Jurnal Komputer, Informasi dan Teknologi Vol: 6, No 1, 2026, Page: 1-14

Analisis Manajemen Risiko SI/TI Pada PT XYZ Menggunakan ISO 31000:2018

Nova Magdalena Br Hombing, Welmi Simanjuntak, Febrianti Maharani L P Lubis, Sri Andayani*

Universitas Katolik Musi Charitas

Abstrak: Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi tata kelola risiko SI/TI pada PT XYZ guna menyusun strategi penanganan yang tepat berbasis kerangka kerja ISO 31000:2018. Penelitian ini menggunakan metode deskriptif dengan pendekatan campuran (*mixed methods*). Pengumpulan data primer dilakukan melalui observasi, wawancara, dan penyebaran kuesioner berskala Likert 1–5 kepada departemen TI untuk mengukur nilai kemungkinan (*Likelihood*) dan dampak (*Impact*) dari 17 risiko yang teridentifikasi. Hasil evaluasi menunjukkan bahwa secara keseluruhan risiko di perusahaan tersebut berada pada kategori *Medium Risk* (Kuning). Ancaman dengan prioritas penanganan tertinggi adalah Mati Listrik (R01) dan Internet Terputus (R06), sedangkan ancaman berisiko fatal seperti *Ransomware* (R11) dan *Hacking* (R12) memiliki frekuensi kejadian yang sangat rendah (*Rare*). Sebagai tindak lanjut, penelitian ini merekomendasikan strategi mitigasi yang berfokus pada penguatan infrastruktur fisik, seperti penyediaan UPS dan *backup* ISP, serta peningkatan kewaspadaan keamanan siber karyawan melalui edukasi rutin guna menekan potensi kerugian operasional di masa mendatang.

Kata kunci: ISO 31000:2018, Manajemen Risiko, Sistem Informasi, Mitigasi Risiko, Perusahaan Konstruksi

DOI: https://doi.org/10.53697/jkomitek.v6i1.4165
*Correspondence: Sri Andayani
Email: andayani_s@ukmc.ac.id

Received: 30-03-2026
Accepted: 30-04-2026
Published: 30-05-2026

Abstract: *This study aims to identify, analyze, and evaluate IS/IT risk governance at PT XYZ to formulate appropriate treatment strategies based on the ISO 31000:2018 framework. This research employs a descriptive method with a mixed-methods approach. Primary data was collected through observation, interviews, and the distribution of questionnaires using a 1–5 Likert scale to the IT department to measure the likelihood and impact of 17 identified risks. The evaluation results indicate that overall, the risks in the company fall into the Medium Risk (Yellow) category. The highest priority threats for treatment are Power Outages (R01) and Internet Disconnection (R06), while fatal threats such as Ransomware (R11) and Hacking (R12) have a very low frequency of occurrence (Rare). As a follow-up, this study recommends mitigation strategies focusing on strengthening physical infrastructure, such as providing UPS and backup ISPs, as well as enhancing employees cybersecurity awareness through regular education to minimize potential future operational losses.*

Keywords: *ISO 31000:2018, Risk Management, Information Systems, Risk Mitigation, Construction Company*

Pendahuluan

Perkembangan pesat sistem informasi (SI) dan teknologi informasi (TI) saat ini telah menjadi pendorong utama bagi kelangsungan operasional berbagai sektor industri. Khususnya pada perusahaan yang bergerak di bidang penyedia solusi konstruksi dan distribusi material, keandalan infrastruktur digital merupakan syarat mutlak untuk menjamin kelancaran rantai pasok, keakuratan data inventaris, dan kecepatan merespons

pasar (Natalie & Manuputty, 2022). Meskipun demikian, tingginya penggunaan teknologi ini sejalan dengan munculnya risiko SI/TI yang semakin rumit. Jika tidak dikelola melalui pendekatan yang sistematis, ancaman tersebut dapat mengganggu stabilitas operasional, terutama pada entitas bisnis berskala besar dengan jaringan yang luas (Harefa & Hartomo, 2022).

Entitas bisnis berskala besar dengan jaringan yang luas tersebut salah satunya adalah PT XYZ, sebuah perusahaan penyedia solusi konstruksi dan industri terkemuka di Indonesia. Untuk menopang operasionalnya di berbagai wilayah, PT XYZ sangat bergantung pada penggunaan *Enterprise Resource Planning* (ERP) dan infrastruktur komputasi awan (*cloud*) sebagai pusat pengelolaan data logistik. Pada skala bisnis yang kompleks ini, kehadiran tata kelola TI yang tangguh sangat penting guna memastikan kegiatan perusahaan terus berjalan, mendukung pengambilan keputusan strategis, serta mengendalikan berbagai ancaman risiko di lapangan (Chrisanty & Tambotoh, 2023;Andika & Wijaya, 2022).

Berbagai ancaman risiko di lapangan tersebut terbukti menjadi tantangan nyata yang membayangi pemeliharaan TI pada area operasional PT XYZ. Permasalahan yang sering muncul meliputi gangguan fisik seperti pemadaman arus listrik, koneksi jaringan yang tidak stabil, potensi hilangnya data penting, hingga kelalaian yang disebabkan oleh faktor manusia (*human error*). Berbagai kejadian ini memiliki potensi besar untuk menghentikan aktivitas bisnis secara tiba-tiba dan merugikan perusahaan (Effendy & Andayani, 2025)Setiawan et al., 2021). Merespons rentetan ancaman tersebut, sangat dibutuhkan sebuah metode evaluasi risiko yang terstandar secara internasional agar organisasi mampu memetakan kondisi risikonya secara tepat dan terukur (Andika & Wijaya, 2022).

Metode evaluasi risiko yang terstandar secara internasional tersebut salah satunya diwujudkan melalui kerangka kerja ISO 31000:2018. Standar pedoman manajemen risiko ini diakui secara global karena menawarkan tahapan yang terarah dan logis, mulai dari identifikasi, analisis, hingga evaluasi, dengan tujuan memastikan bahwa setiap ketidakpastian dapat dikendalikan dengan baik (Marlando et al., 2025). Fleksibilitas langkah-langkah yang ditawarkan oleh ISO 31000:2018 menjadikannya sangat tepat untuk diterapkan. Standar ini tidak hanya berguna untuk mengatasi ancaman saat ini, tetapi juga berfungsi sebagai sarana untuk menciptakan perlindungan dan nilai tambah yang berkelanjutan bagi perusahaan (Harefa & Hartomo, 2022).

Perlindungan dan nilai tambah yang berkelanjutan melalui ISO 31000:2018 juga telah dibuktikan dalam berbagai penelitian terdahulu, khususnya pada analisis risiko sistem informasi dan teknologi informasi. Beberapa penelitian menerapkan ISO 31000:2018 pada aset teknologi informasi dan aplikasi digital, seperti penelitian Fachrezi et al. (2021), Mahardika et al. (2023), Ayu et al. (2023), serta Aprikasari et al. (2024). Selain itu, ISO 31000:2018 juga digunakan pada sistem informasi akuntansi, sistem informasi sekolah, sistem *e-gudang*, dan sistem informasi organisasi pemerintahan maupun perusahaan (Azzahra et al., 2024; Setyaningrum & Maria, 2024; Rahayu et al., 2025; Febriyanti et al., 2024; Syarifah et al., 2024). Penelitian Suawa & Chernovita. (2024) serta Patrick et al. (2022) juga menunjukkan bahwa ISO 31000:2018 dapat membantu organisasi dalam mengidentifikasi, menganalisis, mengevaluasi, dan menentukan strategi penanganan risiko teknologi informasi secara lebih terarah.

Meskipun berbagai penelitian terdahulu telah membuktikan bahwa ISO 31000:2018 efektif digunakan dalam analisis risiko SI/TI, sebagian besar penelitian masih berfokus pada instansi pemerintahan, aplikasi digital, sistem pendidikan, sistem informasi akuntansi, dan aset teknologi informasi secara umum. Penelitian yang secara khusus membahas manajemen risiko SI/TI pada perusahaan penyedia solusi konstruksi dan distribusi material dengan ketergantungan pada ERP, layanan *cloud*, serta infrastruktur jaringan operasional masih terbatas. Selain itu, beberapa penelitian terdahulu lebih menitikberatkan pada identifikasi dan pemetaan risiko, sedangkan pembahasan mengenai keterkaitan antara risiko infrastruktur fisik, risiko keamanan siber, dan faktor manusia dalam mendukung stabilitas operasional perusahaan belum banyak dijelaskan secara terintegrasi. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan menganalisis dan mengevaluasi risiko SI/TI pada PT XYZ menggunakan ISO 31000:2018 serta menyusun rekomendasi mitigasi yang sesuai dengan kondisi operasional perusahaan.

Berdasarkan celah penelitian tersebut, penelitian ini difokuskan untuk menganalisis dan mengevaluasi tata kelola risiko sistem informasi pada PT XYZ dengan menggunakan pedoman ISO 31000:2018. Melalui evaluasi ini, diharapkan akan terbentuk gambaran yang menyeluruh terkait kondisi risiko nyata di perusahaan, yang kemudian dilengkapi dengan rencana penanganan yang tepat guna menekan potensi kerugian operasional di masa mendatang

Metodologi

Pendekatan Penelitian

Penelitian ini menggunakan pendekatan deskriptif dengan metode campuran (*mixed methods*), yaitu menggabungkan pengumpulan data kualitatif dan kuantitatif. Objek penelitian difokuskan pada infrastruktur dan tata kelola sistem informasi di PT XYZ. Pendekatan ini dipilih agar proses pengumpulan dan pengolahan data dapat menghasilkan analisis yang tidak hanya mendalam secara teori, tetapi juga terukur secara angka dan objektif (Kholifah & Yulhendri, 2024).

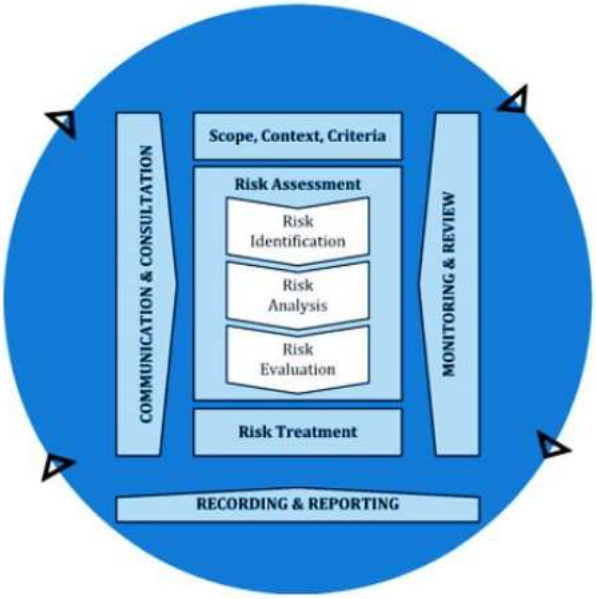
Pemilihan pendekatan deskriptif dalam penelitian ini juga sejalan dengan beberapa penelitian terdahulu yang menggunakan ISO 31000:2018 untuk menggambarkan kondisi risiko secara sistematis berdasarkan data yang diperoleh dari objek penelitian. Febriyanti et al. (2024) menerapkan ISO 31000:2018 pada sistem informasi unit organisasi BPIW Kementerian PUPR, sedangkan Astuti & Vista. (2025)menggunakan pendekatan serupa dalam menganalisis risiko pada aplikasi LMS Sevima Edlink. Selain itu, Barus et al. (2026)juga menggunakan ISO 31000:2018 untuk menganalisis risiko pada sistem e-learning, sehingga pendekatan ini dinilai sesuai untuk memetakan risiko SI/TI berdasarkan kondisi nyata organisasi.

Teknik Pengumpulan Data

Proses pengumpulan dan pengolahan data dalam penelitian ini dilaksanakan melalui dua tahapan utama. Tahap pertama adalah pengumpulan data primer melalui observasi dan wawancara langsung dengan pihak PT XYZ. Langkah ini bertujuan untuk memetakan daftar aset digital, riwayat gangguan sistem, serta potensi celah keamanan yang ada. Tahap kedua melibatkan penyebaran instrumen kuesioner daring (*Google Form*) kepada beberapa

narasumber di perusahaan terkait guna menilai tingkat kemungkinan (*Likelihood*) dan besaran dampak (*Impact*) dari setiap ancaman. Hasil dari kuesioner tersebut kemudian diukur menggunakan Skala Likert dengan rentang nilai 1 hingga 5 (Juliantara et al., 2025).

Tahapan Penilaian Risiko



Gambar 1. Tahapan Manajemen Risiko ISO 31000:2018

Skala Likert dengan rentang nilai 1 hingga 5 tersebut selanjutnya difungsikan sebagai dasar perhitungan dalam tahapan penilaian risiko (*Risk Assessment*) yang mengacu pada pedoman ISO 31000:2018. Mengutip Gambar 1 sebagai kerangka kerja, tahapan penilaian risiko dibagi menjadi tiga langkah inti (Marhaditha & Pangeran, 2022), yaitu sebagai berikut:

a. Identifikasi Risiko (*Risk Identification*) untuk mencatat seluruh potensi bahaya yang mengancam aset.
b. Analisis Risiko (*Risk Analysis*) untuk memberikan penilaian terhadap masing-masing risiko berdasarkan kriteria penilaian *Likelihood* dan *Impact.*
c. Evaluasi Risiko (*Risk Evaluation*) untuk mengelompokkan skor tersebut guna menentukan tingkat keparahan dan prioritas penanganan.

Tahapan identifikasi risiko, analisis risiko, dan evaluasi risiko tersebut juga digunakan dalam penelitian Gunawan et al. (2024), Trisnadi et al. (2025), dan Syaikhurrahman et al. (2025) yang berfokus pada pengelolaan risiko aset teknologi informasi. Ketiga penelitian tersebut menunjukkan bahwa ISO 31000:2018 dapat membantu organisasi dalam mengenali aset yang berpotensi terdampak, menentukan sumber risiko, menilai tingkat kemungkinan dan dampak, serta menyusun rekomendasi perlakuan risiko yang sesuai dengan kebutuhan organisasi.

Matriks Evaluasi dan Penilaian Risiko

Tingkat keparahan dan prioritas penanganan risiko tersebut divisualisasikan melalui penggunaan matriks evaluasi risiko berukuran 5x5. Matriks ini mengklasifikasikan hasil analisis ke dalam lima tingkatan, mulai dari Rendah (*Low*), Sedang (Medium), hingga Tinggi (*High*). Melalui pemetaan pada matriks ini, manajemen PT XYZ dapat melihat dengan jelas daftar ancaman yang membutuhkan tindakan segera. Hasil dari pemetaan ini kemudian dilanjutkan pada tahap akhir yaitu *Perlakuan Risiko* (*Risk Treatment*), di mana peneliti akan memberikan usulan strategi mitigasi yang paling sesuai agar operasional perusahaan dapat berjalan dengan lebih aman dan efisien (Ivander & Papilaya, 2023).

Hasil dan Pembahasan

Manajemen risiko sistem informasi dan teknologi informasi (SI/TI) di PT XYZ dievaluasi menggunakan standar ISO 31000:2018. Berdasarkan standar ini, langkah paling awal adalah mengenali hal-hal apa saja yang bisa menghambat tujuan perusahaan. Karena operasional bisnis sangat bergantung pada infrastruktur SI/TI, maka tahapan ini dimulai dengan mendata seluruh aset SI/TI tersebut secara menyeluruh.

Penilaian Risiko *(Risk Assessment)*

1. Identifikasi Risiko *(Risk Identification)*

a. Identifikasi Aset

Hasil dari proses mendata seluruh aset SI/TI secara lengkap di PT XYZ dirangkum pada Tabel 1 berikut.

Tabel 1. Identifikasi Aset SI/TI

Kategori SI/TI	Aset
Data	Akun Layanan *Cloud*
	Data Operasional
	Dokumen Digital
	File Penting
Software	Aplikasi Bisnis Spesifik
	Keamanan (antivirus)
	Sistem ERP (*Enterprise Resource Planning*)
	Sistem Operasi (OS)
Hardware	CCTV
	Komputer *Desktop*
	Laptop
	Router
	Perangkat Jaringan
	Printer
	Server

b. Identifikasi Kemungkinan Risiko

Untuk memudahkan evaluasi, seluruh kemungkinan risiko (*likelihood*) tersebut selanjutnya dikelompokkan ke dalam empat faktor pemicu utama pada Tabel 2 berikut.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Lingkungan/Fisik	R01	Mati Listrik
	R02	Suhu Panas Berlebih
	R03	Penumpukan Debu
Sistem & Infrastruktur	R04	*Server Down*
	R05	Sistem *Error*
	R06	Internet Terputus
	R07	Kerusakan *Hardware*
	R08	Masalah Implementasi Sistem
Keamanan Siber	R09	Serangan *Phishing*
	R10	Infeksi *Malware*
	R11	*Ransomware*
	R12	*Hacking* & Akses Ilegal
Faktor Manusia	R13	Salah Konfigurasi Sistem
	R14	Salah Klik Tautan Bahaya
	R15	Salah Kirim Email
	R16	Kata Sandi Lemah
	R17	Kehilangan/Kerusakan Data

c. Identifikasi Dampak Risiko

Selain tingkat kemungkinan, evaluasi juga dilakukan untuk mengetahui besaran dampak kerugian (*Impact*) jika risiko tersebut benar-benar terjadi, sebagaimana dirincikan pada Tabel 3.

Tabel 3. Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
R01	Mati Listrik	Operasional berhenti total, risiko kerusakan komponen PC, dan hilangnya data yang belum tersimpan
R02	Suhu Panas Berlebih	Perangkat *server* menjadi lambat (*overheat*) dan mempercepat kerusakan komponen internal
R03	Penumpukan Debu	Mengganggu sirkulasi udara perangkat keras yang memicu kemacetan fungsi hingga risiko arus pendek
R04	*Server Down*	Karyawan tidak dapat mengakses sistem ERP, sehingga proses distribusi dan input data terhenti
R05	Sistem *Error*	Pekerjaan individu staf terhambat dan menyebabkan antrean tugas administrasi
R06	Internet Terputus	Komunikasi antar cabang terganggu dan akses ke layanan cloud tidak dapat dilakukan
R07	Kerusakan *Hardware*	Koneksi antar komputer dalam kantor terputus, sehingga pertukaran data internal mati total

ID	Kemungkinan Risiko	Dampak
R08	Masalah Implementasi Sistem	Munculnya *bug* pada aplikasi yang membuat fitur tertentu tidak bisa digunakan secara normal
R09	Serangan *Phishing*	Pencurian identitas login karyawan yang bisa disalahgunakan untuk masuk ke sistem rahasia
R10	Infeksi *Malware*	Kinerja sistem menjadi sangat lambat dan munculnya risiko kerusakan file-file sistem
R11	*Ransomware*	Seluruh data operasional terkunci (tidak bisa dibuka) dan munculnya pemerasan finansial
R12	*Hacking* & Akses Ilegal	Kebocoran data transaksi perusahaan atau informasi pelanggan kepada pihak luar
R13	Salah Konfigurasi Sistem	Terbukanya celah keamanan baru atau sistem berjalan tidak sesuai dengan prosedur operasional
R14	Salah Klik Tautan Bahaya	Masuknya virus ke perangkat yang berpotensi menyebar ke seluruh jaringan kantor
R15	Salah Kirim Email	Informasi penting atau rahasia perusahaan terkirim ke pihak yang tidak berwenang
R16	Kata Sandi Lemah	Akun staf menjadi sangat mudah dibobol oleh pihak luar untuk melakukan tindakan merugikan
R17	Kehilangan/Kerusakan Data	Rekam jejak transaksi hilang yang mengakibatkan kesulitan saat audit atau pelaporan keuangan

2. Analisis Risiko *(Risk Analysis)*

Setelah identifikasi selesai, tahapan selanjutnya adalah analisis risiko dengan mengevaluasi peluang terjadinya setiap ancaman yang telah dipetakan. Pengukuran tingkat kemungkinan *(Likelihood)* ini kemudian dikelompokkan berdasarkan frekuensi kejadiannya, sebagaimana dijabarkan pada Tabel 4 berikut.

Tabel 4. Nilai Kemungkinan *(Likelihood)*

Nilai	Kemungkinan *(Likelihood)* Kriteria	Deskripsi	Frekuensi Kejadian
1	Sangat Jarang (*Rare)*	Peluang terjadinya hampir tidak ada	>2 Tahun
2	Jarang (*Unlikely)*	Peluang terjadinya sangat kecil	1 - 2 Tahun
3	Mungkin (*Possible)*	Peluang terjadinya sangat kecil	1 - 2 Tahun
4	Sering (*Likely)*	Besar kemungkinan terjadi	4 - 6 Bulan

Nilai	Kemungkinan *(Likelihood)* Kriteria	Deskripsi	Frekuensi Kejadian
5	Hampir Pasti (*Certain)*	Sangat sering atau pasti terjadi	1 - 6 Bulan

Pengukuran lain yang dilakukan adalah menilai seberapa parah dampak (*Impact*) kerusakan pada SI/TI apabila risiko tersebut terjadi yang dapat dilihat pada Tabel 5 berikut.

Tabel 5. Dampak *(Impact)*

Dampak		Deskripsi
Nilai	**Kriteria**	
1	Tidak Signifikan *(Insignificant)*	Tidak ada pengaruh terhadap kelancaran operasional
2	Kecil *(Minor)*	Terdapat kendala ringan, namun aktivitas inti tetap berjalan normal
3	Sedang *(Moderate)*	Mengganggu sebagian proses bisnis sehingga operasional melambat
4	Besar *(Major)*	Menghambat hampir seluruh aktivitas utama perusahaan
5	Katastropik*(Catastrophic)*	Melumpuhkan seluruh kegiatan hingga operasional terhenti total

Tingkat risiko akhir ditentukan dengan menggabungkan nilai dari Tabel 4 dan Tabel 5, sebagaimana ditunjukkan pada Tabel 6.

Tabel 6. Penilaian Nilai Risiko *Likelihood* dan *Impact*

ID	Kemungkinan Risiko	*Likelihood*	*Impact*
R01	Mati Listrik	3	4
R02	Suhu Panas Berlebih	3	2
R03	Penumpukan Debu	3	2
R04	*Server Down*	2	4
R05	Sistem *Error*	4	2
R06	Internet Terputus	4	3
R07	Kerusakan *Hardware*	2	3
R08	Masalah Implementasi Sistem	2	3
R09	Serangan *Phishing*	3	3
R10	Infeksi *Malware*	3	3
R11	*Ransomware*	1	5
R12	*Hacking* & Akses Ilegal	1	4
R13	Salah Konfigurasi Sistem	2	3
R14	Salah Klik Tautan Bahaya	3	3
R15	Salah Kirim Email	3	2
R16	Kata Sandi Lemah	4	2
R17	Kehilangan/Kerusakan Data	2	4

Tabel 6 menyajikan hasil kuantifikasi nilai *Likelihood* (kemungkinan) dan I*mpact* (dampak) dari kuesioner. Dari data tersebut, risiko seperti internet terputus (R06), Sistem *Error* (R05), dan kata sandi lemah (R16) merupakan insiden yang paling sering terjadi (skor 4). Sementara itu, *ransomware* (R11) tercatat sebagai ancaman dengan dampak kerugian paling fatal (skor 5). Kombinasi nilai *likelihood* dan *impact* dari setiap risiko tersebut akan dievaluasi lebih lanjut ke dalam matriks risiko untuk menentukan prioritas penanganannya.

3. Evaluasi Risiko *(Risk Evaluation)*

Hasil evaluasi risiko selanjutnya dikelompokkan menjadi tiga level (*Low, Medium, High*) untuk mempermudah penentuan prioritas penanganannya disajikan pada Tabel 7 berikut.

Tabel 7. Matriks Evaluasi Risiko

Matriks Evaluasi Risiko			***Impact***				
			1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Likelihood	5	*Certain*	*Medium*	*Medium*	*High*	*High*	*High*
	4	*Likely*	*Medium*	*Medium*	*Medium*	*High*	*High*
	3	*Possible*	*Low*	*Medium*	*Medium*	*Medium*	*High*
	2	*Unlikely*	*Low*	*Low*	*Medium*	*Medium*	*Medium*
	1	*Rare*	*Low*	*Low*	*Low*	*Medium*	*Medium*

Tabel 7 menunjukkan pedoman Matriks Evaluasi Risiko yang digunakan untuk menentukan level akhir dari setiap ancaman (Hijau, Kuning, atau Merah).

Tabel 8. Matriks Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact*

Matriks Evaluasi Risiko			***Impact***				
			1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Likelihood	5	*Certain*					
	4	*Likely*		R05, R16	R06		
	3	*Possible*		R02, R03, R15	R09, R10, R14	R01	
	2	*Unlikely*			R07, R08, R13	R04, R17	
	1	*Rare*				R12	R11

Berdasarkan hasil pemetaan pada matriks evaluasi risiko, dapat dilihat bahwa mayoritas ancaman di PT XYZ terpusat pada zona Medium Risk (Kuning). Meskipun terdapat risiko dengan nilai dampak (*Impact*) tertinggi (5) seperti *Ransomware* (R11), namun karena peluang terjadinya sangat jarang (*Rare*), risiko tersebut secara perhitungan matriks tetap masuk dalam kategori *Medium* dan dapat dikendalikan dengan prosedur *backup* yang sudah berjalan. Tidak ditemukan adanya risiko yang masuk ke zona *High Risk* (Merah), yang mengindikasikan bahwa tata kelola IT di perusahaan sudah cukup memadai dalam menekan frekuensi terjadinya insiden fatal.

Penanganan Risiko *(Risk Treatment)*

Setelah melakukan evaluasi dan pemetaan risiko, tahap selanjutnya adalah menentukan tindakan penanganan risiko (*Risk Treatment*). Berdasarkan hasil evaluasi pada

Tabel 8, seluruh risiko di PT XYZ berada pada kategori *Medium Risk* (Kuning). Oleh karena itu, strategi penanganan yang direkomendasikan berfokus pada Mitigasi Risiko (*Risk Mitigation*) guna mengendalikan dampak dan mencegah peluang risiko tersebut meningkat ke level *High Risk*.

Tabel 9. Penanganan Risiko

ID	Kemungkinan Risiko	*Risk Level*	Usulan Mitigasi Risiko
R01	Mati Listrik	*Medium*	Menyediakan perangkat *Uninterruptible Power Supply* (UPS) sebagai daya cadangan sementara serta melakukan pemeliharaan genset secara berkala agar siap digunakan saat terjadi pemadaman Listrik
R06	Internet Terputus	*Medium*	Menggunakan dua layanan penyedia internet (ISP) yang berbeda untuk memastikan koneksi otomatis beralih ke jalur cadangan jika jalur utama mengalami gangguan
R09	Serangan *Phishing*	*Medium*	Memberikan edukasi berkala kepada karyawan mengenai cara mengenali email penipuan (*phishing*) serta mengaktifkan fitur penyaring keamanan pada sistem email perusahaan
R10	Infeksi *Malware*	*Medium*	Menginstal perangkat lunak antivirus resmi pada seluruh komputer kerja karyawan dan memastikan fitur pembaruan otomatis selalu aktif
R14	Salah Klik Tautan Bahaya	*Medium*	Membatasi atau memblokir akses ke situs web yang berpotensi bahaya di jaringan kantor guna mencegah karyawan mengklik tautan yang merugikan secara tidak sengaja
R04	*Server Down*	*Medium*	Melakukan pemeriksaan rutin terhadap kondisi fisik dan perangkat lunak server, serta menjadwalkan waktu pemeliharaan (*maintenance*) di luar jam operasional kerja
R05	Sistem *Error*	*Medium*	Menyusun panduan tertulis sederhana untuk mengatasi kendala sistem standar dan menyediakan tim teknis yang responsif dalam membantu staf operasional
R16	Kata Sandi Lemah	*Medium*	Mewajibkan penggunaan kata sandi yang kuat (kombinasi huruf, angka, dan simbol) serta menerapkan kebijakan pembaruan kata sandi secara berkala bagi seluruh karyawan
R17	Kehilangan/Kerusakan Data	*Medium*	Menerapkan sistem pencadangan data otomatis setiap hari dan menyimpannya di media penyimpanan terpisah (seperti *cloud storage* atau server eksternal)
R02	Suhu Panas Berlebih	*Medium*	Melakukan pemeliharaan pendingin ruangan (AC) secara rutin di ruang server serta memasang alat pemantau suhu untuk memastikan ruangan tetap dingin
R03	Penumpukan Debu	*Medium*	Menjadwalkan pembersihan debu secara berkala pada komputer kerja dan seluruh perangkat keras di ruang server
R07	Kerusakan *Hardware*	*Medium*	Merencanakan pembaruan bagi perangkat komputer yang sudah terlalu tua serta menyediakan stok komponen cadangan di kantor untuk pergantian cepat

ID	Kemungkinan Risiko	*Risk Level*	Usulan Mitigasi Risiko
R08	Masalah Implementasi Sistem	*Medium*	Melakukan uji coba menyeluruh dan memberikan pelatihan yang matang kepada karyawan sebelum sistem atau aplikasi baru resmi diterapkan untuk pekerjaan sehari-hari
R13	Salah Konfigurasi Sistem	*Medium*	Mewajibkan pencatatan atau dokumentasi tertulis setiap kali dilakukan perubahan pengaturan sistem agar mempermudah pelacakan jika terjadi kendala
R15	Salah Kirim Email	*Medium*	Mengimbau karyawan untuk memeriksa kembali alamat tujuan sebelum mengirim email serta mengaktifkan fitur pembatalan pengiriman (*undo send*) pada sistem email kantor
R11	*Ransomware*	*Medium*	Menyimpan salinan data penting pada media penyimpanan luar (seperti hardisk eksternal) yang tidak terhubung ke jaringan internet kantor guna menghindari virus pengunci data
R12	*Hacking* & Akses Ilegal	*Medium*	Membatasi hak akses data sensitif hanya untuk karyawan yang berwenang serta memperkuat kata sandi pada jaringan Wi-Fi dan sistem internal kantor

Dari Tabel 9 di atas secara keseluruhan, seluruh risiko di PT XYZ berada pada kategori *Medium Risk* (Kuning). Prioritas penanganan difokuskan pada penguatan infrastruktur fisik untuk mengatasi gangguan listrik (R01) dan internet (R06) selaku pemilik skor tertinggi. Sementara itu, risiko siber dan *human error* dimitigasi melalui pengetatan kontrol sistem serta edukasi berkala bagi karyawan. Rencana tindakan ini menjadi landasan utama dalam menjaga stabilitas operasional perusahaan yang selanjutnya dirangkum pada bagian kesimpulan.

Simpulan

Penelitian ini menunjukkan bahwa seluruh risiko SI/TI yang teridentifikasi pada PT XYZ berada pada kategori *Medium Risk* atau risiko sedang. Risiko dengan prioritas penanganan tertinggi adalah gangguan infrastruktur fisik, terutama mati listrik (R01) dan internet terputus (R06). Temuan ini mengindikasikan bahwa stabilitas operasional perusahaan sangat bergantung pada keandalan fasilitas pendukung, seperti listrik, jaringan internet, perangkat keras, serta kesiapan pengguna dalam menjalankan sistem. Implikasi dari penelitian ini menunjukkan bahwa risiko kategori sedang tetap perlu dikendalikan agar tidak meningkat menjadi risiko tinggi. Oleh karena itu, PT XYZ disarankan untuk memperkuat infrastruktur melalui penyediaan *Uninterruptible Power Supply* (UPS), penggunaan *backup ISP*, pencadangan data berkala, pembatasan hak akses, serta edukasi keamanan siber bagi karyawan. Untuk penelitian selanjutnya, disarankan menggunakan kombinasi kerangka kerja seperti COBIT, NIST, atau ISO/IEC 27001 agar evaluasi kontrol keamanan informasi dapat dilakukan secara lebih mendalam.

Referensi

Andika, D. Y., & Wijaya, A. F. (2022). MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR. Jurnal MNEMONIC, 5(2), 111–118. https://doi.org/https://doi.org/10.36040/mnemonic.v5i2.4778

Aprikasari, M., Benedicta, L., & Adrielvino, N. A. (2024). Penerapan ISO 31000 : 2018 untuk Manajemen Risiko IT pada Sistem Penerbitan PT . X. Jurnal Informasi, Sains Dan Teknologi, 7(2), 154–167. https://doi.org/https://doi.org/10.55606/isaintek.v7i2.269

Astuti, B., & Vista, U. F. (2025). Analisis Manajemen Risiko Teknologi Informasi Pada Aplikasi LMS Sevima Edlink Menggunakan Framework ISO 31000 (Studi Kasus : Prodi Teknologi Informasi). Jurnal Manajemen Risiko, 06(01), 53–68. https://ejournal.uki.ac.id/index.php/mr/index

Ayu, U., Nieng, S., & Liperda, R. I. (2023). ANALISIS MANAJEMEN RESIKO APLIKASI MYPERTAMINA DENGAN MENGGUNAKAN ISO 31000 Urbina. Infotech Journal, 9(2), 361–370. https://doi.org/https://doi.org/10.31949/infotech.v9i2.6232

Azzahra, A., Aditya, P., & Andayani, S. (2024). ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI AKUNTANSI PADA PT. BATU BARA XYZ ISO 31000:2018. Jurnal Sistem Informasi (JUSIN), 5(1), 41–50. https://doi.org/https://doi.org/10.32546/jusin.v5i1.2474

Barus, H. J. I. B., Tanaamah, A. R., & Muttamaqin, A. (2026). Analisis manajemen risiko pada e-learning SMAN 1 Ambarawa dengan menggunakan ISO 31000 : 2018. Jurnal Teknologi Informasi (AITI), 23(1), 1–13. https://doi.org/10.24246/aiti.v23i1.1-13

Chrisanty, T. W., & Tambotoh, J. (2023). ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI MENGGUNAKAN ISO 31000:2018 di PT. XYZ. Jurnal Sistem Informasi (ZONAsi), 5(2). https://doi.org/https://doi.org/10.31849/zn.v5i2.13198

Effendy, E., & Andayani, S. (2025). Identifikasi dan Pengelolaan Risiko Aset Digital di Bengkel Mobil XYZ Menggunakan Framework ISO 31000 : 2018. Jurnal Sistem & Teknologi Informasi Komunikasi Volume: 8 No: 2 Juli 2025, 83–91. https://doi.org/https://doi.org/10.32524/jusitik.v8i2.1443

Fachrezi, M. I., Cahyono, A. D., & Tanaem, P. F. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018 Diskominfo Kota Salatiga. Jurnal Teknik Informatika Dan Sistem Informasi, 8(2), 764–773. https://doi.org/10.35957/jatisi.v8i2.789

Febriyanti, L., Febrinazahra, M., Kraugusteeliana, & Masdiyasa, I. G. S. (2024). MANAJEMEN RISIKO SISTEM INFORMASI UNIT ORGANISASI BPIW

KEMENTERIAN PUPR MENGGUNAKAN FRAMEWORK ISO 31000:2018. Jurnal Sistem Informasi Dan Aplikasi (JSIA), 2(2), 1–12. https://doi.org/https://doi.org/10.52958/jsia.v2i2.8850

Gunawan, A., Filikano, T., & Andayani, S. (2024). ANALISIS RISIKO SISTEM INFORMASI AKUNTANSI MENGGUNAKAN ISO 31000:2018 DI PT. XYZ. Jurnal Ilmiah Sistem Informasi (SIMASI), 4(1), 31–45. https://doi.org/10.46306/sm.v4i1.71

Harefa, W., & Hartomo, K. D. (2022). Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang. Jurnal Teknik Informatika Dan Sistem Informasi, 9(1). https://doi.org/https://doi.org/10.35957/jatisi.v9i1.1478

Ivander, D. L., & Papilaya, F. S. (2023). Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2018. Kajian Ilmiah Informastika Dan Komputer (KLIK), 4(2), 1042–1051. https://doi.org/10.30865/klik.v4i2.1174

Juliantara, I. W. A., Ariawan, W. E., & Guna, I. N. A. (2025). ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI DALAM PENGGUNAAN APLIKASI E-PURCHASING BERBASIS ISO 31000 (STUDI KASUS TOKO ASHA). Jurnal Science Teknologi Sosial Humaniora (SUTASOMA), 03(01), 51–60. https://doi.org/https://doi.org/10.58878/sutasoma.v3i2.385

Kholifah, S. N., & Yulhendri. (2024). ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFROMASI PADA PT JAKARTA NOTEBOOK MENGGUNAKAN FRAMEWORK ISO 31000. Jurnal Ilmiah Sains Dan Teknologi (Scientica), 2, 126–138. https://doi.org/https://doi.org/10.572349/scientica.v2i2.906

Mahardika, F., H, M. A., Fatimah, S. A., & F, L. T. N. (2023). Manajemen Risiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000 : 2018. Media Informasi Untuk Pengembangan Penelitian Teknik (INFOTEKNIKMESIN), 14(02), 237–243. https://doi.org/10.35970/infotekmesin.v14i2.1877

Marhaditha, S., & Pangeran, P. (2022). Supply Chain Risk Management Based on ISO 31000:2018 - Balanced Scorecard to Improve Company Performance: Case Study on UD INTR Yogyakarta. International Journal of Social Science Research and Review (IJSSRR), 5(11), 306–319. https://doi.org/10.47814/ijssrr.v5i11.705

Marlando, P., Mardiana, & Susanto, M. (2025). PENILAIAN RISIKO BERBASIS ISO 31000 : 2018 PADA UNIT TIK PERGURUAN TINGGI (STUDI KASUS : POLITEKNIK NEGERI LAMPUNG). Jurnal Informatika Dan Teknik Elektro Terapan (JITET), 13(3). https://doi.org/http://dx.doi.org/10.23960/jitet.v13i3.6672

Natalie, D. P., & Manuputty, A. D. (2022). Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000 : 2018 pada PT Bayu Buana Tbk. Jurnal Riset Komputer (JURIKOM), 9(5), 1290–1301. https://doi.org/10.30865/jurikom.v9i5.4797

Patrick, V., Wijaya, P., & Manuputty, A. D. (2022). Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000 : 2018. Jurnal Teknik Informatika Dan Sistem Informasi, 9(2), 1295–1307. https://doi.org/10.35957/jatisi.v9i2.2087

Rahayu, I., Setiadi, D., & Yuniarto, D. (2025). Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO 31000:2018. Jurnal Teknik Mesin, Industri, Elektro Dan Informatika, 4. https://doi.org/https://doi.org/10.55606/jtmei.v4i1.4819

Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO / EIC 27001 di Tripio Purwokerto Information System Risk Management Using ISO 31000 and ISO / EIC 27001 Control Standards in Tripio Purwokerto. Jurnal Manajemen, Teknik Informatika, Dan Rekayasa Komputer (Matrik), 20(2), 389–396. https://doi.org/10.30812/matrik.v20i2.1093

Setyaningrum, N. N., & Maria, E. (2024). Penerapan iso 31000:2018 untuk manajemen risiko pada sistem informasi sekolah terpadu. Jurnal Pendidikan Teknologi Informasi (JUKANTI), April, 31–44. https://doi.org/https://doi.org/10.37792/jukanti.v7i1.1164

Suawa, H. C. S., & Chernovita, H. P. (2024). ANALISIS MANAJEMEN RISIKO APLIKASI SRIKANDI PADA KANTOR DISKOMINFO KOTA MANADO MENGGUNAKAN ISO 31000. Jurnal Pendidikan Teknologi Informasi Dan Komunikasi (EduTIK), 4(April), 131–143. https://doi.org/10.53682/edutik.v3i5.8562

Syaikhurrahman, Ashari, M., & Fadli, S. (2025). MANAJEMEN RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000:2018 (STUDI KASUS: BPBD LOMBOK TENGAH) Syaikhurrahman1,. Jurnal Informatika Teknologi Dan Sains (JINTEKS), 7(4), 2250–2259. https://doi.org/https://doi.org/10.51401/jinteks.v3i3.1260

Syarifah, G., Yustika, A., & Anita, E. (2024). Analysis of Risk Management Using E-Office Application with ISO 31000 : 2018 in National Public Procurement Agency (NPPA / LKPP). Airlangga Journal of Innovation Management (AJIM), 05(02), 260–277. https://doi.org/https://doi.org/10.20473/ajim.v5i2.56656

Trisnadi, Y., Zaen, M. T. A., & Bagye, W. (2025). MANAJEMEN RISIKO KEAMANAN ASET TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000:2018 PADA KANTOR LURAH PRAPEN Yudi. Jurnal Informatika Teknologi Dan Sains (JINTEKS), 2240–2249. https://doi.org/10.51401/jinteks.v7i4.6007