Jurnal Ilmu Siber dan Teknologi Digital (JISTED)
ISSN2986-7312 Vol 2, No 1, 2023, 61-73 https://doi.org/10.35912/jisted.v2i1.2351

Manajemen Risiko Teknologi Informasi Pada Aplikasi CMS di PT. Sarana Citranusa Kabil - Batam Menggunakan ISO31000:2018 *(Information Technology Risk Management in CMS Applications at PT. Citranusa Kabil Facility - Batam Using ISO31000:2018)*

Suroto Suroto[1*], John Friadi[2]
Universitas Batam, Batam[1,2]
suroto@univbatam.ac.id[1*], john.friadi@univbatam.ac.id[2]

Riwayat Artikel
Diterima pada 22 Juli 2023
Revisi 1 pada 24 Juli 2023
Revisi 2 pada 6 Agustus 2023
Disetujui pada 21 Agustus 2023

Abstract
Purpose: The purpose of this research is to assist PT SCN in improving its ability in risk management, by minimizing the risks contained in the CMS application. In addition, it aims to provide recommendations some risk action for risks that have been identified.
Methodology/approach: Object of this research is PT Sarana Citranusa Kabil – Batam. In order to support its business activities, PT SCN uses a application, called Cash Management System (CMS). This study was conducted using method of case study research. Technique of data collection is in the form of observation. The procedures of this research follow the ISO31000:2018 standard.
Results/findings: This study found that (i) there are 20 possible risks, which can disrupt the performance of the CMS and business activities; (ii) 2 possible risks with high level; (iii) 10 possible risks with medium level; (iv) 8 possible risks with low level.
Limitations: This research focuses on risk management in the use of CMS applications. The research does not address risks outside of information technology, for example, health and safety environmental issues.
Contribution: The result of this risk analysis is a proposed action recommendation based on the impact and frequency of occurrence. Finally, PT SCN can prevent and minimize risks so that the function of the CMS application can run optimally.
Keywords: *Risk Management, IT Risk, Risk Assessment, ISO13000*
How to cite: Suroto, S., Friadi, J. (2023). Manajemen Risiko Teknologi Informasi Pada Aplikasi CMS di PT. Sarana Citranusa Kabil - Batam Menggunakan ISO31000:2018. *Jurnal Ilmu Siber dan Teknologi Digital*, 2(1), 61-73.

1. Pendahuluan

Teknologi informasi (TI) adalah tulang punggung inovasi teknologi. Inovasi ini telah memainkan peran besar dalam mengembangkan manajemen bisnis. Saat ini, tidak ada satu pun bisnis di dunia ini yang tidak menggunakan teknologi TI. Beberapa bidang dimana teknologi sangat penting untuk bisnis termasuk sistem penjualan, penggunaan TIK dalam manajemen, sistem akuntansi, dan aspek kompleks lainnya dari aktivitas bisnis sehari-hari (Lamarco, 2018). Teknologi memungkinkan kita mengotomatiskan proses bisnis, sehingga meningkatkan produktivitas kita (anonymous, 2022). Teknologi memungkinkan kita untuk menggunakan lebih sedikit sumber daya, untuk meningkatkan kualitas dan kecepatan pelayanan kepada pelanggan. Teknologi juga memudahkan untuk menyimpan lebih banyak informasi dengan tetap menjaga integritas informasi tersebut. Kita lebih mampu menyimpan informasi yang sensitif dan rahasia. Informasi dapat diambil secara instan saat dibutuhkan, dan dapat dianalisis untuk mempelajari tren masa lalu dan untuk meramalkan masa depan.

Namun, dengan semakin meningkatnya penggunaan teknologi informasi, maka semakin meningkat pula ancaman atau risiko yang dapat terjadi suatu saat. Entitas bisnis perlu melakukan pengendalian risiko terhadap risiko SI/TI, dengan melakukan manajemen risiko yang tepat (Angraini & Pertiwi, 2017). Manajemen risiko dilakukan dengan cara melakukan analisis risiko hingga mengevaluasi risiko. Sehingga hasil yang diharapkan berupa rekomendasi pengendalian risiko dapat maksimal dan sesuai dengan yang diharapkan oleh instansi tersebut.

Studi kasus pada penelitian ini adalah PT. Sarana Citranusa Kabil (PT. SCN) - Batam. PT. SCN merupakan perusahaan swasta yang bergerak di bidang usaha Kepelabuhan. Sebagai pengelola pelabuhan umum di Kabil. Dalam rangka untuk menunjang kegiatan bisnisnya, PT. SCN menggunakan sebuah aplikasi *Cash Management System* (CMS). Aplikasi CMS digunakan untuk mengelola transaksi jasa kepelabuhan dan sistem pembayarannya. Aplikasi CMS sangat membantu, namun disisi lain aplikasi ini juga memiliki risiko yang dapat terjadi sewaktu-waktu. Sebagai contoh, risiko berupa Human Error, kegagalan koneksi jaringan dan Server Down (Friadi, Yani, Zaid, & Sikumbang, 2023). Oleh karena itu, sebuah analisis dan evaluasi manajemen risiko pada aplikasi CM diperlukan. Ini dengan cara mengidentifikasi risiko dan potensi risiko yang ada serta bagaimana dampak dari kemungkinan risiko yang akan terjadi.

Dari permasalahan tersebut, maka diperlukan analisis risiko dengan menggunakan kerangka kerja ISO 31000:2018, dimana ISO31000:2018 memiliki standar dan tinjauan yang lebih luas dan dapat diterapkan di berbagai ruang lingkup instansi serta lebih ideal dibandingkan standar lainnya (RUMBA, MIRSEL, & SABU, 2022). Tujuan dari penelitian ini adalah untuk membantu PT. SCN dalam meningkatkan kemampuan dalam manajemen risiko, dengan cara meminimalisir risiko dan potensi risiko yang terdapat pada aplikasi CMS. Selain itu, bertujuan untuk memberikan rekomendasi yang tepat terhadap risiko yang telah diidentifikasi atau risiko yang sewaktu-waktu dapat muncul dan mengganggu kinerja sistem .

2. Tinjauan Pustaka

2.1. Penelitian Sebelumnya

Lela Dina Berliana dan Andeka Rocky Tanamaah pada tahun 2021 melakukan studi mengenai manajemen risiko dengan menggunakan ISO 31000:2009 dilakukan oleh. Penelitian tersebut dengan studi kasus yang dilakukan pada bidang industri Disperinnaker Kota Salatiga. Dari penelitian tersebut didapatkan hasil, bahwa ada 14 kemungkinan risiko yang mengganggu jalannya aktivitas kegiatan pada bidang industri Disperinnaker Kota Salatiga. Dari 14 kemungkinan risiko, ada 3 yang masuk ke dalam risiko tinggi , 6 yang masuk ke dalam level sedang, 5 yang masuk dalam level rendah (Berliana & Tanamaah, 2021).

Vania Rizqita Putri1, Agustinus Fritz Wijaya melakukan penelitian manajemen risiko teknologi informasi dengan menggunakan ISO 31000 pada tahun 2022. Studi kasus di PT. XYZ yang merupakan salah satu kantor cabang anak perusahaan perbankan di Indonesia yang fokus pada penyediaan fasilitas leasing, investasi dan modal kerja (Suciati, Simamora, Panusunan, & Fauzan, 2023). Hasil penelitian ini didapatkan 13 kemungkinan risiko yang memiliki tingkat risiko rendah , 6 kemungkinan risiko yang memiliki tingkat risiko sedang tingkat risiko serta 2 kemungkinan risiko yang memiliki tingkat risiko tinggi . Selain itu, dihasilkan proposal *risk treatment* yang dapat dijadikan acuan oleh PT. XYZ untuk meminimalkan kerugian yang diakibatkan oleh risiko tersebut. (Putri & Wijaya, 2022).

Selain itu, Elly, Hanes dan Joosten melakukan penelitian dengan judul ISO 31000:2018-Based IT Infrastructure Risk Management Study (Case Study: Universitas Mikroskil) pada tahun 2022. Berdasarkan penelitian, hasil dari tingkat risiko adalah 2 kemungkinan risiko dengan level rendah, 10 kemungkinan risiko dengan level tinggi, dan 3 kemungkinan risiko dengan level ekstrim (Elly, Hanes, & Joosten, 2022).

2.2. Manajemen Resiko SI/TI

(Johnson, 2019) menyatakan, risiko adalah bagian penting dalam melakukan bisnis, dan di dunia dimana sejumlah besar data diproses dengan kecepatan yang semakin tinggi. Risiko TI meliputi kegagalan perangkat keras dan perangkat lunak, kesalahan manusia, spam, virus, dan serangan jahat, serta bencana alam seperti kebakaran, topan, atau banjir. Jika kita memiliki bisnis yang menggunakan TI, penting untuk mengidentifikasi risiko terhadap sistem dan data TI. Sehingga kita dapat mengurangi atau mengelola risiko tersebut, dan untuk mengembangkan rencana respons jika terjadi krisis TI. Aktifitas mengidentifikasi dan mengurangi risiko merupakan tantangan bagi perusahaan manapun. Manajemen risiko merupakan istilah yang digunakan tim TI dan keamanan setiap hari, disadari atau tidak (What is Information Technology (IT) Risk Management, 2022). Ini adalah proses yang konsisten untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani eksposur kerugian sambil juga mengamati pengendalian risiko dan sumber daya dalam upaya untuk mengurangi dampak kerugian yang merugikan. Ini sering kali merupakan praktik yang juga digunakan di dalam departemen TI tetapi digunakan untuk sistem, jaringan, dan perangkat perusahaan untuk memitigasi potensi ancaman dunia maya.

Cara tim mendekati manajemen risiko dari sudut pandang bisnis tidak selalu diterjemahkan ke dalam metodologi yang sama tentang pendekatan manajemen risiko TI untuk keamanan TI. Ini sering menjadi masalah umum di seluruh perusahaan saat mendekati risiko bisnis versus risiko keamanan TI. Keamanan TI sering kali mengharuskan profesional dan pemimpin TI untuk melihat lebih dalam akar penyebab peningkatan manajemen risiko TI mereka. Di bawah ini adalah beberapa akar penyebab umum untuk masalah manajemen risiko TI (What is Information Technology (IT) Risk Management, 2022).

- *Third-party IT Solutions (Shadow IT Solutions)*
- *mmaturity of Processes*
- *Technical Debt*
- *Lack of Communication*

2.3. Aplikasi CMS

Transaksi yang terjadi antara PT. SCN dengan pelanggan merupakan transaksi jual beli jasa, bukan barang. Layanan / jasa yang disediakan oleh PT.SCN , selaku pengelola pelabuhan, adalah layanan labuh, tambah, supply air, pembuangan sampah. Pelanggan sebagai pengguna jasa harus membayar lunas sebelum kapal meninggalkan pelabuhan. Pembayaran melalui transfer bank. Guna memudahkan dalam pengelolaan data transaksi, SCN mengembangkan sendiri sebuah sistem informasi, yang dinamakan Cash Management System (CMS). CMS merupakan sistem informasi basis web yang berfungsi untuk mengelola transaksi jasa kepelabuhan dan sistem pembayarannya. Manfaat yang dapat dirasakan, bahwa pelanggan (agen kapal & perusahaan bongkar muat) tidak perlu ke bank untuk membayar atas suatu transaksi jasa di pelabuhan SCN. Cukup top up saldo dan selanjutnya aplikasi CMS akan meminta sistem bank untuk melakukan auto debit pada rekening pengguna jasa.

2.4. ISO 31000:2018

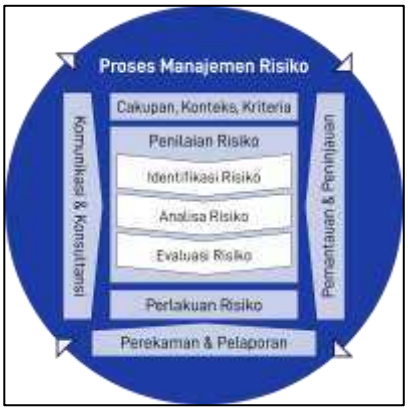
Pada Februari 2018, organisasi standar internasional ISO menerbitkan ISO 31000:2018 Risk management — Guidelines. Standar ini menggantikan ISO 31000:2009 Risk management — Principles and Guidelines yang diterbitkan pada November 2009. ISO 31000 adalah panduan penerapan risiko yang terdiri atas tiga elemen: prinsip (principle), kerangka kerja (framework), dan proses (process). Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko. Kerangka kerja adalah pengaturan sistem manajemen risiko secara terstruktur dan sistematis di seluruh organisasi. Proses adalah aktivitas pengelolaan risiko yang berurutan dan saling terkait (Vorst, Priyarsono, & Budiman, 2018)

Delapan prinsip ISO 31000, yaitu:

- Manajemen risiko harus diintegrasikan ke dalam seluruh operasi dan aktivitas bisnis.
- Pendekatan harus terstruktur dan komprehensif.

- Proses dan kerangka kerja manajemen risiko harus disesuaikan agar sesuai dengan tujuan dan konteks organisasi.
- Pemangku kepentingan harus dilibatkan dalam kerangka pengelolaan; itu harus inklusif.
- Manajemen risiko harus dinamis dan kuat; pemikiran preemptive, mengantisipasi, mendeteksi, mengakui dan menanggapi perubahan.
- Manajemen risiko memperhitungkan keterbatasan informasi yang tersedia.
- Faktor manusia dan budaya adalah yang terpenting, dan harus dipertimbangkan pada semua tahapan dan aspek manajemen risiko.
- Kerangka manajemen risiko terus ditingkatkan melalui pembelajaran dan pengalaman.

Sedangkan, proses manajemen resiko dapat dijelaskan dalam diagram di bawah ini



Gambar 1. Proses Manajemen Resiko Berdasar Standar ISO 31000:2018
Sumber: proxsisgroup.com (2020)

ISO 31000 membantu organisasi mengembangkan strategi manajemen risiko untuk mengidentifikasi dan memitigasi risiko secara efektif, sehingga meningkatkan kemungkinan pencapaian tujuan dan meningkatkan perlindungan aset perusahaan. Tujuan menyeluruhnya adalah untuk mengembangkan budaya manajemen risiko di mana karyawan dan pemangku kepentingan menyadari pentingnya pemantauan dan pengelolaan risiko.

3. Metodologi Penelitian

Penelitian manajemen risiko pada aplikasi CMS di PT. SCN ini dilakukan dengan menggunakan metode penelitian studi kasus. Studi kasus merupakan penelitian kualitatif dimana peneliti melakukan eksplorasi secara mendalam terhadap program, proses, aktivitas atau orang. Hal ini karena objek penelitian (aplikasi CMS) terikat oleh waktu dan aktivitas.

Peneliti melakukan pengumpulan data secara mendetail dengan menggunakan teknik pengumpulan data berupa observasi. Observasi atau pengamatan langsung ke lapangan dilakukan dalam waktu yang berkesinambungan.

Prosedur penelitian ini mengikuti standar ISO31000:2018, seperti gambar 1 di atas. Dengan demikian, langkah atau tahapan penelitian ini adalah sebagai berikut:

1) Identifikasi Risiko
   Langkah ini untuk menemukan, mengenali, dan mendeskripsikan peristiwa atau risiko yang tidak pasti yang dapat membantu atau mencegah departemen mencapai tujuannya. Ini melibatkan identifikasi sumber risiko, peristiwa, penyebab dan konsekuensi potensial mereka. Informasi yang relevan, tepat dan terkini penting dalam mengidentifikasi risiko. Dalam penelitian ini, bagaimana memperoleh dan menyajikan data risiko yang mungkin timbul dan yang dapat mengganggu proses bisnis pada penggunaan aplikasi CMS.
2) Analisis Risiko
   Langkah untuk memahami sifat risiko dan menentukan tingkat eksposur risiko. Ini melibatkan pertimbangan ketidakpastian, sumber risiko, konsekuensi, kemungkinan, peristiwa, skenario, kontrol dan efektivitasnya. Tahap analisis risiko pada aplikasi CMS.

3) Evaluasi Risiko
   Membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan apakah diperlukan tindakan tambahan. Hal ini dapat menyebabkan keputusan untuk: (1) tidak melakukan apa-apa lagi (2) mempertimbangkan opsi penanganan risiko (3) melakukan analisis lebih lanjut untuk lebih memahami risiko (4) mempertahankan kontrol yang ada (5) mempertimbangkan kembali tujuan.
4) Penanganan Risiko
   Memilih dan menerapkan opsi untuk mengatasi peristiwa yang tidak pasti - terima, pantau, bagikan, hindari, kurangi kemungkinan/dampak ancaman atau optimalkan peluang. Menyeimbangkan manfaat potensial yang diperoleh dalam kaitannya dengan pencapaian tujuan terhadap biaya, usaha atau kerugian implementasi. Toleransi terhadap risiko harus menentukan jenis dan luasnya respons.

4. Hasil dan Pembahasan

4.1. Penilaian Resiko

Ini adalah langkah pertama yang perlu dilakukan terkait proses manajemen resiko pada aplikasi CMS. Langkah ini melalui beberapa tahapan kecil secara berurutan, yaitu mengidentifikasi risiko, kemudian menganalisis risiko, dan terakhir mengevaluasi risiko.

4.1.1. Identifikasi Risiko

4.1.1.1. Identifikasi Aset

Pada tahap ini dilakukan identifikasi aset-aset yang terkait dengan aplikasi CMS. Aset-aset meliputi data, perangkat lunak, dan perangkat keras. Fokus pada identifikasi 3 aset tersebut.

Tabel 1. Identifikasi Aset

Komponen SI/TI	Aset
Data	Data pelanggan, data kapal, data berth, data transaksi pengguna jasa
Software	Cash Management System
Hardware	Server

Sumber: Data primer dari observasi (2023)

4.1.1.2. Mengidentifikasi Risiko yang Mungkin Terjadi

Selanjutnya dari identifikasi kemungkinan risiko, kita dapat mengklasifikasikan sumber resiko dalam 3 faktor, yaitu faktor alam, faktor manusia, dan faktor sistem atau infrastruktur. Berdasarkan hasil identifikasi risiko, ditemukan 20 risiko yang mungkin terjadi pada aplikasi CMS. Hasil identifikasi kemungkinan risiko dapat dilihat pada tabel 2.

Tabel 2. Mengidentifikasi Risiko Yang Mungkin Terjadi

Faktor	Id	Risiko Yang Mungkin Terjadi
Alam	R01	Banjir
	R02	Kebakaran
	R03	Gempa bumi
	R04	Hujan badai
MANUSIA	R05	Kesalahan Manusia
	R06	Penyalahgunaan hak akses
	R07	Pencurian dan Kebocoran Data
	R08	Perangkat keras pencurian
	R09	Peretasan

	R10	Antarmuka Pengguna yang sulit untuk memahami
	R11	Kerusakan pada fasilitas
	R12	Karyawan baru yang masih awam dengan sistem
SISTEM DAN INFRASTRUKTUR	R13	Koneksi jaringan yang buruk
	R14	Kerusakan peralatan jaringan
	R15	Database Server bermasalah
	R16	Kehilangan data
	R17	Suhu ruang terlalu panas
	R18	Backup data bermasalah
	R19	Kesalahan sistem
	R20	Tidak ada daya listrik

Sumber: Data primer dari observasi (2023)

4.1.1.3. Mengidentifikasi Dampak dari Risiko yang Mungkin Terjadi

Selanjutnya pada tahap ini dilakukan identifikasi dampak dari risiko yang mungkin terjadi pada aplikasi CMS. Pada tahap ini, dilakukan identifikasi terhadap dampak dari kemungkinan risiko yang telah diidentifikasi pada tabel 2. Hasil identifikasi dampak disajikan dalam tabel 3.

Tabel 3. Mengidentifikasi Dampak dari Risiko yang Mungkin Terjadi

Faktor	**Id**	**Risiko Yang Mungkin Terjadi**	**Dampak**
Alam	R01	Banjir	Aset yang terekspos banjir dapat menyebabkan kerusakan
	R02	Kebakaran	Dapat menyebabkan kerusakan pada aset
	R03	Gempa bumi	Dapat menyebabkan kerusakan pada aset
	R04	Hujan badai	Memungkinkan terjadinya kerusakan aset
MANUSIA	R05	Kesalahan Manusia	Ada miskomunikasi data, data invalid
	R06	Penyalahgunaan hak akses	karyawan lain dapat mengakses sistem menggunakan akun pengguna lain. Data tidak valid
	R07	Pencurian dan Kebocoran Data	Data rahasia (tarif, transaksi) terekpos keluar.
	R08	Perangkat keras pencurian	Kerugian keuangan perusahaan
	R09	Peretasan	Bocornya data perusahaan, sistem down yang pada akhirnya timbul kehilangan waktu kerja

	R10	Antarmuka Pengguna yang sulit untuk dipahami	Pengguna bingung dalam menjalankan aplikasi
	R11	Kerusakan pada fasilitas	Kerusakan aset dan Kerugian finansial
	R12	Karyawan baru yang masih awam dengan sistem	Potensi problem yang akhirnya menimbulkan kehilangan waktu kerja (waktu yang dibutuhkan untuk troubleshooting)
SISTEM DAN INFRASTRUKTUR	R13	Koneksi jaringan yang buruk	Pengguna mengalami kesulitan mengakses sistem.
	R14	Kerusakan peralatan jaringan	Pengguna tidak dapat mengakses sistem.
	R15	Database Server bermasalah	Pengguna tidak dapat mengakses sistem.
	R16	Kehilangan data	Data perusahaan yang hilang
	R17	Suhu ruang terlalu panas	Hardware stuck, respon sistem lambat bahkan mungkin sistem tak dapat diakses.
	R18	Backup data bermasalah	Tak ada data backup. Potensi kehilangan data.
	R19	Kesalahan sistem	Pengguna tidak dapat mengakses sistem
	R20	Tidak ada daya listrik	Pengguna tidak dapat mengakses sistem

Sumber: Data primer dari observasi (2023)

4.1.2. Analisis Resiko

Pemeriksaan dampak peristiwa risiko pada hasil tujuan tertentu. Analisis dampak risiko dilakukan secara kualitatif dan kuantitatif. Setiap ancaman, resiko dan kemungkinan dinilai. Berikut tabel kriteria kemungkinan (*likelihood*) atau frekuensi kemungkinan risiko yang terjadi.

Tabel 4. Tabel Kriteria Kemungkinan (*Likelihood*)

Likelihood		**Deskripsi**	**Frekuensi Kejadian**
Skor	**Kriteria**		
1	Rare	Risiko tidak pernah terjadi	> 2 tahun
2	Unlikely	Risiko jarang terjadi	1 – 2 tahun
3	Possible	Tidak sering	7 – 12 bulan
4	Likely	Sering terjadi	4 – 6 bulan
5	Certain	Pasti terjadi	1 – 3 bulan

Sumber: Data primer dari observasi (2023)

Selanjutnya, nilai dari setiap dampak risiko yang terjadi ditentukan. Hal ini dapat dilihat dari tabel dampak yang terdiri dari risiko yang mungkin terjadi. Pada tabel Evaluasi Dampak digabungkan menjadi 5 kriteria dan dampak tersebut dinilai berdasarkan pada tidak berpengaruh hingga dampak yang sangat berpengaruh.

Tabel 5. Kriteria Dampak dan Skor

***Impact* (Dampak)**		**Deskripsi**
Skor	**Impact Level**	
1	Not Significant (Tidak signifikan)	tidak berdampak langsung pada operasi bisnis
2	Minor (Kecil)	mungkin termasuk kerusakan fitur yang tidak kritis atau keluhan pengguna dengan prioritas rendah.
3	Moderate (Sedang)	dapat memengaruhi fungsi non-kritis atau menyebabkan ketidaknyamanan bagi pengguna.
4	Major	Dampak yang signifikan dan mengganggu kegiatan bisnis. Hal ini dapat mencakup gangguan sistem parsial atau memengaruhi fungsi penting.
5	Severe	secara signifikan berdampak pada operasi bisnis, menyebabkan waktu henti yang lama, atau mengakibatkan kerugian finansial yang besar.

Sumber: Data primer dari observasi (2023)

Selanjutnya, setelah mendapatkan kriteria dari frekuensi kejadian pada tabel 4 dan kriteria dampak pada tabel 5, kemudian dilakukan penilaian risiko yang mungkin terjadi terhadap frekuensi kejadian dan kriteria dampak yang akan terjadi.

Tabel 6. Penilaian Kemungkinan dan Dampak

Id	**Possible Risk**	**Likelihood**	**Impact**
R01	Banjir	1	4
R02	Kebakaran	2	2
R03	Gempa bumi	1	5
R04	Hujan badai	2	3
R05	Kesalahan Manusia	4	3
R06	Penyalahgunaan hak akses	2	2
R07	Pencurian dan Kebocoran Data	1	2
R08	Perangkat keras pencurian	1	3
R09	Peretasan	1	3

R10	Antarmuka Pengguna yang sulit untuk dipahami	2	1
R11	Kerusakan pada fasilitas	1	3
R12	Karyawan baru yang masih awam dengan sistem	4	2
R13	Koneksi jaringan yang buruk	4	4
R14	Kerusakan peralatan jaringan	2	4
R15	Database Server bermasalah	4	4
R16	Kehilangan data	1	4
R17	Suhu ruang terlalu panas	4	1
R18	Backup data bermasalah	1	2
R19	Kesalahan sistem	3	4
R20	Tidak ada daya listrik	3	3

Sumber: Data primer dari observasi (2023)

Pada tabel 6, nilai dari setiap risiko yang mungkin terjadi telah ditentukan dalam tabel frekuensi kejadian dan tabel kriteria dampak.

4.1.3. Evaluasi Resiko

Pada langkah ini, kita membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan apakah risiko residual masih dapat ditoleransi. Sehingga melalui evaluasi ini, hasilnya akan dikelompokkan ke dalam matriks evaluasi risiko sesuai dengan 3 level, yaitu rendah, sedang, dan tinggi.

Tabel 7. Matriks Evaluasi Risiko

			***Impact* (Dampak)**				
			1	2	3	4	5
			Not significant	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood	**Certain**	5	Sedang	Sedang	Tinggi	Tinggi	Tinggi
	Likely	4	Sedang	Sedang	Sedang	Tinggi	Tinggi
	Possible	3	Rendah	Sedang	Sedang	Sedang	Tinggi
	Unlikely	2	Rendah	Rendah	Sedang	Sedang	Sedang
	Rare	1	Rendah	Rendah	Rendah	Sedang	Sedang

Sumber: Data primer dari observasi (2023)

Selanjutnya, setiap risiko yang mungkin terjadi dimasukkan ke dalam matriks penilaian risiko sesuai dengan kriteria frekuensi kejadian dengan kriteria dampak. Hasil disajikan dalam table 8 berikut.

Tabel 8. Matriks Evaluasi Risiko Berdasarkan Kemungkinan dan Dampak

			***Impact* (Dampak)**				
			Not significant	**Minor**	**Moderate**	**Major**	**Severe**
			1	**2**	**3**	**4**	**5**
Likelihood	**Certain**	5					
	Likely	4	R17	R12	R05	R13 R15	
	Possible	3			R20	R19	
	Unlikely	2	R10	R02 R06	R04	R14	
	Rare	1		R07 R18	R08 R09 R11	R01 R16	R03

Sumber: Data primer dari observasi (2023)

Pada tahap selanjutnya, matriks risiko dijabarkan ke dalam bentuk tabel yang telah diurutkan berdasarkan level Tinggi, Sedang, dan Rendah. Hasil disajikan dalam table 9 berikut.

Tabel 9. Pengelompokan Risiko Berdasarkan Tingkatan

Id	Possible Risk	Likelihood	Impact	Tingkat Resiko
R13	Koneksi jaringan yang buruk	4	4	Tinggi
R15	Database Server bermasalah	4	4	Tinggi
R01	Banjir	1	4	Sedang
R03	Gempa bumi	1	5	Sedang
R04	Hujan badai	1	3	Sedang
R05	Kesalahan Manusia	4	3	Sedang
R12	Karyawan baru yang masih awam dengan sistem	4	2	Sedang
R14	Kerusakan peralatan jaringan	2	4	Sedang
R16	Kehilangan data	1	4	Sedang
R17	Suhu ruang terlalu panas	4	1	Sedang
R19	Kesalahan sistem	3	4	Sedang
R20	Tidak ada daya listrik	3	3	Sedang
R02	Kebakaran	2	2	Rendah
R06	Penyalahgunaan hak akses	2	2	Rendah
R07	Pencurian dan Kebocoran	1	2	Rendah

	Data			
R08	Pencurian Perangkat keras	1	3	Rendah
R09	Peretasan	1	3	Rendah
R10	Antarmuka Pengguna yang sulit untuk dipahami	2	1	Rendah
R11	Kerusakan pada fasilitas	1	3	Rendah
R18	Backup data bermasalah	1	2	Rendah

Sumber: Data primer dari observasi (2023)

Tahap evaluasi ini menemukan beberapa kemungkinan risiko yang masuk dalam klasifikasi tertentu sesuai tingkat risiko, yaitu 2 potensi risiko, yaitu: R013 dan R015. Selain itu, beberapa risiko juga diklasifikasikan ke dalam tingkat risiko yang memiliki level *medium* (sedang) yaitu 10, yaitu: R001, R003, R004, R005, R012, R014, R016, R017, R020 dan R019. Sedangkan, potensi risiko yang tergolong pada tingkat level *low* (rendah) ada 8, yaitu: R002, R006, R007, R008, R009, R010, R011, dan R018.

4.2. Penanganan Resiko

Setelah tahap penilaian risiko selesai dilakukan, proses selanjutnya adalah Penanganan risiko (*risk treatment*). Tujuan dari penanganan risiko adalah untuk mengelola signifikansi risiko pada aplikasi CMS, dengan menangani *likelihood* (kemungkinan) atau *impact* (dampak) atau keduanya. Untuk setiap risiko tingkat Tinggi, Sedang atau Rendah, maka satu atau beberapa tindakan penanganan risiko akan ditentukan.

Tabel 10. Penanganan Risiko

Id	Possible Risk	Tingkat Resiko	Tindakan Terhadap Resiko
R13	Koneksi jaringan yang buruk	Tinggi	Pemeriksaan unjuk kerja semua perangkat jaringan, ganti perangkat jika diperlukan. Termasuk review konfigurasi perangkat, khususnya DNS, Routing
R15	Database Server bermasalah	Tinggi	Pemeriksaan database, web server.
R01	Banjir	Sedang	Menempatkan alat-alat infrastruktur di tempat yang aman
R03	Gempa bumi	Sedang	Menyediakan backup sistem di kota lain.
R04	Hujan badai	Sedang	Memperkuat dinding bangunan dan menyediakan penangkal petir
R05	Kesalahan Manusia	Sedang	Mengadakan pelatihan dan berbagi pengetahuan
R12	Karyawan baru yang masih awam dengan sistem	Sedang	Membuat panduan (*user guide*) dan melakukan pelatihan dan berbagi pengetahuan kepada karyawan baru
R14	Kerusakan peralatan jaringan	Sedang	Menyediakan perangkat cadangan
R16	Kehilangan data	Sedang	Pemeriksaan dan backup data secara teratur
R17	Suhu ruang terlalu	Sedang	Pemasangan air conditioning (AC) & Alat

	panas		pengukur suhu
R19	Kesalahan sistem	Sedang	Monitoring sistem (resources, log file) secara berkala, update software sistem secara rutin.
R20	Tidak ada daya listrik	Sedang	Menyediakan backup power listrik/ genset
R02	Kebakaran	Rendah	Menyediakan alat pemadam kebakaran,
R06	Penyalahgunaan hak akses	Rendah	Memberikan batasan akses atau session login untuk setiap pengguna. Penggunaan OTP (*One Time Password*).
R07	Pencurian dan Kebocoran Data	Rendah	Pengamanan komunikasi data dengan beberapa teknik, seperti penggunaan protocol https daripada http, certificate SSL, VPN, point to point, enkripsi data.
R08	Pencurian Perangkat keras	Rendah	Penggunaan door lock, pemasangan CCTV
R09	Peretasan	Rendah	Penerapan keamanan jaringan (Update sistem operasi & software lain, firewall, strength password, validasi input form di aplikasi dan lainnya)
R10	Antarmuka Pengguna yang sulit untuk dipahami	Rendah	Modifikasi user interface
R11	Kerusakan pada fasilitas	Rendah	Berikan aturan untuk tidak melakukan kerusakan fasilitas
R18	Backup data bermasalah	Rendah	Lakukan backup data dan pantau hasil backup untuk memastikan proses backup berhasil.

Sumber: Data primer dari observasi (2023)

Tabel 10 di atas merupakan rekomendasi penanganan risiko untuk meminimalisir kemungkinan terjadinya risiko pada aplikasi CMS di PT. SCN

5. Kesimpulan

Penelitian manajemen risiko SI/TI menggunakan ISO31000:2018 pada aplikasi CMS. Penelitian melalui beberapa tahapan, dari tahapan risk assessment hingga tahapan risk treatment. Hasil penelitian menemukan :

1) Ada 20 risiko yang mungkin terjadi, dimana mereka dapat mengganggu kinerja aplikasi CMS dan aktifitas bisnis.
2) Ada 2 kemungkinan resiko yang memiliki tingkat tinggi, yaitu koneksi jaringan buruk, dan software server bermasalah.
3) Ada 10 kemungkinan risiko yang memiliki tingkat sedang, yaitu banjir, kebakaran, petir, kesalahan manusia, dan beberapa potensi risiko lainnya.
4) Ada 8 kemungkinan risiko yang memiliki tingkat rendah, yaitu gempa bumi, penyalahgunaan hak akses, pencurian data, pencurian perangkat keras, peretasan, antarmuka pengguna yang sulit dipahami, vandalisme, dan pencadangan masalah.

Selain itu, hasil penelitian memberikan berbagai rekomendasi *risk action* untuk masing-masing risiko yang mungkin terjadi. Diharapkan penelitian dapat dijadikan pedoman bagi PT. SCN untuk meminimalisir kemungkinan resiko yang dapat mengganggu kinerja aplikasi CMS dan aktifitas bisnis.

References

Angraini, A., & Pertiwi, I. D. (2017). Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, 3*(2), 70-76.

anonymous. (2022). 6 manfaat otomatisasi proses bisnis. Retrieved from https://powerautomate.microsoft.com/id-id/business-process-automation-benefits/

Berliana, L. D., & Tanamaah, A. R. (2021). Analisis Risiko dengan Metode ISO 31000 pada Disperinnaker Kota Salatiga Bidang Industri. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8*(3), 1105-1118.

Elly, E., Hanes, H., & Joosten, J. (2022). ISO 31000: 2018-Based IT Infrastructure Risk Management Study (Case Study: Universitas Mikroskil). *Jurnal Riset Informatika, 5*(1).

Friadi, J., Yani, D. P., Zaid, M., & Sikumbang, A. (2023). Perancangan Pemodelan Unified Modeling Language Sistem Antrian Online Kunjungan Pasien Rawat Jalan pada Puskesmas. *Jurnal Ilmu Siber dan Teknologi Digital, 1*(2), 125-133. doi:10.35912/jisted.v1i2.2298

Johnson, L. (2019). *Security controls evaluation, testing, and assessment handbook*: Academic Press.

Lamarco, N. (2018). Information Technology & Its Uses in Business Management: Retrieved from smallbusiness. chron. com/: https://smallbusiness. chron. com ….

Putri, V. R., & Wijaya, A. F. (2022). Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ. *Journal of Information Systems and Informatics, 4*(3), 574-588.

RUMBA, M. F., MIRSEL, R., & SABU, F. X. (2022). Risk Management Information Technology Based on ISO 31000: 2018 at Institute of Philosophy and Creative Technology, Ledalero. *American Journal of Computer Science and Technology, 5*(3).

Suciati, H., Simamora, A. W., Panusunan, P., & Fauzan, F. (2023). Analisa Campuran CPHMA terhadap Penambahan Variasi Aspal Penetrasi 60/70 pada Karakteristik Marshall. *Jurnal Teknologi Riset Terapan, 1*(2), 75-86. doi:10.35912/jatra.v1i2.2294

Vorst, C. R., Priyarsono, D. S., & Budiman, A. (2018). ISO 31000:2018 Manajemen Resiko. Jakarta.