talenta PUBLISHER

Recht Studiosum Law Review

Journal homepage: https://talenta.usu.ac.id/rslr

Analisis Kebijakan Otoritas Jasa Keuangan dalam Upaya Menanggulangi *Cyber Crime* di Sektor Perbankan

Afiah Nurrizky[1], Wahyu Nugroho[2]
[1,2] *Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Sleman, 55281, Indonesia*
[*]Corresponding Author: afiahnr.rizky@gmail.com

ARTICLE INFO

Article history:
Received 10 October 2024
Revised 10 May 2025
Accepted 10 May 2025
Available online
https://talenta.usu.ac.id/rslr

E-ISSN: 2961-7812
PISSN: 2985-9867

How to cite:
Nurrizky, A. & Nugroho, W. (2020). Analisis Kebijakan Otoritas Jasa Keuangan dalam Upaya Menanggulangi Cyber Crime di Sektor Perbankan. Recht Studiosum Law Review, 4(1), 84-94.

10.32734/rslr.v4i1.18452

ABSTRACT

This research aims to analyze the Financial Services Authority's policies in mitigating cybercrime in the banking sector, starting from the legal basis, policy framework, risk management, and practical policies that have been implemented by the OJK for the sake of the cyber resilience of Indonesian banks.This paper uses a normative legal research method with a policy analysis approach. The data collection technique is a literature study by collecting legal bases in the form of laws and regulations. The results show that the Financial Services Authority has issued policies related to cybersecurity in the banking sector starting when banks first adapted Information Technology in their banking activities. Some of these policies are in the form of regulations or POJK, and some other are in the form of circular letters or SEOJK. Those policies were made with a strong legal basis, and have a clear direction determined in their blueprint. One of the policies issued is related to the security risk management process and procedures.
Keyword: *Policy, Financial Services Authority, Cyber Crime, Banking*

ABSTRAK

Penelitian ini bertujuan untuk menganalisis kebijakan Otoritas Jasa Keuangan dalam memitigasi kejahatan siber di sektor perbankan, mulai dari landasan hukum, kerangka kebijakan, manajemen risiko, serta kebijakan praktis yang telah dijalankan OJK demi ketahanan siber perbakan Indonesia. Tulisan ini menggunakan metode penelitian hukum normatif dengan pendekatan *policy analysis*. Teknik pengumpulan data yang dilakukan berupa studi pustaka dengan mengumpulkan dasar-dasar hukum berupa peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa Otoritas Jasa Keuangan telah mengeluarkan kebijakan-kebijakan terkait keamanan siber di sektor perbankan dimulai saat bank pertama kali mengadaptasi teknologi informasi dalam kegiatan perbankannya. Kebijakan-kebijakan tersebut ada yang berupa peraturan atau POJK, ada pula berupa surat edaran atau SEOJK. Kebijakan-kebijakan tersebut dibuat dengan dasar hukum yang kuat, serta memiliki arah yang jelas ditentukan dalam cetak biru. Salah satu kebijakan terkait yang dikeluarkan ialah terkait proses dan prosedural manajemen risiko keamanan siber.
Kata Kunci: Kebijakan, Otoritas Jasa Keuangan, Kejahatan Siber, Perbankan

1. Pendahuluan

Perkembangan teknologi informasi yang semakin pesat tentu memberi banyak sumbangsih terhadap segala kemudahan dalam setiap kegiatan masyarakat. Selain optimalisasi akses informasi dan komunikasi, teknologi informasi juga memberi dampak besar dalam perkembangan pelayanan di berbagai sektor, baik pelayanan pemerintahan, pendidikan, kesehatan, transportasi hingga keuangan. Dalam pelayanan keuangan, salah satu sektor yang terdampak langsung oleh teknologi informasi adalah perbankan.

Tren perbankan digital pun mulai menggeser perbankan konvensional karena nilai efisiensi, ekfektifitas, aksesibilitas hingga kenyamanan yang lebih unggul. Transformasi layanan perbankan digital ini sebenarnya tidak jauh dari dorongan digitalisasi dan penetrasi teknologi informasi di masyarakat global. Layanan perbankan digital kemudian semakin merambah dan memberikan manfaat signifikan bagi nasabah dan juga lembaga keuangan.[1] Melalui layanan perbankan digital, kini nasabah dapat membuka rekening, melakukan transaksi dan mengakses segala layanan perbankan lain dengan lebih cepat dan mudah hanya melalui platform digital tanpa harus datang ke kantor bank. Di samping membawa dampak positif, perkembangan teknologi informasi juga memunculkan konsekuensi logis berupa risiko siber (*cyber risk*) yang kapan saja dapat menyerang keamanan bank.

Sektor keuangan dan perbanakan merupakan sektor yang akan selalu menjadi target empuk bagi penjahat siber. Meskipun bank-bank memiliki sistem keamanan yang cukup kompleks, faktanya kerentanan sistem terhadap serangan siber masih tetap tinggi. Buktinya, sektor perbankan konsisten berada di puncak daftar sektor yang rentan terhadap serangan siber. Berdasarkan data *Checkpoint Research* 2023, sektor keuangan/perbankan mengalami serangan siber dengan rata-rata 1.162 kali kasus per pekannya, meningkat 3% dari catatan tahun 2022.[2] Bahkan menurut *International Monetary Fund* (IMF), secara global sektor keuangan diperkirakan mengalami kerugian dari serangan siber hingga mencapai USD$100 miliar atau lebih dari Rp1.433 triliun pada tahun 2020. Dalam konteks Indonesia, menurut laporan Direktorat Operasi Keamanan Siber BSSN, sektor keuangan merupakan salah satu sektor yang mengalami anomali trafik jaringan terbanyak per tahun, tepatnya terdapat 1,6 miliar insiden pada tahun 2021, 976,4 juta pada tahun 2022, dan 160 juta pada tahun 2023.[3]

Ancaman-ancaman siber yang sering dijumpai menyerang industri keuangan/perbankan adalah:[4]

a. *Skimming* yakni perekaman kegiatan transaksi di mesin ATM.
b. *Phinsing attack* atau pengelabuan nasabah dengan website bank palsu.
c. *Ransomeware attack* yang menyerang sistem komputer bank dan menyandera datanya.
d. *Malware attack* yaitu mengakses data bank melalui software berbahaya.
e. *Distributed denial of service* dengan membanjiri situs web bank menggunakan lalu lintas internet palsu.
f. *Insider threads* yakni orang internal yang membocorkan informasi sensitif, mencuri data dan/atau merusak sistem.

Oleh karena memegang data sensitif dalam jumlah besar, perbankan menjadi sangat rentan terhadap pelanggaran akses data dan serangan siber. Selain karena banyak menyimpan data sensitif, yang menyebabkan kerentanan perbankan adalah keamanan umum yang kurang. Hal ini nampak pada penggunaan kata sandi yang lemah atau mudah, perangkat lunak yang tidak aktual, dan enkripsi data yang kurang baik sehingga mudah diakses oleh penyerang.[5] Selain itu, kerentanan bank juga dikarenakan kompleksitas infrastruktur bank yang membuatnya sulit untuk mengamankan setiap bagian dari jaringan. Kemudian, faktor ketergantungan pada teknologi yang pada akhirnya membuka peluang bagi siapa saja untuk

---

[1] Dwi Setyaningrat, dkk. (2023). Strategi Digitalisasi Untuk Mendorong Inklusi Keuangan Nasabah Bank Syariah: Pendekatan Technology Acceptance Model (TAM). Proceedings of Islamic Economics, Business, and Philanthropy, 2(1), 54.

[2] Check Point Research Team. (2024, Januari). Check Point Research: 2023 – The Year of Mega Ransomware Attack with Unprecedented Impact on Global Organizations. Dikutip dari https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/.

[3] Estu Suryowati. (2023, Desember) BSSN: Sektor Keuangan Peringkat Ketiga Paling Rentan Kejahatan Siber Setelah Administrasi Pemerintahan Dan Energi. Jawa Pos. Dikutip dari https://www.jawapos.com/ekonomi-digital/013669836/bssn-sektor-keuangan-peringkat-ketiga-paling-rentan-kejahatan-siber-setelah-administrasi-pemerintahan-dan-energi.

[4] Muhammad Khairul Faridi. (2018). Kejahatan Siber Dalam Bidang Perbankan. CyberSecurity dan Forensik Digital, 1(2), 59–60.

[5] Budi Harto, dkk. (2023). Transformasi Bisnis di Era Digital (Teknologi Informasi dalam Mendukung Transformasi Bisnis di Era Digital). Jambi: Sonpedia Publishing Indonesia. 29

memanfaatkan setiap kelemahan yang ada. Hal ini ditambah dengan kurangnya pemahaman dan pelatihan karyawan bank tentang taktik serangan siber.

Belakangan ini, terjadi insiden *cyber-ransomeware* yang menyerang Bank Syariah Indonesia (BSI) sejak Senin, 8 Mei 2023 silam. Ketika itu nasabah tidak dapat mengakses serta bertransaksi melalui MBanking, mesin ATM, dan teller di kantor bank cabang. [6] Kasus ini perlu menjadi perhatian, tidak hanya kepada BSI tapi juga seluruh perbankan Indonesia untuk terus meningkatkan ketahanan siber (*cyber resilience*), sebab serangan siber akan semakin massif dan canggih seiring perkembangan teknologi.

Dalam rangka menangani hal tersebut, pemerintah berperan dalam menetapkan hukuman yang tegas bagi pelaku kejahatan siber. Dengan adanya undang-undang dan regulasi yang ketat, bank-bank merasa terdorong untuk memperkuat kebijakan keamanan mereka dan memastikan keamanan sistem mereka. Selain itu, Otoritas Jasa Keuangan (OJK) sebagai lembaga yang berwenang terhadap segala lalu lintas ekonomi di Indonesia juga telah mengeluarkan banyak kebijakan yang berhubungan dengan pertahanan dinding siber perbankan. Salah satu upaya peningkatan ketahanan siber adalah dengan memperkuat manajemen risiko keamanan siber (*cyber security risk management*). Kebijakan ini dapat dilakukan dengan mendeteksi, mengidentifikasi, merespon, melindungi, dan mengatasi ancaman risiko siber secara akuntabel. Adapun langkah-langkah secara spesifik biasanya diatur oleh masing-masing bank sebagai bentuk pengendalian internal maupun adaptasi dari regulasi, prosedur opsional, dan konsultasi resmi dari OJK.[7]

Terlihat peranan OJK sangat penting sebagai garda terdepan dalam upaya mempersempit ruang gerak kejahatan siber di sektor perbankan. Titik inilah yang menarik perhatian peneliti untuk mengkaji lebih jauh terkait kebijakan OJK meliputi dasar, kualitas hingga perannya dalam memperkuat ketahanan siber perbankan di Indonesia. Kajian tentang serangan siber akan terus menjadi topik menarik bagi para peneliti karena merupakan masalah yang sangat relevan di era digital saat ini. Sehingga penelitian sejenis ini telah banyak dilakukan sebelumnya dengan beragam fokus dan metode.

Kajian dalam topik ini dimulai dengan pengidentifikasian jenis dan bentuk kejahatan siber di industri perbankan hingga langkah-langkah penanggulangannya. Penelitan terakhir dilakukan oleh Edy Soesanto, dkk yang berjudul "Sistem Kebijakan Objek Vital, Pengamanan File, Pengamanan *Cyber* PT Bank Negara Indonesia (Persero) Tbk." mengkaji sistem kebijkan pengamanan *cyber* oleh Bank Negara Indonesia (BNI) dengan pendekatan empiris ke kantor BNI cabang Jawa Barat. Sementara itu, penerapan kebijakan tentu diperlukan evaluasi terkait efektivitas dan efisiensi penerapannya. Terkait hal tersebut, telah dikaji oleh Dewi Chirzah dan Evendi Yudhi Al-Fadli dengan judul "Analisis Evaluasi Kebijakan Pada *Cyber Security* Perbankan". Penelitian ini memperlihatkan keragaman kebijakan tiap bank dalam menghadapi *cybercrime* serta analisis dan evaluasi efektivitasnya yang juga berbeda-beda mengingat masalah dan upaya penaggulangan tiap bank berbeda.

Rangkaian kajian tersebut semakin mengerucut hingga pada kajian terdekat dengan penelitian ini yaitu berkaitan dengan peran OJK. Ini terlihat pada penelitian Albertus Makur dan Sri Astutik yang berjudul "Analisis Peran Otoritas Jasa Keuangan (OJK) dalam Pengawasan dan Regulasi Industri Perbankan di Indonesia". Penelitian tersebut menganalisis peran OJK dalam mengawasi dan meregulasi industri perbankan di Indonesia khususnya pada perkembangan industri digital. Konteks ini yang menghadapkan OJK pada dinamika yang berkaitan dengan: perubahan layanan keuangan setelah adanya *fintech*, muncul tantangan perlindungan konsumen dalam dunia digital, meningkatnya risiko keamanan siber, adaptasi perubahan kebijakan global, standarisasi regulasi internasional, persaingan dan konsolidasi industri, serta misi peningkatan literasi keuangan. Berdasarkan kajian tersebut, penelitian ini akan berfokus pada substansi kebijakan OJK dalam keamanan siber perbankan, bagaimana OJK mitigasi serangan siber dalam sektor perbankan, membahas lebih dalam mengenai landasan kebijakan tersebut, kerangka kebijakan yang dibagun,

[6] Nurma Tambunan, dkk. (2023). Berita Utama Tentang Error Service Di Bank Syariah Indonesia (BSI). Community Development Journal, 4(2), 5097.

[7] Otoritas Jasa Keuangan. (2021). Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum. Jakarta: Departeme Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan.

manajemen risiko yang digunakan, serta kebijakan praktis yang telah dijalankan OJK untuk memastikan keamanan siber dalam sektor perbankan.

2. Metode Penelitian

Metode yang akan digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan *policy analysis* (analisis kebijakan). Teknik pengumpulan bahan hukum dilakukan melalui studi pustaka dengan mengumpulkan dasar-dasar hukum berupa peraturan perundang-undangan, Peraturan OJK serta Surat Edaran OJK. Selain itu, analisis kebijakan dilakukan secara kualitatif dengan mengkaji dasar serta isi dari suatu kebijakan publik. Data yang diperoleh selanjutnya akan dipersiapkan kemudian dianalisis secara kualitatif dengan melalui tiga tahap, yakni reduksi data, penyajian data, dan penarikan kesimpulan.

3. Hasil dan Pembahasan

3.1. Soal Otoritas Jasa Keuangan

Otoritas Jasa Keuangan (OJK) merupakan lembaga yang bertanggung jawab dalam mengawasi dan mengatur sektor jasa keuangan di Indonesia. OJK didirikan berdasarkan UU No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan. Tujuan pendirian OJK adalah untuk melindungi kepentingan nasabah, memelihara stabilitas sistem keuangan, serta mendorong perkembangan dan keberlanjutan industri jasa keuangan di Indonesia.[8] OJK memiliki wewenang untuk melakukan pengawasan terhadap bank-bank di Indonesia. Hal ini termasuk pengawasan terhadap tata kelola bank, manajemen risiko, dan pencegahan kegiatan perbankan yang terkait dengan kejahatan seperti pencucian uang dan pendanaan terorisme.

OJK juga memiliki peran dalam pembuatan aturan dan kebijakan di sektor perbankan. Diketahui, OJK membuat peraturan yang berkaitan dengan ketentuan operasional bank, produk dan layanan perbankan, serta standar perlindungan konsumen. Selain itu, OJK mengawasi aspek-aspek yang berhubungan dengan perlindungan nasabah perbankan, seperti transparansi informasi, kepastian hukum, dan penyelesaian sengketa. Memelihara stabilitas sistem keuangan Indonesia juga merupakan domain OJK. Jadi, OJK melakukan pemantauan terhadap risiko-risiko yang dapat mempengaruhi stabilitas sistem keuangan, serta mengambil tindakan yang diperlukan untuk mencegah dan menangani krisis keuangan.

Kebijakan OJK mengenai keamanan siber dimulai dari pengenalan dan pemanfaatan teknologi informasi dalam menjalankan kegiatan perbankan, mulai dari pengelolaan data keuangan hingga penyediaan layanan jasa perbankan. Bentuk-bentuk penggunanan teknologi informasi dalam perbankan adalah internet banking, mobile banking, sistem informasi akuntansi, hingga *start-up* teknologi keuangan atau *fintech*.[9] Bentuk kebijakan inilah yang kemudian menjadi payung dari pelaksanaan mitigasi resiko keamanan siber pada sektor perbankan.

Secara umum, terdapat beberapa jenis badan usaha bank di Indonesia. Badan usaha bank tersebut meliputi bank umum, bank perekonomian, bank konvensional, dan bank syariah. Oleh karena itu, ketentuan terkait penyelenggaraan teknologi informasi dalam perbankan juga memiliki konstruksi yang berbeda-beda tergantung dari jenis banknya. Bank perekonomian sebagaimana diatur dalam Peraturan OJK No. 75 tahun 2016 tentang Standar Penyelenggaraan Teknologi Informasi untuk BPR dan BPRS, belum diatur secara spesifik mengenai *cyber security*. Hal ini dikarenakan penyelenggaraan teknologi informasi dalam bank perekonomian yang masih tergolong sederhana. Adapun pengaturan tentang teknologi informasi untuk bank

[8] Nabilah Farah Diba, Hari Sutra Disemadi, dan Paramita Prananingtyas. (2019). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) di Indonesia. EKSPOSE: Jurnal Penelitian Hukum dan Pendidikan, 18(2), 870.

[9] Inarotul A'yun, Silvia Dwi, dan Aprilia Putri. (2022). Peran Digitalisasi dan Informasi terhadap Kinerja Perbankan Syariah dalam Perspektif Society 5.0 di Perekonomian di Indonesia. Jurnal Perbankan Syariah, 2(1), 2.

umum terdapat dalam Peraturan Otoritas Jasa Keuangan (POJK) tahun 2017 tentang Manajemen Resiko Teknologi Informasi.[10]

Berdasarkan penjelasan tersebut, dapat dikatakan bahwa fokus antara bank perekonomian dan bank umum memiliki perbedaan. Bank perekonomian masih membahas seputar bagaimana penyelenggaraan teknologi informasi dapat berjalan dengan aman. Berbeda dengan bank umum yang memiliki perangkat yang lebih kompleks daripada bank perekonomian. Ditambah lagi, sejak saat pertama kali mengadopsi teknologi informasi dalam kegiatan perbankan, bank umum acap kali menghadapi serangan siber. Maka dari itu, pengaturan bank umum terkait *cyber security* juga memiliki konstruksi lebih konkrit.

Pengaturan terkait keamanan siber OJK telah termaktub dalam Peraturan Otoritas Jasa Keuangan (POJK) No. 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.[11] Setelah Peraturan OJK, kemudian dibentuk juga ketentuan pelaksananya berbentuk Surat Edaran OJK (SEOJK). Perbedaannya, POJK mengatur secara umum dan prinsip, sedangkan SEOJK mengatur secara konkrit dan teknis. SEOJK biasanya berisi laporan apa saja yang perlu bank lampirkan, formatnya seperti apa, hingga langkah langkah penilaian tingkat risiko keamanan siber.[12]

Beberapa landasan hukum yang menjadi dasar dalam kebijakan OJK terkait keamanan siber antara lain: *Pertama*, UU No. 21 Tahun 2008 tentang Perbankan Syariah. Dalam undang-undang *a quo*, dibahas mengenai pengaturan keamanan sistem teknologi informasi yang harus dilakukan oleh bank syariah. Berdasarkan ketentuan ini juga, bank syariah diwajibkan untuk menerapkan sistem keamanan siber yang melindungi data dan informasi nasabah dari kejahatan siber. *Kedua*, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini menjelaskan bahwa pihak pengelola sistem informasi diwajibkan untuk menjaga kerahasiaan data dan informasi konsumen, serta mendukung keamanan dalam penggunaan teknologi informasi. Ketentuan ini menjadi landasan hukum bagi OJK dalam mengeluarkan kebijakan keamanan siber yang ditujukan pada pelaku usaha di sektor keuangan.

Ketiga, Peraturan Bank Indonesia No. 18/11/PBI/2016 tentang Penyelenggaraan Sistem Pembayaran. Dalam peraturan ini, termaktub ketentuan mengenai kewajiban penyelenggara sistem pembayaran dalam melindungi data dan informasi pelanggan dari akses tidak sah, serta kerahasiaannya harus dijaga. Ketentuan ini dasar bagi OJK untuk membuat kebijakan terkait keamanan siber yang berkaitan dengan lembaga penyelenggara sistem pembayaran. *Keempat*, POJK No. 13/POJK.02/2018 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Peraturan ini mengatur mengenai perlindungan konsumen di sektor jasa keuangan. Salah satu poin yang diatur dalam peraturan *a quo* adalah perlindungan terhadap keamanan data dan informasi para konsumen. Landasan hukum ini kemudian menjadi dasar bagi OJK untuk mengeluarkan kebijakan keamanan siber untuk menghindari masalah pencurian dan data sensitif.

Selanjutnya, *blueprint* dalam landasan hukum kebijakan OJK dalam keamanan siber memiliki arti sebagai rencana aksi yang terdiri dari kerangka konseptual dan prinsip-prinsip dasar dalam rangka meningkatkan ketahanan dan keamanan siber bagi bank umum. *Blueprint* merupakan salah satu tindak lanjut dari keluarnya SEOJK No. 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Dapat dilihat bahwa OJK memiliki seperangkat landasan hukum yang kuat dalam mengeluarkan kebijakan keamanan siber di sektor keuangan. Kebijakan ini bertujuan untuk memberikan proteksi terhadap data dan informasi pelanggan sehingga dapat menjaga kepercayaan publik terhadap lembaga keuangan dan mengurangi risiko kejahatan siber yang dapat merugikan pelaku usaha. Dengan adanya kebijakan ini, diharapkan para pelaku usaha dapat mematuhi dan menerapkannya secara efektif dalam menjalankan aktivitas usaha mereka dan mampu mengatasi berbagai ancaman kejahatan siber.

3.2. Kerangka Kebijakan OJK

[10] Johan, diwawancarai oleh Afiah Nurrizky, 27 Oktober 2023.

[11] *Ibid.*

[12] *Ibid*.

OJK sebagai lembaga pengawas keuangan di Indonesia memiliki *framework* kebijakan dalam bidang keamanan siber untuk sektor perbankan.[13] *Framework* kebijakan ini bertujuan untuk memastikan keberlanjutan dan keamanan bank dalam menghadapi ancaman siber. Salah satu peraturan utama yang diterapkan oleh OJK adalah SEOJK No. 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Peraturan ini mendorong praktik pengendalian internal yang baik dalam keamanan siber dan mendorong kerjasama yang erat antara tiga lini pertahanan dalam sebuah bank.[14] Peraturan ini menekankan pentingnya memiliki langkah-langkah keamanan siber yang kuat untuk melindungi dari ancaman potensial.

Selain peraturan tersebut, OJK telah mengeluarkan perarturan lain yang relevan dalam bentuk POJK untuk mengatasi pengelolaan risiko keamanan siber. Beberapa peraturan tersebut meliputi POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, serta POJK No. 13/POJK.03/2020 yang merubah POJK No. 38/POJK.03/2016 tentang Penerapan Manajexmen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Seperangkat pengaturan ini memberikan pedoman dan persyaratan bagi bank untuk secara efektif mengelola dan mitigasi risiko keamanan *cyber* dalam operasional mereka.

Dalam kerangka kebijakan di OJK dikenal sebuah inovasi digital bernama *blueprint* atau cetak biru, yakni dokumen yang menggambarkan arah kebijakan dan strategi OJK dalam mengatur dan mengawasi industri perbankan serta sektor jasa keuangan lainnya. Cetak biru ini dirancang untuk mendorong transformasi digital, meningkatkan efisiensi operasional, dan mewujudkan industri keuangan yang inovatif juga berdaya saing tinggi.[15] Melalui cetak biru ini, OJK merancang kebijakan yang mendukung perkembangan industri perbankan dalam menghadapi perubahan digital yang cepat. Cetak biru OJK dalam kebijakannya mencakup poin-poin strategis seperti pengembangan *fintech*, digitalisasi pembiayaan dan layanan keuangan, perlindungan konsumen, serta peningkatan literasi dan inklusi keuangan.

Cetak biru ini juga mencakup upaya OJK dalam meningkatkan sumber daya manusia dalam sektor jasa keuangan melalui pembangunan kurikulum pendidikan keuangan, program pelatihan, dan pengembangan kompetensi. OJK berkomitmen untuk menciptakan sumber daya manusia yang profesional, berintegritas, dan dapat bersaing secara global dalam meningkatkan kinerja sektor jasa keuangan. *Framework* dan *blueprint* ini oleh OJK bertujuan untuk meningkatkan postur keamanan siber sektor perbankan di Indonesia, sehingga melindungi data nasabah dan menjaga stabilitas keseluruhan sistem keuangan.[16]

3.3. Manajemen Resiko Keamanan Siber

Dalam rangka merealisasikan *blue print* atau cetak biru OJK, untuk menjamin oprasional dan mutu pelayanan yang baik tentunya, dibutuhkan suatu Standar Oprasional Prosedur (SOP) degan menjadikan kepastian (*certainty*) sebagai tolak ukur. Namun dalam penerapannya, akan ada saja kendala-kendala baik teknis maupun non teknis. Hal ini mengakibatkan kondisi yang tidak pasti atau yang biasa disebut sebagai "risiko" (*effect of uncertainly on objectives*) atau ketidakpastian pada tujuan.[17] Tidak dapat dipungkiri bahwa terdapat sistem, infrastuktur (sarana dan prasarana), serta sumber daya manusia (*human resources*) yang belum memadai. Oleh karena itu, diperlukan suatu alat manajemen mutu yang dapat mengantisipasi adanya masalah atau tidak tercapaiya suatu kebijakan sesuai tujuan yang diharapkan. Maka, hadirlah manajemen risiko (*risk* management) untuk mengatasi permasalahan tersebut. Manajemen risiko akan digunakan untuk menganalisis risiko (*risk analysis*) guna mejamin tercapainya jaminan mutu pelayanan (*quality management insurance*) yang harmoni. Segala hal yang mengandung potensi risiko selanjutnya akan diidentifikasi serta

---

[13] Surat Edaran Otoritas Jasa Keuangan No. 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum.

[14] KPMG Siddharta Advisory. (2023, Januari). Ketahanan dan Keamanan Siber bagi Sektor Perbankan Indonesia. Dikutip dari https://assets.kpmg.com/content/dam/kpmg/id/pdf/2023/01/id-seojk-cyber-newsflash-jan23.pdf.

[15] Johan, diwawancarai oleh Afiah Nurrizky, 27 Oktober 2023.

[16] Otoritas Jasa Keuangan (OJK). (2021, Oktober). Cetak Biru Transformasi Digital Perbankan OJK. Dikutip dari https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx.

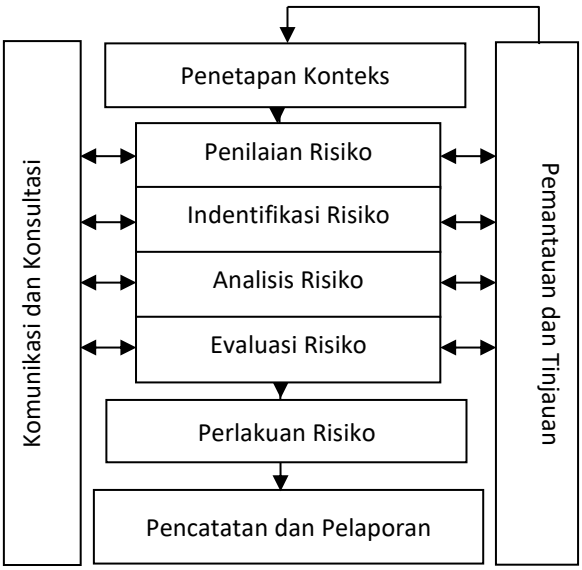
[17] I Putu Sugih Arta, dkk. (2020). Manajemen Risiko Tinjauan Teori dan Praktis. Bandung: Widina Bhakti Persada. 8.

dianalisis, bagaimana kriteria risiko tersebut kemudian nantinya akan diketahui dengan cara apa risiko tersebut akan dikelola dan ditangani.[18]

Terdapat tiga hal penting dalam suatu manajemen risiko; *Pertama,* efek atau pengaruh merupakan suatu konsekuensi penyimpangan yang tidak diharapkan baik positif maupun negative. *Kedua*, suatu tujuan dapat mengandung aspek yang berbeda (misalnya sekaligus memiliki aspek finansial, keamanan dan lingkungan) serta dapat harapkan dalam tingkatan yang berbeda (seperti di tingkat strategi, proyek, dan proses). *Ketiga,* risiko biasanya ditandai dengan adanya suatu peristiwa atau konsekuensi yang berpotensi, bisa pula karena keduanya.[19]

Penilaian risiko secara umum terdiri atas beberapa elemen inti yang membentuk proses manajemen risiko itu sendiri. Elemen-elemen tersebut antara lain, yakni komunikasi dan konsultasi, penetapan konteks, penilaian risiko (terdiri atas identifikasi, analisis dan evaluasi risiko), perlakuan risiko, pemantauan, dan tinjauan. Kegiatan-kegiatan penilaian risiko tidak berdiri sendiri, melainkan terintegrasi sepenuhnya dalam komponen-komponen lain pada proses manajemen risiko.[20]

Tabel 1. Proses Manajemen Risiko



Jika diterapkan dalam konteks mitigasi kejahatan siber, manajemen risiko memiliki peran yang sangat vital dalam misi peningkatan ketahanan siber (*cyber resilience*). Manajemen risiko keamanan siber (*cyber security risk management*) digunakan untuk mengatasi insiden siber yang membahayakan keamanan sistem informasi, melanggar kebijakan, dan prosedur keamanan. Adapun manajemen risiko keamanan siber perbankan dilaksanakan guna menanggulangi risiko siber yang mengganggu proses oprasional perbankan. Hal ihwal yang mempengaruhi risiko keamanan siber perbankan dapat berasal dari faktor internal yakni sumber daya mausia, proses dan sistem, serta bisa pula berasal dari faktor eksternal bank tersebut seperti *security awareness* nasabah.

Pada tingkat internasional, telah ditetapkan beberapa standar penerapan manajemen risiko keamanan siber yang dijadikan acuan diseluruh dunia. Standar tersebut diantaranya terdapat *National Institute of Standards*

[18] Hairul. (2020). Manajemen Risiko. Yogyakarta: Deepublish. 55.

[19] Pengadilan Agama Nangabulik. (2022). Analisis Manajemen Resiko Tahun 2022. Dikutip dari https://pn-nangabulik.go.id/images/dokumen/Dokumen%20Manajemen%20Resiko.pdf.

[20] Badan Standarisasi Nasional. (2016). Manajemen Risiko-Teknik Penilaian Risiko SNI IEC/ISO 31010:2016. Jakarta: Badan Standarisasi Nasional.

and Technology (NIST) Framework for Improving Cyber Security, *NIST Risk Management Framework*, dan ISO 27001 – *Information Security Management Standard*. Untuk menerapkan standar internasional manajemen risiko keamanan siber tersebut dalam praktik perbankan Indonesia, ditetapkanlah POJK No. 38/POJK.03/2016 sebagaimana telah diubah dengan POJK No. 13/POJK.03/2020 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, serta SEOJK No. 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Seperangkat peraturan tersebut diharapkan menjadi *guideline* perbankan Indonesia dalam penerapan manajemen risiko keamanan siber yang efektif.

Dalam penerapan dan penyelenggaraan manajemen risiko, OJK menetapkan SOP yang wajib mencakup mengenai beberapa hal penting, yakni pengawasan aktif dewan komisaris dan direksi, kecukupan kebijakan sistem dan prosedur, kecukupan proses identifikasi, pengukuram pemantauan serta pengendalian risiko, serta sistem pengendalian internal.[21] Dari komponen-komponen tersebut, dapat ditarik lagi menjadi beberapa elemen yang harus ada dalam setiap penerapan manajemen risiko. Dalam hal ini, terdapat tata kelola, strategi, perlindungan, ketanggapan, ketahanan, serta sistem pengendalian internal. Keempat elemen tersebut meliputi:[22]

a. Tata kelola risiko keamanan siber mencakup pengawasan aktif Direksi dan Dewan Komisaris, struktur organisasi yang jelas untuk menangani keamanan siber, sumber daya manusia yang kompeten, budaya dan kesadaran keamanan siber yang kuat, peningkatan kapasitas untuk mengelola risiko keamanan siber.
b. Strategi manajemen risiko siber dilakukan dengan menetapkan tujuan dan sasaran keamanan siber, mengidentifikasi aset informasi yang berharga, melakukan analisis ancaman dan kerentanan, mengembangkan rencana mitigasi risiko, serta menerapkan kontrol keamanan siber yang tepat.
c. Perlindungan, Ketanggapan dan Ketahanan dalam manajemen risiko siber meliputi: perlindungan atas asset informasi, tanggap dengan rencana mendeteksi, merespon, dan memulihkan insiden siber, serta peningkatan ketahanan siber dengan sarana, prasarana dan SDM yang baik dan berkualitas.
d. Pengendalian internal dilakukan dengan memastikan bahwa kontrol keamanan siber efektif dan efisien, melakukan audit dan pemantauan kontrol keamanan siber secara berkala, serta melaporkan risiko keamanan siber kepada Direksi dan Dewan Komisaris.

Seperangkat elemen tersebut berjalan beriringan dengan kerangka manajemen risiko keamanan siber yang mencakup tiga instrument, yakni penetapan tingkat risiko, penetapan strategi manajemen risiko, serta kebijakan, prosedur dan penetapan limit. Dari ketiga instrument tersebut kemudian dapat dilakukan dengan beberapa metode sebagai berikut:

Tabel 2. Kerangka Manajemen Risiko Keamanan Siber

Instruemen	Metode
Penetapan Tingkat Risiko	Analisis risiko Klasifikasi risiko Penentuan toleransi risiko
Penetapan Strategi Manajemen Risiko	Strategi pencegahan Strategi deteksi Strategi respon Strategi pemulihan

[21] Surat Edaran Otoritas Jasa Keuangan No. 1/SEOJK.03/2019 tentang Penerapan Manajemen Risiko bagi Bank Perkreditan Rakyat.

[22] Otoritas Jasa Keuangan. (2021). Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum. Jakarta: Departeme Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan.

Kebijakan, Prosedur dan Penetapan Limit	Kebijakan akses data, penggunaan perangkat lunak, kata sandi Prodder pelaporan, manajemen patch, pengujian penetrasi Penetapan limit akses data, penggunaan perangkat lunak, penggunaan bandwidth

3.4. Kebijakan Praktis OJK dalam Mitigasi Serangan Siber Perbankan

Dalam era digital saat ini, sektor perbankan menjadi salah satu target utama para pelaku kejahatan siber. Ancaman kejahatan siber seperti pencurian identitas, *fraud*, dan serangan *malware* telah menyebabkan kerugian finansial yang signifikan bagi perbankan dan nasabahnya. Untuk mengatasi masalah ini, OJK telah menerapkan kebijakan-kebijakan guna mitigasi kejahatan siber di sektor perbankan.[23] Salah satu kebijakan yang diterapkan oleh OJK dalam mitigasi kejahatan siber di sektor perbankan adalah kebijakan peningkatan sistem keamanan teknologi informasi di bank. Hal ini bertujuan untuk mencegah serangan siber yang dapat mengancam keamanan data dan informasi nasabah. OJK telah mewajibkan bank untuk melaksanakan kebijakan-kebijakan keamanan seperti penggunaan *firewall*, enkripsi data, dan identifikasi biometrik. Selain itu, OJK juga mendorong bank untuk melakukan audit keamanan secara teratur guna mengidentifikasi dan mengatasi kelemahan dalam sistem keamanan teknologi informasi.[24]

Selanjutnya, OJK juga telah menerapkan kebijakan peningkatan sistem pelaporan kejahatan siber di bank. Dalam kebijakan ini, OJK mewajibkan bank untuk memiliki mekanisme pelaporan yang efektif terkait dengan adanya indikasi atau serangan kejahatan siber. Bank diharuskan melaporkan kejadian tersebut kepada OJK secara cepat dan akurat agar tindakan yang tepat dapat segera diambil. OJK juga berperan dalam melakukan koordinasi dengan lembaga penegak hukum dalam menindaklanjuti laporan kejahatan siber ini. Dengan adanya kebijakan ini, diharapkan bank dapat lebih proaktif dalam mengatasi dan menanggapi serangan kejahatan siber.[25]

Selain kebijakan peningkatan sistem keamanan teknologi informasi dan peningkatan sistem pelaporan kejahatan siber, OJK juga memiliki kebijakan pendidikan dan pelatihan untuk meningkatkan kesadaran akan kejahatan siber. OJK menyadari bahwa salah satu faktor penting dalam mitigasi kejahatan siber adalah kesadaran dan pengetahuan yang mencukupi dari pihak bank dan nasabahnya. Oleh karena itu, OJK mendorong bank untuk menyelenggarakan program pendidikan dan pelatihan terkait dengan keamanan siber, termasuk pencegahan dan deteksi kejahatan siber. Selain itu, OJK juga melakukan kampanye kesadaran kejahatan siber kepada masyarakat melalui berbagai media guna meningkatkan pemahaman dan sikap waspada terhadap ancaman kejahatan siber.[26]

OJK telah mengambil langkah-langkah yang penting untuk melindungi bank dan nasabah dari ancaman kejahatan siber. Kebijakan peningkatan sistem keamanan teknologi informasi di bank, peningkatan sistem pelaporan kejahatan siber di bank, dan kebijakan pendidikan dan pelatihan telah memberikan kontribusi yang signifikan dalam membangun ketangguhan sektor perbankan terhadap serangan kejahatan siber. Meski demikian, masih terdapat beberapa aspek yang dapat diperbaiki dalam implementasi kebijakan-kebijakan tersebut. *Pertama*, penting bagi OJK untuk terus memperbarui dan mengkaji ulang kebijakan-kebijakan terkait kejahatan siber. Hal ini mengingat evolusi dan kompleksitas serangan yang terus berkembang. *Kedua*,

---

[23] Otoritas Jasa Keuangan (OJK). (2021). Kebijakan OJK Dalam Memitigasi Ancaman Kejahatan Siber Di Sektor Perbankan. Dikutip dari https://www.ojk.go.id/id/berita-dan-kegiatan/berita/pantau-keamanan-informasi-opini-ngakan-ojk-soal-ancaman-kejahatan-siber-di-sektor-keuangan.

[24] Otoritas Jasa Keuangan (OJK). (2019). OJK Regulasi Mengenai Sistem Keamanan Werkills. Dikutip dari https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/PERATURAN/OJK-Regulasi-Mengenai-Sistem-Keamanan-Kartu-Debit-dan-Kartu-Kredit-Implementasi-CKYC.pdf.

[25] Otoritas Jasa Keuangan (OJK). (2017). OJK Mewajibkan Bank Mengenosentrasikan Laporan Kejahatan Sistem Ke Lembaga Penegak Hukum. Dikutip dari https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/Kebijakan-OJK-Mewajibkan-Bank-Mengenosentrasikan-Laporan-Kejahatan-Ke-LPH-Hadi.

[26] Otoritas Jasa Keuangan (OJK). (2020). OJK Bansos Diskusi Publik Literasi dan Keuangan Digital, Jangan Go Show Go Ahli.

OJK perlu meningkatkan kerjasama dan koordinasi dengan instansi lain seperti Kementerian Komunikasi dan Informatika serta Kepolisian dalam rangka memperkuat mitigasi kejahatan siber di sektor perbankan. *Ketiga*, OJK sebaiknya lebih intensif dalam mengawasi dan mengevaluasi implementasi kebijakan-kebijakan keamanan siber di bank demi meningkatkan efektivitas dan efisiensi pelaksanaannya.

4. Kesimpulan

Otoritas Jasa Keuangan (OJK) merupakan lembaga yang bertanggung jawab dalam mengawasi dan mengatur sektor jasa keuangan di Indonesia. OJK didirikan berdasarkan UU No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan. Tujuan pendirian OJK adalah untuk melindungi kepentingan nasabah, memelihara stabilitas sistem keuangan, serta mendorong perkembangan dan keberlanjutan industri jasa keuangan di Indonesia.[27] OJK memiliki wewenang untuk melakukan pengawasan terhadap bank-bank di Indonesia. Hal ini termasuk pengawasan terhadap tata kelola bank, manajemen risiko, dan pencegahan kegiatan perbankan yang terkait dengan kejahatan seperti pencucian uang dan pendanaan terorisme.

OJK memiliki landasan hukum yang mengatur manajemen risiko keamanan siber dalam industri perbankan di Indonesia. Landasan hukum ini termasuk SEOJK No. 29/SEOJK.03/2022 dan beberapa POJK lainnya, seperti POJK No. 13/POJK.03/2020, POJK No. 21/SEOJK.03/2017, dan POJK No. 12/POJK.03/2018. Dalam hal ini, OJK mempromosikan praktik pengendalian internal yang baik dan mendorong kerjasama antara tiga lini pertahanan dalam bank: manajemen, keamanan informasi, dan unit teknologi. OJK juga memiliki blue print dan framework kebijakan yang telah ditetapkan untuk menuntun arah kebijakan OJK dalam memastikan keamanan siber di industri perbankan.

Melalui manajemen risiko keamanan siber yang efektif, OJK menjaga keamanan finansial dan stabilitas industri perbankan. OJK mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan siber yang dihadapi oleh lembaga keuangan. OJK memberikan pedoman dan persyaratan bagi bank untuk memperkuat infrastruktur keamanan siber mereka, termasuk implementasi kontrol yang tepat, kebijakan keamanan, dan pelatihan kepada karyawan. Dengan ini, OJK dapat melindungi data nasabah, menjaga stabilitas sistem keuangan, dan memastikan kelangsungan operasional perbankan secara keseluruhan. OJK memiliki peran penting dalam menciptakan industri perbankan yang aman, stabil, dan inovatif di era digital.

Referensi

Arta, I. P. S., Satriawan, D. G., Bagiana, I. K., Sp, Y. L., Shavab, F. A., Mala, C. M. F., ... & Utami, F. (2021). Manajemen Risiko, Tinjauan Teori Dan Praktis. *Penerbit Widina Bhakti Persada Bandung*, 1-244.

A'yun, Inarotul., Dwi, Silvia., dan Putri, Aprilia. (2022). Peran Digitalisasi dan Informasi terhadap Kinerja Perbankan Syariah dalam Perspektif *Society* 5.0 di Perekonomian di Indonesia. *Jurnal Perbankan Syariah*, 2(1), 1-10.

Badan Standarisasi Nasional. (2016). Manajemen Risiko-Teknik Penilaian Risiko SNI IEC/ISO 31010:2016. http://repository.crmsindonesia.org/bitstream/123456789/89/1/RASNI%20ISO%20IEC%2031010%202016%20Bilingual.pdf.

Check Point Research Team. (2024, Januari). Check Point Research: 2023 – The Year of Mega Ransomware Attack with Unprecedented Impact on Global Organizations. https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/

Departeme Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan. (2021). Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum,

[27] Nabilah Farah Diba, Hari Sutra Disemadi, dan Paramita Prananingtyas. (2019). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) di Indonesia. EKSPOSE: Jurnal Penelitian Hukum dan Pendidikan, 18(2), 870.

https://www.ojk.go.id/id/kanal/perbankan/implementasibasel/Documents/Pages/ConsultativePapers/Consultative%20Paper%20Manajemen%20Risiko%20Keamanan%20Siber%20Bank%20Umum.pdf.

Diba, Nabilah Farah., Disemadi, Hari Sutra., dan Prananingtyas, Paramita. (2019). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) di Indonesia. *EKSPOSE: Jurnal Penelitian Hukum dan Pendidikan*, 18(2), 868-876.

Faridi, Muhammad Khairul. (2018). Kejahatan Siber Dalam Bidang Perbankan. *CyberSecurity dan Forensik Digital*, 1(2), 57-61.

Hairul. (2020). *Manajemen Risiko*. Yogyakarta: Deepublish.

Harto, Budi., dkk. (2023). *Transformasi Bisnis di Era Digital (Teknologi Informasi dalam Mendukung Transformasi Bisnis di Era Digital)*. Jambi: Sonpedia Publishing Indonesia.

Johan, diwawancarai oleh Afiah Nurrizky, 27 Oktober 2023.

KPMG Siddharta Advisory. (2023, Januari). Ketahanan Dan Keamanan Siber Bagi Sektor Perbankan Indonesia https://assets.kpmg.com/content/dam/kpmg/id/pdf/2023/01/id-seojk-cyber-newsflash-jan23.pdf.

Otoritas Jasa Keuangan (OJK). (2021, Oktober). Cetak Biru Transformasi Digital Perbankan OJK. https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx.

Otoritas Jasa Keuangan (OJK). (2021). Kebijakan OJK Dalam Memitigasi Ancaman Kejahatan Siber Di Sektor Perbankan. https://www.ojk.go.id/id/berita-dan-kegiatan/berita/pantau-keamanan-informasi-opini-ngakan-ojk-soal-ancaman-kejahatan-siber-di-sektor-keuangan.

Otoritas Jasa Keuangan (OJK). (2020). OJK Bansos Diskusi Publik Literasi Dan Keuangan Digital, Jangan Go Show Go Ahli.

Otoritas Jasa Keuangan (OJK). (2019). OJK Regulasi Mengenai Sistem Keamanan Werkills. https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/PERATURAN/OJK-Regulasi-Mengenai-Sistem-Keamanan-Kartu-Debit-dan-Kartu-Kredit-Implementasi-CKYC.pdf.

Otoritas Jasa Keuangan (OJK). (2017). OJK Mewajibkan Bank Mengenosentrasikan Laporan Kejahatan Sistem Ke Lembaga Penegak Hukum. https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/Kebijakan-OJK-Mewajibkan-Bank-Mengenosentrasikan-Laporan-Kejahatan-Ke-LPH-Hadi.

Pengadilan Agama Nangabulik. (2022). Analisis Manajemen Resiko Tahun 2022. https://pn-nangabulik.go.id/images/dokumen/Dokumen%20Manajemen%20Resiko.pdf.

Setyaningrat, Dwi., dkk. (2023). Strategi Digitalisasi Untuk Mendorong Inklusi Keuangan Nasabah Bank Syariah: Pendekatan Technology Acceptance Model (TAM). Proceedings of Islamic Economics, Business, and Philanthropy, 2(1), 53-76.

Surat Edaran Otoritas Jasa Keuangan No. 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum.

Surat Edaran Otoritas Jasa Keuangan No. 1/SEOJK.03/2019 tentang Penerapan Manajemen Risiko bagi Bank Perkreditan Rakyat.

Surat Edaran Otoritas Jasa Keuangan No. 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Suryowati, Estu. (2023, Desember) BSSN: Sektor Keuangan Peringkat Ketiga Paling Rentan Kejahatan Siber Setelah Administrasi Pemerintahan Dan Energi. Jawa Pos. https://www.jawapos.com/ekonomi-

digital/013669836/bssn-sektor-keuangan-peringkat-ketiga-paling-rentan-kejahatan-siber-setelah-administrasi-pemerintahan-dan-energi.

Tambunan, Nurma., dkk. (2023). Berita Utama Tentang Error Service Di Bank Syariah Indonesia (BSI). *Community Development Journal*, 4(2), 5096-5098.