Arus Jurnal
Psikologi dan Pendidikan (AJPP)
Website: http://jurnal.ardenjaya.com/index.php/ajpp
Email: jurnal.ajpp@ardenjaya.com

Analisis Manajemen Risiko Teknologi Informasi pada PT XYZ Menggunakan ISO 31000:2018

INFO PENULIS

Mayer Dani Sitompul
Universitas Katolik Musi Charitas
mayerdanis11@gmail.com

Risky Surya Saputra
Universitas Katolik Musi Charitas
riskysuryasaputra40@gmail.com

Sri Andayani
Universitas Katolik Musi Charitas
andayani_s@ukmc.ac.id

INFO ARTIKEL

ISSN: 2963-8933
Vol. 5, No. 2 Juni 2026
http://jurnal.ardenjaya.com/index.php/ajpp

© 2026 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi :

Sitompul, M. D., Saputra , R. S., & Andayani, S. (2026). Analisis Manajemen Risiko Teknologi Informasi pada PT XYZ Menggunakan ISO 31000:2018. *Arus Jurnal Psikologi dan Pendidikan 5*(2),1388-1397.

Abstrak

Penelitian ini bertujuan menganalisis manajemen risiko teknologi informasi pada PT XYZ menggunakan kerangka kerja ISO 31000:2018. Metode yang digunakan adalah deskriptif kualitatif dengan pendekatan studi kasus melalui wawancara, observasi, dan studi literatur. Hasil penelitian menemukan sepuluh risiko TI yang dapat mengganggu operasional perusahaan, dengan empat risiko berkategori High yaitu kehilangan data, serangan siber, server down, dan kebocoran informasi, serta enam risiko berkategori Medium. Rekomendasi pengendalian risiko meliputi penerapan backup data, peningkatan keamanan sistem, pemeliharaan infrastruktur, pemulihan bencana, dan peningkatan kesadaran pengguna. Penerapan ISO 31000:2018 membantu perusahaan mengelola risiko TI secara sistematis untuk menjaga keberlangsungan operasional.

Kata kunci: Manajemen Risiko, Teknologi Informasi, ISO 31000:2018, *Risk Assessment*.

'Abstract

This study aims to analyze information technology risk management at PT XYZ using the ISO 31000:2018 framework. The research method used is descriptive qualitative with a case study approach through interviews, observations, and literature studies. The results identified ten IT risks that could disrupt company operations, with four risks categorized as High, namely data loss, cyberattacks, server downtime, and company information leakage, while six risks were categorized as Medium. Recommended risk controls include data backup implementation, system security enhancement, IT infrastructure maintenance, disaster recovery planning, and improving user awareness. The implementation of ISO 31000:2018 helps the company manage IT risks systematically to support business operational continuity.

Keywords: Risk Management, Information Technology, ISO 31000:2018, Risk Assessment.

A. Pendahuluan

Perkembangan teknologi informasi telah menjadi faktor penting dalam mendukung aktivitas operasional perusahaan, termasuk pada industri pupuk. Dalam konteks ini, manajemen risiko teknologi informasi menjadi aspek kritis yang menentukan kelangsungan organisasi (Fadiyah & Ilham, 2025). Risiko merupakan suatu hal yang pasti akan dihadapi oleh perusahaan dalam menjalankan bisnisnya (Pratama & Pratika, 2020). Risiko akan selalu ada dalam setiap proses bisnis yang dijalankan sesuai dengan skema dan alur yang telah disepakati (Angkat & Arsyadona, 2025). Pemanfaatan teknologi informasi memungkinkan perusahaan meningkatkan efisiensi proses bisnis, pengelolaan data, komunikasi, serta pengambilan keputusan secara lebih cepat dan akurat. Namun, penggunaan teknologi informasi juga menimbulkan berbagai risiko yang dapat mengganggu keberlangsungan operasional perusahaan, seperti kegagalan sistem, gangguan jaringan, kehilangan data, kesalahan manusia (human error), serangan siber, maupun bencana alam yang berdampak pada infrastruktur teknologi informasi.

PT XYZ merupakan salah satu perusahaan yang bergerak di bidang industri pupuk NPK. Dalam menjalankan proses bisnisnya, perusahaan memanfaatkan teknologi informasi untuk mendukung berbagai aktivitas operasional dan administrasi. Ketergantungan yang tinggi terhadap teknologi informasi menyebabkan perusahaan perlu menerapkan manajemen risiko yang efektif guna mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko yang dapat menghambat pencapaian tujuan organisasi. Manajemen risiko merupakan proses sistematis yang bertujuan untuk mengidentifikasi, menilai, dan mengendalikan risiko yang dapat mempengaruhi pencapaian sasaran organisasi (Utamajaya et al., 2021). Salah satu *tools* berstandar internasional mengenai manajemen risiko yaitu ISO 31000:2018.

ISO 31000:2018 merupakan pedoman standar, instruksi, dan tuntutan bagi sebuah organisasi untuk membangun sebuah pondasi dan kerangka kerja bagi suatu program manajemen risiko (Zagoto & Sitokdana, 2021). Standar ISO 31000:2018 menyediakan pedoman internasional mengenai prinsip, kerangka kerja, dan proses manajemen risiko yang dapat diterapkan pada berbagai jenis organisasi. ISO 31000:2018 menekankan bahwa manajemen risiko harus terintegrasi dengan seluruh aktivitas organisasi melalui proses identifikasi risiko, analisis risiko, evaluasi risiko, perlakuan risiko, serta pemantauan dan peninjauan secara berkelanjutan. Tujuan dari standarisasi ini adalah menyediakan prinsip-prinsip dan acuan dari program manajemen risiko kepada organisasi.

Berdasarkan hasil wawancara dengan staf Teknologi Informasi PT XYZ, ditemukan beberapa potensi risiko yang dapat mempengaruhi operasional teknologi informasi perusahaan, antara lain gangguan jaringan internet, kerusakan perangkat keras, kegagalan sistem aplikasi, kehilangan data akibat kesalahan pengguna, keterlambatan pemeliharaan perangkat, serta ancaman keamanan informasi. Risiko-risiko tersebut berpotensi menghambat proses bisnis dan menurunkan produktivitas perusahaan apabila tidak dikelola dengan baik. Oleh karena itu, penelitian ini dilakukan untuk menganalisis risiko teknologi informasi yang terdapat pada PT XYZ menggunakan kerangka kerja ISO 31000:2018. Hasil penelitian diharapkan dapat memberikan gambaran mengenai tingkat risiko teknologi informasi yang dihadapi perusahaan serta memberikan rekomendasi pengendalian risiko yang sesuai guna mendukung keberlangsungan operasional perusahaan.

B. Metodologi

1. Jenis Penelitian

Penelitian ini menggunakan metode penelitian deskriptif kualitatif dengan pendekatan studi kasus. Metode deskriptif digunakan untuk menggambarkan kondisi manajemen risiko teknologi informasi yang diterapkan pada PT XYZ serta mengidentifikasi berbagai risiko yang berpotensi mengganggu operasional teknologi perusahaan. Pendekatan ini dipilih karena penelitian berfokus pada satu objek penelitian, yaitu PT XYZ sehingga memungkinkan analisis yang lebih mendalam terhadap risiko teknologi informasi informasi yang ada. Penelitian ini mengacu pada standar ISO 31000:2018 sebagai kerangka kerja dalam proses manajemen risiko yang meliputi identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko. Langkah ini sejalan dengan (Chrisanty & Tambotoh, 2023) menggunakan kerangka kerja ISO 31000:2018 dalam melakukan analisis manajemen risiko.

2. Lokasi dan Waktu Penelitian

Penelitian dilaksanakan di PT XYZ yang bergerak di bidang industri pupuk NPK. Waktu pelaksanaan penelitian berlangsung dari bulan Maret 2026 sampai Mei 2026.

3. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui beberapa metode berikut:

a. Wawancara

Wawancara dilakukan secara langsung dengan staf Teknologi Informasi dan pihak terkait yang bertanggung jawab terhadap pengelolaan sistem informasi di PT XYZ. Wawancara bertujuan untuk memperoleh informasi mengenai kondisi teknologi informasi, permasalahan yang sering terjadi, serta risiko-risiko yang berpotensi mengganggu operasional perusahaan.

b. Observasi

Observasi dilakukan dengan mengamati secara langsung kondisi infrastruktur teknologi informasi, proses operasional, penggunaan sistem, serta pengelolaan perangkat teknologi informasi di lingkungan PT XYZ.

c. Studi Literatur

Studi literatur dilakukan dengan mempelajari buku, jurnal ilmiah, standar ISO 31000:2018, dan sumber referensi lain yang berkaitan dengan manajemen risiko teknologi informasi.

4. Teknik Analisis Data

Analisis data merupakan proses untuk mencari dan menyusun data secara terstruktur dari penentuan masalah hingga pada pembuatan kesimpulan. Analisis dilakukan dengan mengidentifikasi potensi risiko teknologi informasi yang umum dihadapi oeh perusahaan berdasarkan kajian literatur dalam industri. Metode analisis data pada penelitian ini yakni menggunakan kerangka kerja ISO 31000:2018 yang bertujuan untuk mengidentifikasi kemungkinan ancaman risiko yang terjadi pada PT XYZ. Berikut tahapan analisis data pada penelitian ini.

Gambar 1. Metode Analisis Data

Pada gambar diatas, terdapat 2 tahapan besar yaitu *risk assessment* (penilaian risiko) dan *risk treatment* (perlakuan risiko). Tahap pertama yaitu tahap *risk assessment* (penilaian risiko) terdapat 3 proses yang dilakukan yaitu identifikasi risiko, analisis risiko, dan terakhir evaluasi risiko. Tahapan kedua yaitu tahap *risk treatment* (perlakuan risiko), tahap ini dilakukan untuk menyeleksi kemungkinan-kemungkinan risiko, mengurangi bahkan menghilangkan dampak serta kemungkinan terjadinya risiko yang akan muncul.

5. Tahapan Penelitian

Tahapan penelitian mengacu pada proses manajemen risiko dalam ISO 31000:2018 sebagai berikut:

1) Identifikasi Risiko (*Risk Identification*)

Identifikasi risiko merupakan proses untuk mengindentifikasi dan mengevaluasi risiko-risiko yang kemungkinan terjadi dalam proses operasional bisnis di perusahaan (Jayonata & Sitokdana, 2024). Mengidentifikasi seluruh risiko yang dapat mempengaruhi operasional teknologi informasi di PT XYZ berdasarkan hasil wawancara dan observasi. Risiko yang ditemukan kemudian dikelompokkan berdasarkan sumber dan dampaknya.

2) Analisis Risiko (*Risk Analysis*)

Analisis risiko merupakan usaha untuk menganalisis disbanding hasil data yang telah diperoleh dari proses identifikasi risiko untuk menentukan tingkat risiko (Ramadhan et al., 2020). Pada tahap ini dilakukan analisis terhadap setiap risiko berdasarkan tingkat kemungkinan terjadinya (*Likelihood*) dan tingkat dampak (*Impact*) yang ditimbulkan.

Tabel 1. Kriteria Nilai Kemungkinan
Skala *Likelihood*

Nilai	Kategori	Deskripsi
1	Sangat Jarang (*Rare*)	Peluang terjadinya hampir tidak ada
2	Jarang (*Unlikely*)	Peluang terjadinya sangat kecil
3	Mungkin (*Possible*)	Peluang terjadinya kecil
4	Sering (*Likely*)	Peluang terjadinya besar kemungkinan terjadi
5	Sangat Sering (*Almost Certain*)	Peluang terjadinya sangat sering terjadi

Tabel 2. Kriteria Nilai Dampak
Skala *Impact*

Nilai	Kategori	Deskripsi
1	Sangat Rendah (*Insignificant*)	Tidak berdampak signifikan terhadap operasional.
2	Rendah (*Minor*)	Menimbulkan gangguan kecil pada operasional.
3	Sedang (*Moderate*)	Menghambat sebagian aktivitas operasional.
4	Tinggi (*Major*)	Mengganggu sebagian besar aktivitas operasional.
5	Sangat Tinggi (*Catastrophic*)	Menghentikan operasional dan menyebabkan kerugian besar.

3) Evaluasi Risiko (*Risk Evaluation*)
Tahap terakhir yaitu melakukan evaluasi risiko dengan membandingkan tingkat risiko dari yang paling rendah hingga yang paling tinggi atau paling berbahaya. Melalui proses ini, risiko dapat dianalisis dan dikelompokkan sesuai dengan tingkat risikonya masing-masing. Tujuan evaluasi risiko adalah untuk mendukung proses pengambilan keputusan terkait penanganan risiko berdasarkan hasil analisis risiko yang telah dilakukan (Andika & Wijaya, 2022).

4) Perlakuan Risiko (*Risk Treatment*)
Pada tahap ini disusun rekomendasi pengendalian terhadap risiko yang telah dievaluasi (Manuputty et al., 2022). Strategi penanganan risiko mengacu pada ISO 31000:2018, sebagai berikut:
   a. Risk Avoidance (menghindari risiko), yakni menghindari atau mencegah terjadinya risiko terjadi.
   b. Risk Reduction (mengurangi risiko), yakni mengurangi kemungkinan terjadinya risiko (preventif) dengan menyusun dan mengimplementasikan pengendalian dan memadai untuk mencegah dan mengurangi kemungkinan terjadinya risiko.
   c. Risk Sharing (memindahkan atau berbagi risiko), yakni membagi risiko dengan pihak lain.
   d. Risk Acceptance (menerima risiko), yakni menerima kemungkinan terjadinya risiko dan dampak yang ditimbulkannya

C. Hasil dan Pembahasan

1. Penilaian Risiko (*Risk Assesment*)

Berdasarkan hasil wawancara dan observasi yang dilakukan pada PT XYZ, tahap penilaian risiko dilakukan dengan mengidentifikasi aset teknologi informasi, kemungkinan risiko yang terjadi, serta dampak yang ditimbulkan terhadap operasional perusahaan. Proses ini mengacu pada kerangka kerja ISO 31000:2018 yang bertujuan untuk mengetahui risiko-risiko yang dapat mengganggu keberlangsungan layanan teknologi informasi pada PT XYZ.

1) Identifikasi Risiko (*Risk Identification*)

a. Identifikasi Aset

Aset teknologi informasi yang dimiliki PT XYZ merupakan komponen penting yang mendukung aktivitas operasional dan administrasi perusahaan. Berdasarkan hasil wawancara, aset tersebut meliputi perangkat keras, perangkat lunak, jaringan, dan data perusahaan yang digunakan untuk mendukung proses bisnis.

Tabel 3. Identifikasi Aset SI/TI

Komponen SI/TI	Aset
Hardware	Server, komputer/laptop, perangkat jaringan (router, switch, access point).
Software	Sistem informasi perusahaan, sistem operasi, database.
Data	Data produksi, data keuangan, data karyawan.
Jaringan	Internet dan LAN

b. Identifikasi Kemungkinan Risiko

Tahap berikutnya yakni mengidentifikasi risiko yang berpotensi terjadi pada aset teknologi informasi PT XYZ. Risiko-risiko ini diperoleh berdasarkan wawancara yang dilakukan.

Tabel 4. Identifikasi Kemungkinan Risiko

ID	Risiko	Kemungkinan Risiko
R1	Gangguan jaringan internet	Kegagalan koneksi ISP, gangguan jaringan internal
R2	Kerusakan perangkat keras	Usia perangkat, penggunaan berlebih, gangguan Listrik
R3	Kegagalan sistem aplikasi	Bug sistem, kesalahan konfigurasi, overload server
R4	Kehilangan data	Human error, kesalahan penghapusan data
R5	Keterlambatan pemeliharaan perangkat	Kurangnya jadwal maintenance
R6	Serangan siber	Malware, hacking, akses illegal
R7	Server down	Gangguan perangkat keras atau sistem operasi
R8	Kerusakan infrastruktur akibat bencana alam	Banjir, petir, gempa bumi
R9	Kesalahan pengguna (human error)	Kurangnya
R10	Kebocoran informasi perusahaan	Akses tidak sah terhadap data perusahaan

c. Identifikasi Dampak Kemungkinan Risiko

Setelah melakukan identifikasi kemungkinan risiko, Langkah selanjutnya adalah menentukan dampak yang dapat ditimbulkan apabila risiko tersebut terjadi.

Tabel 5. Idenfitikasi Dampak Kemungkinan Risiko

ID	Risiko	Dampak
R1	Gangguan jaringan internet	Terhambatnya komunikasi dan akses sistem informasi
R2	Kerusakan perangkat keras	Operasional perusahaan terganggu dan biaya perbaikan meningkat
R3	Kegagalan sistem aplikasi	Aktivitas bisnis tidak dapat berjalan normal
R4	Kehilangan data	Hilangnya informasi penting perusahaan
R5	Keterlambatan pemeliharaan perangkat	Penurunan kinerja sistem dan meningkatnya risiko kerusakan
R6	Serangan siber	Kebocoran data dan

		kerugian finansial
R7	Server down	Seluruh layanan sistem informasi berhenti sementara
R8	Kerusakan infrastruktur akibat bencana alam	Kerusakan infrastruktur TI dan penghentian operasional
R9	Kesalahan pengguna (human error)	Kesalahan pengolahan data dan kehilangan informasi
R10	Kebocoran informasi perusahaan	Kerusakan reputasi perusahaan dan kerugian bisnis

2) Analisis Risiko (*Risk Analysis*)

Tahap analisis risiko dilakukan dengan memberikan penilaian terhadap setiap risiko berdasarkan dua parameter utama, yaitu tingkat kemungkinan terjadinya risiko (Likelihood) dan tingkat dampak yang ditimbulkan (Impact). Penilaian ini bertujuan untuk mengetahui tingkat risiko TI yang dihadapi oleh PT XYZ sehingga dapat menentukan prioritas penanganan risiko. Metode penilaian mengacu pada ISO 31000:2018 dengan mengombinasikan nilai kemungkinan dan nilai dampak menggunakan matriks risiko.

Tabel 6. Analisis Risiko

ID	Risiko	*Likelihood*	*Impact*
R1	Gangguan jaringan internet	4	3
R2	Kerusakan perangkat keras	3	4
R3	Kegagalan sistem aplikasi	3	4
R4	Kehilangan data	3	5
R5	Keterlambatan pemeliharaan perangkat	4	3
R6	Serangan siber	3	5
R7	Server down	3	5
R8	Kerusakan infrastruktur akibat bencana alam	2	5
R9	Kesalahan pengguna (human error)	4	3
R10	Kebocoran informasi perusahaan	3	5

3) Evaluasi Risiko (*Risk Evaluation*)

Tahap terakhir adalah evaluasi risiko, yaitu dilakukan proses evaluasi terhadap segala kemungkinan risiko yang tadinya sudah dilakukan analisis pada tahapan sebelumnya. Hingga kemudian menghasilkan analisis risiko untuk dapat dikategorikan menjadi 3 level risiko yaitu : *Low, Medium* dan *High*.

Tabel 7. Warna Level Risiko

Level Risiko	Keterangan
Low (Rendah)	Risiko dapat diterima dan dilakukan pemantauan secara berkala
Medium (Sedang)	Risiko membutuhkan pengendalian dan pemantauan lebih lanjut
High (Tinggi)	Risiko menjadi prioritas utama dan membutuhkan tindakan pengendalian segera

Tabel 8. Matriks Evaluasi Risiko

Likelihood	Sangat Sering (5)	Low	Medium	High	High	High
	Sering (4)	Low	Medium	R1, R5, R9	High	High
	Mungkin (3)	Low	Low	Medium	R2, R3	R4, R6, R7, R10
	Jarang (2)	Low	Low	Low	Medium	R8
	Sangat Jarang (1)	Low	Low	Low	Low	Medium
		Sangat Jarang (1)	Jarang (2)	Mungkin (3)	Sering (4)	Sangat Sering (5)
		Impact				

Tabel 9. Tingkat Risiko

ID	Risiko	*Likelihood*	*Impact*	Tingkat Risiko
R1	Gangguan jaringan internet	4	3	Medium
R5	Keterlambatan pemeliharaan perangkat	4	3	Medium
R9	Kesalahan pengguna (*human error*)	4	3	Medium
R2	Kerusakan perangkat keras	3	4	Medium
R3	Kegagalan sistem aplikasi	3	4	Medium
R4	Kehilangan data	3	5	High
R6	Serangan siber	3	5	High
R7	Server down	3	5	High
R10	Kebocoran informasi perusahaan	3	5	High
R8	Kerusakan infrastruktur akibat bencana alam	2	5	Medium

Berdasarkan hasil evaluasi risiko menggunakan matriks *Likelihood* dan *Impact*, terdapat 4 risiko dengan tingkat High, yaitu R4 (Kehilangan Data), R6 (Serangan Siber), R7 (Server Down), dan R10 (Kebocoran Informasi Perusahaan). Risiko tersebut menjadi prioritas utama karena memiliki dampak yang sangat tinggi terhadap operasional perusahaan. Selain itu, terdapat 6 risiko dengan tingkat Medium, yaitu R1, R2, R3, R5, R8, dan R9 yang tetap memerlukan pengendalian dan pemantauan secara berkala. Tidak terdapat risiko dengan tingkat Low, sehingga seluruh risiko yang teridentifikasi perlu mendapatkan perhatian dan tindakan pengelolaan sesuai tingkat risikonya.

4) Perlakuan Risiko (*Risk Treatment*)

Setelah mendapatkan data dari proses evaluasi risiko, proses selanjutnya adalah perlakuan risiko. Tahapan ini merupakan sebuah tindakan untuk meningkatkan peluang dan mengurangi ancaman dari kemungkinan dan dampak risiko yang ditimbulkan. Untuk perlakuan terhadap risiko yang dihasilkan dapat dilihat pada tabel 10 sebagai berikut.

Tabel 10. Perlakuan Risiko

ID	Risiko	*Risk Level*	Perlakuan Risiko
R1	Gangguan jaringan internet	Medium	Membuat monitoring jaringan secara berkala, menyediakan koneksi internet cadangan (backup link), melakukan pemeliharaan perangkat jaringan, serta

			membuat prosedur penanganan gangguan jaringan.
R2	Kerusakan perangkat keras	Medium	Melakukan pemeliharaan perangkat secara rutin, membuat jadwal pengecekan hardware, melakukan penggantian perangkat yang sudah tidak optimal, serta menyediakan perangkat cadangan untuk mendukung operasional.
R3	Kegagalan sistem aplikasi	Medium	Melakukan pengujian sistem secara berkala, melakukan update dan perbaikan aplikasi, membuat dokumentasi konfigurasi sistem, serta menyediakan mekanisme pemulihan apabila terjadi kegagalan sistem.
R4	Kehilangan data	High	Menerapkan sistem backup data secara rutin, menyediakan penyimpanan cadangan (backup storage), menerapkan pengujian proses pemulihan data (data recovery).
R5	Keterlambatan pemeliharaan perangkat	Medium	Membuat jadwal preventive maintenance, melakukan pencatatan riwayat pemeliharaan perangkat, serta menetapkan prosedur dan tanggung jawab pemeliharaan agar dilakukan tepat waktu.
R6	Serangan siber	High	Meningkatkan keamanan sistem melalui penggunaan firewall, antivirus, pemantauan aktivitas jaringan, pembaruan sistem keamanan, edukasi keamanan informasi bagi pengguna, serta menggunakan layanan keamanan dari pihak ketiga apabila diperlukan.
R7	Server down	High	Melakukan monitoring performa server, menyediakan server cadangan atau sistem failover, melakukan pemeliharaan server secara berkala, serta membuat rencana pemulihan layanan.
R8	Kerusakan infrastruktur akibat bencana alam	Medium	Melakukan perlindungan terhadap perangkat TI, menyediakan lokasi penyimpanan cadangan data, membuat rencana pemulihan bencana (disaster recovery), serta mempertimbangkan kerja sama dengan penyedia layanan eksternal untuk pemulihan infrastruktur.
R9	Kesalahan pengguna (*human error*)	Medium	Melakukan pelatihan pengguna, membuat panduan penggunaan sistem, menerapkan pembatasan hak akses, sesuai kebutuhan, serta meningkatkan kesadaran pengguna terhadap keamanan informasi.
R10	Kebocoran informasi perusahaan	High	Menerapkan control akses data, enkripsi informasi penting, melakukan audit keamanan secara berkala, menerapkan kebijakan keamanan informasi, serta melakukan pemantauan terhadap aktivitas akses data.

2. Pencatatan dan Pelaporan

Pencatatan dan pelaporan manajemen risiko teknologi informasi pada PT XYZ dilakukan berdasarkan tahapan ISO 31000:2018, mulai dari identifikasi aset, identifikasi risiko, analisis tingkat kemungkinan dan dampak, evaluasi risiko, hingga penentuan perlakuan risiko. Hasil pencatatan menunjukkan terdapat sepuluh risiko teknologi informasi yang berpotensi mengganggu operasional perusahaan, seperti gangguan jaringan, kerusakan perangkat keras, kegagalan sistem aplikasi, kehilangan data, serangan siber, server down, hingga kebocoran informasi perusahaan.

Berdasarkan hasil evaluasi, terdapat empat risiko dengan tingkat High, yaitu kehilangan data, serangan siber, server down, dan kebocoran informasi, serta enam risiko dengan tingkat Medium yang tetap memerlukan pengendalian dan pemantauan secara berkala. Pelaporan risiko digunakan sebagai dasar pengambilan keputusan dalam menentukan strategi pengendalian, seperti penerapan backup data, peningkatan keamanan sistem, pemeliharaan perangkat, penyediaan sistem pemulihan bencana, serta peningkatan kesadaran pengguna terhadap keamanan informasi.

D. Kesimpulan

Berdasarkan hasil penelitian mengenai analisis manajemen risiko teknologi informasi pada PT XYZ menggunakan ISO 31000:2018, dapat disimpulkan bahwa terdapat sepuluh risiko utama yang dapat memengaruhi operasional teknologi informasi perusahaan. Hasil evaluasi menunjukkan bahwa terdapat empat risiko dengan tingkat High, yaitu kehilangan data, serangan siber, server down, dan kebocoran informasi perusahaan, serta enam risiko dengan tingkat Medium yang tetap memerlukan pengendalian. Penerapan ISO 31000:2018 membantu perusahaan dalam melakukan identifikasi, analisis, evaluasi, dan penanganan risiko secara sistematis sehingga dapat mendukung keberlangsungan operasional dan meningkatkan kesiapan perusahaan dalam menghadapi gangguan teknologi informasi.

Saran

PT XYZ disarankan untuk melakukan pemantauan dan evaluasi risiko teknologi informasi secara berkala agar risiko yang muncul dapat segera ditangani. Perusahaan juga perlu meningkatkan pengendalian terhadap risiko dengan tingkat tinggi melalui penerapan backup data rutin, peningkatan keamanan sistem, pemeliharaan infrastruktur, penyediaan sistem pemulihan bencana, serta penguatan kebijakan keamanan informasi. Selain itu, pelatihan bagi pengguna sistem perlu dilakukan untuk mengurangi risiko akibat kesalahan manusia dan meningkatkan kesadaran terhadap keamanan TI.

E. Referensi

Andika, D. Y., & Wijaya, A. F. (2022). *Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerinvital Timur*. *5*(2), 111–118.

Angkat, N. H., & Arsyadona. (2025). *Analisis Penerapan Iso 3100 Dalam Manajemen Risiko Di Pt.Xyz*. *3*(1), 377–386.

Chrisanty, T. W., & Tambotoh, J. (2023). *Analisis Manajemen Risiko Sistem Informasi Menggunakan Iso 31000:2018 Di Pt. Xyz*. *5*(2), 372–381.

Fadiyah, S. K., & Ilham. (2025). *Analisis Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 Pada Pt Xyz*. *9*(1), 1613–1618.

Jayonata, K. C. D., & Sitokdana, M. N. . (2024). *Analisis Risiko Teknologi Informasi Menggunakan Iso 31000 Pada Aplikasi Cupk Mobile (Studi Kasus : Ksp Abc)*. *9*(1), 16–25.

Manuputty, G. P., Azis, A. A., & Pratami, N. A. N. (2022). *Analisis Manajemen Risiko Berbasis Iso 31000 Pada Aspek Operasional Teknologi Informasi Pt. Schlumberger Geophysics Nusantara*. *3*(1), 1–20.

Pratama, I. P. A. E., & Pratika, M. T. S. (2020). *Manajemen Risiko Teknologi Informasi Terkait Manipulasi Dan Peretasan Sistem Pada Bank Xyz Tahun 2020 Menggunakan Iso 31000:2018*. *15*(2), 63–70.

Ramadhan, D. L., Febriansah, R., & Dewi, R. S. (2020). *Analisis Manajemen Risiko Menggunakan Iso 31000 Pada Smart Canteen Sma Xyz*. *7*(1), 91–96. Https://Doi.Org/10.30865/Jurikom.V7i1.1791

Utamajaya, J. N., Afrina, & Fitriah, A. N. (2021). *Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam Paser Utara Menggunakan Framework Iso 31000 : 2018*. *25*(2), 326–334.

Zagoto, S. P., & Sitokdana, M. N. . (2021). *Analisis Risiko Teknologi Informasi Di Organisasi Xyz Cabang Salatiga Menggunakan Iso 31000*. *4*(1), 1–9.