MANAJEMEN RESIKO KEBOCORAN DATA NASABAH DAN SERANGAN SIBER MENGGUNAKAN NIST-RISK MANAGEMENT FRAMEWOK

Angellica Sheren Romauli Sirait[1], Adinda Syifa Kamalia[2], Askia Diska[3], Mercurius Broto Legowo

Fakultas Teknologi Informasi, Perbanas Institute, Jakarta, Indonesia

Abstrak *– Dalam dekade terakhir, industri perbankan Indonesia dihadapkan dengan risiko yang semakin kompleks, sehingga mewajibkan bank untuk meningkatkan kebutuhan akan penerapan manajemen risiko untuk meminimalisasi risiko yang terkait dengan kegiatan usaha perbankan. Di era internet sakarang marak terjadi fenomena risiko yang mengancam berjalannya operasional pada industri perbankan. Beberapa resiko yang menjadi perhatian serius adalah terkait kebocoran data nasabah serta adanya berbagai serangan siber yang sering terjadi. Untuk mengkaji dan menganalisa resiko yang disebut dapat menggunakan pendekatan NIST.-Risk Management Framework (RMF),dimana kerangka kerha ini merupakan pendekatan yang komprehensif dan terstandarisasi untuk mengelola risiko keamanan informasi Tujuan studi adalah kajian dan melakukan analisis manajemen risiko teknologi informasi untuk resiko kebocoran data nasabah dan serangan siber pada industri perbankan dengan menggunakan NIST-RMF (Risk Manajemen Framework). Metode penelitian untuk studi ini menggunakan metode deskriptif dengan pendekatan kuaslitatif. Pengumpulan data yang terutama melalui studi literatur, dan dalam teknik analisis resikonya menggunakan metode NIST-Risk Management Framework. Hasil kajian dan analisis manajemen risiko teknologi informasi untuk resiko kebocoran data nasabah dan serangan siber pada industri perbankan dengan menggunakan NIST-RMF menyatakan bahwa analisis resiko telah sesuai dengan komponen utama NIST-RMF, yaitu:komponen Prepare, Categorize, Select, Implement, Assess, Authoriza dan Monitor .Studi ini bisa bermanfaat dalam meberikan masukan untuk industri perbankan guna meminimalisasi resiko kebocoran data nasabah serta serangan siber yang semakin marak saat ini..*

Kata Kunci: *kebocoran data nasabah, manajemen risiko, NIST-RMF, serangan siber*
.

I. PENDAHULUAN

Perbankan merupakan industri yang harus responsif terhadap berbagai risiko fundamental yang dapat mempengaruhi kinerjanya (Kurniawan, Rahayu, & Wibowo, 2021). Menurut Vaidyula & Kavala (2018) Manajemen risiko pada industri perbankan menjadi sorotan, terutama setelah terjadinya gejolak yang terjadi belakangan ini, yang memberikan dampak yang sangat buruk terhadap eksistensi sektor perbankan sebagai industri yang layak. Tidak hanya perbankan, bahkan berbagai instansi pemerintah pun telah menyadari akibat/dampak dari tidak efektifnya pengelolaan risiko pada bank, oleh karena itu telah ditetapkan beberapa peraturan untuk mengendalikan risiko-risiko yang timbul dalam bisnis industri perbankan.

Beberapa resiko yang menjadi perhatian serius adalah terkait kebocoran data nasabah serta adanya berbagai serangan siber yang sering terjadi. Risiko kebocoran data nasabah merupakan risiko yang muncul karena adanya pengunggahan data pribadi yang bersifat sensitive, seperti NIK dan NPWP. Risiko ini

adalah salah satu bentuk beretasan atau kegagalan system keamanan (Gumilang, 2023). Kebocoran data juga terjadi dari pihak pelaku usaha jasa keuangan dengan cara menjual data konsumen, memberikan data pada pihak ketiga, system aplikasi perlindungan data mudah di retas hacker (Soemitra & Adlina, 2022). Sedangkan, Serangan siber adalah serangan yang dilakukan oleh network komputer atau telekomunikasi terhadap network komputer atau telekomunikasi yang lain seperti website, sistem komputer, dan komputer individu (Farhat et al., 2017). Risiko serangan siber merupakan upaya yang dilakukan oleh individu atau kelompok untuk menyusup, merusak, memanipulasi, atau mengakses sistem komputer atau jaringan secara ilegal atau tanpa izin (Sutisnawinata, 2023)

Akhir-akhir ini terjadi fenomena kebocoran data nasabah dan serangan siber terhadap industri perbankan di Indonesia. Ada fenomena 15 juta data nasabah salah satu bank syariah terbesar di Indonesia ini mengalami error dan kebocoran data pada Mei tahun ini. Total data yang bocor dan dicuri mencapai 1,5 Terabyte, termasuk 15 juta data pengguna dan kata sandi untuk akses dan layanan internal, serta data pribadi pelanggan dan informasi pinjaman (CNN Indonesia, 2023). Selain itu, terganggunya layanan perbankan syariah yang diduga kuat akibat serangan siber jenis ransomware juga patut menjadi pembelajaran bagi bank-bank lain di Indonesia.

Kejadian terkait risiko lainnya adalah perusahaan asuransi milik Bank Nasional di Indonesia juga mengalami kebocoran data pada Juli 2021. Data dua juta nasabah asuransi milik Bank Nasional bocor dan dijual secara online. Informasi kebocoran data nasabah terkait data nasabah BRI Life diunggah ke akun Twitter pada Selasa 27 Juli 2021. Peretas diduga mencuri 250 gigabyte data nasabah perusahaan asuransi tersebut dan menjualnya seharga US$ 7.000 atau Rp. 101,5 juta (Rosana, 2017). Menurut Kementerian Komunikasi dan Informatika yang diperkuat dengan data Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan, terdapat fenomena Indonesia menerima 1,225 miliar serangan siber setiap harinya (Yuliani, 2017).

Fenomena tersebut dapat menjadi perhatian bagi para akademisi dan praktisi di industri perbankan untuk mengkajinya.

NIST-RMF adalah pendekatan yang komprehensif dan terstandarisasi untuk mengelola risiko keamanan informasi di tingkat federal system informasi (NIST, 2018). Framework ini menekankan pentingnya pemantauan berkelanjutan dan perbaikan proses manajemen risiko secara berulang, serta integrasi risikomanajemen dengan strategi keamanan organisasi secara keseluruhan (NIST, 2018).

Gambar 1 NIST-Risk Management Framework

Dalam Gambar 1. ,emnunjukkan bahwa NIST-RMF memiliki komponen yang menjadi tahapan dalam analisa resiko, yaitu tahap persiapan (*prepare*), kategorisasi(*categorize*), Seleksi(*select*), Impelemtasi(*implement*), Penilaian (*assess*), Otorisasi *(authorize*), dan Monitor(*monitor)*. Adapun tahap an manajemen resiko sesuai standar yang umum meliputi : tahap identifikasi resiko, tahap analisa resiko(NIST-RMF) dan tahap evaluasi resiko.

Penelitian terdahulu yang dilakukan oleh Tony Tan dan Benfano Soewito (2022) dalam penelitiannya yang berjudul "Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity Di Universitas ZXC" menggunakan metode kuantitatif. Penelitian tersebut membahas tentang pendidikan tinggi yang memerlukan sumber daya kompleks, terutama dalam hal infrastruktur dan aset IT, untuk mendukung pendidikan berbasis penelitian dan industri

terbarukan. Dalam konteks ini, keamanan transmisi data menjadi krusial untuk produktivitas operasional institusi pendidikan tinggi karena berpotensi mengalami serangan siber. Studi kasus Universitas ZXC di Batam menyoroti tantangan serius terkait keamanan infrastruktur jaringan dan sistem layanan web internal yang dapat diretas, mengganggu aktivitas staf dan mahasiswa. Untuk mengatasi risiko serangan siber, penelitian merekomendasikan penerapan penetration testing dan penerapan NIST Cybersecurity Framework.. Hasil studi ini beserta langkah-langkahnya ini dapat meminimalisir risiko dan meningkatkan keamanan sistem layanan web dan situs web di Universitas ZXC dan dapat digunakan pada tempat lain khususnya pada perguruan tinggi.

Tujuan dari studi untuk membuat analisis manajemen teknologi informasi untuk resiko kebocoran data nasabah dan serangan siber pada industri perbankan dengan menggunakan NIST- RMF (Risk Management Framework). Dalam studi ini, NIST-RMF Framework tdapat membantu perbankan dalam mengelola risiko dimana sasaran yang hendak dicapai dalam studi ii antara lain :

1) melakukan identifikasi resiko kebocoran data nasabah dan serangan siber sesuai analisis manajemen resiko teknologi informasi
2) menganalisa resiko kebocoran data nasabah dan serangan siber menggunakan NIST_RMF
3) evaluasi resiko kebocoran data nasabah dan serangan siber

Kajian dan analisis Manajemen Risiko kebocoran data nasabah dan serangan siber pada Industri Perbankan dengan ISO 31000:2018 framework merupakan kebaruan dalam studi ini.

II. METODE

Dalam penelitian ini, metode yang digunakan adalah metode kualitatif. Penelitian kualitatif adalah salah satu metode penelitian yang bertujuan untuk mendapatkan pemahaman tentang kenyataan melalui proses berfikir induktif (Adlini et al., 2022).

Di dalam metode penelitian kualitatif juga lazimnya data di kumpulkan dengan beberapa teknik pengumpulan data kualitatif, yaitu : 1) wawancara, 2) observasi, 3) dokumentasi, dan 4) diskusi terfokus (Focus Group Discussion) (Kawasati, n.d.). Teknik pengumpulan data lain yang digunakan dalam penelitian ini melalui dokumentasi yaitu melalui jurnal-jurnal yang telah dibuat sebelumnya. Menurut Gottschalk dokumentasi adalah proses pembuktian yang didasarkan atas jenis sumber apapun, baik yang bersifat tulisan lisan, gambaran, atau arkeologis(Nilamsari, 2014).

Selain itu, teknik analisa dalampenelitian ini menggunakan framework NIST-RMF(NIST, 2018). Framework ini menekankan pentingnya pemantauan berkelanjutan dan perbaikan proses manajemen risiko secara berulang, serta integrasi risiko manajemen dengan strategi keamanan organisasi secara keseluruhan (NIST, 2018).

III. HASIL DAN DISKUSI

Hasil dan diskusi dalam penelitian ini didasari oleh tiga tahapan manajemen resiko teknologi informasi secara umum, yaitu identifikasi risiko, analisa, dan evaluasi.

3.1. Identifikasi Risiko

Identifikasi risiko adalah bagian dari manajemen risiko yang menyediakan proses terstruktur yang mengidentifikasi bagaimana tujuan organisasi dapat dipengaruhi oleh risiko (Wardhana, n.d.). Tahap ini dilakukan untuk mengidentifikasi risiko– risiko apa saja yang dihadapi oleh suatu organisasi (Supriyo, 2017). Berikut identifikasi dari level resiko , seperti pada Tabel 1.

Tabel 1 Hasil Identifikasi Risiko

Level Resiko	Deskripsi Level	Keterangan
1	*Low Probability Low Impact* **(Low Risk)**	risiko dengan tingkat pengaruh yang paling kecil dibandingkan dengan risiko lainnya sehingga dengan kebijakan tertentu risiko ini dapat diabaikan
2	*Low Probability High Impact* **(Low–High Risk)**	risiko dengan tingkat pengaruh menengah. Meskipun begitu risko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan tergantung

Level Resiko	Deskripsi Level	Keterangan
		dari dampak yang diberikan..
3	*High Probability Low Impact* **(High-Low Risk)**	Risiko dengan tingkat pengaruh menengah. Berbeda dengan *low probability high impact* risiko ini hanya perlu dimonitor.
4	*High Probability High Impact* **(High Risk)**	Risiko dengan pengaruh yang paling tinggi dibandingkan dengan lainnya. Risiko ini memiliki tingkatan yang paling berbahaya sehingga harus diatasi secara cepat

Berdasarkan level resiko, maka selanjutnya melakukan identifikasi resiko. Hasil identifikasi resiko kebocoran data nasabah dan serangan siber ditunjukkan pada Tabel 2.

Tabel 2 Hasil Identifikasi Risiko

Jenis risiko	Identifikasi Risiko	Level Risiko
Risiko Kebocoran Data Nasabah	Risiko kebocoran data nasabah merupakan risiko yang muncul karena adanya pengunggahan data pribadi yang bersifat sensitive, seperti NIK dan NPWP. Risiko ini adalah salah satu bentuk beretasan atau kegagalan system keamanan (Gumilang, 2023). Kebocoran data juga terjadi dari pihak pelaku keuangan dengan cara menjual data konsumen, memberikan data pada pihak ketiga, system aplikasi perlindungan data mudah di retas hacker (Soemitra & Adlina, 2022).	4
Risiko Serangan Siber	Serangan siber adalah serangan yang dilakukan oleh network komputer atau telekomunikasi terhadap network komputer atau telekomunikasi yang lain seperti website, sistem komputer, dan komputer individu (Farhat et al., 2017). Risiko serangan siber merupakan upaya yang dilakukan oleh individu atau kelompok untuk menyusup, merusak, memanipulasi, atau mengakses sistem atau tanpa izin (Sutisnawinata, 2023).	4

3.2. Analisis Risiko

Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah melakukan analisa resiko. Analisis risiko adalah upaya untuk memahami risiko lebih dalam (Novia et al., 2015).

Tabel 3 Hasil Analisis Risikodengan NIST-RMF

NIST-Risk Management Framework Components	Hasil analisis berdasarkan NIST-RMF
Prepare	Dalam tahap ini, penting untuk mengidentifikasi risiko yang akan muncul sehingga dapat mengeksekusi penggunaan Risk Management Framework. Risiko yang sering muncul adalah: A. serangan cyber (phising, malware, ransomware, dll) B. profilling/penyalahgunaan
Categorize	Dalam tahap ini, risiko yang telah diidentifikasi akan dibagi menjadi beberapa kelompok berdasarkan dampak yang dihasilkannya, berikut ini adalah pengelompokkan risikonya: A, Level 1 (dampaknya mudah ditanggulangi):profilling/penyal ahgunaan data B. Level 2 (dampaknya cukup sulit untuk
Select	Dalam tahap ini, pengelompokkan risiko yang sebelumnya telah dibuat akan disesuaikan pengendalian yang sepadan dengan risikonya, A. profilling/penyalahgunaan data (lv. 1): membuat enkripsi data untuk melindungi informasi dari akses illegal, melakukan backup data secara rutin dan diletakkan pada lokasi yang terpisah dengan keamanan yang tinggi, mengaktifkan firewall, menghalau atau memblokir akses tidak sah yang berusaha masuk kedalam sistem B. pembobolan rekening (lv. 2) :perusahaan harus

NIST-Risk Management Framework	Hasil analisis berdasarkan NIST-RMF
	keuangan, menyediakan perencanaan pemulihan krisis kerugian yang mungkin timbul C. serangan cyber (lv. 3) : perusahaan harus meningkatkan keamanan secara menyeluruh dan selalu IT, melakukan pembaruan sistem secara rutin untuk mengurangi kerentanan terhadap serangan cyber
Implement	Pada langkah ini, perusahaan mengimplementasikan hasil pengelompokkan risiko pada pengendalian risiko yang sebelumnya telah ditentukan. A. profilling/penyalahgunaan data: • Enskripsi data, mengubah data menjadi bentuk yang sulit untuk dimengerti dan perlu proses deskripsi dari sistem untuk mencegah pengambilan data dari akses yang tidak sah (Khoirunnisa & Djuniadi, 2021). • Backup data, adanya backup data yang terpisah dari sistem mencegah perusahaan kehilangan data secara sepenuhnya dan mengurangi dampak penyalahgunaan data karena masih memiliki data yang konkret • Firewall, membantu pengaturan akses data yang keluar masuk dari sistem agar hanya data yang sah yang diperbolehkan untuk melewati firewall serta mencegah penyalahgunaan data dengan mengawasi lalu lintas system (Vidya et al., n.d.). B. Pembobolan rekening • Sistem keamanan yang kuat, mencegah akses

NIST-Risk Management Framework	Hasil analisis berdasarkan NIST-RMF
	C. Serangan Cyber • Peningkatan keamanan, mencegah serangan cyber seperti malware, DDos, dan lainnya, melindungi data sensitif dari akses yang tidak sah, memastikan bahwa user mematuhi peraturan atau regulasi keamanan data ada, mendeteksi adanya pergerakan mencurigakan agar perusahaan dapat mengambil tindakan lebih lanjut (KOMINFO, 2015). • Pembaruan sistem, mengurangi risiko serangan dengan menerapkan sistem keamanan end-to-end
Assess	Pada langkah ini, implementasi yang sebelumnya sudah dilakukan akan dianalisa operasinya agar dapat diidentifikasi kerentanan dari tiap risiko yang ada dan membuat laporan atas hasil
Authorize	Setelah laporan telah dibuat, laporan tersebut akan diberikan kepada ahli/pejabat yang bersangkuan untuk menanggapi hasil dari laporan tersebut serta membuat keputusan atas pengendalian yang dilakukan apakah akan dilanjutkan atau diganti dengan pengendalian yang diasumsikan dapat
Monitor	Pada tahap ini, akan dilakukan pemantauan untuk mengevaluasi efektifitas dari pengendalian, perubahan sistem dan lingkungan operasional, sehingga dapat meningkatkan respon terhadap risiko dan membangun dasar yang kokoh

3.3. Evaluasi Risiko

Evaluasi risiko merupakan proses pembandingan antara level risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan sebelumnya (Rachmina, n.d.). Evaluasi risiko menggunakan pemahaman risiko yang diperoleh selama analisis risiko untuk

membuat keputusan tentang tindakan masa depan (BSN, 2016).

Oleh karena itu, perlu dilakukan analisis evaluasi risiko serangan siber dan kebocoran data dengan tujuan untuk membantu mengarahkan sumber daya dan upaya pengelolaan risiko pada risiko yang paling signifikan (Rangkuti, 2023). Evaluasi dari resiko Serangan siber (AMT-IT, 2023) dan kebooran data (Verihubs, 2022) pada Bank dapat dievaluasi sepertipada Tabel 4.

Tabel 4 Evaluasi Risiko

Prioritas Resiko / Kategori Level Resiko	Level Resiko Residual Harapan	Keputusan Mitigasi Resiko	Indikator Resiko Utama (IRU)
Kebocoran Data Nasabah **Level 4**	**Level 3**	Meningkatkan kesadaran dari para karyawan terhadap hal terkait keamanan data dengan melakukan sosialisasi dan pelatihan tentang penyebaran malware, Menerapkan suatu pedoman khusus yang wajib diikuti oleh seluruh karyawan Meningkatkan keamanan data dengan penetration testing atau pengujian penetrasi sehingga kerentanan keamanan dapat ditemukan dan diperbaiki, Menggunakan perlindungan endpoint sebagai tindakan pengamanan untuk melindungi dari pengguna titik akhir atau perangkat pengguna akhir (seperti laptop, desktop, perangkat seluler, dll) sehingga bisa terlindungi dari berbagai serangan pembobolan data	Human error menjadi pemicu terbesar terjadinya kebocoran data, Penyusupan dengan malware sehingga terjadi kerusakan pada sistem komputer dan pencurian data perusahaan Karyawan yang berkhianat
Serangan Siber		Meningkatkan perlindungan terhadap pelanggan agar mengurangi potensi serangan, Memastikan bahwa sistem keamanan dan infrastruktur IT terintegrasi secara Meningkatkan bentuk standar keamanan dalam lingkungan kerja hybrid dengan menerapkan keamanan perangkat (endpoint security), Meningkatkan perlindungan teknis dengan bekerja sama dengan vendor keamanan siber untuk menciptakan sistem keamanan yang maksimal. Menggunakan perlindungan endpoint sebagai tindakan pengamanan untuk melindungi pengguna titik akhir atau perangkat pengguna akhir (seperti laptop, desktop, perangkat seluler, dll) sehingga terlindungi dari serangan pembobolan data	Pesatnya pengembangan digitalisasi di lingkungan bisnis yang tergesa-gesa dapat meningkatkan kerentanan sistem keamanan sehingga memicu terjadinya cyber attack, Pengadaptasian cloud yang beresiko terhadap keamanan data berupa kehilangan data rahasia seperti informasi pribadi, kata sandi dll, Bekerja dalam jarak jauh sehingga berisiko terjadinya cyber attack
Level 4	**Level 3**		

3.4. Diskusi

Manajemen resiko TI dalam studi ini secara khusus difokukan untuk resiko kebocoran data nasabah dan serangan siber dengan menggunakan NIST-RMF, yang menekankan pada beberapa komponen sebagai prinsip analisisnya. Hal ini berbeda dengan penelitian sebelumnya yang bukan di industri perbankan. Penelitian terdahulu yang dilakukan oleh Tony Tan dan Benfano Soewito (2022) dalam penelitiannya yang mengambil judul "Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity Di Universitas ZXC". Juga dalam penelitian terdahulu ini bukan menggunakan NIST-RMF , melainkan NIST-CSF.

Keterbatasan dalam studi ini hanya membahas resiko yang marak terjadi diperbankan yaitu

resiko kebocoran data dan serangan siber. Adapun implikasi penelitian secara managerial maka industri perbankan harus mulai melaksanakan mitigasi kedua resiko yang bisa berdampak besar dalam opersional bisnisnya serts mengoptimalkan analisis menggunakan NIST-RMF ini.

IV. KESIMPULAN

Penelitian ini memfokuskan pada analisis manajemen risiko teknologi informasi untuk kebocoran data nasabah dan serangan siber pada industri perbankan dengan menggunakan NIST-RMF (Risk Manajemen Framework).

Secara umum, kesimpulan dari penelitian ini adalah bahwa 1) Pada tahap prepare, hasil dari identifikasi risiko serangan yang sering timbul adalah serangan siber (phising, malware, dll), profilling/penyalahgunaan data, dan pembobolan rekening; (2) Pada tahap categorize, risiko yang sudah diidentifikasi dikelompokan berdasarkan tiga tingkat dampaknya (level 1, level 2, dan level 3); (3) Pada tahap select, rangkaian pengendalian setiap risiko dipilih berdasarkan proses kategorisasi keamanan; (4) Pada tahap implement, hasil pengelompokkan risiko diterapkan dan didokumentasikan; (5) Pada tahap assess, hasil pengelompokkan risiko yang sudah diterapkan dianalisa dan dievaluasi dalam sebuah laporan; (6) Pada tahap authorize, laporan analisa dan evaluasi ditanggapi untuk diputuskan langkah selanjutnya; (7) Pada tahap monitor, tetap dilakukan pemantauan dan evaluasi efektifitas dan pengendalian dalam rangka mendukung keputusan manajemen risiko.

Penelitian masa depan untuk analisis manajemen resiko ini bisa menggunakan kerangka kerja kerja lain, seperti COSO-ERM Framework, Cobit 5.0, atau ISO 31000:2018.

V. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direktorat Penelitian dan Pengabdian Masyarakat (DP2M) - Perbanas Institute, Jakarta, yang telah memberikan kesempatan mempresentasikan hasil studi ini di Seminar Nasional Perbanas (SNAP) di tahun 2023 ini.

DAFTAR PUSTAKA

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*, *6*(1), 974–980.

AMT-IT. (2023). *Penyebab Cyber Attack PadaSektor Perbankan dan Keuangan*.

BSN. (2016). *Manajemen risiko – Teknik penilaian risiko Risk management – Risk assessment techniques*.

Farhat, V., Mccarthy, B., Raysman And, R., & Canale, J. (2017). *Search the Resource ID numbers in blue on Westlaw for more. Cyber Attacks: Prevention and Proactive Responses What is a Cyber Attack?*

Gumilang, H. A. (2023). *Pengaruh Terpaan Berita Online Kebocoran Data Digital oleh Hacker Bjorka Terhadap Kecemasan Gen Z (Survei pada Mahasiswa Universitas Lampung)*.

Iskandar, I. (2011). Manajemen Resiko Teknologi Informasi Perusahaan Menggunakan Framework RiskIT (Studi Kasus : Pembobolan Pt . Bank Permata , Tbk). *Jurnal Sains, Teknologi Dan Industri*, *9*(1),104.

Kawasati, R. (n.d.). *Teknik Pengumpulan Data Metode Kualitatif*. fPengumpulan Data Metode Kualitatif.pdf

Khoirunnisa, O. G., & Djuniadi, D. (2021). Implementasi Algoritma AES untuk Keamanan Data Rekam Medis. *Petir: Jurnal Pengkajian Dan Penerapan Teknik Informatika*, *15*(1), 21–27.

Nilamsari, N. (2014). Memahami Studi okumen Dalam Penelitian Kualitatif. *Jurnal Wacana*, *13*(2), 177–181. NIST. (n.d.). *NIST Risk ManagementFramework RMF*.NIST. (2018). *Risk Management Framework*. 229–270. https://doi.org/10.4018/978-1-5225-2503-5.ch007

Novia, A., Yanuar, R., St, F. A. W., Dwi, D., & St, J. (2015). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)*. *2*(2), 6201–6208.

Rangkuti, M. (2023). *Manajemen Risiko Pengertian, Ciri, Tujuan, Manfaat, dan Prinsip*. https://feb.umsu.ac.id/manajemen- isiko-pengertian-ciri-tujuan-manfaat-dan-rinsip/

Soemitra, A., & Adlina. (2022). Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia. *Jurnal Insitusi Politeknik Ganesha Medan Juripol*, *5*, 288–303.

Supriyo. (2017). Manajemen Risiko Dalam Perspektif Islam. *Jurnal Pendidikan Ekonomi UM Metro*, *5*(1), 130–142.

Sutisnawinata, K. (2023). *Serangan Cyber: Pengertian, Jenis, Cara Mencegah*.

Verihubs. (2022). *Kenali Penyebab Kebocoran Data dan 4 Upaya Pencegahannya*.

Vidya, vensy, Surono, & Setiarso, G. (n.d.). A*pplication Gateway Dan Stateful Inspection Method Pada Implementasi Firewall Untuk Optimasi Keamanan Jaringan Komputer*.

Wardhana, A. (n.d.). *Identifikasi dan Pengukuran Resiko*. https://www.researchgate.net/publication