MANAJEMEN RESIKO TEKNOLOGI INFORMASI PADA INDUSTRI PERBANKAN DENGAN ISO 31000: 2018 FRAMEWORK

Nurani Buaty[1], Syahnaz Citra Dewi[2], Rama Dutasmara[3] Mercurius Broto Legowo[4]

Program Studi Sistem Informasi , Fakultas Teknologi Informasi , Perbanas Institute

Abstrak *– Industri perbankan di Indonesia saat ini dihadapkan pada berbagai risiko yang dapat mengganggu kelancaran operasionalnya, termasuk risiko seperti kebocoran data nasabah dan serangan siber yang semakin meningkat. Pendekatan ISO 31000: 2018 framework menjadi acuan yang relevan untuk mengidentifikasi dan menganalisis risiko-risiko tersebut. Tujuan studi adalah melakukan kajian dan analisis Manajemen Risiko Teknologi Informasi pada Industri Perbankan dengan ISO 31000:2018 framework. Secara khusus, mengambil kasus Risiko Kebocoran Data Nasabah dan Serangan Siber yang menjadi fenomena besar pada Industri Perbankan. Dalam melakukan penelitian ini, metode penelitian utama yang digunakan adalah studi literatur, dan dalam proses analisis manajemen resikonya merujuk pada ISO 31000:2018. Framework. Hasil utama dari studi ini adalah manajemen risiko teknologi informasi pada industri perbankan dengan ISO 31000:2018 Framework. Secara khusus studi terkait kajian dan analisis dalam mengidentifikasi potensi risiko kebocoran data nasabah dan serangan siber yang dihadapi oleh sektor perbankan. Manajemen risiko yang efisien, perusahaan dapat melindungi nilai dan menciptakan nilai tambah bagi organisasi. Studi ini dapat diharapkan bisa memberikan kontribusi bagi industri perbankan dapat lebih efektif dalam mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko terkait keamanan data dan serangan siber merujuk pada ISO 31000:2018 Framework.*

Kata kunci: *industri perbankan, ISO 31000:2018. kebocoran data nasabah, manajemen resiko, serangan siber*

I. PENDAHULUAN

Teknologi informasi (TI) perbankan indonesia terus berkembang pada bidang teknologi meliputi perkembangan infrastruktur TI seperti perangkat keras (hardware), perangkat lunak (software), teknologi penyimpanan data (storage), serta teknologi komunikasi. Dengan berkembangnya TI pada perbankan banyak resiko yang harus dihadapi. Salah satu risikonya adalah risiko kebocoran data nasabah dan serangan siber. Risiko dapat didefinisikan sebagai suatu kondisi atau peristiwa yang tidak pasti dan memiliki dampak negatif terhadap tujuan atau keinginan yang akan dicapai. Oleh karena itu, manajemen risiko menjadi bagian penting dalam mengelola risiko-risiko ini dengan efektif. Dengan manajemen risiko yang efisien, perusahaan dapat melindungi nilai dan menciptakan nilai tambah bagi organisasi.

Risiko kebocoran data dan serangan siber pada bank-bank di Indonesia merupakan masalah yang memerlukan manajemen. Faktor-faktor yang berkontribusi pada rentannya bank terhadap risiko kebocoran data dan serangan siber semakin meningkat pada teknologi informasi, pertumbuhan pesat aktivitas perbankan digital, serta potensi ancaman yang berasal dari berbagai pihak yang berupaya untuk mengakses dan mengungkapkan informasi rahasia perbankan. Meningkatkan keamanan data dan perlindungan terhadap risiko kebocoran data telah menjadi suatu keharusan dalam sektor perbankan di Indonesia.

Akhir-akhir ini terjadi fenomena kebocoran data nasabah dan serangan siber terhadap

industri perbankan di Indonesia. Kebocoran data merupakan pelanggaran keamanan dimana data sensitif, terlindungi atau data rahasia disalin, ditransmisikan, dilihat, dicuri, atau digunakan oleh individu yang tidak berwenang yang tidak berwenang untuk melakukannya(Ghiffari & Girinoto,, 2023) Risiko kebocoran data dapat terjadi dari pelaku jasa keuangan yang menjual data konsumen, memberikan data kepada pihak ketiga dan kemungkinan sistem aplikasi data mudah diakses dan diretas oleh hacker(Yuspin et al., 2023). Sedangkan serangan siber adalah salah satu risiko paling mengancam keamanan nasional(Vimy et al., 2022). Risiko serangan siber adalah risiko kerugian akibat serangan melalui dunia maya oleh perusahaan yang mengganggu, menghancurkan, atau secara jahat mengendalikan lingkungan/infrastruktur komputasi, merusak integritas data, atau mencuri informasi(Luthfah, 2021).

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.

Pada awal tahun 2022 terjadi kebocoran data di Bank Indonesia melibatkan Kantor Cabang Bengkulu dan kota-kota lainnya, dengan lebih dari 52 ribu dokumen yang bocor dari sekitar 200 komputer, mencapai total ukuran data sebesar 74,82 GB. Bank Syariah Indonesia (BSI) baru-baru ini mengalami kesulitan karena serangan ransomware jenis Lock Bit 3.0, mengakibatkan gangguan dalam sistem layanannya. Serangan siber harus dikelola dengan serius karena memiliki potensi untuk menimbulkan dampak kerugian signifikan pada sektor perbankan. Ancaman keamanan siber yang dihadapi oleh sektor perbankan menegaskan urgensi perlindungan terhadap serangan-serangan semacam iniUntuk memahami apa yang sudah diketahui dari penelitian sebelumnya, pendahuluan harus terdiri dari membahas artikel jurnal yang relevan (dengan kutipan) dan meringkas pemahaman saat ini dari masalah yang dihadapi. 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).

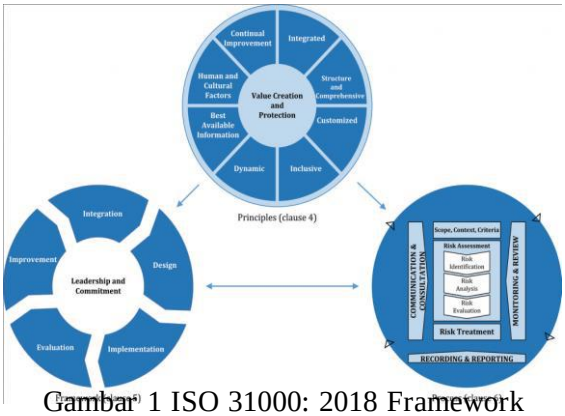
ISO 31000:2018 adalah sebuah pedoman untuk menerapkan manajemen risiko yang terdiri dari tiga komponen utama, yakni prinsip-prinsip, kerangka kerja, dan prosedur. Prinsip-prinsip manajemen risiko adalah landasan dari praktik dan filosofi manajemen risiko. Kerangka kerja mengatur tata kelola sistem manajemen risiko secara terstruktur dan terorganisir di seluruh organisasi. Sementara itu, prosedur melibatkan serangkaian aktivitas yang terstruktur dalam mengelola risiko yang saling terhubung.

ISO 31000:2018 Framework

ISO 31000 mendefinisikan manajemen risiko sebagai "koordinasi pendekatan terintegrasi dan struktur organisasi untuk mengelola risiko yang mendukung pencapaian tujuan organisasi dan meningkatkan nilai"(ISO 31000, 2018) Pendekatan terintegrasi ini menunjukkan perlunya pengelolaan risiko yang menyeluruh dan diintegrasikan ke dalam kebijakan dan proses organisasi.

ISO 31000 merinci tahapan dalam proses manajemen risiko yang melibatkan penetapan konteks, identifikasi risiko, penilaian risiko, pengelolaan risiko, komunikasi dan konsultasi, pemantauan dan tinjauan. Tahapan ini menciptakan suatu siklus yang berkelanjutan, memungkinkan organisasi untuk merespons

perubahan lingkungan dan memastikan bahwa manajemen risiko terus berjalan sesuai dengan tujuan organisasi(ISO 31000, 2018).



Gambar 1 ISO 31000: 2018 Framework

Penelitian terdahulu terkait manajemen resiko dengan ISO 31000 telah dilakukan oleh Evinia & Sitokdana(2023) Hasil rsiet teresebut mengindikasikan kemunginan terdapat 20 resiko yang harus dikelola peruahaan tersebut dengan kerangka kerja ISO 31000. Penelitian mereka dapat menyimpulkan bahwa implementasinya belum mencapai tingkat optimal.

Studi lain dari Fachrezi(2021) juga dengan topik yang sama. Tujuan studinya adalah mengelola resiko keamanan aset Teknologi Informasi dengan ISO 31000:2018 pada Diskomimfo Salatiga. Kesimpulan studi ini perlu adanya tindakan untuk meminimalisir kemungkinan risiko yang akan terjadi yaitu dengan menindaklanjuti perlakuan risiko dengan baik agar proses bisnis berjalan sesuai dengan yang diharapkan

Tujuan dalam studi ini adalah melakukan kajian dan analisis Manajemen Risiko Teknologi Informasi pada Industri Perbankan dengan ISO 31000:2018 *framework*. Secara khusus, mengambil kasus Risiko Kebocoran Data Nasabah dan Serangan Siber yang menjadi fenomena besar pada Industri Perbankan.. Adapun sasaran yang akan dicapai secara khusus adalah dalam penilaian resiko, antara lain:

1) melakukan identifikasi resiko kebocoran data nasabah dan serangan siber,
2) menganalisa resiko kebocoran data nasabah dan serangan siber,
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

Metode penelitian yang digunakan dalam studi ini adalah penelitian deskrptif dengan pendeatan kualitatif(Creswell & Creswell, 2023). Tahapan dalam melakukan proses penelitian agar hasil penelitian yang telah tercapai sesuai dengan ISO 31000, yang merupakan standar manajamen risiko dengan tujuan untuk memberikan prinsip-prinsip dan pedoman dalam melakukan manajemen risiko(Fachrezi, 2021)

Pengumpulan data untuk studi ini dilakukan melalui studi liteartur, Informasi fenomenas kebocoran data nasabah serta adanya serangan sber dari media online, serta wawancara dengan beberapa praktisi perbankan dan akademisi terkait topik studi ini

Teknik analisis yang digunakan dalam penelitian ini melibatkan penerapan kerangka kerja ISO untuk mengidentifikasi potensi risiko kebocoran data nasabah dan serangan siber dalam konteks lingkungan teknologi informasi perbankan. Penilaian risiko dilakukan dengan merujuk pada panduan ISO 31000:2018 sebagai landasan untuk mengevaluasi tingkat risiko yang telah diidentifikasi.

III. HASIL DAN DISKUSI

3.1 Hasil Manajemen Resiko dengan ISO 3100: 2018 Framework

Secara Umum, menurut ISO 31000:2018 *Risk Management Guideline* proses manajemen risiko adalah proses sistematis penerapan kebijakan, prosedur, dan praktik terkait aktivitas komunikasi dan konsultasi risiko,

penetapan cakupan, konteks, dan kriteria risiko, pelaksanaan penilaian risiko (*risk assessment*) yang terdiri dari identifikasi risiko, analisis risiko, dan evaluasi risiko, perlakuan risiko (*risk treatment*), pemantauan dan peninjauan, perekaman, dan pelaporan(ISO 31000, 2018). Komunikasi dan Konsultasi dalam implementasi manajemen resiko dengan ISO 31000 adalah sesuatu yang wajib dilakukan. Scope dalam hal ini meliupti prinsip, framework dan proses, dan dalam Context Manajmen Resiko TI serta memiliki criteria resiko non finansial, yaitu resiko kebocoran data nasabah dan serangan siber.

Risk Assesment

Secara umum, tahap penilaian resiko, meliput tahap identifikasi resiko, analisis resiko dan evaluasi resiko.

Risk Identification

Tabel 1 Identifikasi Resiko

Klasifikasi Resiko	Jenis Resiko	Identifikasi Resiko
Resiko Non Financial (Teknologi Informasi)	Kebocoran Data Nasabah	Risiko kebocoran data pelanggan merupakan risiko akibat pengunggahan data pribadi sensitif secara berlebihan ke internet. Risiko kebocoran data dapat terjadi dari jasa keuangan yang menjual data konsumen, memberikan data kepada pihak ketiga dan kemungkinan sistem aplikasi data mudah diakses dan diretas oleh hacker(Yuspin et al., 2023)
Resiko Non Financial (Teknologi Informasi)	Serangan Siber	Serangan siber adalah salah satu risiko paling mengancam keamanan nasional(Vimy et al., 2022). Risiko serangan siber adalah risiko kerugian akibat serangan melalui dunia maya oleh perusahaan yang mengganggu, menghancurkan, atau secara jahat mengendalikan lingkungan/infrastruktu komputasi, merusak integritas data, atau mencuri informasi (Luthfah, 2021).

Risk Analysis

Analisis risiko dilakukan untuk mengevaluasi tingkat risiko yang terjadi, seberapa sering risiko terjadi, serta seberapa besar dampak yang akan ditimbulkan jika risiko terjadi. Analisis risiko juga meliputi identifikasi faktor yang mempengaruhi risiko, seperti probabilitas terjadinya risiko, kerentanan organisasi terhadap risiko, dan dampak yang mungkin timbul. Kemungkinan resiko serta kategorinya ditunjukkan pada Tabel 2.

Tabel 2 Kemungkinan Frekwensi Kejadian

Frekwensi	Kategori Resiko	Keterangan
1	Sangat Kecil	Kecil kemungkinan terjadi / tidak pernah terjadi
2	Kecil	Risiko jarang terjadi 3-5 tahun
3	Sedang	Risiko terkadang terjadi pada
4	Berat	Risiko sering terjadi 1-2 tahun
5	Sangat Berat	Risiko pasti terjadi < 1 tahun

Pada Tabel 3 menyatakan nilai dari dampak akibat resiko.

Tabel 3 Penilaian Dampak Resiko

Nilai	Keterangan
1	Risiko tidak mengganggu aktivitas proses bisnis
2	Risiko sedikit menghambat proses bisnis
3	Risiko mengganggu proses bisnis
4	Risiko menghambat bagian tertentu proses bisnis
5	Risiko menghambat serta mengganggu seluruh proses bisnis

Sedangkan pada Tabel 4 analisis frekwensi dan dampak untuk tahap identifikasi resiko nantinya.

Tabel 4 Analisis Frekwensi dan Dampak Resiko

No	Kemungkinan Resiko	Frekwensi	Dampak
1	Kebocoran Data Nasabah	5	Risiko bisa menghambat serta mengganggu seluruh proses bisnis
2	Serangan Siber	5	Risiko bisa

No	Kemungkinan Resiko	Frekwensi	Dampak
			menghambat serta mengganggu seluruh proses bisnis

Analisa resiko dengan menggunakan komponen-komponen utama dalam ISO31000:2018, hasilnya ditunjukkan pada Tabel 5.

Tabel 5 Analisa Resiko

Komponen ISO 31000 Framework	Jenis Resiko	Analisa Resiko berbasis ISO
Kepemimpinan dan Komitmen	Kebocoran Data Nasabah	Pemimpin atau eksekutif yang tidak memahami sepenuhnya urgensi dan dampak kebocoran data. Ketidaksetujuan atau kurangnya komitmen dari pihak eksekutif untuk alokasi sumber daya cukup untuk keamanan data
	Serangan Siber	Pemimpin atau eksekutif yang tidak memahami sepenuhnya kompleksitas dan urgensi serangan siber. Tidak ada komitmen yang cukup dari pihak eksekutif untuk melibatkan sumber daya yang diperlukan dalam perlindungan terhadap serangan siber.
Integrasi	Kebocoran Data Nasabah	Tantangan dalam mengintegrasikan kebijakan dan kontrol keamanan dengan sistem yang sudah ada. Kurangnya koordinasi antar departemen dapat menyebabkan celah dalam perlindungan data
	Serangan Siber	Tantangan mengintegrasikan kebijakan dan kontrol keamanan dengan sistem yang sudah ada, meninggalkan celah keamanan. Kurangnya koordinasi antar departemen dapat menyebabkan kehilangan informasi dan kurangnya pemahaman tentang risiko serangan siber.
Disain	Kebocoran Data Nasabah	Jika desain keamanan tidak mepertimbangkan konteks organisasi, risiko kebocoran dapat meningkat. Kurangnya penerapan enkripsi pada data sensitif dapat kembali meningkatkan risiko kebocoran.
	Serangan Siber	Jika desain keamanan tidak mempertimbangkan konteks organisasi, risiko serangan siber dapat meningkat. Kurangnya penerapan enkripsi pada data sensitif dapat meningkatkan risiko pencurian data.
Implementasi	Kebocoran Data Nasabah	Tanpa sistem deteksi intrusi yang memadai, serangan siber mungkin tidak terdeteksi tepat waktu. Implementasi yang buruk atau tidak teratur dari perangkat lunak keamanan dapat meninggalkan celah keamanan.
	Serangan Siber	Jika implementasi tidak menyertakan pembaruan rutin, risiko eksploitasi melalui kerentanan yang sudah diketahui dapat meningkat. Implementasi yang buruk dari perangkat lunak keamanan dapat meninggalkan celah yang dimanfaatkan oleh penyerang.

Komponen ISO 31000 Framework	Jenis Resiko	Analisa Resiko berbasis ISO
Evaluasi	Kebocoran Data Nasabah	Pemantauan yang tidak rutin atau kurangnya alat pemantauan dapat mengakibatkan kegagalan mendeteksi perubahan dalam risiko. Jika penilaian risiko dilakukan secara dangkal, risiko potensial mungkin tidak teridentifikasi.
	Serangan Siber	Jika pemantauan tidak dilakukan secara rutin, risiko serangan siber mungkin tidak terdeteksi tepat waktu. Jika penilaian risiko dilakukan secara dangkal, risiko potensial mungkin tidak teridentifikasi.
Perbaikan	Kebocoran Data Nasabah	Jika organisasi tidak dapat belajar dari insiden keamanan, risiko kebocoran data dapat terulang. Respon yang lambat terhadap insiden dapat memperburuk dampak dan meningkatkan risiko.
	Serangan Siber	Jika organisasi tidak dapat belajar dari serangan siber sebelumnya, risiko keberlanjutan serangan dapat meningkat. Kurangnya respons cepat terhadap insiden dapat memperburuk dampak dan meningkatkan risiko serangan selanjutnya.

Risk Evalution

Evaluasi risiko dilakukan untuk menentukan risiko tersebut apakan diterima atau dihilangkan, evaluasi risiko dilakukan dengan membandingkan hasil analisis risiko dengan kriteria yang diterapkan oleh organisasi atau perusahaan. Jika risiko dianggap terlalu besar maka organisasi harus mencari cara untuk mengurangi risiko tersebut. Hasil evaluasi resiko ditunjukkan pada Tabel 6.

Tabel 6 Evaluasi Resiko

Prioritas Resiko / Kategori Level Resiko	Level Resiko Residual Harapan	Keputusan Mitigasi Resiko	Indikator Resiko Utama (IRU)
Kebocoran Data Nasabah **Sangat Berat (5)**	**Berat (4)**	Kepemimpinan dan komitmen dalam proses pengambilan keputusan dan komunikasi terkait dengan keamanan informasi. Lakukan audit dan penilaian rutin untuk memastikan bahwa sistem dan proses terintegrasi dengan baik dan memenuhi standar keamanan yang ditetapkan. Pastikan desain sistem manajemen risiko sesuai dengan konteks dan kebutuhan organisasi Pastikan alokasi sumber daya yang cukup untuk implementasi manajemen risiko, termasuk kebutuhan sumber daya manusia dan teknologi. Lakukan pemantauan teratur untuk mendeteksi perubahan dalam lingkungan risiko. Identifikasi dan analisis mendalam setiap insiden keamanan. Terapkan perubahan pada proses dan kebijakan untuk mencegah terulangnya insiden serupa.	Frekuensi Akses Tidak Biasa Volume Data yang Dikirim ke Alamat yang Tidak Biasa Peningkatan Aktivitas Pengguna dengan Hak Akses Tinggi Perubahan Konfigurasi atau Pengaturan Sistem yang Tidak Dikenal Permintaan Data yang Tidak Biasa Terjadi Penggunaan Kredensial yang Dicurigai: Deteksi Malware atau Aktivitas APT (Advanced Persistent Threat): Terjadi Peningkatan Penggunaan Bandwidth yang Tidak Biasa:
Serangan Siber		Pemimpin organisasi harus terus meningkatkan pemahaman mereka tentang	

Prioritas Resiko / Kategori Level Resiko	Level Resiko Residual Harapan	Keputusan Mitigasi Resiko	Indikator Resiko Utama (IRU)
Sangat Berat (5)	**Berat (4)**	ancaman siber dan dampaknya. Memastikan bahwa sistem keamanan dan infrastruktur IT terintegrasi secara efektif untuk mendeteksi dan melindungi dari berbagai jenis serangan siber Memilih dan mengimplementasikan perangkat keras dan perangkat lunak yang aman dengan mengurangi kerentanan terhadap serangan siber Melibatkan pengguna dalam pelatihan keamanan siber untuk mengurangi risiko yang timbul dari kelalaian atau manipulasi manusia\ Melakukan pemantauan terus-menerus terhadap tren keamanan siber dan menganalisis hasil pemantauannya	

Risk Treatment

Risk Treatment atau perlakuan risiko merupakan tindakan yang diberikan berupa usulan perlakuan dalam menangani risiko yang ada. Tabel 7 menunjukan perlakukan dari kedua resiko dengan memperhatikan kategori level resiko.

Tabel 7 Risk Treatment

Kemungkinan Resiko	Kategori Level Resiko	Usulan Perlakuan Resiko
Kebocoran Data Nasabah	**Sangat Berat (5)**	Mempersiapkan implemetasi untuk Tatakelola TI yang baik, serta memperbaiki budaya perusahaan
		Menyiapkan suatu implementasi
Seragan Siber	**Sangat Berat (5)**	cyber security system yang handal dan melakukan monioring dan evaluasi

Monitoring and Review

Proses pencatatan dan pelaporan risiko menjadi krusial untuk menjaga transparansi dan akuntabilitas dalam pengelolaan risiko. Informasi tentang risiko yang diidentifikasi, hasil evaluasi, dan tindakan yang diambil untuk mengelolanya harus dicatat dengan cermat. Selain itu, melaporkan risiko secara berkala kepada pihak-pihak yang berkepentingan, seperti manajemen senior, pemilik perusahaan, atau pihak eksternal, membantu memastikan pemahaman yang konsisten tentang status risiko.

Recording and Reporting

Manajemen risiko bukanlah suatu hal yang statis; oleh karena itu, dibutuhkan pemantauan dan peninjauan secara teratur. Ini mencakup pemantauan implementasi strategi pengelolaan risiko, mengidentifikasi perubahan dalam lingkungan bisnis atau organisasi yang dapat mempengaruhi risiko, dan mengevaluasi sejauh mana tindakan yang diambil efektif. Jika terdapat perubahan signifikan dalam kondisi atau konteks, perlu untuk meninjau kembali analisis risiko dan strategi pengelolaan risiko. Dengan cara ini, serangkaian langkah ini membentuk siklus manajemen risiko yang dinamis dan adaptif, membantu organisasi tetap tanggap terhadap perubahan dalam lingkungan bisnis dan menjaga kesiapan mereka dalam menghadapi risiko

3.2 Pembahasan

Manajemen resiko TI dalam studi ini secara khusus difokukan untuk resiko kebocoran data nasabah dan serangan siber dengan menggunakan kerangka ISO 31000: 2018, yang menekankan pada prinsip, proses dan kerangka kerja. Hal ini berbeda dengan beberpa penelitian sebelumnya yang bukan di industri perbankan. Evinia & Sitokdana(2023), yang membahasa analisis manajemen resiko berbasis TI dengan ISO 31000:2018

framework, dengan studi kasus PT.Bawen Mediatama, sedangkan Fachrezi(2021) dalam tujuan studinya adalah mengelola resiko keamanan aset Teknologi Informasi dengan ISO 31000:2018 pada Diskomimfo Salatiga, dimana pada studi mereka, perlu adanya tindakan untuk meminimalisir kemungkinan risiko yang akan terjadi yaitu dengan menindaklanjuti perlakuan risiko dengan baik agar proses bisnis berjalan sesuai dengan yang diharapkan.

Identifikasi resiko terkait kebocoran data nasabah dan serangan siber, dinyatakan bahwa kedua resiko ini memiliki kategori level resiko yang sangat berat (Level 5) dan bardampak menghambat serta mengganggu seluruh proses bisnis di industri perbankan. Hal ini sejalan dengan yang dinyatakan oleh serangan siber adalah salah satu risiko paling mengancam keamanan nasional(Vimy et al., 2022) bahwa serangan siber adalah salah satu risiko paling mengancam keamanan nasional.

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.

IV. KESIMPULAN

Penelitian memiki tujuan yang ditekankan pada kajian dan analisis menajamen resiko teknologi informasi dengan menggunakan ISO 31000: 2018, dengan studi kasus resiko kebocoran data nasabah dan serangan siber pada industri perbankan.

Berdasarkan hasil identifikasi resiko terkait kebocoran data nasabah dan serangan siber, maka dapat dinyatakan bahwa kedua resiko ini memiliki kategori level resiko yang sangat berat (Level 5) dan bardampak menghambat serta mengganggu seluruh proses bisnis di industri perbankan, Hasil analisis resiko dengan menggunakan kerangka kerja 31000:2018 maka ke lima komponen dalam kerangka kerja ini wajib dijalankan dan selanjutnya dilakukan risk trestment, memantau dan meninjau semua prose serta membuat pencatatan dan melaporkannya.

Penelitian masa depan untuk analisis manajemen resiko ini bisa menggunakan kerangka kerja kerja lain, seperti COSO-ERM Framework, Cobit 5.0, atau NIST-Risk Management Framewrok.

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

CNN Indonesia. (2023). Kominfo Clarifies the Alleged BSI Data Leakage Circulating. In *CNN News*. Retrieved from https://www.cnnindonesia.com/teknologi/2023

Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. *SAGE Publications, Inc* (Sixth Edit). SAGE Publications Asia-Pacific Pte. Ltd.

Evinia, E., & Sitokdana, M. N. N. (2023). Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama). *Journal of Information Systems and Informatics*, *5*(1), 380–390.

Fachrezi, M. I. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(2), 764–773.

Ghiffari, M. N., Nurliana, A., & Girinoto. (2023). Analisis Pola Penyebaran Informasi Insiden

Kebocoran Data Melalui Pendekatan Social Network Analysis (SNA). *Info Kripto*, *17*(1), 1–6.ISO 31000. (2018). BSI Standards Publication Risk management — Guidelines. *BSI Standard Publication*.

Luthfah, D. (2021). Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law. *Jurnal Hukum Humaniter Dan HAM*, *3*(1), 11–22.

Rosana, F. C. (2017). BRI Life Customer Data Leaks Evidence of Weak Protection and Regulation. In *Tempo.co.id*.

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). The Threat of Cyber Attacks on Indonesia's National Security. *Jurnal Kewarganegaraan*, *6*(1), 2319–2327.

Yuliani, A. (2017). Indonesia Attacked by Hackers Billion Times Every Day. In *KOMINFO.go.id*. Retrieved from https://www.kominfo.go.id/content/detail/1195

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1),99–130.