DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN *RANSOMWARE* PADA BSI KCP KENCONG JEMBER

SKRIPSI

Oleh:
RIFNI MIFTAHUR ROHMAH
NIM. 212105010052

UNIVERSITAS ISLAM NEGERI
KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS EKONOMI DAN BISNIS ISLAM
FEBRUARI 2025

DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN *RANSOMWARE* PADA BSI KCP KENCONG JEMBER

SKRIPSI

Diajukan kepada Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember
Untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana Ekonomi (S.E)
Fakultas Ekonomi dan Islam
Jurusan Ekonomi Islam
Prodi Studi Perbankan Syariah

Oleh:

RIFNI MIFTAHUR ROHMAH
NIM. 212105010052

UNIVERSITAS ISLAM NEGERI
KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS EKONOMI DAN BISNIS ISLAM
FEBRUARI 2025

DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN *RANSOMWARE* PADA BSI KCP KENCONG JEMBER

SKRIPSI

Diajukan kepada Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember
Untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana Ekonomi (S.E)
Fakultas Ekonomi dan Islam
Jurusan Ekonomi Islam
Prodi Studi Perbankan Syariah

Oleh:

RIFNI MIFTAHUR ROHMAH
NIM. 212105010052

Disetujui Pembimbing

Ana Partiwi, S.E., Ak., M.S.A
198809232019032003

DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN *RANSOMWARE* PADA BSI KCP KENCONG JEMBER

SKRIPSI

Telah diuji dan diterima untuk memenuhi salah satu
persyaratan memperoleh gelar Sarjana Ekonomi (S.E)
Fakultas Ekonomi dan Islam
Jurusan Ekonomi Islam
Prodi Studi Perbankan Syariah

Hari: Kamis
Tanggal: 27 Februari 2025

Tim Penguji:

Ketua	Sekretaris
Dr. Hj. Nurul Setianingrum, S.E., M.M	Zulfa Ahnaf Kurniawan, M.E
NIP. 196905231998032001	NIP.199408042020121004

Anggota:

1. Prof. Dr. Khamdan Rifa'i, S.E., M.Si., CHRA (
2. Ana Pratiwi, M.S.A (

Menyetujui,
Dekan Fakultas Ekonomi dan Bisnis Islam

Dr. H. Ubaidillah, M. Ag
NIP. 196812261996031001

MOTTO

وَاللّٰهُ اَخْرَجَكُمْ مِّنْۢ بُطُوْنِ اُمَّهٰتِكُمْ لَا تَعْلَمُوْنَ شَيْـًٔاۙ وَّجَعَلَ لَكُمُ السَّمْعَ وَالْاَبْصَارَ وَالْاَفْـِٕدَةَۙ لَعَلَّكُمْ تَشْكُرُوْنَ

Artinya: "Allah mengeluarkan kamu dari perut ibumu dalam keadaan tidak mengetahui sesuatu pun dan Dia menjadikan bagi kamu pendengaran, penglihatan, dan hati nurani agar kamu bersyukur."[1]
(QS. An-Nahl [16]: 78)

[1] Falah jamalul, Mujahid. *Al-Quran dan Etika Digital Literacy: Mitigasi CyberCrime di Era Transformasi Digital*. 2023.

PERSEMBAHAN

Segala puji bagi ALLAH SWT, yang telah memberikan rahmat serta hidayah-nya sehingga penulis bisa meyelesaikan skripsi sebagai salah satu persyaratan untuk menyelesaikan program sarjana dengan lancar. Walaupun karya ini jauh dari kata sempurna namun penulis sangat bersyukur dan bangga bisa sampai pada titik ini. Tiada lembar yang paling indah dalam sebuah karya kecil ini kecuali lembar pengesahan, dengan penuh rasa syukur skripsi ini kupersembahkan untuk:

1. Kedua orang tua saya, Alm. Bapak Agus Salim dan Almh. Ibu Siti Zaenab yang saya cintai dan saya banggakan, dengan segenap cinta dan kerinduan yang mendalam. Terima kasih atas cinta, doa, dan pengorbanan tanpa batas yang telah kalian berikan selama hidup kalian. Meski raga telah tiada, kasih sayang dan nasihat kalian selalu menjadi lentera dalam setiap langkahku. Semoga karya ini menjadi bagian kecil dari baktiku kepada kalian dan membawa do'a yang terus mengalir di tempat peristirahatan kalian.
2. Kakak kadung saya, Anis Kurliawati. Terimakasih sudah memberikan semangat untuk terus berjuang melangkah kedepan dan dukungan yang penuh serta rela berkorban untuk adiknya yang memiliki kemauan tinggi dalam mencari ilmunya.
3. Teruntuk sahabat seperjuangan saya Aisyah Shiddiqiyah, Rani Maulida Sari, Anggita Legian terimakasih karena selalu memberikan dukungan, inspirasi, reward agar terus semangat untuk menyelesaikan kewajiban dalam menuntut

ilmunya menjadi mahasiswa yang aktif dalam bangku perkuliahan serta diluar perkuliahan.

4. Teruntuk teman-teman seperjuangan Perbankan Syariah angkatan 2021, khususnya kelas Perbankan Syariah 03 yang selalu memberikan support untuk terus berjuang dalam menyelesaikan perkuliahan dengan tepat waktu, dan terimakasih atas rasa kekeluargaan, kebersamaan yang selalu diberikan di bangku kuliah.
5. YBM BRILiaN terima kasih atas dukungan berupa beasiswa yang tidak hanya membantu meringankan beban finansial, tetapi juga menjadi motivasi besar bagi saya untuk terus berjuang meraih prestasi. Semoga segala kebaikan dan kepedulian yang diberikan oleh YBM Brilian menjadi amal jariyah yang tak terputus, serta membawa keberkahan bagi seluruh pengelola dan donatur lembaga ini.
6. Kepada sahabat-sahabati PMII Rayon FEBI 2024.
7. Kepada teman-teman pengurus Himpunan Mahasiswa Program Studi Perbankan Syariah (HMPS PS) 2023-2024.
8. Kepada teman-teman pengurus Senat Mahasiswa Fakultas Ekonomi dan Bisnis Islam (SEMA FEBI) 2024-2025.
9. Keluarga Besar Perbankan.
10. Almamater tercinta UIN KHAS Jember.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

Alhamdulillah puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya kepada penulis skripsi ini dapat terselesaikan. Sholawat serta salam semoga tercurahkan kepada junjungan Nabi Muhammad SAW. Semoga kita termasuk umatnya dan mendapatkan syafaatnya di yaumul qiyamah. Skipsi dengan judul "Dampak Sistem Manajemen Keamanan Informasi Dalam Pelayanan Nasabah Terhadap Serangan *Ransomware* pada BSI KCP Kencong Jember" ini sebagai salah satu syarat menyelesaikan Program Sarjana Program Studi Perbankan Syariah, Fakultas Ekonomi Dan Bisnis Islam, Universitas Islam Negeri Kiai Haji Ahmad Siddiq Jember. Proses penelitian skripsi ini bukan tidak ada hambatan, melainkan penuh dengan lika-liku yang membuat penulis harus bekerja keras dalam mengumpulkan data-data sesuai dengan maksud dan tujuan penelitian serta dalam penyusunan skripsi ini. Untuk itu penulis ingin mengucapkan terimakasih kepada :

1. Prof. Dr. H. Hepni, S.Ag., M.M., CPEM. Selaku Rektor UIN KHAS Jember yang telah memberikan kesempatan kepada saya untuk menuntut ilmu dikampus ini.
2. Dr. H. Ubaidillah, M.Ag Selaku Dekan Fakultas Ekonomi dan Bisnis Islam yang telah memberikan dukungan serta menyediakan fasilitas untuk mahasiswa dalam proses perkuliahan.

3. Dr. M.F. Hidayatullah, S.H.I, M.S.I Selaku Ketua Jurusan Ekonomi Islam yang selalu merangkul serta memberikan dukungan tanpa henti kepada seluruh mahasiswa.
4. Ana Pratiwi, SE.,AK., MSA, selaku Koordinator Program Studi Perbankan Syariah sekaligus Pembimbing saya yang selalu memberikan motivasi dan arahan selama perkuliahan dalam menyelesaikan skripsi, Terimakasih atas bimbingan, perhatian dan kesabaran yang diberikan sehinggan saya mampu menyelesaikan tugas akhir dengan baik dan sesuai harapan.
5. Dwi Ismanto, selaku *Branch Manager* BSI KCP Kencong Jember yang telah memberikan kesempatan serta waktu untuk melakukan penelitian di BSI KCP Kencong Jember.
6. Bapak dan Ibu Dosen UIN KHAS JEMBER, Khususnya dosen fakultas ekonomi dan bisnis islam yang telah memberikan ilmu yang bermanfaat sebagai bekal hidup.
7. Pihak pihak yang telah membantu peneliti dalam melakukan penelitian, yang tidak bisa disebutkan satu persatu sehingga bisa menyelesaikan skripsi dengan baik dan lancar.

Jember, 10 Februari 2025

Penulis

ABSTRAK

Rifni Miftahur Rohmah, 2025: *Dampak Sistem Manajemen Keamanan Informasi dalam Pelayanan Nasabah Terhadap Serangan Ransomware pada BSI KCP Kencong Jember*.

Kata kunci: Standar Sistem Manajemen Keamanan Informasi, Pelayanan Nasabah, Ransomware.

BSI KCP Kencong Jember adalah salah satu cabang dari Bank Syariah Indonesia yang berfokus pada penyediaan layanan perbankan berbasis syariah. Dalam era teknologi yang semakin maju, bank ini memanfaatkan inovasi digital, seperti aplikasi mobile banking dan memperketat sistem keamanannya dengan menggunakan CISCO untuk mengelola dan memantau sistem keamanan perusahaan dan meningkatkan kualitas pelayanan kepada nasabah. Namun, kemajuan teknologi juga membawa risiko, termasuk ancaman serangan *ransomware* yang dapat membahayakan keamanan data dan transaksi nasabah.

Fokus penelitian dalam skripsi ini yaitu (1) Bagaimana penerapan Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan ransomware pada BSI KCP Kencong Jember? (2) Bagaimana dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan ransomware pada BSI KCP Kencong Jember?

Tujuan dari penelitian ini adalah (1) Mengetahui penerapan Standar Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember. (2) Mengetahui dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember.

Pelitian skripsi ini menggunakan penelitian *field research* (penelitian lapangan) yang merupakan salah satu metode pengumpulan data dalam penelitian kualitatif dengan pendekatan deskriptif. Penentuan informan menggunakan teknik *purposive sampling*. Pengumpulan data dilakukan dengan wawancara. Analisis data menggunakan metode reduksi data, penyajian data, dan penarikan kesimpulan. Keabsahan data dilakukan dengan triangulasi sumber.

Hasil penelitian ini menunjukkan bahwa Penerapan Sistem Manajemen Keamanan Informasi (SMKI) di BSI KCP Kencong Jember telah dilakukan sesuai dengan kebijakan dari kantor pusat, namun masih memerlukan penguatan di beberapa aspek. Dalam menghadapi serangan *ransomware*, BSI mengandalkan tim IT internal yang dikenal sebagai CISCO untuk memantau dan mengamankan akses digital, mencerminkan penerapan teori Triad CIA (*Confidentiality, Integrity, Availability*). Meskipun penerapan SMKI berbasis ISO 27001 telah membantu mitigasi ancaman, serangan *ransomware* yang terjadi berdampak signifikan terhadap kualitas pelayanan nasabah, seperti terganggunya transaksi dan meningkatnya kekhawatiran nasabah terkait keamanan data. Temuan menunjukkan bahwa kurangnya pelatihan dan edukasi mengenai SMKI di tingkat cabang menjadi kelemahan yang menghambat respons cepat terhadap ancaman siber.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

A. Konteks Penelitian

Kemajuan teknologi membuat setiap perusahaan atau organisasi makin bergantung pada teknologi informasi yang ada, tentunya keamanan informasi menjadi isu yang sangat penting dan kritis pada era digital saat ini. Terutama di dunia perbankan yang semakin terhubung, tidak ada yang lebih penting selain memastikan data nasabah ataupun perusahaan aman dari ancaman *cyber*. Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting). Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis.[2] Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan.

Dalam era ini, teknologi semakin terintegrasi dalam kehidupan sehari-hari, sehingga organisasi di seluruh dunia menghadapi ancaman

[2] Syafrizal, Melwin. ISO 17799: *Standar Sistem Manajemen Keamanan Informasi*. 2007

keamanan *cyber* yang semakin meningkat dan kompleks. Ancaman keamanan *cyber* dapat menyebabkan kerugian finansial yang signifikan bagi organisasi. Dalam beberapa kasus, serangan *cyber* bahkan dapat mengancam kelangsungan hidup organisasi. Meskipun risiko keamanan *cyber* semakin meningkat, masih banyak organisasi yang kurang memperhatikan manajemen keamanan. Manajemen keamanan adalah serangkaian kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk ancaman *cyber*. Tujuannya adalah untuk melindungi informasi sensitif dan data penting dari akses yang tidak sah, perubahan atau penghapusan, serta untuk memastikan bahwa sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan oleh organisasi tetap aman dan terjaga.[3]

Manajemen keamanan meliputi identifikasi risiko keamanan, pengembangan strategi keamanan yang efektif, dan penerapan kebijakan dan prosedur keamanan. Hal ini melibatkan penggunaan teknologi keamanan seperti perangkat lunak antivirus, *firewall*, sandi kuat dan *enkripsi*, serta manajemen akses pengguna dan pelaporan keamanan yang teratur. Faktor-faktor yang menyebabkan banyak organisasi yang kurang memperhatikan manajemen keamanan, seperti kurangnya kesadaran akan risiko keamanan *cyber* atau kurangnya sumber daya untuk mengimplementasikan strategi keamanan yang efektif. Selain itu, perubahan teknologi dan lingkungan bisnis yang semakin cepat juga menimbulkan tantangan bagi manajemen keamanan.

[3] Putra, Rifqi Galuh, Achmad Fauzi, Ery Teguh Prasetyo, dkk. *Pentingnya Manajemen Security di Era Digitalisasi*. 2023.

Organisasi harus terus memperbarui strategi dan teknik mereka untuk menghadapi ancaman keamanan *cyber* yang semakin kompleks dan terus berkembang.

Pada tahun 2021, Bank Jatim dan BRI Life perusahaan asuransi milik BRI diretas dan data pribadi nasabah diduga bocor di internet. Bahkan hal tersebut terulang kembali pada tahun 2023 dengan adanya gangguan layanan Bank Syariah Indonesia (BSI) yang diduga kuat akibat serangan siber ransomware, semestinya hal-hal sebelumnya sudah menjadi pelajaran bagi perbankan di Indonesia.[4] Menurut pengamat keamanan siber perbankan di Indonesia, perlunya memperkuat sistem pertahanan digital karena serangan siber telah menjadi semakin kompleks dan canggih. Banyaknya fenomena yang sama dan terjadi pada akhir-akhir ini dapat menjadi evaluasi untuk perbankan di Indonesia terutama pada tahun kemarin 2023 adanya gangguan layanan Bank Syariah Indonesia yang menjadi salah satu penyebab keresahan pada nasabah-nasabahnya. Sehingga, hal tersebut mendorong nasabah untuk mengambil semua tabungannya dan memiliki keinginan untuk kembali kepada bank konvensional dengan menutup bank syariah di Indonesia.

Direktur Eksekutif Indonesia ICT Institute, Heru Sutadi, mengatakan "*setiap bank perlu memiliki sistem keamanan standar internasional, minimal sertifikasi ISO 27001*". Ada beberapa *framework* yang dapat digunakan dalam penerapan sistem manajemen keamanan informasi antara lain NIST,GMITS, COBIT, ITIL, COSO, CISA, ISO 27001. Beberapa

[4] https://www.bbc.com/indonesia/articles/cn01gdr7eero

framework keamanan informasi yang ada, yang paling spesifik terhadap keamanan informasi adalah ISO 27001. ISO 27001 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO 27001 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memantau, menganalisa dan memelihara serta mendokumentasikan manajemen keamanan informasi dalam konteks risiko bisnis organisasi keseluruhan. Dalam ISO 27001 keamanan sistem informasi tidak hanya berhubungan dengan penggunaan perangkat lunak antivirus, *firewall*, penggunaan *password* untuk komputer tetapi merupakan pendekatan secara keseluruhan baik dari sisi orang, proses dan teknologi untuk memastikan berjalannya efektivitas keamanan informasi.

Berdasarkan dari fenomena tersebut peran Standar Sistem Keamanan Informasi sangat mempengaruhi perusahaan manapun tentunya pada Bank Syariah Indonesia dalam meningkatkan manajemen keamanan atas fenomena yang telah terjadi dan berdampak juga terhadap pelayanan nasabah pada kantor cabang dibawahnya terutama pada BSI KCP Kencong Jember, segala aktivitas menjadi terhambat bahkan, sampai berhenti beroperasi kurang lebih dalam waktu 2 minggu, maka sangat mendukung adanya penulis untuk melakukan penelitian dan menyelidiki fenomena tersebut dengan judul "**Dampak Sistem Manajemen Keamanan Informasi Terhadap Pelayanan Nasabah Dalam Serangan *Ransomware* pada BSI KCP Kencong Jember.**"

B. Fokus Penelitian

1. Bagaimana penerapan Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember?
2. Bagaimana dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember?

C. Tujuan Penelitian

1. Mengetahui penerapan Standar Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember.
2. Mengetahui dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember.

D. Manfaat Penelitian

Tujuan penelitian dengan judul "Dampak Sistem Manajemen Keamanan Informasi terhadap Pelayanan Nasabah dalam Serangan *Ransomware* pada BSI KCP Kencong Jember." adalah untuk mengetahui dampak sistem manajemen keamanan dalam mempengaruhi pelayanan nasabah ditengah ancaman *ransomware*. Baik penggunaan teoritis maupun aktual suatu sistem dapat dianggap dan dapat digunakan.

1. Manfaat Teoritis
    a. Penelitian ini bertujuan untuk memberikan wawasan kepada penulis dan pembaca tentang Dampak Sistem Manajemen Keamanan Informasi terhadap Pelayanan Nasabah dalam Serangan *Ransomware*.
    b. Memberikan inspirasi lebih lanjut menggunakan satu atau sebagian komponen dari penelitian sebelumnya. Seperti variabel penelitian, metode penelitian, kasus dan lain sebagainya.
    c. Hasil penelitian diharapkan dapat menambah kontribusi pemikiran bagi perkembangan generasi selanjutnya dalam minat membaca serta mengetahui fenomena ataupun kasus yang sedang terjadi pada dunia perbankan.
2. Manfaat Praktis
    a. Bagi peneliti

    Diharapkan temuan penelitian ini dapat memberikan wawasan baru yang dapat menjadi dasar untuk penelitian selanjutnya mengenai fenomena atau kasus yang terjadi pada dunia Perbankan.
    b. Bagi Universitas

    Diharapkan dapat bermanfaat bagi universitas dan menjadi sumber informasi bagi calon peneliti selanjutnya sehingga dapat dijadikan rujukan oleh mahasiswa Perbankan Syariah Universitas Islam Negeri Kiai Haji Ahmad Siddiq Jember.

c. Bagi Institusi/Bank

Hasil akhir dari penelitian ini diharapkan dapat digunakan sebagai bahan penilaian bagi Perbankan untuk lebih berhati-hati dalam sistem digital dan tidak menganggap remeh apabila terdapat kelemahan atau kekurangan dalam menjalankan bisnisnya.

E. Definisi Istilah

Penjabaran atau penguraian konsep variabel yang sedang diteliti dalam suatu penelitaian atau studi menjadi bentuk yang lebih spesifik, terukur dan dapat diamati. Definisi operasional menjelaskan secara jelas dan rinci bagaimana variabel tersebut akan diukur atau dibservasi dalam konteks penelitian tertentu. Definisi operasional berfungsi untuk memberikan petunjuk yang jelas tentang bagaimana variabel atau konsep akan di operasionalisasikan atau diukur dalam penelitian. Hal ini penting untuk memastikan bahwa pengukuran yang dilakukan konsisten, dapat diulang, dan dapat dipahami oleh penelitian lain. Dengan adanya definisi istilah maka diharapkan tidak adanya salah penafsiran terhadap istilah yang dianggap tidak familiar oleh pembaca maka dari itu penelitian berjudul "Dampak Sistem Manajemen Keamanan Informasi terhadap Pelayanan Nasabah dalam Serangan *Ransomware* pada BSI KCP Kencong Jember". Adapun hal-hal yang harus dijelaskan oleh peneliti adalah sebagai berikut:

1. Sistem Manajemen Keamanan Informasi

Dalam era digital saat ini, keamanan informasi menjadi salah satu prioritas utama bagi perusahaan di seluruh dunia. Sistem manajemen

keamanan informasi adalah suatu sistem yang merancang, menerapkan, mengelola, serta memelihara keamanan informasi di suatu bisnis atau organisasi. Dimana pengelolaannya melalui sebuah proses yang terpadu dan secara efektif untuk menjaga kerahasiaan, integritas, dan ketersediaan dari aset informasi tersebut. Di samping itu, sistem manajemen keamanan informasi juga bertugas meminimalisir risiko dan bahaya yang bisa timbul dari kemungkinan yang menyertai informasi tersebut. Dalam mengembangkan dan menyusun sistem manajemen keamanan informasi biasanya akan menggunakan dan akan mengacu pada standar atau *framework* tertentu. Misalnya ISO27001, NIST, PCI DSS, dan sebagainya. Permasalahan yang terjadi selama ini adalah *framework* pada sistem manajemen keamanan informasi umumnya merupakan informasi dengan bentuk dokumen PDF. Informasinya yang panjang terkesan membosankan dan tidak sedikit yang membingungkan. Oleh karena itu, perlu penyederhanaan framework sistem manajemen keamanan informasi tersebut agar mudah dipahami. Jadi *framework* tersebut dibagi menjadi tiga kategori, yaitu control *framework* (kerangka kerja kendali), program *framework* (kerangka kerja program), dan *risk framework* (kerangka kerja risiko). ISO 27001 adalah standar internasional yang diakui secara luas untuk sistem manajemen keamanan informasi (*Information Security Management System, ISMS*). Manajemen risiko merupakan landasan dari ISO/IEC ISMS untuk menentukan kontrol keamanan mana yang perlu

diterapkan dan dipelihara.[5] Dengan sertifikasi ISO 27001, perusahaan akan menggunakan standarisasi ini dalam mengelola dan mengendalikan serta menjaga risiko keamanan informasi perusahaan yang meliputi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

Standar ISO 27001 dikembangkan untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan sistem manajemen keamanan informasi pada sebuah perusahaan. Sertifikasi standar yang terakreditasi dan diakui secara global ini menjadi indikator bahwa ISMS perusahaan sudah sesuai dengan praktik keamanan informasi terbaik yang sudah distandarisasi.

2. Pelayanan Nasabah

Pelayanan menurut Kamus Besar Bahasa Indonesia dinyatakan: "Pelayanan adalah perihal dan memudahkan yang diberikan sehubungan denganjual beli barang dan jasa".[6] Sedangkan definisi pelayanan yang lebih rinci adalah "suatu aktifitas atau serangkaian aktivitas yang bersifat tidak kasat mata yang terjadi sebagai akibat adanya interaksi antara nasabah dengan pegawai atau hal-hal lain yang disebabkan oleh perusahaan pemberi pelayanan yang dimaksudkan untuk memecahkan permasalahan nasabah".[7]

Selain itu pelayanan juga didefinisikan sebagai "kegiatan yang dilakukan oleh seseorang atau sekelompok orang dengan landasan faktor

[5] Ulfaninda, Tika. *ISO 27001:Standar untuk Sistem Manajemen Keamanan Informasi*. 2021.
[6] WJS Poerwa Darminta, *Kamus Umum Bahasa Indonesia*, (Jakarta: Balai Pustaka, 1976), 736.
[7] Ratminto dan Atik, *Manajemen Pelayanan* (Jakarta: Pustaka Pelajar, 2005), 2.

material melalui sistem prosedur dan dengan metode tertentu dalam rangka usaha memenuhi kepentingan orang lain sesuai haknya".[8] Dari beberapa definisi di atas, dapat diketahui bahwa ciri pokok pelayanan adalah tidak kasat mata dan melihat upaya manusia atau peralatan lain yang disediakan perusahaan penyelenggara pelayanan. Hal ini menjelaskan bahwa pelayanan adalah bentuk sistem, prosedur atau metode tertentu yang diberikan kepada orang lain dalam hal pelanggan agar kebutuhan pelanggan tersebut dapat terpenuhi sesuai dengan harapan mereka.[9]

Para konsumen tidak hanya menginginkan pelayanan-pelayanan tertentu tetapi juga menginginkan pelayanan tersebut dalam jumlah dan kualitas yang memadai. Apabila para nasabah bank diharuskan berdiri dalam antrian panjang atau menghadapi karyawan bank yang kurang ramah, para nasabah tersebut kemungkinan akan pindah ke lain bank. Perusahaan perlu mengecek tingkat jasa mereka sendiri maupun jasa para pesaingnya selaras dengan apa yang diharapkan oleh konsumen. Perusahaan bisa mengamati kekurangan-kekurangan jasa yang diberikan dengan berbagai cara: berbelanja untuk memperbandingkan, survei konsumen secara berkala, kotak-kotak saran, dansistem penanganan pengaduan. Hal ini membantu perusahaan mengetahui bagaimana jasa diberikan dan konsumen yang kecewa bisa memperoleh keputusan.[10]

Standar layanan baik perbankan maupun bukan perbankan sangat

[8] A.S Moenir, *Manajemen Pelayanan Umum di Indonesia* (Bandung: PT. Bumi Aksara, 2008), 27.
[9] Khamdan Rifa'i. *Kepuasan Konsumen*
[10] Philip Kotler, *Marketing*,Terj. Herujati Purwoko, (Jakarta: Erlangga, 1999), h.205

penting mengingat industri perbankan berkembang semakin pesat seiring dengan kebutuhan nasabah yang juga semakin meningkat dan kompleks, serta membutuhkan standar penampilan, layanan, pengetahuan, dan keterampilan mengenai produk dan jasa yang ditawarkan oleh bank. Secara umum, standar layanan perbankan yang harus dipenuhi, meliputi:

a. Penampilan Diri

Standar penampilan dibutuhkan untuk menumbuhkan kepercayaan nasabah kepada bank sehingga nasabah dapat terlayani dengan baik dan membuat nasabah puas. Standar penampilan petugas perbankan melipiti standar dalam berpakaian dan penampilan fisik. Dalam pelayanan prima (*service excellent*) diperlukan suatu standar penampilan bagi petugas maupun perusahaan. Standar penampilan petugas diperlukan guna membangun keyakinan bagi nasabah dan image positif bagi perusahaan, meningkatkan pelayanan, dan menjaga kepuasan pelanggan. Pelanggan merupakan aset yang sangat berharga dan harus tetap dipertahankan serta dijaga. Petugas diperlukan guna membangun keyakinan bagi nasabah dan *image positif* bagi perusahaan, meningkatkan pelayanan, dan menjaga kepuasan pelanggan. Pelanggan merupakan aset yang sangat berharga dan harus tetap dipertahankan/dijaga.

b. Kebersihan dan Kerpian Ruang Kerja

Ruang kerja pada umumnya adalah tempat berlangsungnya proses pekerjaan. Standar kebersihan dan kerapian ruang kerja dapat mendukung kenyamanan dalam memberikan layanan. Ruang kerja yang bersih, rapi,

dan nyaman memberikan efek kepuasan dan kenyamanan bagi nasabah. Upaya penataan ruang kerja perlu dilakukan karena berkaitan dengan pihak internal dan eksternal sehingga dapat mencapai kondisi yang memuaskan kedua belah pihak.

c. Pengetahuan Produk dan Jasa Perbankan

Pengetahuan atar produk dan jasa perbankan yang dilayani di mana pegawai bank bekerja, harus dikuasai secara penuh, minimal sesuai dengan job desk dan fungsi jabatan yang diemban sebagai pelayan nasabah perbankan.

d. Standar Berkomunikasi dengan Nasabah

Komunikasi yang baik kepada nasabah dapat membangun kesan positif dari nasabah terhadap bank. Hal tersebut mampu menciptakan keuntungan bagi kelangsungan usaha bank tersebut. Salah satu aspek yang harus dikomunikasikan dengan baik kepada 38 nasabah adalah terkait aspek perlindungan kepada nasabah yang terhubung dengan transparasi informasi produk bank.

e. Standar Penanganan Keluhan Nasabah

Pengaduan nasabah adalah ungkapan ketidakpuasan nasabah yang disebabkan oleh adanya potensi kerugian finansial pada nasabah yang diduga karena kesalahan atau kelalaian bank. Oleh karena itu, untuk mengatasi keluhan nasabahharuslah dilakukan dengan cara yang positif. Berikut adalah beberapa hal penting yang perlu diperhatikan dalam mengatasi keluhan:

1) Empati kepada penyampaian keluhan

2) Kecepatan memberikan tanggapan

3) Permintaan maaf

4) Kredibilitas

5) perhatian[11]

3. *Ransomware*

Ransomware adalah jenis malware yang dikirim peretas untuk mengunci dan mengenkripsi perangkat komputer milik korban. Kata *ransomware* sendiri berasal dari "*ransom*" (tebusan) dan "*malware*" (perangkat lunak berbahaya). Jadi, perangkat korban akan tersandera dan tidak bisa digunakan sampai korban membayar tebusan yang diminta peretas. Selama perangkat dikunci dan disandera, korban tidak akan bisa mengakses ke sistem atau file pada perangkat. Pada saat inilah peretas mengambil semua data-data penting milik korban. Apabila tidak segera ditebus, kemungkinan besar peretas akan menjual data tersebut ke pihak lain. Bahkan, sekalipun sudah ditebus tidak ada yang menjamin bahwa data akan sepenuhnya dipulihkan atau tidak disalahgunakan oleh peretas.

Penyebaran *ransomware* yang paling umum adalah melalui *phishing* email, eksploitasi kerentanan sistem, dan unduhan yang terinfeksi. Menurut Trend Micro, *ransomware* juga dapat menyebar melalui iklan berbahaya (*malvertising*), pesan yang mengandung tautan berbahaya, dan bahkan melalui perangkat penyimpanan eksternal.

[11] Ikatan Bankir Indonesia, *Memahami Bisnis Bank*, (Jakarta: Gramedia, 2012), h 190.

Penyebaran *ransomware* seringkali memanfaatkan kelemahan keamanan sistem atau kelalaian pengguna dalam menerapkan praktik keamanan *cyber* yang baik. Dampak dari serangan *ransomware* adalah gangguan operasional, kerusakan reputasi, dan potensi kebocoran data sensitif.

F. Sistematika Pembahasan

Kajian ini mempunyai lima bab yang masing-masing bab ditulis secara sistematis:

BAB I Pendahuluan, bab ini merupakan dasar dalam sistematika penelitian skripsi, yang mengemukakan latar belakang masalah, fokus penelitian, tujuan penelitian, definisi istilah, dan sistematika penelitian. Hal tersebut berfungsi sebagai gambaran skripsi secara umum.

BAB II Kajian Kepustakaan, bab ini berisi tentang ringkasan kajian terdahulu yang memiliki relevansi dengan penelitian yang akan dilakukan pada saat ini serta memuat kajian teori.

BAB III Metode Penelitian, bab ini berisi tentang metode yang digunakan penelitiyang meliputi pendekatan dan jenis penelitian, lokasi penelitian, sumber data, metode pengumpulan data, keabsahan data dan terakhir tahapan-tahapan penelitian.

BAB IV Hasil penelitian, yang berisi tentang inti atau hasil penelitian, objek penelitian, penyajian data, analisis data dan pembahasan temuan.

BAB V Kesimpulan dan saran, yang berisi kesimpulan dan hasil penelitian yang dilengkapi dengan saran dari peneliti.

BAB II

KAJIAN PUSTAKA

A. Penelitian Terdahulu

Agar penelitian ini menjadi lebih terfokus pada suatu masalah penelitian dan dapat menghasilkan kebaruan penelitian, serta memetakan posisi penelitian yang akan dilakukan oleh peneliti, maka peneliti perlu melakukan studi terhadap penelitian terdahulu yang sejenis dengan judul penelitian yang akan dilakukan. Berdasarkan hal tersebut, peneliti melakukan studi literatur terhadap hasil penelitian terdahulu dan hasilnya dijabarkan sebagai berikut:

a. Elya Rosa Maharani: Pengaruh Ancaman Siber *Ransomware* dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran, 2024. Mengatakan bahwa ancaman *cyber ransomware* dan gangguan yang sering terjadi pada sistem layanan perbankan seluler telah menurunkan kepercayaan pelanggan terhadap Bank Syariah Indonesia (BSI) KCP Kisaran, yang menyebabkan pelanggan merasa tidak aman saat melakukan transaksi.[12]

Pengkajian ini melihat adanya serangan cyber seperti ransomware dan gangguan sistem dalam layanan perbankan seluler telah secara nyata menurunkan kepercayaan pelanggan terhadap Bank Syariah Indonesia (BSI) KCP Kisaran. Penelitian tersebut mengungkap bahwa

[12] Maharani, Elya Rosa. *Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran*. 2024.

pelanggan merasa tidak aman saat melakukan transaksi perbankan, dipicu oleh kekhawatiran akan kerentanan dan ketidakmampuan sistem dalam menghadapi ancaman tersebut. Dampaknya sangat meresahkan, karena keamanan data dan privasi pelanggan menjadi terancam, mempengaruhi persepsi mereka terhadap kehandalan dan integritas layanan perbankan yang ditawarkan. Temuan ini menegaskan urgensi untuk meningkatkan infrastruktur keamanan cyber dalam sektor perbankan, tidak hanya untuk melindungi informasi sensitif pelanggan tetapi juga untuk memulihkan kepercayaan yang mungkin terkikis akibat serangkaian insiden yang mengganggu.

b. E. Budi, D. Wira, dan A. Infantono: Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di Era *Society* 5.0. 2021. Serangan ransomware telah menjadi ancaman yang semakin kompleks dan canggih. Pelaku serangan *ransomware* menggunakan berbagai metode dan teknik yang terus berkembang untuk menghindari deteksi dan merusak sistem informasi target. Oleh karena itu, diperlukan strategi keamanan sistem informasi yang efektif untuk memerangi serangan *ransomware* dan melindungi integritas, kerahasiaan, dan ketersediaan data dalam sistem informasi.[13]

Penelitian ini menyatakan bahwa serangan *ransomware* telah menjadi ancaman yang semakin kompleks dan canggih. Pelaku serangan menggunakan berbagai metode dan teknik yang terus berkembang untuk

[13] Budi. E, D. Wira, dan A. Infantono: *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0*. 2021.

mengelabui sistem keamanan dan merusak sistem informasi target. Kehadiran *ransomware* tidak hanya menimbulkan kerugian finansial tetapi juga mengancam integritas, kerahasiaan, dan ketersediaan data dalam sistem informasi. Dalam konteks ini, strategi keamanan sistem informasi yang efektif menjadi sangat penting. Hal ini mencakup penerapan langkah-langkah preventif seperti penggunaan perangkat lunak keamanan yang mutakhir, pendidikan karyawan tentang praktik keamanan digital, serta implementasi kebijakan backup data yang teratur dan pemulihan setelah serangan. Selain itu, upaya untuk meningkatkan kesadaran akan potensi ancaman *ransomware* dan kesiapan dalam menanggapi insiden juga menjadi bagian krusial dari strategi perlindungan yang komprehensif. Dengan pendekatan yang terintegrasi dan proaktif, organisasi dapat memperkuat ketahanan mereka terhadap serangan *ransomware* dan menjaga keberlangsungan operasional serta kepercayaan publik dalam pengelolaan dan perlindungan data mereka.

c. Kartika Aghni Safitri: Strategi Keamanan Sistem Informasi untuk Melawan Serangan *Ransomware*, 2023. Pandangan terhadap strategi keamanan sistem informasi untuk melawan serangan *ransomware* harus proaktif dan holistik. Terapkan perlindungan teknis yang kuat termasuk firewall, anti-virus, anti-malware, dan solusi keamanan jaringan lainnya. Pastikan bahwa semua perangkat keras dan perangkat lunak yang

digunakan dalam sistem informasi diperbarui secara berkala dengan tambalan terbaru untuk mengatasi kerentanan yang diketahui.[14]

Peneliti ini memiliki pandangan terhadap strategi keamanan sistem informasi untuk melawan serangan ransomware harus bersifat proaktif dan holistik. Hal ini mencakup penerapan perlindungan teknis yang kuat seperti *firewall*, anti-virus, anti-*malware*, dan solusi keamanan jaringan lainnya. Pentingnya memastikan bahwa semua perangkat keras dan perangkat lunak yang digunakan dalam sistem informasi selalu diperbarui secara berkala dengan tambalan terbaru untuk mengatasi kerentanan yang diketahui tidak boleh diabaikan. Selain itu, strategi ini juga mencakup pendidikan dan pelatihan bagi pengguna agar meningkatkan kesadaran mereka terhadap ancaman *cyber* dan praktik keamanan yang baik. Dengan pendekatan yang komprehensif ini, organisasi dapat meningkatkan ketahanan mereka terhadap serangan *ransomware* dan meminimalkan risiko serta dampak yang mungkin ditimbulkan terhadap integritas dan ketersediaan data mereka.

d. Anisa Solikhawati, Andriani Samsuri: Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja, 2023. Ada berbagai ancaman siber yang terjadi di Indonesia, salah satunya yaitu Denial of Service (DoS) yaitu suatu serangan yang memberhentikan layanan sementara ataupun permanen pada sebuah server website atau aplikasi dengan cara menggunakan botnet yang dijalankan secara

[14] Safitri, Kartika Aghni. *Strategi Keamanan Sistem Informasi untuk Melawan Serangan Ransomware.* 2023.

bersamaan dalam satu waktu, membanjiri permintaan request server agar tidak dapat terhubung, membanjiri pesan ICMP pada server dengan mengirim paket-paket yang sudah rusak oleh sang attacker, serangan ini dapat menyebabkan kerugian bagi client atau user tidak dapat mengakses sebuah website atau aplikasi yang dituju, serangan DoS dapat berupa ICMP Flood dan SYN Flood.[15]

Peneliti ini mengetahui di Indonesia menghadapi berbagai ancaman siber, salah satunya adalah serangan Denial of Service (DoS). DoS merupakan serangan yang bertujuan untuk menghentikan layanan sementara atau permanen pada server website atau aplikasi dengan cara membanjiri server dengan permintaan yang berlebihan. Serangan ini biasanya dilakukan dengan menggunakan botnet, di mana banyak perangkat yang dikendalikan bersamaan untuk membanjiri server dengan permintaan, sehingga server tidak dapat merespons dengan baik atau bahkan menjadi tidak dapat diakses sama sekali. Dua jenis serangan DoS yang umum adalah ICMP Flood, di mana attacker mengirimkan banyak paket ICMP (Internet Control Message Protocol) yang rusak atau palsu ke server, serta SYN Flood, di mana attacker membanjiri server dengan permintaan koneksi SYN yang tidak lengkap. Dampak dari serangan DoS ini dapat sangat merugikan, karena dapat mengakibatkan pengguna atau klien tidak dapat mengakses website atau aplikasi yang menjadi target, yang pada gilirannya dapat mengganggu operasional bisnis dan

[15] Solikhawati, Anisa. Andriani Samsuri: *Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja*. 2023.

menyebabkan kerugian finansial serta reputasi yang serius bagi organisasi yang diserang. Oleh karena itu, perlindungan terhadap serangan DoS menjadi sangat penting dengan menerapkan strategi keamanan yang sesuai dan pengelolaan lalu lintas jaringan yang efektif.

e. Abdul Rahman: Urgensi Penerapan Iso 27001 Pada Perbankan Syariah Di Indonesia, 2024. Menyatakan dari hasil penelitiannya, bahwa: 1) Penerapan ISO 27001 tentang sistem manajemen keamanan informasi bagi industri perbankan syariah di Indonesia sangatlah penting dalam menjaga imunitas sistem keamanan informasi di bank syariah. 2) Melalui pendekatan berbasis risiko, bank syariah dapat melindungi aset informasi, menjaga keamanan fisik dan personel, serta mengelola akses ke sistem informasi. 3) ISO 27001 mendorong pengawasan dan perbaikan terus-menerus dan dengan mengimplementasikan standar ini bank syariah dapat meningkatkan keamanan informasi dan melindungi informasi penting mereka dengan lebih efektif; 4) Bank syariah yang mematuhi standar yang diakui secara internasional ini menunjukkan dedikasinya dalam melindungi data sensitif dan menjaga kepatuhan terhadap peraturan, serta menanamkan kepercayaan pada klien.[16]

Penelitian ini mengkaji bahwa penerapan ISO 27001 mengenai sistem manajemen keamanan informasi sangatlah penting bagi industri perbankan syariah di Indonesia dalam menjaga imunitas sistem keamanan informasi. Pertama, melalui pendekatan berbasis risiko, bank syariah

[16] Rahman, Abdul: *Urgensi Penerapan Iso 27001 Pada Perbankan Syariah Di Indonesia*. 2024

dapat melindungi aset informasi, menjaga keamanan fisik dan personel, serta mengelola akses ke sistem informasi. Kedua, ISO 27001 mendorong pengawasan dan perbaikan terus-menerus, dengan mengimplementasikan standar ini bank syariah dapat meningkatkan keamanan informasi dan melindungi informasi penting mereka dengan lebih efektif. Ketiga, bank syariah yang mematuhi standar yang diakui secara internasional ini menunjukkan dedikasinya dalam melindungi data sensitif, menjaga kepatuhan terhadap peraturan, serta menanamkan kepercayaan pada klien dan pemangku kepentingan.

f. Tosun: Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja, 2021. Mengatakan bahwa, dalam sektor layanan moneter, penyebaran cepat transaksi cryptocurrency baru-baru ini terutama tidak diatur atau dilarang di beberapa yurisdiksi atau tidak dikendalikan oleh otoritas perbankan.[17] Hal ini merupakan perhatian utama bagi komunitas keuangan global dan memerlukan adopsi pendekatan menejemen risiko yang tidak terfokus. Serangan siber dapat mengancam stabilitas ekonomi dan menuntut pra-penilaian yang cermat dan manajemen risiko yang hati-hati bagi perbankan dan lembaga keuangan.

Peneliti ini melihat adanya sistem keamanan yang kurang dalam sektor layanan moneter, penyebaran cepat transaksi *cryptocurrency* baru-baru ini kebanyakan tidak diatur atau bahkan dilarang di beberapa

[17] Tosun: *Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja*. 2021.

yurisdiksi, dan tidak dikendalikan oleh otoritas perbankan. Situasi ini menjadi perhatian utama bagi komunitas keuangan global dan memerlukan adopsi pendekatan manajemen risiko yang tidak terfokus pada satu aspek saja. Serangan siber dapat mengancam stabilitas ekonomi, sehingga diperlukan penilaian awal yang cermat dan manajemen risiko yang hati-hati bagi perbankan dan lembaga keuangan.

g. I. Afrianto dan E. B. Setiawan, Kajian Virtual Private Network (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom, 2021. Beberapa aspek penting dari strategi keamanan sistem informasi terhadap serangan ransomware mencakup praktik keamanan yang kuat, penggunaan teknologi keamanan terbaru, keterlibatan pengguna, serta perencanaan dan pemulihan darurat.[18]

Peneliti ini melihat adanya beberapa aspek penting dalam strategi keamanan sistem informasi untuk menghadapi serangan ransomware. Pertama, praktik keamanan yang kuat, seperti pembaruan rutin perangkat lunak dan pengelolaan akses yang ketat, sangat penting untuk mencegah serangan. Kedua, penggunaan teknologi keamanan terbaru, termasuk solusi antivirus dan firewall canggih, membantu mendeteksi dan menghalau ancaman secara efektif. Ketiga, keterlibatan pengguna melalui pelatihan dan edukasi mengenai kesadaran keamanan siber memastikan bahwa setiap individu di organisasi memahami dan menerapkan langkah-langkah keamanan yang tepat. Terakhir, perencanaan dan pemulihan

[18] Afrianto, I dan E. B. Setiawan, *Kajian Virtual Private Network (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom).* 2021.

darurat yang komprehensif diperlukan untuk meminimalkan dampak serangan ransomware dan memastikan kelangsungan operasional melalui prosedur pemulihan yang telah disiapkan sebelumnya.

h. J. Ericka dan W. Prakasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi, 2020. Serangan *ransomware* telah menjadi ancaman yang semakin kompleks dan canggih. Pelaku serangan ransomware menggunakan berbagai metode dan teknik yang terus berkembang untuk menghindari deteksi dan merusak sistem informasi target. Oleh karena itu, diperlukan strategi keamanan sistem informasi yang efektif untuk memerangi serangan *ransomware* dan melindungi integritas, kerahasiaan, dan ketersediaan data dalam sistem informasi.[19] Semakin berkembangnya sistem informasi dewasa ini diikuti dengan peningkatan serangan terhadapsistem informasi. Hal ini disebabkan semakin banyak sistem informasi yang menyimpan data – data sensitif penggunanya seperti nomor telepon, Nomor Induk Kependudukan, tanggal lahir bahkan sampai nomor rekening bank. Data – data tersebut sangat rawan untuk di salah gunakan oleh pihak – pihak yang tidak bertanggung jawab. Maka keamanan merupakan salah satu faktor yang harus menjadi pertimbangan utama dalam pengembangan sistem informasi.

Peneliti ini menatakan bahwa ada masalah yang terdapat dalam serangan ransomware merupakan ancaman yang semakin kompleks dan

[19] Ericka, J dan W. Prakasa, *Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi*, 2020.

canggih. Para pelaku serangan ransomware menggunakan berbagai metode dan teknik yang terus berkembang untuk menghindari deteksi dan merusak sistem informasi target. Metode yang digunakan termasuk *phishing*, eksploitasi kerentanan perangkat lunak, dan penggunaan *malware* yang dirancang khusus untuk mengenkripsi data korban. Oleh karena itu, diperlukan strategi keamanan sistem informasi yang efektif untuk memerangi serangan *ransomware*. Strategi ini harus mencakup implementasi praktik keamanan terbaik, seperti penggunaan perangkat lunak antivirus terkini, pengelolaan akses yang ketat, dan pembaruan rutin sistem. Selain itu, pelatihan dan edukasi pengguna tentang kesadaran keamanan siber sangat penting untuk mengurangi risiko serangan. Dengan menerapkan langkah-langkah ini, organisasi dapat melindungi integritas, kerahasiaan, dan ketersediaan data dalam sistem informasi mereka. Serangan *ransomware* yang semakin kompleks dan canggih menunjukkan urgensi untuk meningkatkan keamanan sistem informasi. Pelaku *ransomware* terus mengembangkan teknik mereka untuk menghindari deteksi, sehingga membuat sistem informasi menjadi rentan. Dalam era digital yang semakin maju, banyak sistem informasi menyimpan data sensitif seperti nomor telepon, NIK, tanggal lahir, hingga informasi rekening bank, yang sangat rawan disalahgunakan. Oleh karena itu, keamanan harus menjadi prioritas utama dalam pengembangan sistem informasi. Tidak hanya untuk melindungi integritas dan ketersediaan data, tetapi juga untuk menjaga kepercayaan pengguna terhadap sistem

tersebut. Strategi keamanan yang efektif dan proaktif sangat dibutuhkan guna mencegah kerugian yang lebih besar akibat serangan siber ini.

i. Muhammad Subhan Abdullah: Perkembangan Terbaru Dalam Keamanan Siber, Ancaman yang Diidentifikasi Dan Upaya Pencegahan. 2023. Meningkatnya risiko serangan siber di Indonesia, terutama serangan *ransomware* dan *malware*, dan tekanan perlunya pemerintah dan penyelenggara sistem elektronik (PSE) meningkatkan keamanan sistem dan perlindungan data. Regulasi seperti Undang-Undang Pelindungan Data Pribadi (PDP) juga penting dalam menjaga keamanan dan kedaulatan ruang virtual. Kelemahan keamanan siber di Indonesia, termasuk indeks perlindungan siber yang rendah, kurangnya regulasi keamanan siber yang ditandatangani oleh Presiden, dan kesulitan memenuhi anggaran peningkatan investasi keamanan siber, berdampak negatif terhadap kepercayaan investor dan pengembangan teknologi.[20]

Masalah yang dibicarakan dalam penelitian tersebut adalah dampak dari risiko serangan siber di Indonesia, terutama serangan *ransomware* dan *malware* yang semakin meningkat. Kondisi ini menimbulkan tekanan bagi pemerintah dan penyelenggara sistem elektronik (PSE) untuk meningkatkan keamanan sistem dan perlindungan data. Regulasi seperti Undang-Undang Pelindungan Data Pribadi (PDP) menjadi sangat penting dalam menjaga keamanan dan kedaulatan ruang virtual. Sayangnya, Indonesia masih menghadapi berbagai kelemahan dalam keamanan siber.

[20] Abdullah, Muhammad Subhan. *Perkembangan Terbaru Dalam Keamanan Siber, Ancaman yang Diidentifikasi Dan Upaya Pencegahan*. 2023.

Indeks perlindungan siber yang rendah menunjukkan kerentanan terhadap ancaman siber. Selain itu, kurangnya regulasi keamanan siber yang ditandatangani oleh Presiden menghambat upaya penegakan kebijakan yang lebih ketat. Kesulitan dalam memenuhi anggaran untuk peningkatan investasi keamanan siber juga menjadi hambatan serius. Semua faktor ini berdampak negatif terhadap kepercayaan investor dan pengembangan teknologi di Indonesia, menghambat kemajuan di sektor ini.

j. Eko Budi: *Strategies For Strengthening Cyber Security To Achieve National Security in Society* 5.0. 2021. Pandemi Covid-19 menjadi topik utama dalam tren keamanan siber. Para peretas memanfaatkan keresahan masyarakat sebagai celah dalam meluncurkan berbagai serangan, mulai dari *phishing* hingga *ransomware*, kasus kebocoran data 91 juta pengguna situs belanja online Tokopedia dan kebocoran data 1,2 juta pengguna situs Bhinneka. Indonesia pun terdampak oleh kasus keamanan siber global seperti *Coronavirus Ransomware, Covidlock Malware,* peretasan *Border Gateway Protocol,* kerentanan pada produk *router Draytek Vigor,* adanya *Remote Code Execution* pada beberapa versi produk sistem operasi *Windows,* kerentanan terjadinya *Arbitrary Code Execution* pada seluruh sistem operasi *Google Android*, hingga eksploitasi produk S*olar Winds Orion Platform*. Kesimpulannya adalah saat ini Indonesia tengah dalam keadaan darurat cyber security dan sudah mencapai tahap memprihatinkan. Strategi *cyber security* yang harus dilakukan Indonesia untuk mewujudkan keamanan nasional di era *society* 5.0, adalah 1)

capacity building, 2) Pembentukan undang-undang khusus tentang tindak pidana siber, 3) Peningkatan sumberdaya manusia, 4) Kerjasama *stakeholder* di dalam negeri dan kerjasama internasional bidang *cyber security* untuk mewujudkan keamanan nasional di era *society* 5.0.[21]

Permasalahan yang diangkat dalam jurnal ini adalah tentang pengaruh para peretas dengan memanfaatkan keresahan masyarakat sebagai celah untuk meluncurkan berbagai serangan, mulai dari phishing hingga *ransomware*. Contoh nyata dari ancaman ini adalah kebocoran data 91 juta pengguna situs belanja *online* Tokopedia dan kebocoran data 1,2 juta pengguna situs Bhinneka. Selain itu, Indonesia juga terdampak oleh kasus keamanan siber global, seperti *Coronavirus Ransomware*, *Covidlock Malware*, peretasan *Border Gateway Protocol*, kerentanan pada produk *router Draytek Vigor*, adanya *Remote Code Execution* pada beberapa versi produk sistem operasi *Windows*, kerentanan *Arbitrary Code Execution* pada sistem operasi *Google Android*, hingga eksploitasi produk *Solar Winds Orion Platform*. Kesimpulannya, Indonesia saat ini berada dalam keadaan darurat keamanan siber yang memprihatinkan. Untuk mewujudkan keamanan nasional di era *society* 5.0, diperlukan strategi keamanan siber yang mencakup beberapa langkah penting: pertama, peningkatan kapasitas (*capacity building*); kedua, pembentukan undang-undang khusus tentang tindak pidana siber; ketiga, peningkatan sumber daya manusia; dan keempat, kerjasama antara pemangku

[21] Budi, Eko. *Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0*. 2021.

kepentingan di dalam negeri serta kerjasama internasional di bidang keamanan siber.

k. (Muslim: Analisis Keamanan Siber (*Cyber Security*) Dalam Era Digital "Tantangan Dan Strategi Pengamanan". 2024) Keamanan sistem informasi telah menjadi isu penting di era digital saat ini. Artikel ini membahas tantangan utama yang dihadapi organisasi dalam memastikan keamanan sistem TI mereka dan menyajikan strategi keamanan yang efektif untuk mengatasi tantangan ini. Ancaman seperti serangan *malware*, *phishing*, dan ancaman orang dalam menjadi semakin kompleks dan seringkali memerlukan pendekatan yang komprehensif. Strategi penting untuk diterapkan dalam konteks ini adalah *enkripsi* data, pemantauan keamanan waktu nyata, dan pelatihan karyawan tentang keamanan.[22] Dengan memperkuat pertahanan dan meningkatkan kesadaran akan ancaman keamanan, organisasi dapat mengurangi kemungkinan terjadinya insiden keamanan yang merugikan.

Peneliti ini menguraikan tantangan utama yang dihadapi oleh organisasi dalam upaya memastikan keamanan sistem TI mereka. Di antara tantangan tersebut adalah ancaman dari serangan *malware, phishing*, dan ancaman dari orang dalam, yang semakin hari semakin kompleks dan sulit ditangani. Untuk mengatasi tantangan ini, artikel tersebut menyajikan berbagai strategi keamanan yang efektif. Strategi-strategi ini meliputi enkripsi data, pemantauan keamanan secara waktu

[22] Muslim. *Analisis Keamanan Siber (Cyber Security) Dalam Era Digital "Tantangan Dan Strategi Pengamanan"*. 2024.

nyata, dan pelatihan karyawan tentang pentingnya keamanan informasi. Dengan menerapkan strategi-strategi ini, organisasi dapat memperkuat pertahanan mereka dan meningkatkan kesadaran karyawan akan ancaman keamanan. Langkah-langkah ini secara signifikan dapat mengurangi kemungkinan terjadinya insiden keamanan yang merugikan bagi organisasi.

Tabel 2.1

Penelitian Terdahulu

No	Penulis	Judul	Persamaan	Perbedaan
1	Elya Rosa Maharani, 2024.	Pengaruh ancaman siber ransomware dan gangguan sistem layanan mobile banking terhadap kepercayaan nasabah pada bank BSI KCP Kisaran	Persamaan penelitian yaitu melakukan penelitian terkait siber ransomware pada lembaga perbankan dalam meningkatkan kepercayaan nasabah.	Perbedaan terletak pada variabel dalam penelitian tersebut.
2	E. Budi, D. Wira Dan A. Infantono, 2021.	Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0	Persamaan penelitian yaitu dalam bentuk tujuan apabila terjadi sebuah serangan ransomware dengan memanej risiko keamanan menggunakan berbagai metode dan teknik yang terus berkembang dalam era digital.	Perbedaan penelitian terdapat pada penggunaan metode penelitian yang digunakan keduanya.
3	Kartika Aghni	Strategi	Persamaan	Perbedaan

No	Penulis	Judul	Persamaan	Perbedaan
	Safitri, 2023.	Keamanan Sistem Informasi Untuk Melawan Serangan Ransomware	penelitian terletak pada strategi keamanan dalam melawan serangan ransomware untuk mengatasi kerentanan yang diketahui.	penelitian yaitu dengan metode penelitian kualitatif.
4	Anisa Solikhawati, Andrianani Samsuri, 2023.	Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham Dan Kinerja	Persamaan penelitian memiliki persamaan dalam fokus penelitian siber.	Perbedaan penelitian terletak pada serangan siber yan dilakukan pada suatu lembaga.
5	Abdul Rahman, 2024.	Urgensi penerapan ISO 27001 Pada Perbankan Syariah di Indonesia	Persamaan penelitian yaitu dengan menerapkan sertifikasi ISO 27001 pada perbankan	Perbedaan penelitian yakni pada pendekatan pengelolaan sistem informasi yang digunakan keduanya
6	Tosun, 2021.	Evaluasi Bank Syariah Indonesia Pasca Serangan Siber	Persamaan kedua penelitian fokus pada manajemen risiko keamanan pada perbankan	Perbedaan berfokus pada bank syariah sedangkan penelitian ini mencakup seluruh lembaga perbankan
7	I. Afrianto Dan E. B. Setiawan, 2021.	Kajian Virtual Private Network (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (studi kasus jaringan komputer unikom)	Persamaan keduanya yaitu dengan memperkuat dan memberikan pembaharuan pada sistem elektronik untuk meminimal	Perbedaaan penelitian terletak pada studi kasus dan variabel

No	Penulis	Judul	Persamaan	Perbedaan
			dampak serangan *ransomware*	
8	J. Ericka Dan W. Prakasa, 2020.	Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi	Persamaan keduanya menggunakan metode dan teknik yang terus berkembang untuk menghindari deteksi dan merusak sistem informasi target	Perbedaan keduanya yaitu pada variabel independen
9	Muhammad Subhan Abdullah, 2023.	Perkembangan Terbaru Dalam Keamanan Siber, Ancaman yang Diidentifikasi dan Upaya Pencegahan	Persamaan kedua penelitian menggunakan instrumen manajemen risiko dalam penelitiannya dalam mitigasi siber	Perbedaan penelitian pertama mencakup pada perkembangan terbaru dan penelitian kedua mencakup pengaruh sistem keamanan dalam mencegah *ransomware*
10	Eko Budi, 2021.	Strategies For Strengthening Cyber Security To Achieve National Security In Sosiecty 5.0	Persamaan dalam penelitian ini memiliki variabel yang sama pada kasus keamanan siber yang sangat memprihatinkan	Perbedaaan keduanya berada dalam konteks metode penilitian. Penelitian memakai metode kualitatif dan penelitian ini menggunakan kuantitatif
11	Muslim, 2024.	Analisis Keamanan Siber	Persamaan keduanya	Perbedaan keduanya

No	Penulis	Judul	Persamaan	Perbedaan
		Dalam Era Digital "Tantangan Dan Strategi Pengamanan	berfokus dalam strategi pengamanan untuk mencegah serangan siber sebagai tantangan pada era digital	terletak pada variabel yang diambil, penelitian pertama fokus dalam indikator tantangannya, penelitian ini berfokus dalam mitigasi *ransomware* dengan objek perbankan

B. Kajian Teori

Kajian teori adalah proses penyelidikan dan pemahaman terhadap kerangka konseptual, prinsip dan hipotesis yang digunakan dalam sebuah bidang ilmu atau disiplin ilmu tertentu. Tujuan utama kajian teori adalah untuk mengembangkan dan memperdalam pemahaman tentang fenomena yang diamati atau topik yang diteliti. Kajian teori melibatkan studi literatur yang luas untuk mengumpulkan informasi tentang konsep-konsep dan teori-teori yang relevan dalam bidang studi tertentu. Selain itu, kajian teori juga melibatkan analisis, sintesis dan evaluasi terhadap teori-teori yang ada untuk memperoleh pemahaman yang lebih baik tentang fenomena yang diamati.[23]

1. Sistem Manajemen Keamanan Informasi

Sistem manajemen keamanan informasi adalah suatu sistem yang merancang, menerapkan, mengelola, serta memelihara keamanan informasi di suatu bisnis atau organisasi. Sistem keamanan informasi yang

[23] Tim Penyusun, *Pedoman Penulisan Karya Ilmiah, (*Jember: IAIN Jember, 2019)

dibuat oleh international organisasi adalah standar (ISO) dan elektronik international commision (IEC) adalah ISO 27001 yang berspesifikasi untuk sistem manajemen keamanan informasi dengan serangkaian kebijakan, prosedur, dan organisasi proses yang menetapkan proses untuk menerapkan seperangkat kontrol fisik, administratif serta teknis untuk melindungi aset.[24]

Menurut Bahasa, keamanan merujuk pada kondisi bebas dari risiko atau bahaya, di mana suatu entitas atau sistem dilindungi dari ancaman yang dapat membahayakan keberlangsungan, integritas, atau keselamatan Informasi, di sisi lain, adalah data yang memiliki nilai atau kegunaan yang penting hagi entitas yang memilikinya, baik dalam bentuk fisik maupun digital.[25] Penerapan ISO 27001 dalam sebuah perusahaan membutuhkan kerjasama dari seluruh bagian organisasi perusahaan. Spesifikasi di dalam ISO ini mencakup dokumentasi, tanggung jawab manajemen, audit sistem informasi, perbaikan berkelanjutan serta tindakan pencegahan dan korektif dalam sistem keamanan informasi perusahaan. Dalam penerapannya, ISMS melibatkan:

a) Ruang lingkup proyek kerja perusahaan.
b) Komitmen dan anggaran dalam manajemen keamanan.
c) Mengidentifikasi pihak yang berkepentingan, syarat hukum, peraturan dan kontrak.
d) Melakukan penilaian risiko.

[24] Wiyli Yustanti, Rahadian Bisma, Anita Qoiriah, Dkk. *Keamanan Sistem Informasi*. 2018.
[25] Muni, Abdul. Kasmawati. Agung Ramadhan dkk. *Kriptografi untuk keamanan Sistem Informasi.* 2024 (99).

e) Melakukan *review* dan penerapan kontrol yang diperlukan.

f) Mengembangkan kompetensi internal untuk mengelola proyek.

g) Mengembangkan dokumentasi.

h) Melakukan pelatihan staff.

i) Melakukan pelaporan terkait *statement of applicability* (pernyataan penerapan) dan rencana penanggulangan risiko keamanannya.

j) Mengukur, memantau, meninjau dan mengaudit ISMS secara berkelanjutan.

k) Bersikap korektif dan preventif.[26]

Keamanan sistem informasi melibatkan upaya untuk melindungi informasi dari ancaman, gangguan, atau akses yang tidak sah yang dapat mengganggu integritas, kerahasiaan, atau ketersediaan informasi tersebut. Ini mencakup pembuatan kebijakan yang mengatur penggunaan dan akses informasi, penerapan prosedur untuk mengelola risiko keamanan, dan penggunaan sistem teknologi informasi yang sesuai untuk melindungi data dari akses yang tidak sah, modifikasi, atau kehilangan. Kebijakan keamanan mencakup aturan tentang bagaimana data sensitif harus diakses, disimpan, dan dipertahankan, sementara prosedur keamanan berkaitan dengan langkah-langkah konkret untuk mencegah dan merespons terhadap ancaman keamanan. Sistem keamanan, pada gilirannya, mencakup perangkat lunak, perangkat keras, dan infrastruktur

[26] Tika Ulfianinda, *ISO 27001: Standar untuk Sistem Manajemen Keamanan Informasi*. 2021.

lainnya yang digunakan untuk menerapkan kontrol keamanan dan melindungi informasi dari ancaman yang ada.

Tujuan keamanan informasi, yang sering disebut sebagai Triad CIA, adalah untuk menjaga tiga aspek kunci dari informasi: kerahasiaan, integritas, dan ketersediaan.

a. Kerahasiaan (*Confidentiality*): Merujuk pada perlindungan informasi dari akses atau pengungkapan yang tidak sah. Ini berarti hanya orang yang berwenang yang memiliki akses ke informasi yang sensitif atau rahasia, dan bahwa informasi tersebut tidak diketahui oleh pihak yang tidak berhak
b. Integritas (*Integrity*): Merupakan jaminan bahwa informasi tidak diubah, dimodifikasi, atau rusak secara tidak sah selama penyimpanan, pengiriman, atau pemrosesan. Dengan menjaga integritas informasi, organisasi dapat memastikan bahwa data tetap akurat, konsisten, dan dapat diandalkan.
c. Ketersediaan (*Availibility*): Informasi yang selalu tersedia dan dapat diakses oleh mereka yang berwenang saat diperlukan. Ini berarti mencegah gangguan atau gangguan yang dapat menghambat akses atau penggunaan informasi yang penting untuk kegiatan operasional atau pengambilan keputusan, dengan memprioritaskan Triad CIA, organisasi dapat memastikan bahwa informasi mereka dijaga dengan baik, terhindar dari ancaman dan risiko yang dapat merugikan kepentingan mereka.

Adapun dampak yang terjadi jika Sistem Manajemen Keamanan Informasi tidak digunakan sesuai aturan dengan baik.

a. Kerentanan terhadap serangan siber, tanpa penerapan SMKI yang tepat, perusahaan menjadi lebih rentan terhadap berbagai serangan siber seperti *malware*, *ransomware*, *phishing*, dan peretasan. Serangan ini dapat mengakibatkan pencurian data, gangguan operasional, dan kerusakan sistem.[27]
b. Kehilangan data sensitif, tidak mengikuti prosedur SMKI dapat menyebabkan kebocoran atau kehilangan data sensitif pelanggan, informasi keuangan, atau rahasia dagang perusahaan. Hal ini dapat mengakibatkan kerugian finansial, tuntutan hukum, dan kerusakan reputasi.[28]
c. Gangguan operasional, serangan siber atau insiden keamanan yang berhasil dapat mengganggu operasi bisnis sehari-hari, mengakibatkan *downtime*, penundaan pengiriman, dan ketidakmampuan untuk melayani pelanggan.
d. Kerusakan reputasi, kehilangan data pelanggan atau pelanggaran keamanan yang dipublikasikan dapat merusak citra perusahaan dan kepercayaan pelanggan. Membangun kembali kepercayaan membutuhkan waktu dan sumber daya yang signifikan.

[27] Lanang Adi Saputra, Fadel Muhammad Akbar, Febrina Cahyaningtias, dkk. Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal pendidikan siber nusantara.* 2023.
[28] Halimah1 , Lely Dahlia. *Pengaruh Penerapan Sistem Manajemen Keamanan Informasi (ISO 27001) Dan Pengendalian Internal Terhadap Kinerja Karyawan Pada Pt. Bank Jasa Jakarta.*

2. Pelayanan Nasabah

Pelayanan merupakan suatu kegiatan yang bermanfaat dengan melibatkan antar manusia yang bertujuan untuk memuaskan para pelanggan atau nasabah dengan baik.[29] Dalam melayani nasabah ada beberapa proses yang perlu diketahui, proses tersebut dibagi menjadi 3 kelompok yaitu:

a. ***Core Service,*** merupakan pelayanan yang diberikan kepada pelanggan sebagai produk utamanya. Seperti bank menawarkan pelayanan dalam bentuk *offline* dan *online*.

b. ***Facilitating Service,*** merupakan pelayanan yang dinilai sebagai tambahan. Seperti pelayanan pada mobile banking yang dapat diakses selama 24 jam.

c. ***Supporting Service,*** merupakan pelayanan tambahan secara khusus yang tidak dimiliki oleh perusahaan lain. Misalnya *mobile banking*.[30]

Pelayanan secara garis besar memiliki karakteristik, yaitu:

a. ***Ingtangbility,*** pelayanan tidak memiliki wujud atau tidak bisa dilihat, tidak bisa didengar, tidak bisa diraba dan tidak dapat dicium sebelum adanya interaksi pembelian.

b. ***Inseparability,*** merupakan pelayanan yang tidak dapat dipisahkan dari sumbernya, jika sumber tersebut adalah orang atau mesin maka produk fisik yang berwujud tetap dinyatakan ada.

[29] Hersa Farida Quroaini. *Analisis Implementasi Aplikasi BSI Mobile dalam meningkatkan kualitas pelayanan di BSI KCP Jember Balung*
[30] M. Nur Rianto Al Arif, *Dasar - Dasar Pemasaran Bank Syariah* (Bandung: Alfabeta, 2016) 213.

c. ***Variability,*** pada karakteristik ini memiliki arti keberagaman atau standarisasi setiap jasa memiliki perbedaan satu sama lain.

d. ***Perishability,*** karakteristik perishability merupakan pelayanan yang tidak bisa bertahan lama. Pelayanan akan berubah – ubah setiap waktu.[31]

Pelanggan atau calon pelanggan yang akan dihadapi CS berasal dari berbagai tempat, suku bangsa, dan agama. Keragaman ini akan membentuk perilaku pelanggan atau calon pelanggan yang berbeda antara satu dengan yang lainnya. Sementara itu, seorang CS di tuntut untuk memberikan pelayanan yang prima kepada pelanggannya. Oleh karena itu, seorang CS dituntun untuk memiliki dasar-dasar pelayanan yang kuat. Tujuannya adalah agar pelayanan yang diberikan dapat memuaskan pelanggan karena pada dasarnya tujuan pelanggan atau calon pelanggan adalah sama, yaitu ingin mendapatkan kepuasan, baik mutu produk ataupun layanan yang diberikan. Seorang CS harus memiliki dasar-dasar pelayanan yang kokoh pasti akan mampu mengatasi setiap kebutuhan dan keinginan pelanggan maupun calon pelanggan. Pelayanan yang diberikan akan semakin berkualitas jika setiap CS telah dibekali dasar-dasar pelayanan.

[31] Fandy Tjiptono, *Service, Quality and Satisfaction* (Yogyakarta: ANDI, 2014) 13.

Dasar-dasar Pelayanan

a. Berpakaian dan berpenampilan

Pakaian dan penampilan merupakan satu paket yang tidak bisa dipisahkan. Artinya petugas CS harus mengenakan baju dan celana yang sepadan dengan kombinasi yang menarik. Gunakan pakaian seragam jika petugas CS diberikan pakaian seragam sesuai waktu yang telah ditetapkan.

b. Percaya diri, bersikap akrab, dan penuh dengan senyum

Dalam melayani pelanggan, petugas CS harus memiliki rasa percaya diri yang tinggi. Petugas CS juga harus bersikap akrab dengan calon pelanggan, seolah-olah sudah kenal lama. Dalam melayani pelanggan petugas CS harus murah senyum dengan raut muka yang menarik hati, serta tidak dibuat-buat.

c. Menyapa dengan lembut

Pada saat pelanggan atau calon pelanggan datang, petugas CS harus segera menyapa dan kalau sudah pernah bertemu sebelumnyausahakan menyapa dengan menyebutkan namanya. Namun, jika belum kenal dapat menyapa dengan sebutan bapak/ibu, apa yang dapat kami bantu.

d. Tenang, Sopan, Hormat dan Tekun

Usahakan pada saat melayani pelanggan dalam keadaan tenang, tidak terburu-buru, sopan santun dalam bersikap. Kemudian, tunjukkan sikap menghormati pada pelanggan ataucalon pelanggan, tekun mendengarkan, sekaligus memahami keinginannya.

e. Berbicara

Berbicara menggunakan bahasa yang baik dan benar. Artinya dalam berkomunikasi dengan pelanggan gunakan bahasa Indonesia yang benar atau bahasa daerah yang benar pula. Suara yang digunakan harus jelas dalam arti mudah dipahami dan jangan menggunakan istilah-istilah yang sulit dipahami oleh pelanggan.

f. Bergairah

Dalam melayani pelanggan, seorang CS hendaknya menunjukkan peayanan yang prima, seolah-olah memang sangat tertarik dengan keinginan dan kemauan pelanggan.

g. Jangan menyelah

Pada saat pelanggan sedang berbicara, usahakan jangan menyelah pembircaraan. Kemudian, hindarkan kalimat yang bersifat teguran atau sindiran yang dapat menyinggung perasaan pelanggan. Kalau terjadi sesuatu usahakan jangan berdebat.

h. Mampu meyakini pelanggan

Seorang CS harus mampu meyakinkan pelanggan dengan argumen-argumen yang masuk akal. Petugas CS juga harus mampu memberikan kepuasan atas pelayanan yang diberikannya.

i. Jika tidak sanggup?

Jika ada pertanyaan atau permasalahan yang tidak sanggup dijawab atau diselesaikan oleh petugas CS, usahakan meminta bantuan kepada petugas yang mampu.

j. Bila belum dapat melayani?

Bila petugas CS belum dapat melayani, beritahukan kapan akan dilayani. Artinya jika pada saat tertentu, petugas CS sibuk dan tidak dapat melayani salah satu pelanggan, beritahukan kepada tersebut kapan akan dilayani dengan simpatik.

Etika Pelayanan

Kata "Ethics" berasal daribahasa yunani "Ethos" yang berarti karakter atau kebiasaan atau adat istiadat. Ethics adalah karakter atau sikap atau kebiasaan seseorang atau kelompok. Etika adalah ilmu tentang apa yang baik dan apa yang buruk yang dianut oleh masyarakat. Ada yang merupakan etiket artinya kumpulan tata cara dalam pergaulan. Kata etiket berasal dari perancis (etiquette) yang berarti kartu undangan. Akhirnya perkataan etiquette diartikan sebagai ketentuan yang mengatur tindak dan gerak manusia dalam pergaulan dimasyarakat, seperti penampilan, cara bicara, cara berpakaian, sopan santun dan lain-lain. Dalam melakukan transaksi atau jasa bank berpegang pada prosedur atau mekanisme yang telah ditetapkan. Jauhkan unsur-unsur kepentingan pribadi atau kelompok, bank untung nasabah pun puas. Etika pelayanan adalah perilaku petugas bank terutama petugas pelayanan (*customer service*) dalam memenuhi apa yang diinginkan atau diharapkan konsumen/nasabah. Etika pelayanan bertitik tolak pada perilaku petugas bank dalam berbagai lini dalam memenuhi kebutuhan dan keinginan nasabah dengan memperhatikan mana yang baik mana yang buruk, mana yang benar mana yang salah. Ada

beberapa karakter yang harus dimiliki oleh petugas bank dalam melakukan pelayanan kepada nasabah, diantaranya adalah:

a. Tidak melakukan perbuatan tercela.
b. Memegang teguh amanah.
c. Menjaga nama baik bank dan nasabah.
d. Beriman dan merasa mempunyai tanggung jawab moral.
e. Sabar tapi tegas dalam menghadapi permasalahan, seperti keluhan nasabah.
f. Memiliki integritas, bertindak juur dan benar.
g. Manners, artinya tidak egois, disiplin dan tidak kasar.

Produk dan jasa merupakan suatu yang tidak jauh dari kualitas pelayanan yang dapat memberikan manfaat yang baik bagi konsumen. Oleh karena itu dalam hal ini jika suatu pelayanan memberikan kebaikan bagi sesama. Allah SWT berfirman dalam al-Qur'an surat Al-Imran ayat 159, yang berbuyi:

فَبِمَا رَحْمَةٍ مِّنَ ٱللَّهِ لِنتَ لَهُمْ ۖ وَلَوْ كُنتَ فَظًّا غَلِيظَ ٱلْقَلْبِ لَٱنفَضُّوا۟ مِنْ حَوْلِكَ ۖ فَٱعْفُ عَنْهُمْ وَٱسْتَغْفِرْ لَهُمْ وَشَاوِرْهُمْ فِى ٱلْأَمْرِ ۖ فَإِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى ٱللَّهِ ۚ إِنَّ ٱللَّهَ يُحِبُّ ٱلْمُتَوَكِّلِينَ ١٥٩

Artinya: "Maka disebabkan rahmat dari Allah-lah kamu berlaku lemah lembut terhadap mereka. Sekiranya kamu bersikap keras lagi berhati kasar, tentulah mereka menjauhkan diri dari sekelilingmu. Karena itu maafkanlah mereka, mohonkanlah ampun bagi mereka, dan bermusyawaratlah dengan mereka dalam urusan itu. Kemudian apabila kamu telah membulatkan tekad, maka bertawakkallah kepada Allah. Sesungguhnya Allah menyukai orang-orang yang bertawakkal kepada-Nya". (QS. Al-Imran ayat: 159).[32]

[32] Kementerian Agama RI, Al-Quran Transliterasi Per Kata dan Terjemahan Per Kata., 17.

Pada ayat di atas memberikan pelajaran kepada setiap individu maupun kelompok agar menggunakan sikap yang lemah lembut kepada sesama, bersikap kasar atau tidak menerapkan kenyamanan bagi sesama tentunya sangat tidak dianjurkan dalam Islam. Oleh karena itu dalam melakukan sebuah pelayanan harus sepenuhnya diberikan yang baik dan sopan kepada konsumen agar merasa aman dan damai. Kualitas pelayanan dalam islam dilandasi oleh beberapa hal yang meliputi kepribadian yang dimiliki perusahaan agar amanah dan terpercaya pada konsumen atas perilaku dan sifatnya. Oleh karena itu dalam islam kualitas pelayanan memberikan artikulasikan pada sifat Rasullallah SAW, yaitu:

a. **Shiddiq,** merupakan sifat para Nabi dan Rosul yang berarti jujur atau benar. sifat ini dapat digunakan dalam indikator jujur dan benar dalam setiap perbuatan, perkataan serta perjanjian. Dalam segi bisnis di kenal dengan istilah berjualan dengan jujur sepesifikasi barang yang ditawarkan agar sesuai yang diharapkan pembeli.
b. **Amanah,** secara umum berarti bertanggung jawab terhadap apa yang dibawanya, menepati janji, melaksanakan perintah, menunaikan keadilan, memberi hukum yang sesuai dan dapat menjalankan sesuatu sesuai kesepakatan.[33]
c. **Tabligh,** merupakan salah satu sifat Nabi Muhammad SAW yang wajib ditiru ini adalah termasuk menyampaikan kebenaran kepada seluruh manusia yang juga masih terkait dengan sifat jujur

[33] Zaidah Kusumawati, *Ensiklopedia Nabi Muhammad SAW Sebagai Utusan Allah* (Jakarta: Lentera Abadi, 2011), 34.

d. **Fathonah,** para Nabi dan Rasul memiliki sifat cerdas, maksudnya adalah akalnya cerdas, sehat pikirannya, hatinya tulus, dan tajam perasaannya. Sifat cerdas diterapkan Rasulluah SAW dalam momentum dan strategi marketing untuk menarik konsumen. Indikator dari sifat menyampaikan yaitu memberikan nasihat terhadap orang lain dan tetap berpegang teguh terhadap perintah Allah SWT. [34]

Nasabah adalah pelanggan yang memperoleh manfaat dari produk ataupun jasa yang diberikan oleh lembaga keuangan. Manfaat yang diperoleh yaitu pembelian, penyewaan dan pelayanan jasa pada produk yang ditawarkan. Pasal 1 ayat 17 UU. No. 10 Tahun 1998 Nasabah merupakan pengguna maupun pihak utama yang dapat menggunakan produk atau jasa lembaga keuangan dan berperan penting dalam proses transaksi.

Nasabah diartikan sebagai konsumen yang memiliki rekening simpanan dan tabungan pada bank. Selain itu nasabah dapat memeperoleh fasilitas yang diberikan oleh bank seperti melakukan transaksi, transfer maupun menyimpan dana. Ada 2 jenis nasabah dalam perbankan, antara lain:

a. Nasabah Debitur, yaitu nasabah yang mendapatkan fasilitas pinjaman maupun pembiayaan sesuai dengan prinsip syariah

[34] Mustafa Kamal Rokan, *Bisnis Ala Nabi: Teladan Rasulullah SAW dalam Berbisnis* (Yogyakarta: Bunyan, 2013), 12.

b. Nasabah penyimpan, yaitu nasabah yang memperoleh dana dari bank dalam bentuk simpanan yang dipergunakan sesuai dengan perjanjian dan berdasarkan prinsip syariah.[35]

3. *Ransomware*

Serangan ransomware terus menjadi ancaman besar bagi organisasi diseluruh dunia. Serangan ini melibatkan perangkat lunak jahat yang mengenskripsi file pada sistem yang terinfeksi, dengan pelaku serangan kemudian menuntut pembayaran tebusan untuk deskripsi file. Dampak dari serangan ini bisa sangat merusak, tidak hanya menyebabkan kehilangan data yang signifikan tapi juga menghentikan operasi bisnis. dengan bervariasinya metode penyebaran mulai dari lampiran email yang terinfeksi hingga eksploitasi kerentangan jaringan *ransomware* memperlihatkan kebutuhan mendesak untuk pendekatan keamanan yang berlapis, termasuk pelatihan karyawan, backup data yang teratur, keamanan yang konsisten.[36]

Ransomware adalah serangan malware yang dikirim peretas untuk mengunci dan mengenkripsi perangkat komputer milik korban. Lalu, peretas akan meminta uang tebusan untuk memulihkan aksesnya. Kurang lebih, seperti itulah gambaran apa itu *Ransomware* secara sederhana. Namun, pada kenyataannya cara kerja *Ransomware* dan proses penanganannya tidaklah sederhana. Jika beruntung, kamu masih bisa

[35] Abd. Shomad, Trisadini P. Usanti, *Hukum Perbankan* (Depok: Kencana, 2017), 17.
[36] Rakhmadi Rahman, Made Suci Arianti, Abdul Hadi, dkk. *Keamanan Jaringan Komputer*. 2024.

mendapatkan kembali akses ke perangkatmu. Namun jika tidak, ucapkan selamat tinggal pada data-data penting yang kamu miliki.[37]

Untuk dapat mendekripsi data pada perangkat yang terinfeksi *ransomware*, kamu memerlukan kode dekripsi yang akan ditawarkan oleh peretas dengan membayar tebusan. Jika dalam waktu tertentu kamu belum dapat mendekripsikan perangkatmu, maka data-data yang ada di perangkat akan hilang. Dari semua jenis *malware* yang ada, *ransomware* adalah salah satu yang paling berbahaya. Berbeda dengan malware lainnya, *ransomware* dapat mengacaukan sistem perangkat hingga tidak dapat dioperasikan. Selain itu, *ransomware* juga memiliki sifat yang dapat menyebar dan menginfeksi perangkat di sekitarnya. Sehingga, sangat berbahaya jika tidak segera ditangani dengan cepat. Berikut ini statistik perkembangan *ransomware* beberapa tahun terakhir berdasarkan situs web *cyber security PurpleSec*:

1. Tebusan *Ransomware* rata-rata pada tahun 2021 meningkat sebesar 82% dari tahun ke tahun, menjadi $570.000 atau setara dengan 8,1 miliar rupiah.
2. Sebanyak 121 serangan *Ransomware* dilaporkan pada Q1 2021, meningkat 64% dari tahun ke tahun.
3. *Ransomware* terbukti meningkat dengan salah satu jenis *Ransomware*, Ryuk, yang mengalami peningkatan pesat sebesar 543% selama Q4 2018.

[37] Mike Napizahny, *Apa itu Ransomware?*, 2022.

4. Pada 2019, *Ransomware* dengan cara *phising* meningkat sebesar 109%, dengan varian *Ransomware* baru tumbuh sebesar 46%.
5. Serangan *Ransomware* meningkat 41% pada tahun 2019 dengan 205.000 bisnis kehilangan akses data mereka.
6. *Ransomware* telah menjadi bentuk serangan siber yang populer dalam beberapa tahun terakhir, tumbuh sebesar 350% pada 2018.

Jenis-Jenis *Ransomware*

Ada beberapa jenis *Ransomware* yang dibedakan berdasarkan cara kerjanya. Berikut ini dua jenis Ransomware yang paling umum ditemukan:

a) *Encrypting Ransomware*

Ransomware jenis ini menginfeksi perangkat dengan cara mengenkripsi file maupun folder penting yang ada di perangkat korban. Setelah target berhasil terkunci dan terenkripsi, akan muncul notifikasi mengenai tebusan yang harus dibayarkan untuk membuka kembali data yang telah terkunci. Contoh *Encrypting Ransomware: WannaCry, CryptoWall, CryptoLocker, Locky*.

b) *Locker Ransomware*

Ransomware jenis ini tidak bekerja dengan cara mengenkripsi file maupun folder milik korban, melainkan mengunci akses korban ke perangkat. Biasanya, target *Locker Ransomware* adalah penguncian file maupun perangkat. Tapi terkadang, malware jenis ini juga menyasar hardware milik korban seperti *keyboard* atau *mouse*.

Locker Ransomware termasuk gangguan tingkat rendah yang masih bisa ditangani cukup dengan menghapus script, dsb. Sehingga, tebusan yang dibayarkan untuk malware jenis ini bisa dibilang lebih sedikit. Contoh *Locker Ransomware: Winlocker, Reveton.*

BAB III

METODE PENELITIAN

A. Pendekatan dan Jenis Penelitian

Pendekatan yang digunakan peneliti dalam penelitian ini adalah penelitian kualitatif. Penelitian kualitatif merupakan suatu pendekatan untuk mengeksplorasi dan memahami makna yang dianggap berasal dari suatu masalah.[38] Proses penelitian kualitatif melibatkan beberapa prosedur penting seperti mengajukan pertanyaan, mengumpulkan data yang spesifik dari para partisipan, menganalisis data, dan menafsirkan data.[39] Prosedur yang dilakukan dalam penelitian kualitatif menghasilkan temuan-temuan yang didapatkan dari data-data yang telah dikumpulkan melalui beragam sarana seperti observasi, wawancara, ataupun studi kasus.[40]

Jenis penelitian yang digunakan peneliti adalah penelitian kualitatif deskriptif. Penelitian kualitatif deskriptif merupakan jenis penelitian yang memberikan gambaran dan penjabaran mengenai peristiwa, fenomena, dan situasi sosial yang diamati.[41]

[38] Nurul Widyawati, *Metodologi Penelitian Kualitatif*
[39] John Cresswell, *Research Design: Qualitative, Quantitative, and Mixed MethodsApproaches* (California, 2014).
[40] Urip Sulistiyo, *Metode Penelitian Kualitatif* (Jambi: Salim Media Indonesia, 2019), https://books.google.co.id/books?hl=id&lr=&id=nJm8EAAAQBAJ&oi=fnd&pg=PP1&dq=metode+penelitian+kualitatif+deskriptif&ots=GGDHefux8D&sig=fA6ohJLZHJUeULD2Fb1WXbHde9E&redir_esc=y#v=onepage&q=metode penelitian kualitatif deskriptif&f=false.
[41] Marinu Waruwu, "Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif Dan Metode Penelitian Kombinasi (Mixed Method)," *Jurnal Pendidikan Tambusai 7*, no. 1 (2023): 2896–2910.

Peneliti deskriptif bertujuan untuk memberikan deskripsi, penejelasan, dan validasi terkait peristiwa yang sedang diteliti[42]. Alasan peneliti menggunakan jenis penelitian kualitatif deskriptif karena peneliti ingin mendeskripsikan dan memberikan gambaran mengenai peran standar sistem manajemen keamanan informasi dalam meningkatkan ketahanan perbankan Indonesia terhadap serangan *ransomware*. Dengan demikian, melalui penelitian ini diharapkan dapat memberikan informasi terkait standar sistem manajemen keamanan informasi dalam meningkatkan ketahanan perbankan Indonesia dan sampak pelayanan nasabah terhadap serangan *ransomware* di BSI KCP Kencong Jember.

B. Lokasi Penelitian

Lokasi penelitian yang digunakan peneliti adalah BSI KCP Kencong Jember yang beralamat di Jl. Krakatau No.45, Ponjen, Kencong, Kabupaten Jember, Jawa Timur. Pemilihan lokasi BSI KCP Kencong Jember dalam penelitian ini didasarkan pada beberapa alasan strategis. Sebagai salah satu kantor cabang pembantu Bank Syariah Indonesia, BSI KCP Kencong Jember memiliki peran penting dalam melayani masyarakat, terutama di wilayah dengan dominasi sektor UMKM. Hal ini menjadikan lokasi ini relevan untuk mengkaji penerapan strategi manajemen keamanan informasi dalam konteks perbankan syariah yang menghadapi tantangan digitalisasi, termasuk ancaman serangan ransomware. Selain itu, BSI KCP Kencong Jember merupakan

[42] Muhammad Ramdhan, *Metode Penelitian* (Surabaya: Cipta Media Nusantara, 2021), https://books.google.co.id/books?hl=id&lr=&id=Ntw_EAAAQBAJ&oi=fnd&pg=PR1&dq=metode+penelitian+kualitatif+deskriptif&ots=f3nF6LPq4z&sig=MbmpZlqaLHH4G9gGru9U35k1_o&redir_esc=y#v=onepage&q=metode penelitian kualitatifdeskriptif&f=false.

lokasi yang memungkinkan peneliti untuk mengakses data terkait implementasi kebijakan keamanan informasi, dampaknya terhadap ketahanan operasional bank, serta pengaruhnya terhadap pelayanan nasabah. Faktor aksesibilitas dan keterbukaan pihak bank juga menjadi alasan kuat untuk memilih lokasi ini sebagai objek penelitian. Dengan memilih lokasi ini, diharapkan hasil penelitian dapat memberikan rekomendasi yang aplikatif tidak hanya untuk BSI KCP Kencong Jember, tetapi juga bagi bank syariah lain di daerah serupa.

C. Subjek Penelitian

Subjek penelitian diambil menggunakan teknik *purposive sampling* merupakan informan yang dimanfaatkan oleh peneliti untuk memberikan informasi mengenai situasi dan kondisi tempat penelitian dengan karakter tertentu.[43] Kajian ini mencakup pemilihan kategori informan berikut:

1) *Branch Manager* : Dwi Ismanto
2) *Branch Operasional Service Manager* : Alex Ari Gustopo
3) *Operational staff* : Icha Reviliani
4) *Customer service Representative* : Achmad Sidqi
5) *Teller* : Putriana
6) *Nasabah* : Rani Maulidasari, Elsa

D. Teknik Pengumpulan Data

Dalam ranah penelitian, teknik pengumpulan data meliputi taktik sengaja yang digunakan untuk mendapatkan data yang diinginkan. Tujuan utama

[43] Moleong, 2010.

penelitian ini adalah untuk mengumpulkan informasi yang relevan mengenai subjek yang diminati.[44] Kegiatan ini meliputi kegiatan mengamati, melakukan wawancara, dan mendokumentasikan informasi. Pengetahuan yang kurang mengenai metodologi pengumpulan data akan mengakibatkan peneliti memperoleh data yang tidak sesuai dengan standar data yang telah ditetapkan. Adapun macam-macam metode yang harus dilakukan dalam teknik pengumpulan data ini adalah:

1. Observasi

Observasi yang digunakan peneliti ialah observasi non-partisipan, jenis observasi di mana peneliti sebagai pengamat independen dengan mengamati objek penelitian secara langsung tanpa menggunakan perantara atau media lain. Peneliti mencatat, menganalisis, dan selanjutnya dapat membuat kesimpulan tentang perilaku objek yang diamati.

2. Wawancara

Wawancara adalah suatu metode komunikasi yang mempunyai tujuan tertentu. Dialog dilakukan oleh semua pihak yang terlibat. Secara spesifik, individu yang terlibat dalam wawancara adalah orang yang diwawancarai (sumber) dan pewawancara atau penanya (yang melakukan wawancara). Wawancara yang dilakukan bersifat tidak terstruktur. Wawancara tidak terstruktur dicirikan oleh sifatnya yang terbuka dan fleksibel, sehingga cocok untuk investigasi eksplorasi dan studi komprehensif terhadap subjek penelitian. Dengan menggunakan

[44] Sugiyono. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta*, 2016.

metodologi wawancara ini, peneliti dapat memperoleh informasi dan data sebagai berikut:

a) Visi misi Bank Syariah Indonesia
b) Struktur Organisasi Bank Syariah Indonesia
c) Teknologi dan sistem perlindungan data yang digunakan
d) Pemulihan bencana (*Disaster Recovery Plan*)
e) data-data yang lainnya

3. Dokumentasi

Dokumentasi sama pentingnya untuk melakukan wawancara dan observasi. Secara khusus peneliti mencari informasi objek atau variabel yang berupa bahan tertulis seperti catatan, transkrip, buku, koran, majalah, agenda, dan lain sebagainya. Adapun yang dikumpulkan dengan metode ini ialah dokumentasi wawancara, antara peneliti dan pihak bank serta observasi selama peneliti melakukan penelitian dengan adanya dokumentasi ini bisa membuktikan bahwasannya hasil yang diperoleh bukan hasil plagiat melainkan hasil penelitian tersendiri.

E. Analisis Data

Penelitian kualitatif memungkinkan analisis data dilakukan baik di lapangan atau setelah peneliti kembali, sebelum analisis sebenarnya. Analisis data dilakukan bersamaan dengan prosedur pengumpulan data. Proses analisisnya menganut paradigma analisis interaktif yang dikemukakan oleh (Miles dan Huberman). Pendekatan analisis data dapat direpresentasikan secara visual. Penelitian ini menggunakan metode analisis empat tahap, yang

meliputi Pengumpulan Data, Reduksi Data, Penyajian Data, dan Penarikan Kesimpulan[45].

Adapun langkah-langkahnya sebagai berikut :

1. Pengumpulan Data

Catatan lapangan berfungsi sebagai sarana untuk menangkap informasi yang dikumpulkan melalui wawancara, observasi, dan jenis dokumentasi lainnya. Catatan lapangan dibagi menjadi dua bagian berbeda: deskriptif dan reflektif. Catatan deskriptif mengacu pada observasi obyektif yang dilakukan peneliti, mendokumentasikan apa yang dilihat, didengar, dan dialami sendiri tanpa adanya pandangan atau interpretasi subyektif terhadap kejadian yang diamati. Catatan reflektif adalah catatan tertulis yang menangkap persepsi subjektif peneliti, keterangan, pendapat, dan interpretasi tentang hasil yang diperoleh. Catatan-catatan ini berfungsi sebagai bahan berharga untuk mengembangkan strategi pengumpulan data untuk tahap penelitian selanjutnya.

Pengumpulan data yang dilakukan oleh peneliti merupakan suatu cara dalam memperoleh suatu data yang dibutuhkan, langkah awal yang dilakukan peneliti ialah melakukan observasi terlebih dahulu melihat bagaimana kondisi perusahaan setelah dirasa perusahaan tersebut siap dilakukan penelitian maka peneliti membuat pedoman wawancara guna nantinya memudahkan peneliti dalam memperoleh data, setelah membuat pedoman wawancara peneliti melakukan penelitian di Bank Syariah

[45] Salim dan Syahrum. *Metode Penelitian Kualitatif* (Bandung: Citapustaka Media. 2012).

Indonesia (BSI) KCP Kencong Jember, dalam penelitiannya peneliti membedakan data yang dilihat secara langsung dengan data wawancara, dimana hal ini dilakukan agar memperoleh data yang relevan. Setelah proses penelitian dengan cara wawancara selesai maka peneliti juga mengumpulkan data dengan cara dokumentasi beberapa objek atau hal yang bisa memperkuat penelitian.

2. Reduksi Data

Reduksi data mengacu pada proses mengurangi jumlah data dengan menghilangkan informasi yang tidak perlu atau berlebihan. Setelah data dikumpulkan, reduksi data dilakukan untuk mengidentifikasi dan menyimpan informasi yang relevan dan signifikan, menekankan data yang berkontribusi terhadap pemecahan masalah, penemuan, signifikansi, atau menjawab pertanyaan penelitian. Selanjutnya, sederhanakan dan atur secara metodis, sambil menjelaskan aspek-aspek penting dari penemuan tersebut dan signifikansinya. Selama proses reduksi data, hanya data penemuan atau temuan yang relevan langsung dengan topik kajian yang dipadatkan. Pada saat yang sama, data yang tidak berhubungan dengan topik penelitian akan dihapus. Reduksi data adalah suatu proses yang digunakan dalam analisis untuk menyempurnakan, mengklasifikasikan, memandu, dan menghilangkan informasi yang tidak relevan, sekaligus menyusun data sedemikian rupa sehingga memudahkan peneliti dalam menarik kesimpulan.

Terkait hasil yang diperoleh, peneliti menemukan beberapa data atau temuan yang dibutuhkan, pada dasarnya reduksi data merupakan suatu cara atau teknik guna mencari point penting yang dibutuhkan oleh seorang peneliti. Temuan sudah mencakup bagaimana peran standarisasi sistem manejemen keamanan informasi guna meningkatkan ketahanan perbankan Indonesia dan pengembangan pelayanan nasabah terhadap serangan *ransomware*, mulai dalam awal perencanaan dan pengembangan sampai evaluasi perusahaan, bukan hanya terkait ekspansi saja yang ditemukan, namun manfaat yang diberikan adanya peningkatan ketahanan dan evaluasi dampak pelayanan kepada nasabah maupun perusahaan itu sendiri. Dalam reduksi data peneliti hanya memberikan point-point yang diperoleh sedangkan untuk lebih jelasnya peneliti menyajika pada bab pembahasan.

3. Penyajian Data

Data dapat disajikan melalui beberapa cara seperti teks tertulis, gambar visual, grafik, dan tabel. Tujuan penyajian data adalah untuk menggabungkan informasi agar dapat menggambarkan skenario yang ada secara akurat. Untuk memudahkan peneliti memahami temuan penelitian, penting untuk mengembangkan narasi, matriks, atau grafik yang menyajikan informasi atau data secara efektif. Hal ini akan mencegah terjadinya kesulitan dalam memahami penelitian secara keseluruhan atau bagian-bagian tertentu. Dengan pendekatan ini, peneliti dapat mempertahankan otoritas atas data dan menghindari kewalahan oleh kesimpulan-kesimpulan berbasis informasi yang membosankan. Tujuan

pengorganisasian data adalah untuk mencegah peneliti mengambil kesimpulan yang terburu-buru dan bias akibat adanya informasi yang tersebar dan tidak terorganisir. Visualisasi data harus diakui sebagai komponen integral dari analisis data.

4. Penarikan Kesimpulan

Kesimpulan diambil sepanjang proses penelitian, bersamaan dengan proses reduksi data, setelah data diperoleh cukup. Kesimpulan sementara kemudian dibuat, dan kesimpulan akhir dibuat setelah semua data terkumpul sepenuhnya. Sejak awal penyelidikan, para ilmuwan selalu berusaha memastikan pentingnya data yang dikumpulkan. Oleh karena itu, penting untuk mencari pola, tema, korelasi, kesejajaran, kejadian berulang, teori, dan sejenisnya. Hasil aslinya masih bersifat awal, ambigu, dan dipertanyakan. Namun, ketika lebih banyak bukti dikumpulkan dari wawancara, observasi, dan penyelidikan secara keseluruhan, kesimpulannya menjadi lebih pasti. Sepanjang penelitian, kesimpulan ini harus dijelaskan dan divalidasi. Data yang sudah ada kemudian digabungkan menjadi elemen informasi yang, sesuai dengan prinsip holistik, merupakan kategori dan dapat ditafsirkan sendiri. Penggabungan data-data mengenai informasi yang dianggap identik ke dalam satu kategori memungkinkan munculnya kategori-kategori baru dari kategori-kategori yang sudah ada sebelumnya

F. Keabsahan Data

Setelah data diperoleh dan dikumpulkan, peneliti melanjutkan untuk memperbaiki data yang diperoleh dengan melakukan referensi silang dengan data yang diperoleh dari observasi, sebelum melaporkan temuan penelitian. Selanjutnya, data yang diperoleh dari peneliti dapat divalidasi dan dipertanggung jawabkan.[46] Validasi data perlu dilakukan untuk memastikan bahwa data yang diterima benar-benar autentik dan dapat dibuktikan secara ilmiah. Data yang digunakan dalam penelitian ini divalidasi dengan triangulasi sumber dan triangulasi teknologi. Triangulasi adalah metode pengumpulan data yang melibatkan penggabungan beberapa prosedur dan sumber untuk mendapatkan informasi dengan tujuan untuk menilai kredibiltas data hal ini dilakukan dengan memastikan bahwa data berasal dari sumber dan metode yang sama. Misalnya saja data yang dikumpulkan melalui wawancara.[47] Triangulasi sumber adalah metode yang digunakan untuk menilai keandalan data dengan melakukan referensi silang informasi yang diperoleh dari banyak sumber. Hal ini dapat dicapai dengan mengikuti langkah-langkah berikut:

1. Bandingkan data yang diperoleh dari observasi dengan hasil wawancara.
2. Membandingkan pernyataan publik seseorang dengan pernyataan pribadinya.
3. Analisis wacana seputar situasi penelitian dan bandingkan dengan kemajuan aktual yang dicapai selama periode waktu tertentu.

[46] Muri Yusuf, *Metode Penelitian Kuantitatif, Kualitatif, dan Penelitian Gabungan* (Jakarta: Prenadamedia Group, 2014), 395.
[47] Muri Yusuf, 395.

4. Terlibat dalam analisis perbandingan kondisi dan sudut pandang seseorang dengan beragam gagasan dan sudut pandang orang lain.
5. Bandingkan hasil wawancara dengan isi banyak makalah yang relevan.

G. Tahap-Tahap Penelitian

Pada tahapan kali ini peneliti melakukan penelitian dengan berbagai tahap antara lain:[48]

1. Tahap pra lapangan

   Tahap pertama yang dilakukan peneliti adalah mengidentifikasi beberapa permasalahan yang sudah ada sebelumnya, dilanjutkan dengan melakukan pencarian referensi yang relevan. Peneliti menyikapi permasalahan sistem keamanan dengan merumuskan judul "Dampak Sistem Manajemen Keamanan Informasi Dalam Pelayanan Nasabah Terhadap Serangan *Ransomware* pada BSI KCP Kencong Jember."

   Adapun tahap-tahap Pra Lapangan adalah sebagai berikut :

   a) Menentukan lokasi penelitian
   b) Menyusun rancangan penelitian
   c) Mengurus perizinan
   d) Menyiapkan perlengkapan yang dibutuhkan dalam penelitian.

2. Tahap pelaksanaan

   Setelah izin penelitian diperoleh, maka peneliti akan menuju ke lokasi subjek penelitian dan segera mengumpulkan data melalui wawancara

[48] Etta Mamang Sangadji dan Sopiah, *Metodologi Penelitian Pendekatan Praktis Dalam Penelitian* (Yogyakarta: C.V Andi Offset, 2010), 213.

dan observasi guna memperoleh informasi terkait dengan standar sistem manajemen keamanan informasi yang diterapkan oleh BSI Kencong.

3. Tahap penyusunan laporan

Setelah data diperoleh peneliti, barulah dianalisis. Peneliti kemudian melanjutkan dengan penyusunan laporan penelitian. Laporan penelitian selanjutnya disampaikan kepada pembimbing Ibu Ana Pratiwi, S.E.

BAB IV

PENYAJIAN DATA DAN ANALISIS

A. Gambaran Obyek Penelitian

1. Profil BSI Kencong Jember

Nama Perusahaan : PT. Bank Syariah Indonesia KCP Kencong.

Alamat : Jl. Krakatau No. 45, Ponjen, Kencong Kec. Kencong Kabupaten Jember, Jawa Timur 68167

No. Telepon : (0336)321942

Jam Buka : 08.00-15.00 WIB

Situs Website : https;//www.bankbsi.co.id

Jenis Usaha : Lembaga Keuangan Perbankan

2. Sejarah Berdirinya BSI Kencong Jember

Sebelum terjadi penggabungan ketiga Bank Syariah di Indonesia, awalnya masih dalam keadaan status Bank Negara Indonesia (BNI) Syariah KCP Kencong Jember yang pertama didirikan pada 1 April 2013 tepatnya Jl. Krakatau No. 45, Dusun Krajan Desa Kencong Kabupaten Jember, Jawa Timur 68187.

Bank Syariah memainkan peranan penting sebagai fasilitator pada seluruh aktivitas ekonomi dalam ekosistem industri halal. Keberadaan

industri ini dalam perbankan Syariah di Indonesia sendiri telah mengalami peningkatan pengembangan yang signifikandalam kurun tiga dekade ini. Dalam inovasi produk, peningkatan layanan, serta pengembangan jaringan yang menunjukkan trend yang positif dari tahun ke tahun.

Pada tahun 2021 tepatnya pada tanggal 01 Februari pukul 13.00 WIB dan bertepatan dengan 19 Jumadil Akhir 1442 H, menjadi satu entitas yaitu Bank Syariah Indonesia (BSI). Dengan hasil merger anak perusahaan BUMN dibidang perbankan diantaranya Bank Rakyat Indonesia (BRI) Syariah, Bank Negara Indonesia (BNI) Syariah, Bank Syariah Mandiri kini telah bergabung menjadi satu menjadi Bank Syariah Indonesia (BSI). Penggabungan ini akan menyatukan kelebihan dari ketiga Bank Syariah sehingga menghadirkan layanan yang lebih lengkap, memiliki kapasitas permodalan yang lebih baik, serta jangkauan yang lebih luas. Didukung sinergi dengan perusahaan induk (BRI, BNI, Mandiri) serta komitmen pemerintah melalui kementrian BUMN, Bank Syariah Indonesia (BSI) didorong untuk dapat bersaing ditingkat global. Penggabungan ketiga Bank Syariah tersebut merupakan suatu ikhtiar untuk melahirkan Bank Syariah kebanggan umat, yang dapat diharapkan menjadi energi baru dalam pembangunan ekonomi nasional serta berkontribusi terhadap kesejahteraan masyarakat luas. Keberadaan Bank Syariah di Indonesia juga menjadi cerminan wajah perbankan syariah di Indonesia yang sangat modern, memberikan kebaikan bagi segenap alam, dan universal.

3. Visi Misi BSI KCP Kencong Jember

Demi memajukan atau mengembangkan perusahaan dalam mencapai suatu tujuan, perlu adanya acuan sebagai arahan dalam melaksanakan pekerjaan dengan Visi Misi sebagai berikut:

a) Visi Perusahaan

Visi BSI KCP Kencong Jember ada 6 Core Values yaitu AKHLAK:

1. Amanah : Memegang teguh kepercayaan yang diberikan.
2. Kompeten : Terus Belajar dan mengembangkan kapabilitas.
3. Harmonis : Saling Peduli dan menghargai perbedaan.
4. Loyal : Berdedikasi dan mengutamakan kepentingan Bangsa dan Negara.
5. Adaptif : Terus berinovasi dan antusias dalam menggerakkan ataupun menghadapi perubahan.
6. Kolaboratif : Membangun kerjasama yang sinergis.

b) Misi Perusahaan

Misi BSI KCP Kencong ada 18 key Behaviors, diantaranya:

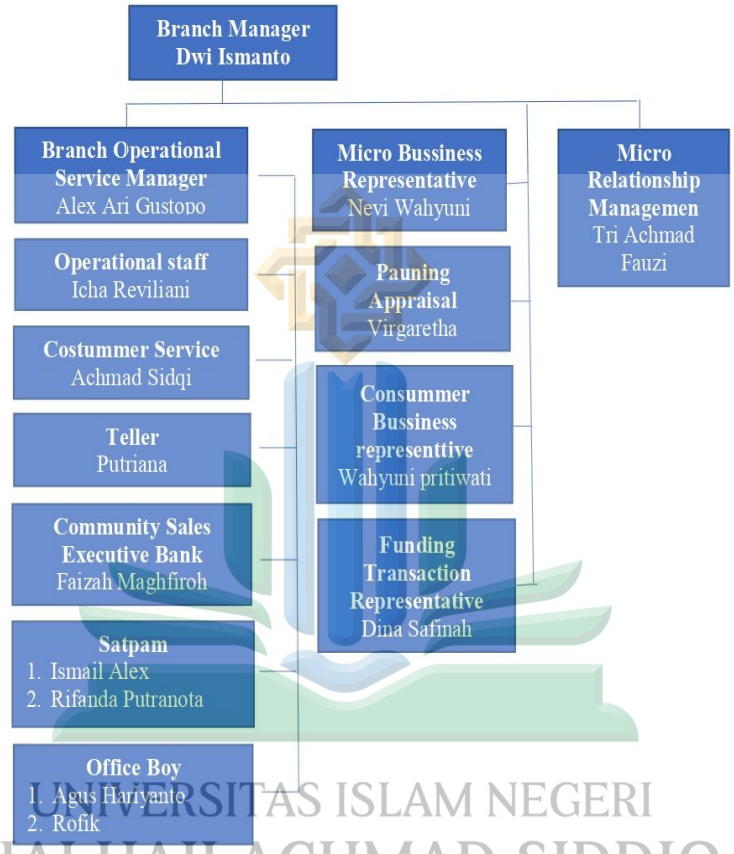
1. Memenuhi janji dan komitmen.
2. Bertanggung jawab atas tugas keputusan dan tindakan yang dilakukan
3. Berpegang teguh pada moral dan etika.
4. Meningkatkan kompetensi diri untuk menjawab tantangan yang selalu berubah.
5. Membantu orang lain belajar.

6. Menyelesaikan tugas dengan kualitas baik.
7. Menghargai setiap orang apapun latar belakangnya.
8. Suka menolong orang lain.
9. Membangun lingkungan kerja yang kondusif.
10. Rela berkorban untuk mencapai tujuan yang lebih besar.
11. Menjaga nama baik sesame karyawan, pimpinan, BUMN, dan Negara.
12. Patuh pada pimpinan sepanjang tidak bertentangan dengan hukum dan etika.
13. Cepat menyesuaikan diri untuk menjadi lebih baik.
14. Terus menerus melakukan perbaikan mengikuti perkembangan teknologi.
15. Bertindak proaktif.
16. Memberi kesempatan kepada berbagai pihak untuk berkontribusi.
17. Terbuka dalam bekerja sama untuk menghasilkan nilai tambah.
18. Menggerakkan pemanfaatan berbagai sumber daya untuk tujuan bersama.

4. Struktur Organisasi BSI KCP Kencong Jember

Struktur organisasi adalah kerangka terstruktur yang mendefinisikan hubungan antara berbagai posisi pekerjaan dan memfasilitasi pelaksanaan kegiatan. Setiap perusahaan berharap bahwa tujuannya akan berhasil dicapai, oleh karena itu, setiap kegiatan usaha

perlu direncanakan dan dilaksanakan secara matang. Jika perusahaan mempunyai manajemen yang terorganisasi dengan baik dan struktur organisasi yang jelas, hasil ini akan tercapai.



Gambar Struktural 4.1
Sumber: wawancara dan dokumentasi
BSI KCP Kencong Jember

Berdasarkan gambar diatas setiap karyawan memiliki tugas masing-masing maka, dapat dijabarkan sebagai berikut:

a. *Branch Manager*

Adapun tugas dan wewenang dari pimpinan cabang pembantu ialah:

1) Mengawasi serta melakukan pengkoordinasian terhadap semua kegiatan operasional yang dikerjakan maupun dilakukan oleh kepegawaian di kantor cabang pembantu syariah.
2) Memimpin jalannya kegiatan pemasaran di kantor cabang agar program pemasaran yang direncanakan bisa dijalankan dengan lancar dan baik.
3) Melakukan kegiatan monitoring pada seluruh kegiatan operasional dalam ruang lingkup perusahaan.
4) Memastikan tercapainya target segmen bisnis pembiayaan (Micro, business banking, consumer), pendanaan, FBI, contribution margin dan laba bersih di kantor cabang pembantu atau dalam ruang lingkup perusahaan.
5) Melakukan pengembangan kegiatan operasional di ruang lingkup kantor cabang yang dipimpin.
6) Mengkoordinasikan dengan pihak terkait untuk melakukan analisis terhadap proses kerja yang ada dan memberikan peningkatan proses kerja di kantor cabang utama, pembantu, ataupun kantor kas supaya dapat berjalan dengan efektif.
7) Melakukan observasi terhadap performa kinerja kepegawaian atau karyawan.

b. *Branch Operational Service Manager*

Tugas dan wewenang Branch Operational Service Manager (BOSM) ialah :

1) Memastikannya telah terlaksananya pelayanan nasabah yang sesuai dengan standar layanan branch office.
2) Membuktikan transaksi harian operasional yang telah sesuai dengan ketentuan SOP ditentukan.
3) Menyusun semua kerangka dan anggaran perusahaan untuk waktu yang akan datang serta berusaha memanifestasikannya.
4) Bertaanggung jawab kepada Branch Manager untuk tugas serta kewajibannya.
5) Memastikan pelaksanaan semua kegiatan pengadministrasian tabungan, deposito, pembiayaan, kearsipan, dan dokumentasi yang sesuai dengan keputusan berlaku.
6) Menandatangani seluruh bukti-bukti pembukuan seperti nisbah tabungan, nisbah deposito, serta nota-nota yang lainnya.
7) Memastikan semua ketersediaan likuiditas yang memadai.

c. *Operational Staff*

1) Memberikan layanan kepada nasabah secara langsung di kantor cabang, seperti pembukaan rekening, pengelolaan dana, dan transaksi lainnya.
2) Membantu nasabah memahami produk dan layanan berbasis syariah yang tersedia di BSI.

3) Memproses transaksi harian nasabah, seperti setoran, penarikan, transfer dana, pencairan pembiayaan, dan transaksi lainnya.
4) Memastikan seluruh transaksi dilakukan dengan akurat dan sesuai dengan kebijakan bank.
5) Mengelola dokumen administrasi terkait aktivitas operasional, seperti formulir pembukaan rekening, dokumen pembiayaan, dan laporan transaksi.
6) Memastikan semua data nasabah dan transaksi tercatat dengan rapi sesuai standar perbankan.
7) Mengelola kas harian di kantor cabang, termasuk perhitungan uang masuk dan keluar.
8) Melakukan rekonsiliasi data transaksi harian untuk memastikan tidak ada selisih dalam laporan keuangan.

d. ***Costummer Service***

Tugas dari Costumer Service sebagai berikut :

1) Memberikan serta menerima permohonan pelayanan nasabah untuk transaksi pembukaan rekening dan penutupan rekeninng.
2) Mengontrol kebenaran serta kelengkapan pengisian formulir.
3) Memberikan penjelasan mengenai produk-produk yang ada pada Bank Syariah Indonesia (BSI) Kantor Cabang Pembantu (KCP) Kencong Jember.

4) Menerima seluruh pertanyaan serta menindaklanjuti keluhan nasabah dan memberikan solusi atas permasalahan yang sedang dihadapi nasabah.
5) Melakukan pengadministrasian deposito seperti aplikasi deposito, bilyet deposito, kartu deposito, kartu deposito, serta nota lainnya yang diperlukan nasabah.
6) Melayani permintaan bilyet giro, buku cek, surat keterangan/referensi bank, dan surat yang lainnya.

e. ***Teller***

Tugas dari Teller sebagai berikut :

1) Melakukan transaksi tunai serta non tunai sesuai dengan ketentuan.
2) Mengelola anggaran serta keuangan sesuai dengan rencana perusahaan.
3) Melayani pelayanan terhadap nasabah atas dasar transaksi penyetoran uang, penarikan, dan transfer.
4) Menjaga kerahasiaan dan keamanan kartu specimen tanda tangan.
5) Mencocokkan atau menyamakan saldo kas yang telah dicatat,
6) merekapitulasi kas ke daftar perincian uang tunai pada setiap tutup buku kas.
7) Menghitung transaksi tunai, melakukan pemeriksaan kas, dan membuat laporan kas harian.

8) Melayani nasabah dalam hal transaksi, jual beli valas dan melayani penukaran uang kecil.
9) Mengawasi seluruh aktivitas transaksi pembukuan pembiayaan di KCP.

B. Penyajian dan Analisis Data

Penyajian merupakan proses mencari, menemukan dan dapat mendeskripsikan kembali secara terus-menerus untuk memvalidkan menguji teori-teori yang sudah ada, melalui prosedur penelitian yang sebelumnya sudah dijelaskan peneliti, baik itu laporan hasil observasi (pengamatan), interview (wawancara) dan perolehan data dari dokumentasi yang diperoleh peneliti selama dilapangan.

Penyajian data dalam penelitian sendiri merupakan laporan tertulis dari peneliti tentang aktivitas-aktivitas penelitian yang dilakukan di lapangan (BSI KCP Kencong Jember). Sehingga data-data yang didapatkan oleh peneliti dituangkan ke dalam laporan ini.

Maka adapun penyajian data dalam hal ini adalah sebagai berikut:

1. Penerapan Sistem Manajemen Keamanan Informasi Terhadap Pelayanan Nasabah dalam Serangan *Ransomware* pada BSI KCP Kencong Jember.

Sistem Manajemen Keamanan Informasi (SMKI), atau Information Security Management System (ISMS), adalah suatu standar internasional yang mengatur pengelolaan risiko keamanan informasi dalam sebuah organisasi. SMKI memberikan kerangka kerja dan pedoman sistematis

untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi melalui penerapan proses manajemen risiko[49]

Dalam perannya, penerapan konsep ini secara aktif mengimplementasikan langkah-langkah yang relevan untuk mencapai tujuan keamanan informasi dalam perusahaan. Namun, proses ini sering kali menghadapi tantangan sosial dan etika, seperti isu privasi, keamanan, dan aksesibilitas data. Jika tidak dilakukan secara etis, penerapan tersebut dapat melanggar privasi individu dan menyebabkan penyalahgunaan data pribadi. Bahkan, hal ini masih saja di anggap sepele oleh beberapa pihak. Selain itu, serangan siber seperti *ransomware* dapat mengancam integritas dan kerahasiaan data. Oleh karena itu, aksesibilitas sistem harus diatur secara ketat untuk memastikan hanya pihak berwenang yang memiliki akses, sehingga keamanan sistem tetap terjaga.

Hal tersebut diperkuat oleh bapak Alex Ari Gustopo selaku *Branch Operational and Service Manager* di BSI KCP Kencong Jember mengatakan bahwa:

> "Standar Sistem Manajemen Keamanan Informasi dikelola oleh tim IT pusat, akan tetapi semenjak terjadinya serangan *ransomware* tersebut keamanan akses teknologi di BSI terutama KCP Kencong semakin ketat dalam mengakases komputer. Segala aktivitas yang berhubungan dengan sistem seperti komputer atau laptop yang digunakan oleh tim operasional memerlukan *password* keamanan khusus yang telah disarankan oleh tim IT pusat, biasanya disebut dengan CISCO dalam mengelola keamanan sebagai *security system*."[50]

[49] https://www.sucofindo.co.id/layanan-jasa/iso-27001-2/
[50] Alex Ari Gustopo. *Wawancara* BSI KCP Kencong Jember, 11 Desember 2024.

Hal tersebut juga disampaikan oleh bapak Dwi Ismanto selaku *Branch Manager* di BSI KCP Kencong dengan memberikan pendapat bahwa:

> "Pada saat ini BSI sedang merekrut banyak SDM untuk digitalisasi sebagai bentuk antisipasi serangan *ransomware* yang telah terjadi sebelumnya. *System* hanya berasal dari pusat, kita hanya sebagai pengguna. Dalam penggunaan sistem, ada beberapa hal yang boleh dilakukan dan tidak boleh dilakukan. Hal tersebut, dijadikan pedoman atau kebijakan dalam pemakaian sistem oleh pengguna karena, bisa jadi penyebab utama dari serangan *ransomware* itu diduga dari pemakaian sistem yang kurang aman. Seperti contoh menggunakan komputer dengan windows 2007 kebawah dan menggunakan *flashdisck* maka, hal tersebut bisa langsung di *claude* oleh pusat."[51]

Selain itu pernyataan serupa dengan ibu Icha Reviliani selaku *Operational Staff* di BSI KCP Kencong Jember juga menjelaskan bahwa:

> "Semua komputer berasal dari pusat. Apabila ada penyelewengan dalam penggunaan *system* maka, kantor pusat bisa langsung memantau hal tersebut dan bisa langsung di *block* kan sistemnya. Akses penggunaan sistem hanya bisa digunakan dalam jam kerja. Bank BSI memiliki web sendiri yang didalamnya berisi perangkat lunak (*software*) seperti *word, excel, office* dll. *System* di input langsung dari email BSI sendiri, setiap komputer memiliki nama-nama karyawan masing-masing sesuai dengan posisi karyawan, hal tersebut digunakan dalam mencegah terjadinya serangan *ransomware* dalam menjaga data nasabah sehingga kita dapat mengembal hati nasabah kembali agar mereka percaya dam tidak khawatir lagi dalam masalah yang terjadi sebelumnya."[52]

Selain meningkatkan kualitas keamanan dalam segi teknologi dan layanan terhadap nasabah, perusahaan juga perlu memastikan karyawan dapat mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku melalui pengendalian

[51] Dwi Ismanto. *Wawancara* BSI KCP Kencong Jember, 10 Desember 2024.
[52] Icha reviliani. *Wawancara* BSI KCP Kencong Jember, 13 Desember 2024.

risiko serta pelatihan terhadap kesadaran karyawan akan terjadi serangan *ransomware*.

Dalam hal ini di tanggapi oleh bapak Achmad Sidqi selaku *Custommer Service Representative* bahwa:

> "Terkait pelatihan khusus karyawan dalam pengendalian risiko terjadinya serangan *ransomware* atau kesadaran karyawan di BSI Kencong KCP Jember itu tidak ada, semua kebijakan ataupun aturan sudah diurus oleh tim IT yang hanya ada dipusat. Sebagai bentuk evaluasi dari karyawan hanya ada pembaruan sistem, jadi sistem yang lama dialihkan ke sistem yang baru, seiring perkembangannya mulai dimunculkan sistem yang baru. Dalam peralihan sistem baru ada *zoom* pelatihan untuk mempermudah penggunaan dalam fitur barunya di sistem tersebut. Hal tersebut sangat efektif dan sudah sesuai dengan standar sistem keamanan yang telah diberikan oleh pusat karena aksesnya bisa lebih cepat untuk menangani permasalahan nasabah."[53]

Berdasarkan hasil wawancara dan observasi, peneliti menemukan bahwa BSI KCP Kencong Jember telah menerapkan beberapa peran Sistem Manajemen Keamanan Informasi dengan mematuhi aturan dan kebijakan dari kantor pusat. Untuk mengatasi serangan *ransomware*, BSI merekrut banyak SDM yang ahli dalam bidang digitalisasi guna meningkatkan sistem keamanannya. Langkah ini sangat penting karena sistem keamanan yang kuat berdampak langsung pada kualitas pelayanan nasabah.

Tim IT Bank BSI yang dikenal sebagai CISCO bertugas memantau dan mengamankan semua akses yang digunakan oleh karyawan. Setelah serangan *ransomware* terjadi, BSI memperketat pengawasan sistem keamanan dengan memperbarui beberapa fitur yang telah ada. Selain itu,

[53] Achmad Sidqi. *Wawancara* BSI KCP Kencong Jember, 16 Desember 2024.

semua aspek yang berhubungan dengan digitalisasi hanya dapat diakses selama jam kerja. Setiap karyawan diberikan akses khusus untuk masuk ke situs *web* perusahaan, sehingga aktivitas mereka dapat dipantau dengan lebih efektif.

2. Dampak Sistem Manajemen Keamanan Informasi Terhadap Pelayanan Nasabah dalam Serangan *Ransomware* pada BSI KCP Kencong Jember.

Dampak dalam sebuah perusahaan merujuk pada konsekuensi atau pengaruh yang ditimbulkan oleh suatu peristiwa, keputusan, atau kondisi tertentu terhadap berbagai aspek operasional, finansial, dan strategis perusahaan. Dampak ini bisa bersifat positif, seperti peningkatan keuntungan atau efisiensi, maupun negatif, seperti kerugian finansial, gangguan operasional, atau penurunan reputasi. Dalam konteks manajemen, memahami dan mengelola dampak sangat penting untuk memastikan keberlanjutan bisnis, terutama ketika perusahaan menghadapi risiko atau tantangan, seperti serangan siber, perubahan regulasi, atau fluktuasi pasar. Dampak yang tidak dikelola dengan baik dapat mengancam stabilitas perusahaan dan mengurangi kepercayaan stakeholder, termasuk pelanggan, karyawan, dan mitra bisnis. Oleh karena itu, identifikasi, analisis, dan mitigasi dampak menjadi bagian integral dari strategi manajemen risiko perusahaan.

Dampak dari serangan *ransomware* yang terjadi pada BSI ini sangat meresahkan nasabah terutama pada nasabah BSI KCP Kencong

Jember. Hal ini sebagaimana disampaikan oleh Ibu Putriana selaku *Teller* di BSI KCP Kencong Jember, bahwa:

> "Saat sistem terganggu, kami harus melayani nasabah secara manual, seperti mencatat transaksi secara tertulis. Ini tentu memperlambat proses, dan beberapa nasabah merasa tidak puas karena waktu tunggu yang lebih lama. Namun, kami terus berusaha menjelaskan situasi dengan sopan dan memberikan pelayanan terbaik yang kami bisa."[54]

Bapak Achmad Sidqi selaku *Custommer Service* juga menambahkan pernyataan mengenai dampak dari serangan *ransomware* terhadap pelayanan nasabah, ia mengatakan bahwa:

> "Banyak nasabah yang khawatir tentang keamanan data mereka, terutama setelah mendengar berita tentang *ransomware*. Kami memberikan penjelasan secara rinci bahwa data mereka tetap aman berkat sistem *enkripsi* dan *backup* yang diterapkan. Kami juga membuka *hotline* khusus untuk menangani keluhan secara langsung dan memberikan solusi alternatif, seperti transaksi manual."[55]

Lebih dari itu bapak Dwi Ismanto selaku *Branch Manager* BSI KCP Kencong juga menambahkan pernyataan, ia mengatakan bahwa:

> "Serangan *ransomware* ini sangat mengganggu operasional kami. Sistem inti sempat lumpuh sehingga beberapa layanan tidak bisa berjalan, seperti transfer antar bank dan akses mobile banking. Kami berusaha memprioritaskan pelayanan manual untuk mengurangi keluhan nasabah. Selain itu, kami langsung berkoordinasi dengan kantor pusat untuk memastikan langkah mitigasi berjalan dengan cepat. Beberapa langkah mitigasi, seperti pemutusan jaringan dari pusat, proses *recovery* data dari cadangan, dan peningkatan lapisan *enkripsi*, membutuhkan waktu dan koordinasi yang lebih baik agar dampak terhadap pelayanan dapat benar-benar diminimalkan. Selain itu, kantor cabang BSI ini tidak memiliki tim IT khusus, sehingga seluruh penanganan dan keputusan terkait keamanan informasi sepenuhnya menunggu arahan dari pusat. Kami sebagai kantor cabang juga belum mendapatkan pelatihan atau edukasi terkait

[54] Putriana. *Wawancara* BSI KCP Kencong. 17 Desember 2024.
[55] Achmad Sidqi. *Wawancara* BSI KCP Kencong. 16 Desember 2024.

sistem manajemen keamanan informasi, sehingga pengelolaan keamanan masih terpusat tanpa ada kemampuan lokal untuk mengidentifikasi atau menangani ancaman secara mandiri.[56]"

Adapun tanggapan dari Ibu Rani Maulidasari selaku nasabah terkait hal tersebut:

"Sebagai nasabah, kami merasa sangat khawatir tentang keamanan data pribadi kami, terutama setelah mendengar banyak berita mengenai serangan *ransomware* yang mengancam sektor perbankan. Kami takut data kami bisa bocor dan disalahgunakan, yang tentunya akan merugikan kami secara finansial dan privasi. Meskipun pihak bank telah menjelaskan bahwa mereka menerapkan sistem *enkripsi* dan *backup* rutin untuk melindungi data kami, serta membuka *hotline* khusus untuk menangani keluhan, kami tetap merasa cemas. Kami menghargai upaya tersebut, tetapi tetap berharap agar ada langkah-langkah yang lebih konkret dan menyeluruh untuk memastikan keamanan layanan perbankan. Selain itu, meskipun ada solusi alternatif seperti transaksi manual, kami ingin agar semua layanan dapat berjalan dengan aman dan lancar tanpa gangguan.[57]"

Lebih dari itu Ibu Elsa selaku nasabah BSI KCP Kencong juga menambahkan pernyataan, ia mengatakan bahwa:

"Sebagai nasabah, kami sangat khawatir tentang keamanan data pribadi kami, terutama setelah mendengar banyak berita mengenai serangan *ransomware* yang semakin marak. Meskipun pihak bank telah menjelaskan bahwa mereka menerapkan sistem *enkripsi* dan *backup* rutin, rasa cemas kami tidak kunjung reda. Kami merasa rentan dan takut data sensitif kami bisa jatuh ke tangan yang salah, yang dapat merugikan kami secara finansial dan mengancam privasi kami. Meskipun ada *hotline* khusus untuk menangani keluhan, kami merasa perlu lebih dari sekadar penjelasan; kami ingin melihat tindakan nyata dan jaminan yang lebih kuat dari pihak bank. Keberadaan solusi alternatif seperti transaksi manual juga tidak cukup untuk menenangkan pikiran kami. Kami berharap pihak bank dapat segera mengambil langkah-langkah tambahan untuk meningkatkan keamanan dan melindungi data kami dengan lebih baik, agar kami bisa merasa aman dalam menggunakan layanan perbankan.[58]"

[56] Dwi Ismanto. *Wawancara* BSI KCP Kencong Jember, 10 Desember 2024.
[57] Elsa. *Wawancara BSI KCP Kencong Jember*, 20 Desember 2024.
[58] Rani Maulidasari. *Wawancara BSI KCP Kencong Jember*, 20 Desember 2024.

Berdasarkan hasil wawancara, serangan *ransomware* yang terjadi di BSI KCP Kencong memberikan dampak signifikan terhadap pelayanan nasabah. Sistem manajemen keamanan informasi (SMKI) berbasis ISO 27001 yang diterapkan oleh BSI membantu dalam langkah mitigasi, seperti pemutusan jaringan, pemulihan data dari cadangan yang aman, dan peningkatan enkripsi sistem. Namun, tantangan tetap ada mengingat kantor cabang tidak memiliki tim IT khusus dan hanya mengandalkan arahan dari pusat untuk menangani ancaman siber. Selain itu, belum adanya pelatihan atau edukasi terkait SMKI di tingkat cabang membuat proses penanganan ancaman cenderung lambat dan terpusat.

Dampak dari kondisi ini terlihat pada terganggunya layanan nasabah, seperti keterlambatan transaksi dan kekhawatiran terhadap keamanan data. Meskipun upaya mitigasi telah dilakukan, keterbatasan sumber daya lokal di cabang membuat dampak terhadap pelayanan nasabah tidak sepenuhnya dapat diminimalkan. Hal ini menunjukkan pentingnya peningkatan kapasitas di tingkat cabang, termasuk pelatihan SMKI dan pengadaan tim IT lokal, untuk mempercepat respons terhadap ancaman keamanan informasi dan meningkatkan kualitas pelayanan kepada nasabah.

C. Pembahasan Temuan

Pengumpulan data dilakukan dengan menggunakan teknik penelitian meliputi observasi, wawancara, dan dokumentasi, semuanya terfokus pada pembahasan topik yang ada. Dalam sub bab ini akan dijelaskan beberapa

uraian pembahasan yang sesuai dengan hasil penelitian, sehingga pembahasan ini peneliti akan menjelaskan hasil penelitian, dengan teori yang telah dijelaskan pada bab sebelumnya. Data-data yang diperoleh dari pengamatan wawancara mendalam serta dokumentasi sebagaimana telah peneliti deskripsikan pada analisis dan kualitatif yang kemudian diidentifikasi agar sesuai dengan tujuan yang diharapkan. Pengamatan wawancara telah dilaksanakan yaitu dengan mengumpulkan data mengenai dampak sistem manajemen keamanan informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember. Berikut adalah penjelasan dari pembahasan yang akan dikomunikasikan dengan teori-teori yang dijadikan sebagai landasan oleh peneliti dalam penelitian.

1. **Penerapan Standar Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember**

   Penerapan sistem manajemen keamanan informasi merupakan sebuah tantangan bagi perusahaan, terutama jika perusahaan tidak siap untuk menghadapi perubahan yang dibutuhkan dalam hal budaya, sumber daya dan teknologi.[59] Sesuai dengan teori yang ada dalam buku Tika Ulfianinda, standar sistem manajemen keamanan informasi melibatkan upaya untuk melindungi informasi dari ancaman, gangguan, atau akses yang tidak sah yang dapat mengganggu integritas, kerahasiaan, atau ketersediaan informasi tersebut. Ini mencakup pembuatan kebijakan yang

[59] Ani Yoraeni, Popon Handayani, Syifa Nur Rakhmah,dkk. *Sistem Informasi Manajemen*.2023.

mengatur penggunaan dan akses informasi, penerapan prosedur untuk mengelola risiko keamanan, dan penggunaan sistem teknologi informasi yang sesuai untuk melindungi data dari akses yang tidak sah, modifikasi, atau kehilangan. Dalam penerapannya standar sistem manajemen keamanan informasi memiliki tujuan yang sesuai dengan menjaga keamanan data pribadi nasabah dan dapat meningkatkan kualitas pelayanan nasabah, yang sering disebut sebagai Triad CIA.

Triad CIA adalah model yang memandu kebijakan keamanan informasi dalam suatu organisasi, dengan tiga aspek utama: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). Tujuan utama Triad CIA adalah untuk memastikan keamanan informasi yang kuat dan efektif. Kerahasiaan berfokus pada pencegahan pengungkapan informasi sensitif kepada pihak yang tidak berwenang[60]. Integritas memastikan bahwa informasi tetap tidak diubah atau dimanipulasi oleh pihak yang tidak berwenang. Ketersediaan berarti bahwa informasi atau sumber daya harus tersedia dan dapat diakses oleh pihak yang berwenang ketika dibutuhkan.[61] Penerapan Triad CIA membantu melindungi aset berharga perusahaan, mematuhi peraturan, meningkatkan kepercayaan pelanggan, dan meningkatkan produktivitas. Model ini membantu dalam mengembangkan sistem klasifikasi data, mengelola izin akses, dan melindungi aset penting. Triad CIA juga

[60] https://ekualindo.com/prinsip-keamanan-informasi-iso-27001/
[61] https://www.dewaweb.com/blog/web-app-security-cia-triad/

berperan dalam mengidentifikasi potensi target serangan siber dan menerapkan kebijakan untuk melindungi aset dari ancaman[62].

Berdasarkan hasil temuan, penerapan Sistem Manajemen Keamanan Informasi (SMKI) di BSI KCP Kencong Jember telah berjalan dengan mengacu pada kebijakan dari kantor pusat saja, meskipun beberapa aspek masih perlu penguatan. Dalam kaitannya dengan indikator SMKI, Bank Syariah Indonesia telah memenuhi beberapa elemen yang sesuai dengan teori Triad CIA, dalam kerahasiaan (*confidentiality*) teori ini merujuk pada perlindungan informasi dari akses yang tidak jelas, hal ini hanya dapat diakses oleh orang yang berwenang dan memiliki akses ke informasi yang sensitif atau rahasia, dibuktikan dengan penguatan tim IT yang disebut sebagai CISCO pada bank BSI KCP Kencong berfungsi untuk bertanggung jawab dalam memantau dan mengamankan semua akses digital yang digunakan oleh karyawan, termasuk situs *web* dan perangkat internal. CISCO adalah perusahaan multinasional terkemuka dalam industri jaringan komputer, yang juga merupakan salah satu produsen perangkat jaringan terbesar di dunia. Perusahaan ini memproduksi *software* dan *hardware* yang berkaitan langsung dengan jaringan komputer, serta turut berkontribusi dalam bidang pendidikan melalui program *Cisco Networking Academy* yang bertujuan untuk mengembangkan keterampilan di bidang *networking*[63]. Dalam penggunaannya, Cisco menjadi alat yang digunakan dalam jaringan area

[62] https://student-activity.binus.ac.id/csc/2022/08/cia-triad/
[63] Laiqa Ayesa, *Cisco Adalah: Pengertian, Sejarah, Fungsi, Produk, dan Sertifikasinya*, 2024. https://myedusolve.com/id/blog/cisco-adalah-pengertian-sejarah-fungsi-produk-dan-sertifikasinya

luas atau *Wide Area Network* (WAN). Melalui penggunaan *router* CISCO, informasi dapat dikirimkan ke berbagai alamat yang berjauhan, serta ke jaringan komputer yang lainnya. Demi menjaga integritas (*integrity*) perusahaan dan kualitas pelayanan nasabah BSI KCP Kencong mendapat pengawasan ketat dari CISCO terhadap akses digital karyawan pada teknologi yang sedang digunakan, dan pembatasan akses hanya pada jam kerja sehingga, bisa menjamin informasi tidak dapat diubah, dimodifikasi, atau rusak serta data dapat dipastikan tetap akurat, dan konsisten. *Integrity* pada bank BSI KCP Kencong juga ditingkatkan dengan pembaruan fitur keamanan oleh CISCO, yang bertujuan untuk menjaga keandalan dan keutuhan data.

Temuan penelitian juga mengungkapkan bahwa setelah terjadinya serangan *ransomware* dapat melumpuhkan sebagian sistem Bank Syariah Indonesia (BSI), termasuk yang berdampak pada operasional KCP Kencong, prinsip *availability* dalam Triad CIA jelas terganggu. Layanan yang seharusnya tersedia bagi nasabah menjadi sulit diakses, menyebabkan ketidakpastian dan potensi kepanikan. Dalam situasi ini, BSI KCP Kencong mengambil langkah untuk berkomunikasi dengan nasabah, meskipun informasinya terbatas, dengan tujuan utama meredakan kepanikan dan memberikan kepastian bahwa bank sedang berupaya memulihkan layanan secepat mungkin.

2. Dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan *ransomware* pada BSI KCP Kencong Jember.

Dampak merupakan konsekuensi atau akibat yang ditimbulkan oleh suatu kejadian, tindakan, atau kondisi tertentu, baik itu positif maupun negatif. Dampak dapat dirasakan oleh individu, kelompok, organisasi, atau lingkungan secara langsung maupun tidak langsung. Dalam konteks penelitian atau evaluasi, dampak sering kali dianalisis untuk memahami sejauh mana suatu peristiwa atau kebijakan memengaruhi aspek-aspek tertentu.[64] Berdasarkan teori Standar Manajemen Keamanan Informasi, dampak negatif akan muncul apabila peran tidak diterapkan, salah satunya kehilangan data sensitif. Tidak mengikuti prosedur SMKI dapat menyebabkan kebocoran atau kehilangan data sensitif pelanggan, informasi keuangan, atau rahasia dagang perusahaan. Hal ini dapat mengakibatkan kerugian finansial, tuntutan hukum, kerusakan reputasi perusahaan, dan kualitas pelayanan nasabah menurun.

Berdasarkan hasil temuan penelitian, serangan *ransomware* yang terjadi di BSI KCP Kencong memberikan dampak besar terhadap kualitas pelayanan nasabah. Hal ini teridentifikasi melalui terganggunya proses transaksi dan munculnya kekhawatiran dari nasabah terkait keamanan data mereka. Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO

[64] Menurut KBBI. *Arti kata dampak.* kbbi.co.id. 2023.

27001 yang diterapkan oleh BSI telah membantu dalam langkah-langkah mitigasi, seperti pemutusan jaringan, pemulihan data dari cadangan aman, dan peningkatan enkripsi sistem. Namun, temuan ini juga mengungkapkan kelemahan penting, yaitu kurangnya pelatihan dan edukasi terkait SMKI di BSI KCP Kencong, yang berdampak pada lambatnya respons terhadap ancaman siber.

Dalam teori SMKI, pelatihan dan edukasi karyawan adalah salah satu elemen kunci yang masuk dalam aspek pengelolaan sumber daya manusia. Pelatihan berperan penting untuk memastikan setiap karyawan memahami perannya dalam menjaga keamanan informasi dan mampu merespons ancaman secara cepat dan efektif. Kurangnya pelatihan di tingkat cabang pada BSI KCP Kencong menunjukkan adanya celah dalam implementasi SMKI, terutama dalam membangun budaya kesadaran keamanan informasi (*security awareness*). Selain itu, ketiadaan tim IT lokal di cabang memperparah situasi, karena kantor cabang sepenuhnya bergantung pada arahan dari kantor pusat untuk menangani ancaman keamanan.

Kondisi ini menunjukkan dampak dalam peran pentingnya peningkatan kapasitas di tingkat cabang melalui program pelatihan SMKI secara rutin dan penyediaan tim IT lokal. Dengan demikian, cabang dapat lebih mandiri dalam merespons ancaman keamanan informasi, mengurangi ketergantungan pada pusat, dan meminimalkan dampak serangan siber terhadap pelayanan nasabah. Upaya ini sejalan dengan prinsip-prinsip

SMKI yang menekankan pentingnya penguatan sumber daya manusia untuk mendukung integritas, kerahasiaan, dan ketersediaan informasi secara menyeluruh.

BAB V

PENUTUP

A. Kesimpulan

Setelah memberikan pengantar dan gambaran secara terpadu dalam menganalisis beberapa permasalahan yang diteliti, maka dapat ditarik kesimpulan sebagai berikut:

1. Penerapan Sistem Manajemen Keamanan Informasi (SMKI) di BSI KCP Kencong Jember telah dilakukan dengan mengacu pada kebijakan kantor pusat, namun masih memerlukan penguatan di beberapa aspek. Dalam menghadapi serangan *ransomware,* BSI mengandalkan tim IT internal yang dikenal sebagai CISCO untuk memantau dan mengamankan seluruh akses digital. Keberadaan tim ini mencerminkan penerapan teori Triad CIA (*Confidentiality, Integrity, Availability*) dengan menjaga kerahasiaan data melalui akses khusus, meningkatkan keamanan data melalui pembaruan fitur keamanan, serta memastikan ketersediaan sistem selama jam kerja.
2. Serangan *ransomware* yang terjadi di BSI KCP Kencong memberikan dampak besar terhadap kualitas pelayanan nasabah, seperti terganggunya transaksi dan meningkatnya kekhawatiran nasabah terkait keamanan data. Meskipun penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO 27001 telah membantu dalam mitigasi ancaman, temuan ini mengungkapkan kelemahan penting, yaitu kurangnya pelatihan dan edukasi

terkait SMKI di tingkat cabang, yang menghambat respons cepat terhadap ancaman siber.

B. Saran

Berdasarkan hasil penelitian yang telah penulis sajikan, maka penulis menyampaikan mengenai saran yang diharapkan dapat memberikan manfaat bagi pihak pihak yang terkait atas hasil penelitian ini. Adapun saran tersebut yaitu:

1. Meningkatan infrastruktur keamanan yang berkelanjutan; BSI KCP Kencong harus fokus pada penguatan infrastruktur keamanan informasi dengan melakukan pembaruan sistem secara rutin, memperkuat enkripsi, serta meningkatkan sistem pemulihan data (*disaster recovery*) yang lebih tangguh. Dengan serangan *ransomware* yang telah terjadi, penting bagi cabang untuk memastikan bahwa sistem yang ada dapat melindungi data nasabah secara maksimal dan dapat pulih dengan cepat setelah insiden. Selain itu, penilaian risiko keamanan harus dilakukan secara berkala untuk mengidentifikasi celah yang mungkin ada dalam sistem keamanan yang ada.
2. Menyedikan pelatihan keamanan siber yang mendalam untuk semua karyawan; Pemberian pelatihan keamanan siber yang mendalam dan berkala bagi seluruh karyawan cabang merupakan langkah penting. Pelatihan ini tidak hanya mengajarkan prosedur dasar SMKI, tetapi juga memperkuat pemahaman tentang potensi ancaman yang berkembang, seperti ransomware, serta bagaimana cara menghadapi dan mencegahnya.

Dengan pelatihan yang lebih mendalam, setiap karyawan dapat menjadi garda terdepan dalam mendeteksi dan merespons ancaman sebelum menimbulkan dampak besar terhadap pelayanan nasabah dan keamanan data.

DAFTAR PUSTAKA

A.S Moenir, *Manajemen Pelayanan Umum di Indonesia* (Bandung: PT. Bumi Aksara, 2008), 27.

Abd. Shomad, Trisadini P. Usanti, *Hukum Perbankan* (Depok: Kencana, 2017), 17.

Abdul Wadud Nafis. *Bank Syariah Teori dan Praktek.*

Abdullah, Muhammad Subhan. *Perkembangan Terbaru Dalam Keamanan Siber, Ancaman yang Diidentifikasi Dan Upaya Pencegahan*. 2023.

Achmad Sidqi. *Wawancara BSI KCP Kencong Jember*, 16 Desember 2024.

Afrianto, I dan E. B. Setiawan, *Kajian Virtual Private Network (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer* (Studi Kasus Jaringan Komputer Unikom). 2021.

Alex Ari Gustopo. *Wawancara BSI KCP Kencong Jember*, 11 Desember 2024.

Anggana, N. D. (2024, May 14). *CISO: Pengertian, Peran, dan Tanggung Jawab.* Widya Security. https://widyasecurity.com/2024/05/15/ciso-pengertian-peran-dan-tanggung-jawab/

Ani Yoraeni, Popon Handayani, Syifa Nur Rakhmah,dkk. *Sistem Informasi Manajemen*. 2023.

Budi, Eko. *Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0*. 2021.

Budi. E, D. Wira, dan A. Infantono: *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0*. 2021.

Calder, A., & Watkins, S. (2008*). IT Governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page.

Dwi Ismanto. *Wawancara BSI KCP Kencong Jember*, 10 Desember 2024.

Dwi Perwitasari Wiryaningtyas, "Pengaruh Keputusan Nasabah dalam Pengambilan Kredit pada Bank Kredit Desa Kabupaten Jember", *Jurnal Ekonomi dan Bisnis Growth*, 14. No. 2 (2016), 50.

Ericka, J dan W. Prakasa, *Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi*, 2020.

Etta Mamang Sangadji dan Sopiah, *Metodologi Penelitian Pendekatan Praktis Dalam Penelitian* (Yogyakarta: C.V Andi Offset, 2010), 213.

Falah jamalul, *Mujahid. Al-Quran dan Etika Digital Literacy: Mitigasi CyberCrime di Era Transformasi Digital*. 2023.

Fandy Tjiptono, *Service, Quality and Satisfaction* (Yogyakarta: ANDI, 2014) 13.

Freddy Rangkuti, *Customer Care Excellent Meningkatkan Kinerja Perusahaan Melalui Pelayanan Prima Plus Analisis Kasus Jasa Raharja* (Jakarta: Gramedia Pustaka Utama, 2017) 46.

Hardiansyah, Z. (2022, August 2). *Siapa Saja yang Wajib Daftar PSE di Indonesia? Ini Rincian Kategorinya. Kompas.* https://tekno.kompas.com/read/2022/08/02/12150087/siapa-saja.

Hersa Farida Quroaini. *Analisis Implementasi Aplikasi BSI Mobile dalam meningkatkan kualitas pelayanan di BSI KCP Jember Balung*.

https://ekualindo.com/prinsip-keamanan-informasi-iso-27001/

https://student-activity.binus.ac.id/csc/2022/08/cia-triad/

https://www.bbc.com/indonesia/articles/cn01gdr7eero

https://www.dewaweb.com/blog/web-app-security-cia-triad/

Icha reviliani. *Wawancara BSI KCP Kencong Jember*, 13 Desember 2024.

Irfansyah, A. (2023a, October 18). *Apa Peran CISO dalam implementasi ISO 27001?* Eduparx Blog. https://eduparx.id/blog/insight/cyber-security/peran-ciso-dalam-implementasi-iso-27001/

Jauhary, H., Pratiwi2, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review. *Media Jurnal Informatika*, 14(1), 43. https://doi.org/10.35194/mji.v14i1.1581.

John Cresswell, *Research Design: Qualitative, Quantitative, and Mixed MethodsApproaches* (California, 2014).

Josefine, M. (2023, June 23). *Mengenal Apa Itu PSE dan Pentingnya Bagi Perusahaan. Kontrak Hukum*. https://kontrakhukum.com/article/pse-adalah/

Kamelia, R., & Raditya, I. N. (2022, July 20). *Aturan PSE Kominfo, Dasar Hukum, Jenis, & Cara serta Syarat Daftar*. Tirto.id. https://tirto.id/aturan-pse-kominfo-dasar-hukum-jenis-cara-serta-syarat-daftar-gucL

Kementerian Agama RI, *Al-Quran Transliterasi Per Kata dan Terjemahan Per Kata*., 17.

Khamdan Rifa'i. *Kepuasan Konsumen*.

M. Nur Rianto Al Arif, *Dasar - Dasar Pemasaran Bank Syariah* (Bandung: Alfabeta, 2016) 213.

Maharani, Elya Rosa. *Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran*. 2024.

Marinu Waruwu, "Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif Dan Metode Penelitian Kombinasi (Mixed Method*)," Jurnal Pendidikan Tambusai* 7, no. 1 (2023): 2896–2910.

Menurut KBBI. *Arti kata dampak*. kbbi.co.id. 2023.

Mike Napizahny, *Apa itu Ransomware?*, 2022.

Mislah Hayati Nasution, 'Faktor-Faktor Yang Mempengaruhi Minat Nasabah terhadap Internet Banking', *Jurnal Nisbah*, 1.1 (2015), 65.

Moleong, 2010.

Muhammad Ramdhan, *Metode Penelitian* (Surabaya: Cipta Media Nusantara, 2021).

Muni, Abdul. Kasmawati. Agung Ramadhan dkk. *Kriptografi untuk keamanan Sistem Informasi*. 2024 (99).

Muri Yusuf, *Metode Penelitian Kuantitatif, Kualitatif, dan Penelitian Gabungan* (Jakarta: Prenadamedia Group, 2014), 395.

Muslim. *Analisis Keamanan Siber (Cyber Security) Dalam Era Digital "Tantangan Dan Strategi Pengamanan*". 2024.

Mustafa Kamal Rokan, *Bisnis Ala Nabi: Teladan Rasulullah SAW dalam Berbisnis* (Yogyakarta: Bunyan, 2013), 12.

Nashar, *Kualitas Pelayanan Akan Meningkatkan Kepercayaan Masyarakat* (Pamekasan: Duta Media Publishing, 2020) 39.

Nikmatul Masruroh, *Literasi Sistem Tranformasi Digital Dalam Optimalisasi Layanan Nasabah*.

Nurul Widyawati, *Metodologi Penelitian Kualitatif*.

Pengaruh *Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran. (n.d.)*.

Putra, Rifqi Galuh, Achmad Fauzi, Ery Teguh Prasetyo, dkk. *Pentingnya Manajemen Security di Era Digitalisasi*. 2023.

Putriana. *Wawancara BSI KCP Kencong*. 17 Desember 2024.

Rahman, Abdul*: Urgensi Penerapan Iso 27001 Pada Perbankan Syariah Di Indonesia*. 2024

Rakhmadi Rahman, Made Suci Arianti, Abdul Hadi, dkk. *Keamanan Jaringan Komputer*. 2024.

Ratminto dan Atik, *Manajemen Pelayanan* (Jakarta: Pustaka Pelajar, 2005), 2.

Rudy Haryanto, *Dasar-dasar Manajemen Pemasaran Bank* (Pamekasan: Duta Media Publishing, 2020), 44.

Safitri, Kartika Aghni. *Strategi Keamanan Sistem Informasi untuk Melawan Serangan Ransomware*. 2023.

Salim dan Syahrum. *Metode Penelitian Kualitatif* (Bandung: Citapustaka Media. 2012).

Sedarmayanti, *Sumber Daya Manusia dan Produktivitas Kerja* (Bandung: Mandar Maju, 2010) 22.

Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, 9(3).

Solikhawati, Anisa. Andriani Samsuri: *Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja*. 2023.

Sugiyono. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2016.

Syafrizal, Melwin. ISO 17799: *Standar Sistem Manajemen Keamanan Informasi*. 2007.

Tika Ulfianinda, *ISO 27001: Standar untuk Sistem Manajemen Keamanan Informasi*. 2021.

Tim Penyusun, *Pedoman Penulisan Karya Ilmiah*, (Jember: IAIN Jember, 2019).

Tosun: *Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja*. 2021.

Triyunanto, C. R. (2024, March 5). *Mitigasi Adalah Apa? Ini Pengertian dan* Contohnya. detikcom. https://www.detik.com/edu/detikpedia/d-7224522/mitigasi-adalah-apa-ini-pengertian-dan-contohnya.

Ulfaninda, Tika. *ISO 27001:Standar untuk Sistem Manajemen Keamanan Informasi*. 2021.

Urgensi *Pendaftaran Penyelenggara Sistem Elektronik Bagi Pelaku Usaha E-Commerce "The Urgency Of Electronic System Registration For ECommerce Entrepreneurs*. (n.d.).

Urip Sulistiyo, *Metode Penelitian Kualitatif* (Jambi: Salim Media Indonesia, 2019).

Wahyu Perkasa, J. E. (2020). Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. *Jurnal Ilmiah Teknologi Informasi Asia*, 14(2).

WATKINS, S. G. (2022*). ISO/IEC 27001:2022. In ISO/IEC 27001*:2022. https://doi.org/10.2307/j.ctv30qq13d.

Wiyli Yustanti, Rahadian Bisma, Anita Qoiriah, Dkk. *Keamanan Sistem Informasi*. 2018.

WJS Poerwa Darminta, *Kamus Umum Bahasa Indonesia*, (Jakarta: Balai Pustaka, 1976), 736.

Zaidah Kusumawati, *Ensiklopedia Nabi Muhammad SAW Sebagai Utusan Allah* (Jakarta: Lentera Abadi, 2011), 34.

Lampiran 1

MATRIKS PENELITIAN

Judul	Variabel	Indikator	Sumber Data	Metodologi Penelitian	Fokus Penelitian
DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN RANSOMWARE PADA BSI KCP KENCONG JEMBER	A. Penerapan sistem manajemen keamanan informasi dalam pelayanan nasabah terhadap serangan *ransomware.* B. Dampak sistem manajemen keamanan informasi dalam pelayanan nasabah terhadap serangan *ransomware.*	A. Peran Sistem Manajemen Keamanan Informasi B. Kebijakan keamanan infromasi. C. Pemantauan sistem dan menganalisis sistem keamanan. D. Kepatuhan terhadap regulasi keamanan. A. Pengendalian risiko keamanan. B. Perbaikan dan keberlanjutan sistem. C. Pelatihan dan kesadaran karyawan.	**Informan:** a. Branch Manager b. Branch Operational Service Manager c. Operational Staff d. Custommer Service e. Teller f. Nasabah **Kepustakaan:** a. Jurnal b. Buku c. Artikel	1. Pendekatan Kualitatif (Deskriptif) 2. Jenis Penelitian Lapangan (*Field Research*) 3. Metode Pengumpulan Data: Wawancara 4. Keabsahan Data dengan Triangulasi sumber	1. Bagaimana penerapan Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan ransomware pada BSI KCP Kencong Jember? 2. Bagaimana dampak Sistem Manajemen Keamanan Informasi terhadap pelayanan nasabah dalam serangan ransomware pada BSI KCP Kencong Jember?

Lampiran 2

PERNYATAAN KEASLIAN TULISAN

Yang bertanda tangan di bawah ini :

Nama : Rifni Miftahur Rohmah

NIM : 212105010052

Fakultas : Fakultas Ekonomi dan Bisnis Islam

Progam Studi : Perbankan Syariah

Institusi : Universitas Islam Negeri KH Achmad Siddiq Jember

Dengan ini menyatakan bahwa isi skripsi ini dengan judul "Dampak Sistem Manajemen Keamanan Informasi dalam Pelayanan Nasabah terhadap Serangan *Ransomware* pada BSI KCP Kencong Jember" Secara keseluruhan adalah hasil penelitian atau karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya. Saya bertanggungjawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa tekanan dan paksaan dari pihak manapun.

Jember, 10 Februari 2025

Peneliti,

Rifni M...

NIM. 212105010052

Lampiran 3

PEDOMAN WAWANCARA

1. Apa visi misi BSI KCP Kencong Jember?
2. Apa saja struktural organisasi di BSI KCP Kencong Jember?
3. Bagaimana sejarah BSI KCP Kencong Jember?
4. Bagaimana sistem manajemen keamanan informasi pada bank BSI KCP Kencong Jember?
5. Bagaimana sistem manajemen keamanan informasi diimplementasikan dalam kegiatan operasional sehari-hari?
6. Apakah ada kebijakan keamanan informasi yang diterapkan di BSI KCP Kencong untuk melindungi data nasabah?
7. Bagaimana pelayanan nasabah setelah terjadinya serangan siber, dan apakah ada perubahan dalam tingkat kepercayaan nasabah terhadap layanan BSI KCP Kencong?
8. Alat atau teknologi apa yang digunakan untuk memantau ancaman keamanan?
9. Apakah ada kebijakan khusus terkait pelatihan karyawan mengenai keamanan informasi, dan bagaimana pelatihan tersebut dilaksanakan?
10. Seberapa sering kebijakan keamanan informasi dievaluasi dan diperbarui berdasarkan perkembangan ancaman siber?
11. Bagaimana serangan *ransomware* yang pernah terjadi mempengaruhi kualitas pelayanan nasabah, dan langkah-langkah apa yang diambil untuk memulihkan layanan setelah insiden tersebut?

Lampiran 4

SURAT IZIN PENELITIAN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS EKONOMI DAN BISNIS ISLAM
Jl. Mataram No. 01 Mangli, Kaliwates, Jember, Jawa Timur. Kode Pos: 68136 Telp. (0331) 487550
Fax (0331) 427005 e-mail: febi@uinkhas.ac.id Website: https://febi.uinkhas.ac.id/

Nomor : B- 1748 /Un.22/7.a/PP.00.9/11/2024 12 November 2024
Lampiran : -
Hal : **Permohonan Izin Penelitian**

Kepada Yth.
Kepala Cabang PT. Bank Syariah Indonesia (BSI)
KCP Kencong Jember.

Disampaikan dengan hormat bahwa, dalam rangka menyelesaikan tugas Skripsi pada Fakultas Ekonomi dan Bisnis Islam, maka bersama ini mohon diizinkan mahasiswa berikut :

Nama	:	Rifni Miftahur Rohmah
NIM	:	212105010052
Semester	:	7
Jurusan	:	Ekonomi Islam
Prodi	:	Perbankan Syariah

Guna melakukan Penelitian/Riset mengenai Peran Standar Sistem Manajemen Keamanan Informasi dalam Meningkatkan Ketahanan Perbankan Indonesia dan Dampak Pelayanan Nasabah Terhadap Serangan *Ranssomware* di BSI KCP Kencong Jember di lingkungan/lembaga wewenang Bapak/Ibu.

Demikian atas perkenan dan kerjasamanya disampaikan terima kasih.

A.n. Dekan
Wakil Dekan Bidang Akademik,

Nurul Widyawati Islami Rahayu

Lampiran 5

SURAT KETERANGAN SELESAI PENELITIAN

SURAT KETERANGAN

No.04/003-3/8169

Yang bertanda tangan di bawah ini :

Nama : Dwi Ismanto

Jabatan : *Branch Manager*

Dengan ini menerangkan bahwa :

Nama : Rifni Miftahur Rohmah
NIM : 212105010052
Institusi : UNIVERSITAS ISLAM NEGERI KH AHMAD SIDIQ JEMBER
Judul Skripsi : Peran Standar Sistem Managemen Keamanan Informasi Dalam Meningkatkan Ketahanan Perbankan Indonesia Dan Dampak Pelayanan Nasabah terhadap serangan Ransomware di PT. Bank Syariah Indonesia Kantor Cabang Pembantu Kencong Jember

Menerangkan bahwa nama yang tertera diatas tersebut benar telah menyelesaikan penelitian pada Bank Syariah Indonesia KCP Kencong pada bulan Desember 2024

Demikian surat keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Jember, 23 Desember 2024

BSI BANK SYARIAH INDONESIA KCP. Kencong

Dwi Ismanto
Branch Manager

Lampiran 6

JURNAL KEGIATAN PENELITIAN

JURNALKEGIATAN PENELITIAN DI BANK SYARIAH INDONESIA

KCP KENCONG JEMBER

Nama : Rifni Miftahur Rohmah

NIM : 212105010052

Judul : Peran Standar Sistem Manajemen Keamanan Informasi Dalam Meningkatkan Ketahanan Perbankan Indonesia dan Dampak Pelayanan Nasabah Terhadap Serangan Ransomware di BSI KCP KENCONG JEMBER

No	Hari/Tanggal	Uraian Kegiatan	Paraf
1	Senin/ 11 November 2024	Menyerahkan Surat Izin Penelitian	
2	Selasa/ 10 Desember 2024	Wawancara Dengan Bapak Dwi Ismanto Selaku Branch Managemen Bsi Kcp Kencong	
3	Rabu/ 11 Desember 2024	Wawancara Dengan Bapak Alex Ari Gustopo Selaku Branch Operational And Service Manager	
4	Jum'at/ 13 Desember 2024	Wawancara Dengan Ibu Ica Reviliani Selaku Operational Staff	
5	Senin/ 16 Desember 2024	Wawancara Dengan Bapak Achmad Sidqi Selaku Customer Service Representative	
6	Selasa/ 17 Desember 2024	Wawancara Dengan Ibu Putriana Selaku Teller	
7	Senin/ 23 Desember 2024	Penelitian Selesai Dan Meminta Surat Penelitian	

Jember, 23 Desember 2024

BSI BANK SYARIAH INDONESIA KCP. Kencong

Dwi Ismanto

Lampiran 7

DOKUMENTASI

Lokasi Penelitian (Bank Syariah Indonesia KCP Kencong Jember)

Wawancara dengan Bapak Dwi Ismanto selaku *Branch Manager* BSI KCP Kencong Jember

Wawancara dengan Ibu Icha Reviliani selaku *Operational Staff* BSI KCP Kencong Jember

Wawancara dengan Bapak Alex Dwi Gustopo selaku *Branch Operational and Service Manager* BSI KCP Kencong Jember

Wawancara dengan Bapak Achmad Sidqi selaku *Custommer Service* BSI KCP Kencong Jember

Wawancara dengan Ibu Putriana selaku *Teller* BSI KCP Kencong Jember

Wawancara dengan Ibu Elsa selaku nasabah BSI KCP Kencong Jember

Wawancara dengan Ibu Rani Maulidasari selaku nasabah KCP Kencong Jember

Lampiran 8

SURAT KETERANGAN SCREENING TURNITIN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS EKONOMI DAN BISNIS ISLAM
Jl. Mataram No. 01 Mangli, Kaliwates, Jember, Jawa Timur. Kode Pos. 68136 Telp. (0331) 487550
Fax (0331) 427005 e-mail: feb@uinkhas.ac.id Website: http://uinkhas.ac.id

SURAT KETERANGAN LULUS PLAGIASI

Bagian Akademik Fakultas Ekonomi dan Bisnis Islam menerangkan bahwa :

Nama	:	Rifni Miftahur Rohmah
NIM	:	212105010052
Program Studi	:	PERBANKAN SYARIAH
Judul	:	DAMPAK SISTEM MANAJEMEN KEAMANAN INFORMASI DALAM PELAYANAN NASABAH TERHADAP SERANGAN RANSOMWARE PADA BSI KCP KENCONG JEMBER

Adalah benar-benar telah lulus pengecekan plagiasi dengan menggunakan aplikasi DrillBit, dengan tingkat kesamaan dari Naskah Publikasi Tugas Akhir pada aplikasi DrillBit kurang atau sama dengan 25%.

Demikian surat keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya.

Jember, 12 Februari 2025
Operator DrillBit
Fakultas Ekonomi dan Bisnis Islam

Hersa Farida Qoriani, M.E.I
NIP. 198611292018012001

Lampiran 9

SURAT KETERANGAN SELESAI BIMBINGAN SKRIPSI

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS EKONOMI DAN BISNIS ISLAM
Jl. Mataram No. 01 Mangli, Kaliwates, Jember, Jawa Timur Kode Pos. 68136 Telp. (0331) 487550
Fax (0331) 427005 e-mail: febi@uinkhas.ac.id Website: http://febi.uinkhas.ac.id

SURAT KETERANGAN

Kami yang bertandatangan di bawah ini, menerangkan bahwa :

Nama : Rifni Miftahur Rohmah
NIM : 212105010052
Semester : VIII (Delapan)

Berdasarkan keterangan dari Dosen Pembimbing telah dinyatakan selesai bimbingan skripsi. Oleh karena itu mahasiswa tersebut diperkenankan mendaftarkan diri untuk mengikuti Ujian Skripsi.

Jember, 10 Februari 2025
Koordinator Prodi. Perbankan Syariah,

ANA PRATIWI M.S.A

Lampiran 10

BIODATA PENULIS

A. DATA PRIBADI

Nama Lengkap	: Rifni Miftahur Rohmah
Tempat Tgl Lahir	: Jember, 19 September 2003
Alamat	: Jl. Letjen Sutoyo Lingk. Kebun Indah RT 01/ RW 039 Kec. Kaliwates, Kab. Jember, Prov. Jawa Timur.
NIM	: 212105010052
Fakultas	: Ekonomi dan Bisnis Islam
Jurusan/Prodi	: Perbankan Syariah
No. Telepon	: 085641756483
Email	: rifnimifta@gmail.com

B. RIWAYAT PENDIDIKAN

1. SDN Kebonsari 04 Jember
2. SMP Plus Darus Sholah Jember
3. SMAN 3 Jember