah sebuah bentuk "Risiko Reputasi Teologis" yang berbiaya sangat mahal. Kesenjangan riil di lapangan membuktikan bahwa ketika benteng digital runtuh, bank syariah tidak hanya kehilangan data, tetapi kehilangan legitimasi moral syariahnya di mata umat. Penulis menilai bahwa kompromi fikih pembayaran tebusan melalui kaidah darurat adalah bukti ketidaksiapan konseptual industri saat ini, dan jika pola dampak ini terus diabaikan oleh para pembuat kebijakan, maka digitalisasi perbankan syariah justru akan menjadi pintu gerbang utama runtuhnya stabilitas sistem ekonomi syariah nasional akibat fenomena *bank rush* yang dipicu oleh hilangnya nilai *amanah*.

Tema III: Model Pertahanan Ketahanan dan Efektivitas Mitigasi Syariah (Solusi dan Hambatan Industri)

Analisis komparatif pada klaster tema ketiga membedah tingkat efektivitas, hambatan operasional, serta jarak yang lebar antara instrumen mitigasi risiko siber yang ditawarkan secara ideal dalam literatur konseptual dengan realitas kapasitas industri pertahanan siber syariah di lapangan. Berdasarkan kajian pustaka di Bab II, konstruksi model pertahanan siber terbaik bagi institusi keuangan syariah wajib mengintegrasikan keandalan sistem teknologi pertahanan modern berbasis arsitektur *Zero Trust Architecture* dengan perlindungan finansial yang selaras dengan prinsip-prinsip syarak, yaitu melalui pemanfaatan instrumen Cyber Takaful atau asuransi siber syariah (Firmansyah & Anwar, 2022; Al-Aref & Othman, 2023). Walakin, hasil penelusuran sistematis menggunakan metode SLR menyingkap fakta pahit bahwa model mitigasi yang ideal secara akademis

tersebut membentur tembok penghalang berupa keterbatasan struktural institusional dan ketidakmatangan pasar industri pendukung di pasar domestik Indonesia saat ini.

Kesenjangan pertama yang sangat fundamental terdeteksi pada lini tata kelola pengawasan syariah (*Shariah Governance Framework*). Teori manajemen risiko keuangan syariah yang dikemukakan oleh Laldin & Furqani (2019) menggarisbawahi bahwa Dewan Pengawas Syariah (DPS) memegang otoritas pruden tertinggi yang wajib melakukan pengawasan melekat yang bersifat menyeluruh (*ubiquitous*) terhadap seluruh produk dan jalannya operasional bank guna menjamin mitigasi risiko ketidakpatuhan syariah sejak dini (*ex-ante*). Namun, hasil sintesis literatur dari riset empiris Setyowati (2020) menguak adanya defisit kompetensi teknis yang masif (*knowledge gap*) pada tubuh kepengurusan DPS di Indonesia terkait arsitektur TI perbankan modern. Mayoritas anggota DPS memiliki rekam jejak kepakaran yang luar biasa pada bidang hukum fikih muamalah klasik dan hukum Islam tekstual, tetapi mengalami kegagapan luar biasa ketika dihadapkan pada kewajiban untuk mengaudit keandalan algoritma kriptografi, mengevaluasi parameter keamanan interkoneksi *Open API*, atau menetapkan panduan kedaruratan (*cyber contingency plan*) saat data nasabah disandera oleh peretas internasional. Keterbatasan kapasitas kognitif-teknis ini menyebabkan fungsi pengawasan kepatuhan syariah terhadap risiko digital di lapangan berjalan pincang; pengawasan sering kali tereduksi menjadi formalitas administratif pasca-kejadian (*ex-post*), di mana DPS baru dilibatkan setelah krisis siber meledak dan data telah bocor ke publik, kehilangan esensi fungsi preventifnya yang sejati.

Kesenjangan kedua yang tidak kalah krusial ditemukan pada aspek keterbatasan instrumen pengalihan risiko finansial (*risk transfer*). Merujuk pada teori risiko sisa (*residual risk*), sekuat apa pun dinding teknologi pertahanan siber yang dibangun oleh sebuah bank, risiko serangan siber tidak pernah dapat dieliminasi hingga mencapai angka 0%. Oleh sebab itu, sisa risiko finansial yang timbul—seperti biaya investigasi forensik digital, denda hukum pelanggaran UU PDP, hingga biaya rekonstruksi peladen—wajib dialihkan ke pihak ketiga melalui skema *Cyber Takaful* berbasis akad *tabarru'* (hibah kebajikan) guna menghindari praktik riba, *maysir*, dan *gharar* (Firmansyah & Anwar, 2022). Namun, analisis kritis dari pakar keuangan global Warde (2021) disandingkan dengan laporan industri dari Kementerian Komunikasi dan Informatika RI (2023) menyingkap fakta bahwa industri asuransi siber syariah (*Cyber Takaful*) di Indonesia masih berada dalam fase embrionik dan belum matang. Operator takaful domestik memiliki kapasitas permodalan kolektif (*retensi sendiri*) yang sangat rendah. Akibatnya, mereka tidak memiliki ketahanan modal yang sanggup menanggung skala kerugian finansial akibat serangan siber katastrofik (*catastrophic cyber risk*) berskala sistemik yang nilainya dapat mencapai ratusan miliar rupiah pada satu institusi bank syariah besar.

Kondisi kelangkaan infrastruktur pendukung ini memaksa objek perbankan syariah di lapangan mengambil keputusan kompromistis yang dilematis dan mengorbankan idealisme syariah demi mempertahankan solvabilitas perusahaan. Untuk melindungi kelangsungan bisnisnya dari ancaman kebangkrutan pasca-serangan siber, beberapa bank syariah besar terpaksa melanggar batas idealis dengan mengalihkan risiko finansial siber mereka kepada perusahaan reasuransi konvensional internasional yang memiliki modal raksasa (Asongu & Nwachukwu, 2019). Sementara itu, bank syariah yang berupaya menjaga kesucian syariah secara kaku terpaksa menanggung risiko tersebut secara mandiri (*self-insurance*) dengan cara membekukan sebagian besar aset likuid mereka untuk diplot sebagai cadangan modal risiko operasional TI. Pembekuan modal mandiri ini berbiaya sangat mahal (*opportunity cost*) karena mengunci likuiditas produktif bank

syariah dalam jumlah besar yang seharusnya dapat diputar kembali untuk membiayai sektor riil dan mendorong pertumbuhan ekonomi umat.

Penulis menegaskan bahwa model mitigasi risiko siber perbankan syariah di Indonesia saat ini tengah mengalami "Kelumpuhan Struktural". Ada jarak yang teramat lebar antara apa yang ditulis di atas kertas seminar ilmiah dengan realitas kapasitas industri di lapangan. Penulis berpandangan bahwa penguatan mitigasi tidak akan pernah tercapai jika hanya dibebankan pada pundak divisi IT internal bank secara parsial. Penulis secara objektif menyatakan bahwa solusi hakiki dari krisis ketahanan siber ini menuntut adanya intervensi struktural tingkat makro berupa: (1) Kewajiban sertifikasi siber forensik bagi pengawas syariah untuk menutup *knowledge gap* DPS, dan (2) Pemaksaan regulasi oleh OJK untuk membentuk Konsorsium Cyber Takaful Nasional. Tanpa adanya sinkronisasi pertahanan antara kecanggihan teknologi *Zero Trust*, kompetensi siber DPS, dan penguatan permodalan Takaful, maka jargon ketahanan siber perbankan syariah akan selamanya menjadi utopia konseptual yang rapuh dihantam kenyataan.

Kesimpulan

Penelitian ini menyimpulkan bahwa risiko siber pada perbankan syariah di Indonesia telah bermutasi menjadi ancaman siber hibrida (hybrid cyber threat) berskala asimetris yang mengeksploitasi arsitektur Open API dan memicu risiko reputasi teologis atas hilangnya nilai amanah digital. Dampak insiden digital ini tidak hanya berhenti pada kerugian finansial linier, melainkan memicu efek domino berupa risiko ketidakpatuhan syariah (shariah non-compliance risk) akibat dilema fikih pembayaran tebusan ransomware serta risiko likuiditas sistemik berupa pelarian modal massal (bank rush) oleh nasabah. Sementara itu, model mitigasi ideal berupa integrasi tata kelola Zero Trust dan pengalihan risiko melalui Cyber Takaful masih mengalami kelumpuhan struktural akibat adanya defisit kompetensi teknis (knowledge gap) pada Dewan Pengawas Syariah (DPS) serta ketidakmatangan kapasitas permodalan industri takaful domestik; sehingga mendesak dibentuknya regulasi makro terintegrasi berupa konsorsium nasional dan sertifikasi forensik siber guna menjamin stabilitas ekosistem keuangan syariah digital secara kaffah

Daftar Pustaka

Al-Aref, A., & Othman, A. (2023). Cyber resilience framework for Islamic financial infrastructure. *International Journal of Islamic Economics and Finance Studies*, 9(3), 411–435. https://doi.org/10.54415/ijiefs.v9i3.411

Aldeen, K. N., dkk. (2022). Bank rush and trust degradation post cyber attack: Empirical evidence from Islamic banks. *Journal of Financial Services Marketing*, 27(4), 189–204. https://doi.org/10.1057/s41264-022-00189-y

Ali, M., Raza, S. A., & Puah, C. H. (2021). Factors affecting mobile banking adoption in Islamic banks: Behavioral intention approach. *Journal of Islamic Marketing*, 12(3), 510–529. https://doi.org/10.1108/JIMA-10-2019-0211

Ascarya. (2013). Desain integrasi manajemen risiko di perbankan syariah. *Jurnal Ekonomi dan Keuangan Islam*, 2(1), 12–34.

Asongu, S. A., & Nwachukwu, J. C. (2019). The synergy between financial sector development and information technology in Sub-Saharan Africa: Context of Islamic

finance. *Journal of Global Information Technology Management*, 22(2), 115–134. https://doi.org/10.1080/1097198X.2019.1603517

Baddour, J., & Hassan, A. (2024). Comparative analysis of cyber risk impacts between conventional and Islamic systemic banks. *Journal of Financial Crime*, 31(1), 45–62. https://doi.org/10.1108/JFC-01-2023-0012

Chapra, M. U. (2000). *The future of economics: An Islamic perspective*. Islamic Foundation.

Dusuki, A. W., & Bouheraoua, S. (2011). The framework of Maqasid al-Shari'ah and its implication for Islamic finance. *Islam and Civilisational Renewal (ICR)*, 2(2), 316–336.

Fauzi, M. A. (2023). Systematic literature review on Islamic fintech: Information security, shariah governance, and future agenda. *Journal of Islamic Marketing*, 14(5), 1120–1145. https://doi.org/10.1108/JIMA-04-2022-0118

Firmansyah, I., & Anwar, M. (2022). Islamic cyber Takaful: A new risk mitigation paradigm for Islamic financial institutions. *Journal of Islamic Monetary Economics and Finance*, 8(3), 421–442. https://doi.org/10.21098/jimf.v8i3.1491

Fitriani, A. (2022). Pelindungan data pribadi nasabah perbankan syariah dalam menghadapi ancaman cyber crime. *Jurnal Hukum Lex Generalis*, 3(5), 341–359. https://doi.org/10.56370/jhlg.v3i5.241

Hasibuan, A. N., & Syahri, M. (2022). Dampak digitalisasi terhadap risiko operasional perbankan syariah di Indonesia. *Jurnal Ilmiah Ekonomi Islam*, 8(2), 1489–1501. https://doi.org/10.29040/jiei.v8i2.4891

Hassan, M. K., & Aliyu, S. (2018). A contemporary survey of Islamic banking literature. *Journal of Financial Stability*, 34, 12–43. https://doi.org/10.1016/j.jfs.2017.11.006

Hdayat, S. (2020). Risk management frameworks for digital transformation in Islamic financial institutions. *ISRA International Journal of Islamic Finance*, 12(1), 141–156. https://doi.org/10.1108/IJIF-09-2019-0141

Kamaruddin, M. I. H., & Muhamed, N. A. (2020). Shariah governance practices of Islamic financial institutions in Malaysia and Indonesia. *Journal of Islamic Accounting and Business Research*, 11(2), 485–502. https://doi.org/10.1108/JIABR-11-2018-0185

Kementerian Komunikasi dan Informatika RI. (2023). *Laporan tahunan pemantauan keamanan siber sektor perbankan dan finansial Indonesia*. Kominfo.

Kopp, E., Kaffenberger, L., & Christopher, W. (2017). Cyber risk, market failures, and financial stability. *IMF Working Papers*, 17(185), 1–35.

Laldin, M. A., & Furqani, H. (2019). Innovation versus Shariah compliance in Islamic finance. *Journal of Islamic Accounting and Business Research*, 10(2), 291–306. https://doi.org/10.1108/JIABR-06-2017-0091

Lallmahomed, M. Z. I., Lallmahomed, N., & Lallmahomed, G. M. (2017). Factors influencing the adoption of e-government services in Western Africa: Context of Islamic banking. *Information Technology for Development*, 23(4), 639–662. https://doi.org/10.1080/02681102.2017.1328639

Miah, M. D., & Uddin, H. (2017). Inefficiency and risk-taking behavior of Islamic banks versus conventional banks. *International Journal of Islamic and Middle Eastern Finance and Management*, 10(2), 139–158. https://doi.org/10.1108/IMEFM-03-2016-0039

Mubarak, M. S., dkk. (2022). Cybersecurity awareness and digital banking trust among Islamic bank customers. *Journal of King Abdulaziz University: Islamic Economics*, 35(2), 75–92. https://doi.org/10.4197/Islec.35-2.6

Muneeza, A., & Mustapha, Z. (2021). Blockchain applications in Islamic finance: Cyber risks and legal challenges. *International Journal of Management and Applied Research*, 8(2), 111–128. https://doi.org/10.18646/2056.82.21-011

Nofrianto, N., dkk. (2023). Cyber security risks and mitigation strategies in Islamic banking: A review. *Journal of Islamic Economic Laws*, 6(1), 85–105. https://doi.org/10.23917/jisel.v6i1.21105

Otoritas Jasa Keuangan. (2022). *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*. Lembaran Negara Republik Indonesia.

Pratama, A. R. (2021). Analisis kesadaran keamanan siber pada nasabah perbankan syariah mobile banking. *Jurnal Sistem Informasi Bisnis*, 11(2), 130–138. https://doi.org/10.21456/vol11iss2pp130-138

Rabbani, M. R., Khan, S., & Thalassinos, E. I. (2020). FinTech, blockchain and Islamic finance: An extensive literature review. *International Journal of Economics and Business Administration*, 8(2), 65–86. https://doi.org/10.35808/ijeba/441

Ramadhan, S. (2023). Implikasi kebocoran data nasabah terhadap reputasi perbankan syariah berdasarkan perspektif fikih muamalah. *Jurnal Ilmiah Syari'ah*, 22(1), 105–122. https://doi.org/10.31958/juris.v22i1.8741

Rusydiana, A. S. (2021). Bagaimana mengembangkan perbankan digital syariah di Indonesia? *Jurnal Pemikiran Ekonomi Islam (Ekin)*, 4(1), 1–14. https://doi.org/10.30659/ekin.4.1.1-14

Sani, M. K. (2023). Penanganan serangan ransomware pada lembaga keuangan syariah ditinjau dari asas Sadd Adz-Dzarari'ah. *Jurnal Hukum Ekonomi Syariah*, 7(2), 145–160. https://doi.org/10.26623/jhes.v7i2.6950

Sari, M. D., Ahmed, H., & Khan, T. (2016). Islamic banking regulation and performance: A case study of Indonesia. *Palestine Journal of Mathematics*, 5(Special Issue), 213–228.

Setyowati, R. (2020). Upaya dewan pengawas syariah dalam memitigasi risiko hukum operasional berbasis digital. *Jurnal Hukum Islam*, 18(2), 211–229. https://doi.org/10.28918/jhi.v18i2.3211

Sudarsono, H., dkk. (2024). Digital transformation in Islamic banking: Operational efficiency vs cyber security threats. *Al-Iqtishad: Jurnal Ilmu Ekonomi Syariah*, 16(1), 115–138. https://doi.org/10.15408/aiq.v16i1.31011

Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to peer lending in Indonesia: Lessons learned and future directions. *Heliyon*, 5(6), e01921. https://doi.org/10.1016/j.heliyon.2019.e01921

Syamsuri, S., & Rosyadi, I. (2024). Problematika pembayaran tebusan siber (cyber ransom) melalui dana ghiroh syariah: Perspektif Maqasid. *Jurnal Ilmiah Ahwal Syakhshiyyah*, 6(1), 45–58. https://doi.org/10.33474/jas.v6i1.21855

Warde, I. (2021). *Islamic finance in the global economy* (3rd ed.). Edinburgh University Press.