LAN TABUR : JURNAL EKONOMI SYARI'AH **p.ISSN: 2716-2605**
VOL. 6 NO. 1 September 2024 **e.ISSN: 2721-0677**

TANTANGAN DAN SOLUSI DALAM PENGAWASAN RISIKO DI PERBANKAN SYARIAH PADA ERA CYBER:

TINJAUAN LITERATUR BANK SYARIAH INDONESIA

Surya Karmila Sari[1], Lisa Anggryani[2*], Rahmat Hidayat[3], Sitti Nikmah Marzuki[4]
Institut Agama Islam Negeri (IAIN) Bone
Email: suryakarmilasari202@gmail.com, lisaanggryani17@gmail.com, rahmat16535@gmail.com , nikmah.marzuki@gmail.com

Abstract

This research aims to identify and analyze the challenges and solutions in risk supervision within Islamic banking in the cyber era, with a particular focus on literature related to Bank Syariah Indonesia. It adopts a qualitative approach using the Literature Review method, collecting data from written sources such as books, online materials, and scientific articles on risk supervision in Islamic banking. The process is meticulous and systematic, utilizing only credible sources without direct interaction with the research subjects. This approach provides comprehensive and in-depth information, focusing on the search and analysis of existing references. The results of this study reveal that the cyber attack on Bank Syariah Indonesia (BSI) from May 8-16, 2023, exposed vulnerabilities in the banking system, with a suspected ransomware attack by LockBit 3.0. BSI responded quickly via social media, demonstrating its commitment to securing customer funds and data while investigating the incident. The impact included significant operational disruptions and customer concerns, with potential financial and reputational losses. Challenges in risk supervision in the cyber era involve the use of social media, which can threaten data security but also enhance digital knowledge. Blockchain technology is proposed as a solution to improve the security of financial transactions. This incident highlights the urgent need to enhance awareness and preparedness against cyber threats through proactive measures and adaptive regulatory policies.

Keywords: *Challenges, Solutions, Risk Supervision, Islamic Banking, Cyber Era*

Abstrak

Penelitian ini untuk mengidentifikasi dan menganalisis tantangan serta solusi dalam pengawasan risiko di perbankan syariah pada era cyber, dengan fokus khusus pada literatur yang berkaitan dengan Bank Syariah Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan metode Studi Kepustakaan, mengumpulkan data dari sumber tertulis seperti buku, materi online, dan artikel ilmiah tentang pengawasan risiko di perbankan syariah. Prosesnya teliti dan sistematis, hanya menggunakan sumber yang kredibel, tanpa interaksi langsung dengan objek penelitian. Pendekatan ini memberikan informasi komprehensif dan mendalam, dengan fokus pada pencarian dan analisis referensi yang ada. Hasil penelitian ini yaitu serangan siber terhadap Bank Syariah Indonesia (BSI) pada 8-16 Mei 2023 mengungkap kerentanan sistem perbankan, dengan dugaan serangan ransomware oleh LockBit 3.0. BSI merespon cepat melalui media sosial, menunjukkan komitmen menjaga keamanan dana dan data nasabah serta menyelidiki insiden tersebut. Dampaknya termasuk gangguan operasional besar dan kekhawatiran nasabah, dengan potensi kerugian finansial dan reputasi yang signifikan. Tantangan pengawasan risiko di era siber melibatkan penggunaan media sosial yang bisa mengancam keamanan data tetapi juga meningkatkan pengetahuan digital. Teknologi blockchain diusulkan sebagai solusi untuk meningkatkan keamanan transaksi keuangan. Insiden ini menyoroti kebutuhan mendesak untuk meningkatkan kesadaran dan kesiapan menghadapi ancaman siber dengan langkah proaktif dan kebijakan regulasi adaptif.

Kata Kunci: Tantangan, Solusi, Pengawasan Risiko, Perbankan Syariah, Era Cyber

A. PENDAHULUAN

Seiring dengan kemajuan teknologi, terjadi peningkatan signifikan dalam penggunaan layanan perbankan digital oleh masyarakat. Kemudahan akses internet dan perangkat pintar telah memungkinkan nasabah untuk melakukan transaksi perbankan secara daring, yang pada gilirannya meningkatkan kenyamanan dan efisiensi. Berdasarkan data yang disampaikan oleh Laras[1], Bank Indonesia melaporkan bahwa pada bulan April 2024, nilai transaksi digital banking mencapai Rp5.340,92 triliun, mengalami pertumbuhan tahunan sebesar 19,08%. Setiawati (2024) menambahkan bahwa Bank Indonesia juga mencatat bahwa total transaksi digital banking mencapai Rp15.881,5 triliun pada kuartal pertama tahun 2024, mencatatkan pertumbuhan sebesar 16,15% dibandingkan dengan periode yang sama pada tahun sebelumnya. Di samping itu, laporan dari PT Bank Syariah Indonesia Tbk (BSI) menunjukkan bahwa transaksi digital banking melalui BSI Mobile mengalami pertumbuhan tahunan yang signifikan sebesar 45,02% hingga Juni 2024[2].

Berdasarkan data-data tersebut menunjukkan semakin tingginya adopsi teknologi digital dalam perbankan, maka dari itu penting bagi lembaga keuangan, khususnya perbankan syariah untuk terus berinovasi dan memperkuat sistem keamanan mereka. Namun, di balik semua keuntungan tersebut, terdapat ancaman serius yang mengintai, berupa potensi risiko keamanan yang tidak boleh diabaikan. Peningkatan penggunaan teknologi digital dalam perbankan juga membuka celah bagi berbagai bentuk kejahatan siber. Pencurian identitas, penipuan siber, dan serangan terhadap data nasabah merupakan beberapa ancaman utama yang harus dihadapi oleh perbankan syariah dalam era digital ini. Serangan-serangan ini dapat menyebabkan kerugian finansial yang besar, baik bagi nasabah maupun bagi institusi perbankan itu sendiri. Selain itu, adanya insiden keamanan siber dapat merusak reputasi bank, mengurangi kepercayaan nasabah, dan mempengaruhi stabilitas sistem keuangan secara keseluruhan.

Oleh karena itu, perbankan syariah harus mengambil langkah-langkah proaktif untuk memperkuat sistem keamanan mereka. Implementasi teknologi keamanan canggih seperti enkripsi data, autentikasi multi-faktor, dan sistem deteksi ancaman harus menjadi prioritas utama. Selain itu, edukasi dan pelatihan bagi nasabah tentang cara melindungi diri dari

[1] Laras, A. (2024). *Rapor Pengguna Mobile Banking Bank Jumbo Kuartal I/2024: BRI Teratas, Mandiri Melesat!* Finansial Bisnis. https://finansial.bisnis.com/read/20240529/90/1769456/rapor-pengguna-mobile-banking-bank-jumbo-kuartal-i2024-bri-teratas-mandiri-melesat

[2] Khaerunnisa, R. (2024). *BSI: Transaksi digital banking naik 45,02 persen per Juni 2024*. antaranews. https://www.antaranews.com/berita/4206435/bsi-transaksi-digital-banking-naik-4502-persen-per-juni-2024

ancaman siber juga sangat penting. Dengan pendekatan yang komprehensif dan kolaboratif, bank syariah dapat menghadapi tantangan di era digital ini dengan lebih baik, memastikan keamanan dan kepercayaan nasabah tetap terjaga.

Penelitian tentang pengawasan risiko di perbankan syariah sudah banyak dilakukan oleh peneliti-peneliti sebelumnya, diantaranya penelitian yang dilakukan oleh Rusdan[3] menjelaskan sektor perbankan harus mengelola berbagai risiko secara efektif untuk memastikan kesinambungan bisnis dan kelancaran intermediasi keuangan yang efisien dan berkelanjutan. Menurut Hajar & Wirman[4], penerapan manajemen risiko yang efektif dapat mengurangi kemungkinan kesalahan atau risiko yang dapat mempengaruhi perbankan syariah dalam jangka panjang. Oleh karena itu, sangat penting untuk selalu mampu beradaptasi dan membuat keputusan yang tepat sesuai dengan situasi yang dihadapi. Akbar. C et al[5] menegaskan bahwa manajemen risiko dalam perbankan syariah harus didasarkan pada prinsip kehati-hatian untuk mengidentifikasi, mengukur, dan mengelola risiko secara efektif. Proses ini mencakup identifikasi, evaluasi, dan pengelolaan risiko, yang merupakan langkah krusial agar bank syariah dapat meningkatkan pangsa pasar mereka.

Menurut Syahrir et al[6] perbankan syariah memiliki berbagai jenis investasi yang kompleks dan harus mematuhi ketentuan syariah, meskipun ada inovasi yang terus berkembang dan risiko yang terkait. Oleh karena itu, perbankan syariah perlu mampu mengidentifikasi, menilai, dan mengelola risiko yang melekat pada aktivitasnya melalui penerapan manajemen risiko yang efisien dan efektif. Selain itu, bank syariah juga menghadapi risiko nilai tukar seperti halnya bank konvensional. Putra et al[7] risiko terbesar dalam penyaluran kredit adalah kredit macet, yang harus dihadapi dengan pengelolaan risiko melalui manajemen risiko. Pada pembiayaan mikro syariah, ini melibatkan identifikasi, pengukuran, pengendalian, dan pengawasan risiko. Setiap potensi kerugian diinventarisasi, dianalisis penyebabnya, dan dicari cara pencegahan melalui mitigasi risiko.

---

[3] Rusdan. (2016). Urgensi Manajemen Pengawasan Risiko Bank Syariah. *PALAPA: Jurnal Studi Keislaman dan Ilmu Pendidikan*, *4*(2), 85–103

[4] Hajar, S., & Wirman. (2023). Implementasi Manajemen Risiko Dalam Dunia Perbankan Syariah. *Jurnal Ilmiah Wahana Pendidikan*, *9*(5), 500–513

[5] Akbar. C, Eril, Abdullah, M. W., & Awaluddin, M. (2022). Manajemen Risiko di Perbankan Syariah. *Milkiyah: Jurnal Hukum Ekonomi Syariah*, *1*(2), 51–56. https://doi.org/10.46870/milkiyah.v1i2.230

[6] Syahrir, D. K., Ickhsanto Wahyudi, Santi Susanti, Darwant, D., & Ibnu Qizam. (2023). Manajemen Risiko Perbankan Syariah. *AKUA: Jurnal Akuntansi dan Keuangan*, *2*(1), 58–64. https://doi.org/10.54259/akua.v2i1.1382

[7] Putra, P. A., Saparuddin, S., & Nurnasrina, N. (2023). Mitigasi Risiko: Analisis Terhadap Antisipasi Risiko Dalam Pembiayaan Mikro Syariah. *Al-Masraf: Jurnal Lembaga Keuangan dan Perbankan*, *8*(1), 62. https://doi.org/10.15548/al-masraf.v8i1.414

Penelitian tentang tantangan dan solusi dalam pengawasan risiko di perbankan syariah pada era cyber memiliki peran yang sangat signifikan dalam berbagai aspek. Pertama, penelitian ini membantu meningkatkan keamanan dan kepercayaan nasabah dengan mengidentifikasi ancaman siber yang relevan serta cara-cara efektif untuk mengatasinya. Penelitian ini juga berperan dalam meningkatkan kesadaran masyarakat tentang pentingnya keamanan siber dalam perbankan, sehingga nasabah dapat mengambil langkah-langkah proaktif untuk melindungi diri mereka dari risiko siber. Terakhir, sebagai tinjauan literatur yang berfokus pada Bank Syariah Indonesia, penelitian ini menyediakan konteks lokal yang sangat relevan bagi praktisi dan akademisi di Indonesia. Penelitian ini membantu dalam memahami tantangan dan solusi yang spesifik untuk lingkungan perbankan syariah di Indonesia, yang mungkin berbeda dari konteks internasional. Dengan demikian, penelitian ini sangat penting dalam mengembangkan strategi yang efektif untuk menghadapi ancaman siber dan melindungi sistem perbankan di era digital.

B. LANDASAN TEORI

Pengertian Manajemen Risiko

Risiko dapat diartikan sebagai kemungkinan terjadinya kerugian akibat suatu peristiwa tertentu. Dalam sektor perbankan, risiko merujuk pada kejadian yang tidak dapat dihindari, baik yang dapat diprediksi maupun yang tidak dapat diprediksi, yang dapat berdampak negatif pada pendapatan dan permodalan bank. Selain itu, risiko juga dapat dianggap sebagai hambatan dalam pencapaian tujuan tertentu[8].

Manajemen, dalam bahasa Inggris disebut 'management,' dan dalam bentuk kata kerja adalah 'to manage,' merujuk pada proses pengaturan, pengurusan, pengendalian, serta pelaksanaan aktivitas atau kegiatan yang berkaitan dengan pengelolaan dan pengendalian suatu bisnis. Syahrir et al[9] mengemukakan bahwa manajemen risiko merupakan elemen krusial yang memerlukan perhatian khusus, terutama dalam konteks lembaga keuangan seperti bank. Meskipun risiko yang dihadapi oleh perbankan syariah umumnya serupa dengan risiko yang dihadapi oleh bank konvensional, bank syariah juga menghadapi risiko-risiko khusus yang berkaitan dengan kepatuhan terhadap prinsip-prinsip syariah. Risiko-risiko

[8] Fasa, M. I. (2016). Manajemen Resiko Perbankan Syariah di Indonesia. *Jurnal Studi Ekonomi dan Bisnis Islam*, *1*(2), 36–53.

[9] Syahrir, D. K., Ickhsanto Wahyudi, Santi Susanti, Darwant, D., & Ibnu Qizam. (2023). Manajemen Risiko Perbankan Syariah. *AKUA: Jurnal Akuntansi dan Keuangan*, *2*(1), 58–64. https://doi.org/10.54259/akua.v2i1.1382

tersebut mencakup risiko kredit, risiko pasar, risiko operasional, dan risiko likuiditas, yang semuanya menjadi tantangan signifikan bagi perbankan syariah. Perbedaan struktur neraca bank syariah dibandingkan dengan bank konvensional, serta penerapan pola bagi hasil, dapat meningkatkan kemungkinan munculnya risiko tambahan seperti risiko penarikan dana, risiko fidusia, dan risiko komersial yang terdisplaced.

Menurut Karim[10], Sasaran manajemen risiko mencakup: (1) Menyajikan informasi komprehensif terkait risiko kepada supervisi; (2) Menjamin bahwa bank tidak menderita kerugian yang tidak dapat diterima; (3) Meminimalisir kerugian yang timbul dari risiko yang tidak terkontrol; (4) Menaksir paparan dan konsentrasi risiko secara akurat; (5) Menginvestasikan modal secara optimal dan mengurangi risiko dengan efektif. Manajemen risiko merupakan prasyarat utama untuk menjaga kesehatan, stabilitas, dan keberlanjutan bank. Dalam operasional perbankan, manajemen risiko menjadi perhatian utama karena bank terlibat dalam aktivitas yang sangat berisiko. Bank-bank mengambil, mengubah, dan mengintegrasikan risiko ke dalam produk dan layanan mereka. Oleh karena itu, manajemen risiko adalah proses berkelanjutan yang harus terus dipantau. Bank harus selalu proaktif dalam mengelola dan mengendalikan risiko inheren yang terkait dengan bisnis perbankan secara efektif

Lingkup Manajemen Risiko

Dalam penerapan manajemen risiko pada Bank Umum Syariah dan Unit Usaha Syariah, terdapat setidaknya sepuluh jenis risiko yang perlu ditangani oleh bank. Menurut Fasa[11], , berikut adalah penjelasan dari risiko-risiko tersebut:

1. Manajemen Risiko Pembiayaan/ Kredit

   Risiko kredit adalah Resiko yang diakibatkan oleh adanya ketidakberhasilan *coounterparty* dalam menjalankan kewajibannya. Dalam bank syariah, resiko pembiayaan meliputi resiko produk dan resiko yang berkaitan dengan pembiayaan koperasi. Menurut Arifin[12], Sebab pokok munculnya resiko kredit adalah mudahnya bank memberikan pinjaman atau berinvestasi karena terlalu ditargetkan untuk mendistribusikan kelebihan dana, sehingga penilaian kredit kurang teliti dalam mencegah berbagai kemungkinan resiko usaha yang diberi modal.

[10] Karim, A. A. (2008). *Bank Syariah Analisis Fiqih dan Keuangan*. PT. Raja Grafindo Persada
[11] Fasa, M. I. (2016). Manajemen Resiko Perbankan Syariah di Indonesia. *Jurnal Studi Ekonomi dan Bisnis Islam*, *1*(2), 36–53
[12] Arif, M. N. R. Al, & Rahmawati, Y. (2018). *Manajemen Risiko Perbankan Syariah (Suatu Pengantar)*. CV. Pustaka Setia.

2. Manajemen Risiko Pasar

   Manajemen risiko pasar mengacu pada proses mengelola kemungkinan kerugian yang dialami oleh portofolio bank akibat pergerakan tidak menguntungkan dalam variabel pasar, seperti fluktuasi nilai tukar dan suku bunga.

3. Manajemen Risiko Operasional

   Manajemen risiko operasional mengacu pada risiko yang timbul akibat ketidakcukupan atau kegagalan proses internal, kesalahan manusia, kegagalan sistem, atau faktor eksternal lainnya yang dapat memengaruhi operasional bank.

4. Manajemen Risiko Likuiditas

   Manajemen risiko likuiditas mengacu pada risiko yang muncul akibat ketidakmampuan bank memenuhi kewajibannya saat jatuh tempo. Sebagai contoh, sebuah bank yang menyalurkan banyak kredit jangka panjang kepada nasabahnya dengan sumber dana yang sebagian besar berasal dari deposito berjangka satu tahun menghadapi potensi risiko likuiditas akibat ketidaksesuaian struktur jatuh tempo dalam neracanya.

5. Manajemen risiko kepatuhan

   Risiko kepatuhan adalah risiko yang timbul akibat ketidakpatuhan terhadap kebijakan yang berlaku. Risiko ini meliputi ketidakpatuhan terhadap berbagai ketentuan seperti: ketentuan Giro Wajib Minimum, Posisi Devisa Neto, Pembiayaan Bermasalah, dan batas maksimal pembiayaan; ketentuan dalam penyediaan produk; kebijakan layanan pembiayaan; ketentuan pelaporan, baik laporan internal, laporan kepada Bank Indonesia, maupun laporan kepada pihak ketiga lainnya; peraturan perpajakan; peraturan dalam akad kontrak; serta fatwa Dewan Syariah Nasional.

6. Manajemen Risiko Hukum

   Menurut Rianto[13], manajemen risiko hukum merujuk pada risiko yang muncul akibat keterbatasan dalam aspek yuridis, seperti tuntutan hukum, tidak adanya peraturan perundang-undangan yang memadai, atau lemah dalam perjanjian, seperti tidak dipenuhinya syarat keabsahan kontrak atau pengikatan jaminan yang tidak lengkap.

7. Manajemen Risiko Strategis

   Manajemen risiko strategis merupakan risiko sebagai akibat implementasi strategi bank yang tidak tepat, pengambilan keputusan bisnis yang kurang tepat, atau ketidakpatuhan bank terhadap transofrmasi perundang-undangan dan kebijakan lain yang ditetapkan. Pengendalian risiko strategis dilaksanakan dengan penerapan sistem

[13] Rianto, R. B. (2013). *Manajemen Resiko Perbankan Syariah di Indonesia*. Salemba Empat.

pengawasam internal secara koheren. Indikator risiko strategis dapat terlihat dari kegagalan dalam meraih target yang sudah ditentukan, baik target keuangan maupun non-keuangan.

8. Manajemen Risiko Reputasi

Manajemen risiko reputasi adalah risiko yang timbul akibat berita negatif terkait aktivitas bank atau anggapan negatif kepada bank tersebut. Sebagai contoh, mesin ATM Bank A sering menghadapi gangguan "offline," menyebabkan kekecewaan bagi nasabah setiap kali bertransaksi. Nasabah yang merasa kecewa kemudian mengungkapkan keluhannya melalui surat pembaca di Harian Nasional. Publikasi ini menyebabkan Bank A berpotensi menghadapi risiko reputasi.

9. Manajemen Risiko Imbal Hasil

Manajemen risiko imbal hasil mengacu pada risiko yang timbul dari perubahan tingkat imbal hasil yang diberikan kepada nasabah sebagai akibat dari fluktuasi imbal hasil yang diterima bank dari pengalokasian dana. Risiko ini dapat memengaruhi persepsi nasabah pihak ketiga terhadap bank syariah, karena perubahan dalam ekspektasi imbal hasil yang mereka terima. Faktor-faktor internal, seperti penurunan nilai aset bank, atau faktor eksternal, seperti peningkatan imbal hasil yang ditawarkan oleh lembaga keuangan lain, dapat memicu perubahan ekspektasi tersebut.

10. Manajemen Risiko Investasi

Manajemen risiko investasi mengacu pada risiko yang timbul ketika bank memikul kerugian dari usaha nasabah yang dimodali melalui pembiayaan berdasarkan bagi hasil. Risiko ini muncul ketika bank memberikan pembiayaan berbasis bagi hasil kepada nasabah, sehingga bank juga berbagi risiko kerugian yang dialami nasabah tersebut (profit and loss sharing).

Prinsip Manajemen Risiko Perbankan Syariah

Menurut Arif & Rahmawati, Prinsip-prinsip yang harus diikuti dalam penerapan model manajemen risiko adalah sebagai berikut[14]:

1. Transparansi

Prinsip transparansi menetapkan bahwa semua kemungkinan risiko terkait suatu aktivitas, khususnya transaksi, harus diungkapkan secara transparan. Risiko yang tidak

[14] Arif, M. N. R. Al, & Rahmawati, Y. (2018). *Manajemen Risiko Perbankan Syariah (Suatu Pengantar)*. CV. Pustaka Setia.

teridentifikasi atau disembunyikan dapat menjadi sumber masalah signifikan yang sulit dikelola secara efektif.

2. Pengukuran yang Kuat

   Prinsip ini mencerminkan aspek ilmiah dari manajemen risiko dan menetapkan adanya investasi yang berkelanjutan dalam berbagai teknik dan alat yang diperlukan untuk mendukung proses manajemen risiko yang efektif.

3. Informasi Berkualitas yang Tepat Waktu

   Prinsip ini menetapkan keakuratan perkiraan risiko dan kualitas keputusan yang ditetapkan. Ketidakpenuhan prinsip ini dapat menyebabkan pengambilan keputusan yang berisiko tinggi. Sistem manajemen risiko yang baik harus memprioritaskan konsep penyebaran dan memerlukan pemantauan terus-menerus. Hal ini karena konsentrasi risiko dapat muncul secara tiba-tiba akibat berbagai perubahan global.

4. Independensi

   Prinsip independensi menekankan pentingnya adanya kelompok manajemen risiko yang berdiri sendiri dan terpisah dari kelompok lainnya. Prinsip ini mencakup otoritas dan tanggung jawab kelompok manajemen risiko, serta hubungan antara kelompok ini dengan unit-unit lain dalam perusahaan, termasuk dalam hal pelaksanaan transaksi yang melibatkan risiko tertentu.

5. Pola Keputusan yang Disiplin

   Walaupun sains telah banyak berkontribusi dalam pengukuran risiko, kualitas keputusan tetap berdasar pada bagaimana manajemen memilih metode dan teknik yang tepat serta memahami keterbatasan masing-masing alat atau teknik tersebut.

6. Kebijakan

   Prinsip ini menetapkan bahwa tujuan dan strategi manajemen risiko perusahaan harus dituangkan dalam prosedur yang jelas. Tujuannya adalah memastikan tentang proses manajemen risiko kepada pihak internal maupun eksternal, termasuk stakeholder.

Cyber

Menurut Julis[15] *Cyber* yaitu dunia maya yang juga disebut dengan pemanfaatan internet. *Cybersecurity* terdiri dari dua kata: "*cyber*" berarti dunia maya atau internet, dan "*security*" yang berarti keamanan. Jadi, sederhananya, *cybersecurity* adalah keamanan siber.

[15] Julis, S. (2018). Komunikasi Dakwah di Era Cyber. *An-Nida' Jurnal Pemikiran Islam*, *42*(2), 30–51

Fungsi utama *cybersecurity* adalah untuk mengidentifikasi, memperbaiki, dan meminimalisir risiko ancaman serta serangan siber. *Cybersecurity* ini mencakup perlindungan semua komponen sistem siber, termasuk perangkat keras, perangkat lunak, data, informasi, dan infrastruktur.

Serangan siber adalah risiko serius bagi keamanan informasi dan infrastruktur teknologi, serta menjadi sasaran bagi ancaman siber. Ancaman ini, yang dilakukan melalui jaringan komputer atau telekomunikasi, menargetkan berbagai elemen seperti situs web, sistem komputer, dan perangkat pribadi. Menurut Uzlah et al.[16], Kemajuan teknologi informasi dan internet telah mempermudah pelaku untuk berselancar dengan mudah, lebih hemat biaya, dan lebih efisien. Kejadian serangan siber seringkali menyertakan spionase industri dan target-target pemerintah, yang dapat menimbulkan kekhawatiran dan ketegangan akibat risiko kebocoran data pribadi dan aset berharga. Selain digunakan sebagai alat politik dalam dunia maya, serangan siber juga dapat dimanfaatkan dalam konteks ekonomi.

C. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan penelitian kualitatif melalui metode Studi Kepustakaan. Penelitian ini melakukan pengumpulan data dari berbagai sumber informasi yang relevan. Dalam pendekatan ini, peneliti tidak melakukan interaksi langsung dengan objek penelitian, melainkan mengandalkan berbagai sumber tertulis untuk mendapatkan wawasan yang mendalam. Metode ini melibatkan survei terhadap buku, materi online, dan artikel ilmiah terdahulu yang berkaitan dengan topik yang diteliti, yaitu pengawasan risiko di perbankan syariah.

Proses penelitian dilakukan dengan cara yang teliti dan sistematis, memastikan bahwa hanya sumber yang dapat diandalkan yang digunakan. Hal ini termasuk buku fisik yang memiliki kredibilitas tinggi, literatur daring yang diakui, dan jurnal akademik yang membahas topik disrupsi digital marketing. Dengan pendekatan ini, peneliti dapat memperoleh informasi yang komprehensif dan mendalam mengenai fenomena disrupsi dalam pemasaran digital tanpa perlu melibatkan interaksi langsung dengan subjek penelitian. Sebaliknya, fokus penelitian adalah pada pencarian dan analisis referensi yang ada, yang memberikan dasar kuat untuk memahami dan menjelaskan dinamika yang terjadi dalam konteks pemasaran digital saat ini. Pendekatan ini memberikan keuntungan dalam menyusun argumen dan temuan yang berbasis pada sumber yang sudah ada, memastikan bahwa analisis dilakukan secara menyeluruh dan berbasis bukti.

[16] Uzlah, L. I., Saputra, R. A., & Isnawaty. (2024). Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2787–2793

D. HASIL DAN PEMBAHASAN

Kronologi Serangan Siber pada Bank Syariah Indonesia

Pada tanggal 8 hingga 16 Mei 2023, Bank Syariah Indonesia (BSI) menghadapi gangguan signifikan pada sistem informasinya yang menyebabkan disrupsi operasional yang luas. Awalnya, gangguan ini diperkirakan sebagai hasil dari proses pemeliharaan sistem yang rutin. Namun, seiring berjalannya waktu, situasi ini memicu kekhawatiran yang mendalam di kalangan nasabah karena permasalahan tersebut semakin kompleks. Pada 11 Mei 2023, muncul indikasi bahwa gangguan tersebut mungkin merupakan serangan siber berupa ransomware. Ketegangan semakin meningkat ketika kelompok hacker yang dikenal sebagai LockBit 3.0 mengklaim bertanggung jawab atas serangan tersebut. Mereka juga mengancam akan membocorkan data pribadi nasabah jika tuntutan mereka tidak dipenuhi, yang memperburuk kekhawatiran akan potensi dampak terhadap keamanan data dan integritas operasional bank[17]. Menurut Maulana & Nasrulloh[18], menanggapi insiden serangan siber, Bank Syariah Indonesia (BSI) menganggap penting untuk memberikan respons yang efektif dan efisien kepada nasabah serta pemangku kepentingan. Untuk meredakan ketegangan dan kekhawatiran yang muncul, BSI segera melaksanakan langkah-langkah komunikasi yang sistematis. Pada 8 Mei 2023, BSI menyampaikan pernyataan resmi melalui akun Instagram resminya, menginformasikan bahwa sistem mereka sedang dalam perbaikan, yang menyebabkan ketidakmampuan nasabah untuk mengakses layanan perbankan sementara waktu. Pernyataan ini bertujuan untuk memberikan klarifikasi mengenai penyebab gangguan dan mengonfirmasi bahwa perbaikan sedang dilakukan dengan prioritas. Selain itu, BSI juga menyampaikan permohonan maaf atas gangguan yang terjadi dan menekankan komitmennya terhadap keamanan data dan dana nasabah.

Selanjutnya, BSI merilis pernyataan pers pada 10 Mei 2023 untuk memberikan update mengenai situasi tersebut. Pernyataan ini mencakup informasi tambahan, yaitu bahwa pemeliharaan sistem masih berlangsung dan BSI meminta maaf atas ketidaknyamanan yang terjadi, sembari menekankan pentingnya keamanan dana nasabah. Direktur Utama BSI, Hery

[17] Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

[18] Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. *EKSISBANK (Ekonomi Syariah dan Bisnis Perbankan)*, *8*(1), 76–91.

Gunardi, menegaskan bahwa bank berkomitmen untuk melindungi keamanan dana dan data nasabah serta memulihkan layanan setelah insiden 8 Mei 2023. Selain itu, BSI berjanji akan menyelidiki kemungkinan serangan siber dan memperkuat pertahanan siber untuk memastikan perlindungan data nasabah.

Dampak Serangan Siber pada Bank Syariah Indonesia

Menurut Solikhawati & Samsuri[19], salah satu ancaman siber yang signifikan adalah serangan DDoS (*Distributed Denial of Service*). Serangan DDoS mengakibatkan ketidakmampuan untuk mengakses jaringan atau situs web dengan membanjiri jaringan tersebut dengan lalu lintas palsu. Serangan semacam ini dapat mengganggu kinerja sistem secara keseluruhan dan menghalangi nasabah untuk mengakses layanan yang mereka butuhkan. Seluruh aktivitatas keuangan nasabah mengalami gangguan yang terkait dengan gangguan atau penghentian operasi ekonomi dan bisnis, terutama di lokasi-lokasi yang sangat bergantung pada layanan BSI. Nasabah yang sudah mempercayakan kebutuhan layanan perbankan mereka kepada BSI memerlukan jaminan keamanan dari pihak bank, agar mereka tidak merasa khawatir dalam mengoperasikan bisnis atau kegiatan lainnya.

Serangan siber yang berhasil bisa menyebabkan dampak keuangan yang berarti bagi perusahaan. Biaya yang terkait dengan penanggulangan serangan, pemeliharaan sistem, audit keamanan, serta kompensasi yang perlu diberikan kepada pelanggan yang terdampak dapat menjadi beban untuk perusahaan. Menurut Radiansyah et al.,[20] hal ini dapat berdampak negatif terhadap kinerja keuangan perusahaan, menyebabkan kekhawatiran di kalangan investor mengenai keumungkinan penurunan laba. Oleh karena itu, sangat penting bagi perusahaan mempunyai tahapan keamanan siber yang kuat dan cepat, serta kapabilitas menangani serangan siber dengan optimal.

Menurut Herera & Sebyar Kita harus memahami bahwa serangan siber tidak hanya menimbulkan ancaman bagi individu atau entitas bisnis tertentu, tetapi juga dapat berdampak luas pada tingkat nasional dan internasional. Serangan siber memiliki potensi untuk merusak dan menghancurkan infrastruktur penting, serta menyebabkan kerugian besar pada sektor bisnis. Oleh karena itu, kebijakan regulasi yang efektif harus mampu mengatasi dan meningkatkan kesiapan menghadapi skala dan kompleksitas serangan siber. Menurut

[19] Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

[20] Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1. https://doi.org/10.22219/jibe.vol7.no1.1-14

Solikhawati & Samsuri, disaat perusahaan menghadapi serangan siber, manajemen harus siaga untuk menguatkan pengawasan internal, mengurangi risiko operasional, dan menjaga citra. Bank mungkin akan mengurangi praktik manajemen laba dan mengoptimalkan kualitas data akuntansi, sesuai bentuk serangan siber yang dihadapi. Kendati demikian, ketika bank menjadi korban serangan siber, bank mungkin akan kehilangan nasabah atau gangguan operasional. Menurut Saputro et al.,[21] Serangan siber yang mengganggu kegiatan operasional bisa memicu penarikan dana besar-besaran oleh nasabah yang gelisah akan keamanan datanya, sehingga berpotensi menimbulkan risiko likuiditas dan mengancam stabilitas keuangan.

Tantangan dan Solusi dalam Pengawasan Risiko di Perbankan Syariah pada Era Cyber

Menurut Al-Alawi et al.,[22] keamanan siber menjadi topik hangat dengan munculnya Inovasi Keuangan Digital (IKD) dalam perbankan syariah. Mengingat krisis kriminalitas di dunia digital yang terus berkembang seiring dengan perkembangan teknologi, maka menjadi penting bagi perbankan syariah untuk memperkuat kesadaran akan keamanan siber. Perbankan syariah perlu melakukan kerjasama ekonomi yang kuat dengan pasar untuk mengembangkan proses penentuan keputusan yang tepat, memungkinkan deteksi masalah dan penerapan langkah-langkah solutif. Kepatuhan terhadap standar keamanan, komitmen, alokasi anggaran, manajemen, dan langkah-langkah keamanan menjadi faktor-faktor utama dalam pencegahan kejahatan siber. Menurut (Wiguna et al., 2023) Risiko keamanan siber merupakan ancaman signifikan bagi sektor perbankan dan keuangan. Serangan siber yang semakin canggih menimbulkan ancaman terhadap integritas dan keamanan data keuangan. Perlindungan terhadap ancaman siber memerlukan investasi besar dalam teknologi keamanan dan pelatihan karyawan.

Menurut Restika & Sonita,[23] hubungan manajemen likuiditas dan keamanan siber merupakan hal yang penting diperhatikan secara detail. Keadaan likuiditas yang optimal membutuhkan proteksi atas serangan siber yang dapat mengganggu operasional dan mengurangi keyakinan nasabah. Dalam konteks tren global keamanan siber di sektor keuangan, penting bagi bank syariah untuk memahami dan menerapkan praktik terbaik yang

[21] Saputro, E. P., Nasir, M., Achyani, F., Arif, M., Setyaningrum, D. P., & Febriyanto, A. (2022). *Digitalisasi Perbankan: Prospek, Tantangan dan Kinerja* (1 ed.). Muhammadiyah University Press.

[22] Al-Alawi, Ismail, A., & Bassam, S. A. A.-. (2019). Assessing the Factors of Cybersecurity Awareness in the Banking Sector , (2019),. *Arab Gulf Journal of Scientific Research*, *37*(4), 17– 32.

[23] 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

relevan dengan perbankan syariah. Analisis tren ini memberikan wawasan berharga untuk mengatasi tantangan keamanan siber secara efektif. Kendala dalam keamanan siber dapat mempengaruhi manajemen likuiditas dalam perbankan syariah, di mana keberhasilan tidak hanya bergantung pada strategi finansial yang efektif, tetapi juga pada kemampuan bank untuk mengelola dan mengatasi ancaman keamanan siber.

Menurut Soesanto et al.,[24] media sosial menghadapi tantangan besar terkait serangan siber. Meskipun media sosial dapat mengancam kedaulatan negara, ia juga berfungsi sebagai sumber pengetahuan mengenai teknologi informasi dan komunikasi, serta meningkatkan keterampilan digital masyarakat. Di Indonesia, penggunaan teknologi digital memiliki potensi dalam konteks perang siber, di mana kerentanannya terhadap serangan dari peretas atau cracker internasional dapat mengakibatkan kerawanan informasi, terutama dalam transmisi informasi intelijen melalui dunia maya.

Menurut Soesanto et al. peningkatan kejahatan siber telah mencapai taraf yang mengkhawatirkan. penanggulangan perilaku melawan hukum di dunia maya tidak dapat dilakukan hanya dengan hukum positif konvensional. Hal ini terjadi karena keberagaman hubungan antara lima faktor terkait, yaitu pelaku dan korban kejahatan, reaksi publik atas kejahatan, dan hukum. Sekalipun hukum mempunyai peran fundamental dalam pencegahan dan penanggulangan kejahatan, menciptakan peraturan hukum yang responsif terhadap perubahan cepat di berbagai bidang, seperti teknologi informasi, bukanlah tugas yang mudah. Untuk menyikapi masalah kejahatan siber, diperlukan kolaborasi beberapa sektor dengan pemerintah, lembaga penegak hukum, sektor swasta, dan masyarakat. Tidak hanya itu, peningkatan rancangan hukum yang sesuai dan pemanfaatan teknologi keamanan siber yang canggih sangat penting untuk menghadapi ancaman siber yang terus meningkat.

Menurut Amelia & Ramdan, Audit internal adalah salah satu faktor kunci yang mempengaruhi kecepatan mitigasi risiko teknologi informasi. Sebagai suatu aktivitas evaluasi independen dalam organisasi, audit internal berfungsi untuk menilai operasi sebagai layanan kepada manajemen. Audit internal berkontribusi pada pencapaian tujuan organisasi melalui pendekatan yang sistematis dalam mengevaluasi serta memaksimalkan efektivitas manajemen risiko. Dalam konteks organisasi, audit internal beroperasi sebagai fungsi mandiri dengan tanggung jawab utama mengevaluasi, serta menyusun laporan yang menganalisis metodologi,

[24] Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

prosedur, dan proses yang terlibat dalam manajemen risiko. Dengan demikian, audit internal berperan dalam menilai langkah-langkah manajemen risiko untuk memastikan kesesuaiannya terhadap paparan risiko yang merupakan fokus utama dalam pengawasan risiko perbankan.

Menurut Fatmala Putri & Ratna Sari,[25] Bank Syariah Indonesia (BSI) telah menerapkan serangkaian tindakan keamanan untuk melindungi nasabahnya. Dalam menangani serangan ransomware, entitas yang terkena dampak perlu segera berkoordinasi dengan penegak hukum, lembaga penanganan darurat serangan siber, atau penyedia layanan keamanan siber. Teknologi keamanan yang diterapkan oleh BSI mencakup enkripsi data, otentikasi dua faktor, dan sistem keamanan tambahan. BSI telah mengalokasikan anggaran sebesar Rp 580 miliar untuk memperkuat upaya digitalisasi dan keamanan data sebagai respons terhadap gangguan layanan dan isu kebocoran data yang terjadi baru-baru ini. Anggaran tersebut diarahkan untuk pengamanan data dan layanan perbankan. BSI juga melaksanakan langkah-langkah preventif untuk memperkuat sistem keamanan teknologi informasi dengan meningkatkan perlindungan dan ketahanan sistem terhadap potensi gangguan data. Selain itu, BSI berkolaborasi dengan pihak-pihak terkait, termasuk Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI).

Teknologi *blockchain* juga bisa menjadi solusi untuk mengurangi risiko serangan siber. Penerapan teknologi blockchain dalam transaksi keuangan pada perbankan syariah memberikan kontribusi yang berarti pada pengoptimalan keamanan. Teknologi blockchain memanfaatkan algoritma kriptografi yang canggih dan alur yang tidak terpusat untuk membuktikan kredibiltas dan keaslian data. Pada sektor perbankan syariah, hal ini berperan penting dalam meminimalisir risiko fraud dan serangan siber yang dapat mengancam keamanan dana nasabah. Pemanfaatan teknologi *blockchain* juga memberi efek signifikan terhadap keterbukaan transaksi keuangan dalam perbankan syariah. Blockchain menyajikan bukti transaksi yang bisa diperiksa secara transparan oleh semua stakeholder. Hal ini meningkatkan kepercayaan nasabah dan otoritas syariah terhadap kredibilitas perbankan syariah. Selain itu, keterbukaan yang ditawarkan oleh blockchain juga mempermudah proses audit eksternal dan pelaporan yang sesuai dengan prinsip syariah.

Adapun tahapan manajemen risiko yang dapat diterapkan dalam mengatasi risiko siber adalah sebagai berikut :

[25] Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi dan Manajemen*, *1*(4), 173–181.

1. *Identify*, risiko kejahatan siber harus diidentifikasi secara berkala untuk mendeteksi potensi ancaman. Proses ini melibatkan penilaian menyeluruh terhadap aspek-aspek yang dapat menyebabkan kerugian, dengan ukuran risiko ditentukan berdasarkan dua parameter utama: Probabilitas terjadinya ancaman dan Dampak yang mungkin ditimbulkan.
2. *Assess*, pada tahap penilaian, fokus utama adalah pada dampak risiko kejahatan siber terhadap berbagai aspek, terutama dalam konteks pertahanan negara. Risiko tidak dapat diukur secara langsung, namun tabel matriks dapat digunakan untuk menilai tingkat risiko tersebut. Metode ini, jika efektif untuk keamanan negara, juga dapat diadaptasi untuk manajemen risiko dalam sektor perbankan.
3. *Treat*, sebagai dasar untuk menentukan pendekatan dalam menangani risiko, apakah risiko tersebut akan diterima, dialihkan, diminimalisir, atau dihindari. Dalam hal ini, penting untuk menerapkan strategi mitigasi guna mengurangi potensi pencurian informasi dan data, yang sering terjadi baik pada tingkat individu maupun institusi.
4. *Control*, adalah pemantauan dan penyesuaian secara berkelanjutan yang diperlukan untuk mengevaluasi efektivitas manajemen risiko. Dalam proses penagwasan ini, sebaiknya terdapat sistem peringatan dini bagi pihak pengelola keamanan, agar mereka dapat mengambil langkah yang diperlukan untuk mencegah potensi ancaman kejahatan siber.

E. KESIMPULAN

Insiden serangan siber terhadap Bank Syariah Indonesia (BSI) pada periode 8 hingga 16 Mei 2023 mengungkap kerentanan yang signifikan dalam sistem perbankan terhadap ancaman dunia maya. Gangguan yang awalnya dianggap sebagai pemeliharaan rutin kemudian berkembang menjadi krisis yang lebih serius dengan munculnya dugaan serangan ransomware oleh kelompok hacker LockBit 3.0. Respon cepat BSI dengan mengomunikasikan situasi melalui media sosial dan pernyataan pers menunjukkan komitmen mereka untuk memelihara keamanan dana dan data nasabah serta melakukan penyelidikan mendalam terhadap insiden ini.

Dampak dari serangan ini meliputi gangguan operasional besar-besaran dan peningkatan kekhawatiran di kalangan nasabah. Selain itu, BSI juga berkolaborasi dengan lembaga penegak hukum dan penyedia layanan keamanan siber untuk mengatasi dan mencegah serangan di masa depan. Tidak hanya menyebabkan gangguan operasional tetapi juga berpotensi menimbulkan kerugian finansial dan reputasi yang besar. Serangan siber yang

mengganggu kegiatan operasional dapat memicu penarikan dana besar-besaran oleh nasabah yang khawatir akan keamanan datanya, sehingga berpotensi menimbulkan risiko likuiditas dan mengancam stabilitas keuangan

Tantangan dalam pengawasan risiko di era siber melibatkan penggunaan media sosial. Meskipun pemanfaatan media sosial dapat mengancam keamanan data, media sosial juga berfungsi sebagai sumber pengetahuan mengenai teknologi informasi, komunikasi, dan digital, yang memungkinkan peningkatan keterampilan digital masyarakat. Di Indonesia, penggunaan teknologi digital memiliki potensi dalam konteks perang siber. Teknologi informasi rentan terhadap serangan dari peretas atau cracker internasional, yang dapat menimbulkan kerentanan informasi, terutama terkait transmisi intelijen melalui dunia maya.

Penggunaan teknologi blockchain diusulkan sebagai solusi potensial untuk meningkatkan keamanan transaksi keuangan di perbankan syariah, mengingat transparansi dan integritas data yang ditawarkannya. Implementasi manajemen risiko siber yang efektif, termasuk identifikasi, penilaian, penanganan, dan kontrol, sangat penting untuk stabilitas dan keamanan sistem perbankan. Insiden ini menyoroti kebutuhan mendesak untuk meningkatkan kesadaran dan kesiapan dalam menghadapi ancaman siber melalui langkah-langkah proaktif yang menggabungkan teknologi canggih dan kebijakan regulasi yang adaptif.

SARAN

Untuk mengomptimalkan keamanan sistem pada sektor perbankan dari serangan siber, perbankan sebaiknya berinvestasi lebih banyak di bidang teknologi dan keamanan yang lebih canggih, sebab kemajuan teknologi tentu beriringan dengan keberagaman bentuk serangan siber, sehingga teknologi yang digunakan setara dengan tingkat kecanggihan ancaman serangan siber yang dihadapi. Selanjutnya, melakukan kolaborasi dengan Badan Siber dan Sandi Negara, OJK, dan Bank Indonesia untuk mempercepat respons terhadap ancaman serangan siber. Terakhir, melakukan training secara berkala untuk meningkatkan kemampuan SDM dalam perbankan untuk menghadapi serangan siber.

DAFTAR PUSTAKA

Akbar. C, Eril, Abdullah, M. W., & Awaluddin, M. (2022). Manajemen Risiko di Perbankan Syariah. *Milkiyah: Jurnal Hukum Ekonomi Syariah*, *1*(2), 51–56. https://doi.org/10.46870/milkiyah.v1i2.230

Al-Alawi, Ismail, A., & Bassam, S. A. A.-. (2019). Assessing the Factors of Cybersecurity Awareness in the Banking Sector , (2019),. *Arab Gulf Journal of Scientific Research*, *37*(4), 17– 32.

Amelia, E., & Ramdan, M. H. (2019). Pengaruh Audit Internal Terhadap Mitigasi Risiko Operasional Perbankan Syariah. *Ad Deenar: Jurnal Ekonomi dan Bisnis Islam*, *3*(1),

57–74. https://doi.org/10.30868/ad.v3i01.500

Arif, M. N. R. Al, & Rahmawati, Y. (2018). *Manajemen Risiko Perbankan Syariah (Suatu Pengantar)*. CV. Pustaka Setia.

Arifin, Z. (2009). *Dasar-dasar Manajemen Bank Syariah*. Azkia Publisher.

Bahanan, M., & Wahyudi, M. (2023). Analisis Pengaruh Penggunaan Teknologi Blockchain dalam Transaksi Keuangan pada Perbankan Syariah. *I'Thisom: Jurnal Ekonomi Syariah*, *2*(1).

Fasa, M. I. (2016). Manajemen Resiko Perbankan Syariah di Indonesia. *Jurnal Studi Ekonomi dan Bisnis Islam*, *1*(2), 36–53.

Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi dan Manajemen*, *1*(4), 173–181.

Hajar, S., & Wirman. (2023). Implementasi Manajemen Risiko Dalam Dunia Perbankan Syariah. *Jurnal Ilmiah Wahana Pendidikan*, *9*(5), 500–513.

Herera, A. ., & Sebyar, H. . (2023). Perlindungan Hukum Terhadap Serangan Siber: Tinjuan Atas Kebijakan dan Regulasi Terbaru. *Jurnal Hukum dan Kewarganegaraan*, *1*(5).

Julis, S. (2018). Komunikasi Dakwah di Era Cyber. *An-Nida' Jurnal Pemikiran Islam*, *42*(2), 30–51.

Kairupan, V. A., & Rahman, A. A. (2022). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung. *Jurnal Darma Agung*, *30*(1), 1164. https://doi.org/10.46930/ojsuda.v30i1.3167

Karim, A. A. (2008). *Bank Syariah Analisis Fiqih dan Keuangan*. PT. Raja Grafindo Persada.

Khaerunnisa, R. (2024). *BSI: Transaksi digital banking naik 45,02 persen per Juni 2024*. antaranews. https://www.antaranews.com/berita/4206435/bsi-transaksi-digital-banking-naik-4502-persen-per-juni-2024

Laras, A. (2024). *Rapor Pengguna Mobile Banking Bank Jumbo Kuartal I/2024: BRI Teratas, Mandiri Melesat!* Finansial Bisnis. https://finansial.bisnis.com/read/20240529/90/1769456/rapor-pengguna-mobile-banking-bank-jumbo-kuartal-i2024-bri-teratas-mandiri-melesat

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. *EKSISBANK (Ekonomi Syariah dan Bisnis Perbankan)*, *8*(1), 76–91.

Nelly, R., Siregar, S., & Sugianto, S. (2022). Analisis Manajemen Risiko Pada Bank Syariah: Tinjauan Literatur . *Reslaj : Religion Education Social Laa Roiba Journal*, *4*(4), 918–930. https://doi.org/10.47467/reslaj.v4i4.1008

Nursaman. (2022). Manajemen Pengawasan Risiko dalam Bisnis Bank Syariah. *Jurnal Ekonomi Rabbani*, *2*(1), 198–204. http://jurnal.steirisalah.ac.id/index.php/rabbani/article/view/87

Putra, P. A., Saparuddin, S., & Nurnasrina, N. (2023). Mitigasi Risiko: Analisis Terhadap Antisipasi Risiko Dalam Pembiayaan Mikro Syariah. *Al-Masraf: Jurnal Lembaga Keuangan dan Perbankan*, *8*(1), 62. https://doi.org/10.15548/al-masraf.v8i1.414

Rabbani, S., & Diana, D. (2023). Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer. *Smatika Jurnal*, *13*(02), 284–293. https://doi.org/10.32664/smatika.v13i02.934

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1. https://doi.org/10.22219/jibe.vol7.no1.1-14

Rahmawati, I. (2017). The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

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

Rianto, R. B. (2013). *Manajemen Resiko Perbankan Syariah di Indonesia*. Salemba Empat.

Rossdiana, R. A., & Fahrisa, T. R. (2023). Strategi Cybersecurity Pemerintah India Dari Perspektif Kautilya. *Indonesian Journal of International Relations*, *7*(1), 140–164. https://doi.org/10.32787/ijir.v7i1.408

Rusdan. (2016). Urgensi Manajemen Pengawasan Risiko Bank Syariah. *PALAPA: Jurnal Studi Keislaman dan Ilmu Pendidikan*, *4*(2), 85–103.

Saputro, E. P., Nasir, M., Achyani, F., Arif, M., Setyaningrum, D. P., & Febriyanto, A. (2022). *Digitalisasi Perbankan: Prospek, Tantangan dan Kinerja* (1 ed.). Muhammadiyah University Press.

Setiawati, S. (2024). *Cashless Makin Digemari, Ini 5 Digital Banking Pilihan Warga RI*. cnbcindonesia. https://www.cnbcindonesia.com/research/20240610063016-128-545113/cashless-makin-digemari-ini-5-digital-banking-pilihan-warga-ri

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

Syahrir, D. K., Ickhsanto Wahyudi, Santi Susanti, Darwant, D., & Ibnu Qizam. (2023). Manajemen Risiko Perbankan Syariah. *AKUA: Jurnal Akuntansi dan Keuangan*, *2*(1), 58–64. https://doi.org/10.54259/akua.v2i1.1382

Tambunan, N., Fitri Wulandari, A., Pangesti, A. N., Anggraini, A., Tunnaja, S., Dewi Gita, A., & Rusmarhadi, I. (2023). Berita Utama Tentang Error Service Di Bank Syariah Indonesia (Bsi). *Community Development Journal*, *4*(2), 5096–5098.

Uzlah, L. I., Saputra, R. A., & Isnawaty. (2024). Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2787–2793.

Wiguna, A., Alfianto, E., Kumala, E. C., & Maryadi, M. G. P. (2023). Problematika dan Tantangan dalam Sektor Perbankan dan Keuangan di Tahun 2024. *Neraca: Jurnal Ekonomi, Manajemen dan Akuntansi*, *2*(6), 627–632.