JTK3TI Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi

Volume 12 Nomor 2, 2026, pp 156-162
ISSN: 2460-1799 P-ISSN: 1432-602743

Analisis Manajemen Risiko Sistem Informasi Menggunakan Standar ISO 31000:2018 pada PT ABC

Michael Imanuel[1*], Kevin Alexander Yech[1]

Michael Imanuel [1,*], Kevin Alexander Yech [1], Sri Andayani [1]

[1] Sistem Informasi; Universitas Katolik Musi Charitas Palembang; Jl. Bangau No.60, 9 Ilir, Kec. Ilir Tim. II, Kota Palembang, Sumatera Selatan 30114, (0711)378171; e-mail: rektorat@ukmc.ac.id

* Korespondensi: e-mail: michaelimanuel242@gmail.com

Diterima: 07/06/2026; Review: 10/06/2026; Disetujui: 01/07/2026

ABSTRAK *– PT ABC merupakan pengembang properti yang sangat bergantung pada pemanfaatan teknologi informasi dalam operasionalnya. Ketergantungan ini memunculkan kerentanan sistem yang berpotensi mengganggu keberlangsungan bisnis. Penelitian ini bertujuan melakukan analisis dan evaluasi manajemen risiko sistem informasi perusahaan dengan menerapkan kerangka kerja ISO 31000:2018. Tahapan penelitian mencakup penetapan ruang lingkup, identifikasi aset dan risiko, analisis kemungkinan beserta dampaknya, evaluasi tingkat risiko, hingga penentuan strategi penanganan. Hasil penelitian memetakan 21 kemungkinan ancaman risiko yang bersumber dari faktor perangkat keras, perangkat lunak, data, dan pengguna. Evaluasi matriks risiko menunjukkan bahwa ancaman paling kritis berada pada level sangat tinggi, seperti insiden pemadaman listrik, serangan siber, dan kegagalan pencadangan data. Untuk mengatasi kerentanan tersebut, penanganan risiko dirumuskan dengan dominasi tindakan mitigasi, disusul oleh upaya penghindaran, penerimaan, dan pembagian risiko. Kontribusi penelitian ini berupa panduan rekomendasi strategis bagi pimpinan perusahaan guna menekan risiko dan meningkatkan keamanan tata kelola aset informasinya.*

Kata Kunci *– Evaluasi Risiko; ISO 31000:2018; Manajemen Risiko; Pengembang Properti; Teknologi Informasi.*

Analysis of Information Systems Risk Management Using ISO 31000:2018 Standard at PT ABC

ABSTRACT *– PT ABC is a property developer that relies heavily on the utilization of information technology in its operations. This dependency creates system vulnerabilities that could potentially disrupt business continuity. This study aims to analyze and evaluate information systems risk management at the company by applying the ISO 31000:2018 framework. The research stages include defining the scope, identifying assets and risks, analyzing likelihood and impact, evaluating risk levels, and determining treatment strategies. The results mapped 21 possible risk threats originating from hardware, software, data, and user factors. The risk matrix evaluation indicates that the most critical threats are at a very high level, such as power outages, cyberattacks, and data backup failures. To address these vulnerabilities, risk treatments are formulated with a dominance of mitigation actions, followed by risk avoidance, acceptance, and sharing. This research contributes as a strategic recommendation guide for company leaders to minimize risks and enhance the security of their information asset governance.*

Keywords *– Information Technology; ISO 31000:2018; Property Developer; Risk Evaluation; Risk Management.*

This is an open access article under the CC BY-SA license

Volume 12 Nomor 2, 2026, pp 156-162
ISSN: 2460-1799 P-ISSN: 1432-602743

1. PENDAHULUAN

Pemanfaatan Teknologi Informasi (TI) pada era digital saat ini telah menjadi fondasi utama bagi berbagai sektor industri, termasuk industri pengembang properti (*real estate*). TI digunakan untuk memfasilitasi integrasi data operasional, mulai dari proses pengadaan (*purchasing*), penjualan, hingga manajemen sumber daya manusia (HRD) dan inventori material [1]. PT ABC merupakan perusahaan pengembang properti (*real estate*) berskala nasional yang bergerak di bidang perhotelan dan pembangunan kawasan perumahan klaster. Untuk mendukung kegiatan operasionalnya, PT ABC menggunakan serangkaian aset TI meliputi server, aplikasi HRD, aplikasi gudang, serta basis data penjualan dan finansial.

Namun, ketergantungan yang tinggi terhadap sistem TI ini menciptakan potensi risiko yang signifikan [2]. Gangguan berupa kerusakan perangkat keras, serangan siber (virus atau peretasan), pemadaman listrik yang berujung pada kerusakan server, hingga kegagalan cadangan (*backup*) data dapat berakibat fatal [3]. Kegagalan sistem tidak hanya menyebabkan kerugian finansial akibat berhentinya operasional pemasaran dan pembangunan, tetapi juga berdampak pada turunnya reputasi perusahaan di mata pelanggan dan pemangku kepentingan (*stakeholder*) [4]. Oleh karena itu, diperlukan sebuah tata kelola dan mekanisme manajemen risiko sistem informasi yang terstruktur untuk mengidentifikasi, menganalisis, dan memitigasi potensi ancaman tersebut sebelum berubah menjadi insiden yang merugikan.

Penelitian-penelitian terdahulu telah membuktikan bahwa kerangka kerja manajemen risiko berstandar internasional sangat efektif untuk memetakan kerentanan sistem informasi. Kajian oleh **Ardius dkk. (2022)** menggunakan ISO 31000 untuk mengevaluasi sistem informasi akademik dan menemukan bahwa pendekatan ini sangat komprehensif dalam menyelaraskan risiko TI dengan tujuan institusi [5]. Penelitian relevan oleh **Fachrezi (2023)** mengkaji risiko TI menggunakan kerangka kerja ISO 31000 mampu menekan *down-time* server secara signifikan [6]. Sementara itu, penelitian yang dilakukan oleh Sulistiawati dan Hartomo (2024) [7] menegaskan bahwa kerangka ISO 31000 versi 2018 sangat adaptif diterapkan pada lingkungan bisnis yang dinamis karena menempatkan integrasi kepemimpinan dan penciptaan nilai sebagai inti penanganan risiko [7].

Selain pada institusi berskala besar, fleksibilitas standar ISO 31000 juga dibuktikan dalam lingkup tata kelola aplikasi spesifik dan platform digital terintegrasi. Sebagai contoh, Putri dan Rudianto (2024) memanfaatkan kerangka kerja ini untuk mengevaluasi risiko pada aplikasi *e-Poin* guna menjamin konsistensi performa sistem layanan [12]. Dalam konteks operasional transaksi dan layanan berbasis web, Miftakhatun (2020) juga menegaskan bahwa pemetaan risiko berbasis ISO 31000 mampu mengidentifikasi celah keamanan kritis pada *source code* dan basis data sistem informasi [14].

Lebih lanjut, penelitian manajemen risiko ini tidak hanya berfokus pada aspek teknologis murni, melainkan juga pada adaptasi infrastruktur pendukung operasional harian. Ramadhan dkk. (2020) mengimplementasikan ISO 31000 untuk memitigasi kegagalan sistem pada ekosistem *smart canteen* yang melibatkan integrasi perangkat keras dan jaringan lokal [13]. Di sisi lain, pentingnya penelitian berbasis area lokal juga ditunjukkan oleh Pebriani dan Zulfikar (2022) dalam audit sistem informasi manajemen pegawai di Kota Palembang, yang menyoroti bahwa faktor kerentanan *brainware* dan kelistrikan daerah sering kali menjadi ancaman utama yang melumpuhkan ketersediaan data [15].

Melalui analisis gap terhadap penelitian-penelitian terdahulu, sebagian besar studi dan implementasi manajemen risiko ISO 31000 masih terpusat pada sektor pemerintahan, perbankan, dan institusi pendidikan [8]–[10]. Meskipun terdapat penelitian oleh Filikano dkk. (2024) yang mengkaji analisis risiko menggunakan ISO 31000:2018 pada sektor korporasi swasta di PT. XYZ [16], ruang lingkup kajian tersebut masih terbatas pada Sistem Informasi Akuntansi saja. Masih sangat terbatas penelitian akademis yang secara spesifik menelaah kerentanan aset TI pada sektor industri pengembang properti berskala nasional yang memiliki kompleksitas alur operasional fisik dan digital yang terdesentralisasi seperti PT ABC.

Melihat urgensi dari celah keamanan tersebut, penelitian ini sangat penting dilakukan guna memberikan panduan kerangka kerja yang sistematis bagi manajemen perusahaan. Tujuan utama dari kajian artikel ini adalah untuk melakukan analisis dan evaluasi manajemen risiko pada tata kelola aset sistem informasi di PT ABC menggunakan instrumen standar ISO 31000:2018. Kontribusi nyata dari penelitian ini adalah menghasilkan sebuah dokumen

penilaian risiko (*risk assessment report*) yang komprehensif dan valid. Hasil rekomendasi ini kelak dapat dijadikan sebagai landasan penyusunan Standar Operasional Prosedur (SOP) bagi divisi TI maupun jajaran pimpinan strategis PT ABC dalam rangka meningkatkan keandalan, ketersediaan, dan integritas aset informasinya.

2. METODE PENELITIAN

Penelitian ini dirancang sebagai penelitian kualitatif dan kuantitatif deskriptif yang berfokus secara eksklusif pada pelaksanaan audit dan analisis risiko sistem informasi. Subjek dari penelitian ini adalah ekosistem sistem informasi pada PT ABC, dengan lokus penelitian di kantor operasional pusat perusahaan. Bahan atau platform utama yang diteliti mencakup seluruh portofolio aset informasi perusahaan. Aset-aset tersebut diklasifikasikan ke dalam kategori data (data *purchasing*, penjualan, keuangan, HRD, gudang, audit), perangkat lunak (aplikasi *purchasing*, penjualan, HRD, gudang, perangkat lunak perkantoran), perangkat keras (komputer, server, printer, CPU), jaringan (router, Wi-Fi), serta *brainware* (sumber daya manusia selaku pengguna).

Teknik pengambilan data dilakukan melalui kegiatan observasi lapangan secara langsung dan wawancara mendalam yang terstruktur kepada pemangku kepentingan kunci. Narasumber meliputi jajaran Direktur Utama, Manajer *Purchasing*, Manajer Pemasaran, Manajer HRD, serta pihak manajemen pengawas operasional proyek. Data empiris terkait keandalan sistem yang dikumpulkan kemudian dianalisis tingkat kematangannya menggunakan kuesioner yang diselaraskan dengan klausul-klausul pada kerangka kerja ISO 31000:2018.

Metode tahapan analitis yang diusulkan dan diterapkan dalam penelitian ini secara presisi mengadopsi struktur alur proses manajemen risiko standar ISO 31000:2018, yang terbagi menjadi rangkaian kegiatan sebagai berikut:

Penentuan Ruang Lingkup, Konteks, dan Kriteria: Menetapkan batasan area operasional penilaian risiko di lokus kantor pusat PT ABC, memahami sejarah pertumbuhan dan struktur organisasi perusahaan. Pada tahap ini turut ditetapkan kriteria risiko parameter penilaian yang digolongkan pada dimensi *hardware*, *software*, data, dan *brainware*.

Penilaian Risiko (*Risk Assessment*): Merupakan inti teknis pengujian yang disusun atas tiga sub-proses:

a. Identifikasi Risiko: Mengobservasi, mengenali, dan mendeskripsikan secara rinci jenis risiko (ancaman dan kerentanan aset) yang dipandang dapat menghambat tercapainya tujuan perusahaan.

b. Analisis Risiko: Membedah sifat insiden risiko guna menentukan perhitungan tingkat estimasi Kemungkinan (*Likelihood*) maupun rentang nilai besaran Dampak (*Impact*) menggunakan skala ordinal empiris bernilai 1 hingga 5.

c. Evaluasi Risiko: Melakukan perbandingan objektif atas hasil analisis risiko dengan kriteria ambang batas yang telah ditetapkan guna memposisikan level kumulatif besaran risiko ke dalam kuadran kategorikal matriks.

Penanganan Risiko (*Risk Treatment*): Memilih dan merumuskan implementasi tindakan korektif untuk memodifikasi paparan risiko. Penentuan taktik penanganan bermuara pada empat opsi: menerima konsekuensi risiko (*Accept*), penghindaran mutlak (*Avoid*), reduksi/mitigasi untuk menekan laju dampak (*Mitigate*), atau membagi liabilitas risiko bersama entitas pihak ketiga (*Share*).

Seluruh metodologi dalam rangkaian penelitian manajemen ini dikerjakan dengan didukung oleh pilar komunikasi dan konsultasi yang terus-menerus kepada semua tingkatan manajemen perusahaan, serta tahap pencatatan dan pelaporan (*recording and reporting*).

3. HASIL DAN PEMBAHASAN

Identifikasi Aset dan Risiko

Berdasarkan serangkaian hasil dari wawancara terarah dan observasi menyeluruh bersama entitas manajemen PT ABC, tahapan fundamental pertama dilakukan dengan menginventarisasi seluruh portofolio aset pada arsitektur sistem informasi. Seluruh basis aset yang terdata dipetakan ke dalam entitas data operasional (*purchasing*, penjualan, HRD, finansial, inventori), perangkat lunak (sistem aplikasi transaksi dan perkantoran), perangkat keras (komputer dan pusat pangkalan data server), hingga infrastruktur jaringan nirkabel dan pengguna.

Beranjak dari fondasi inventaris aset tersebut, proses dilanjutkan dengan mengidentifikasi kejadian nyata dan celah kerentanan (*vulnerability*) sistem yang berpotensi menjadi ancaman (*threat*) bagi keberlangsungan operasional proyek PT ABC. Terdapat total 21 kemungkinan bentuk risiko unik yang berhasil diidentifikasi. Temuan ini direpresentasikan melalui nomenklatur ID dari R01 hingga R21. Ancaman krusial yang tercatat meliputi kerusakan *hardware* secara wajar (R02), insiden hilangnya catu daya listrik (R04), serangan infeksi

virus (R06), peretasan (R09), kegagalan prosedur *backup* data (R18), ancaman dari mantan karyawan yang belum terhapus hak aksesnya (R16), insiden *server down* (R19), hingga bencana fisik luar biasa seperti rambatan petir (R21) maupun kebakaran (R20).

Tabel 1. Identifikasi dan Klasifikasi Risiko

ID Risiko	Kategori Aset	Nama / Deskripsi Risiko
R01	Perangkat Keras	Debu atau kotoran pada perangkat
R02	Perangkat Keras	Kerusakan *hardware*
R03	Perangkat Keras	Perangkat perlu di-*upgrade*
R04	Perangkat Keras	Listrik padam
R05	Perangkat Keras	*Overload* sistem
R06	Perangkat Lunak	Serangan virus
R07	Perangkat Lunak	Aplikasi mati tiba-tiba
R08	Perangkat Lunak	*Maintenance* tidak terjadwal
R09	Perangkat Lunak	*Hacking* (peretasan)
R10	Perangkat Lunak	*Database error*
R11	Data	Kehilangan data
R12	Data	Gagal melakukan penyimpanan
R13	Jaringan	Koneksi jaringan terputus
R14	*Brainware*	Kurangnya sumber daya manusia
R15	*Brainware*	*Human error*
R16	*Brainware*	Mantan karyawan mengakses data penting
R17	*Brainware*	Penyalahgunaan hak akses
R18	Data	Kegagalan *backup* data
R19	Perangkat Keras	*Server down*
R20	Bencana Fisik	Kebakaran
R21	Bencana Fisik	Petir

Analisis dan Evaluasi Matriks Risiko

Setiap risiko yang telah diidentifikasi pada fase sebelumnya diuji kualitas dan besaran ancamannya melalui penentuan parameter Kemungkinan (*Likelihood*) terjadinya peristiwa risiko, berbanding dengan skala destruktif Dampak (*Impact*). Model matriks skala baku manajemen risiko yang disetujui bersama oleh pimpinan operasional PT ABC menggunakan rentang interval 1 sampai dengan batas nilai tertinggi 5 [11]. Skala kemungkinan direpresentasikan dari nilai 1 (Sangat Jarang) hingga 5 (Hampir Pasti). Sementara skala dampak dimulai dari nilai 1 (Tidak Signifikan) hingga skala ekstrem bernilai 5 (Katastrope) di mana proses bisnis terhenti secara total. Sebagai contoh kasus, peristiwa listrik padam (R04) memiliki frekuensi kemungkinan berada pada ambang nilai 4 (kategori "Sering") mengingat tingginya intensitas gangguan pasokan daya pada lokasi operasional. Dampaknya pun dipatok pada interval tertinggi yakni 5 (kategori "Katastrope") karena listrik yang padam tanpa redundansi mematikan lalu lintas data operasional secara masif, sehingga besaran risikonya mencapai 20 dan terkategori Sangat Tinggi.

Setelah kompilasi bobot koefisien Kemungkinan dan besaran Dampak selesai dibakukan, tahapan selanjutnya adalah Evaluasi Risiko. Proses matematis matriks evaluasi silang dilakukan dengan mengalikan parameter kemungkinan dan dampak untuk mendapatkan Besaran Risiko (*Risk Score*). Susunan hierarki pengelompokan level risiko direpresentasikan ke dalam zona lima kode warna standar ISO: zona Biru (Sangat Rendah, skor 1-5), Hijau (Rendah, skor 6-11), Kuning (Sedang, skor 12-15), Oranye (Tinggi, skor 16-19), dan Merah (Sangat Tinggi, skor 20-25). Hasil pemetaan matriks evaluasi untuk 21 sampel risiko PT ABC dijabarkan pada Tabel 2.

Tabel 2. Hasil Evaluasi Matriks Besaran Risiko

ID Risiko	Nama Risiko	Kemungkinan (L)	Dampak (I)	Besaran (L×I)	Level Risiko
R01	Debu atau kotoran pada perangkat	3	2	6	Rendah
R02	Kerusakan *hardware*	2	4	8	Rendah
R03	Perangkat perlu di-*upgrade*	3	2	6	Rendah
R04	Listrik padam	4	5	20	Sangat Tinggi
R05	*Overload* sistem	3	4	12	Sedang
R06	Serangan virus	4	4	16	Tinggi
R07	Aplikasi mati tiba-tiba	3	3	9	Rendah
R08	*Maintenance* tidak terjadwal	3	3	9	Rendah
R09	*Hacking* (peretasan)	4	5	20	Sangat Tinggi
R10	*Database error*	2	4	8	Rendah
R11	Kehilangan data	3	5	15	Sedang
R12	Gagal melakukan penyimpanan	3	4	12	Sedang
R13	Koneksi jaringan terputus	4	3	12	Sedang
R14	Kurangnya sumber daya manusia	2	3	6	Rendah
R15	*Human error*	4	3	12	Sedang
R16	Mantan karyawan	4	4	16	Tinggi

	mengakses data penting				
R17	Penyalahgunaan hak akses	3	4	12	Sedang
R18	Kegagalan *backup* data	4	5	20	Sangat Tinggi
R19	*Server down*	3	5	15	Sedang
R20	Kebakaran	1	5	5	Sangat Rendah
R21	Petir	2	4	8	Rendah

Penanganan Risiko (*Risk Treatment*)

Setelah seluruh risiko dievaluasi dan diposisikan ke dalam matriks pada Tabel 2, tahap akhir dari proses manajemen risiko ISO 31000:2018 adalah penanganan risiko (*risk treatment*). Pada tahap ini, setiap risiko yang berada di atas ambang batas yang dapat diterima organisasi, yakni risiko dengan level Sedang hingga Sangat Tinggi, dipilihkan opsi perlakuan yang sesuai dari empat strategi baku, yaitu menerima risiko (*Accept*), menghindari risiko (*Avoid*), memitigasi atau menekan dampak risiko (*Mitigate*), serta membagi risiko kepada pihak ketiga (*Share*). Hasil pemetaan menunjukkan bahwa tindakan mitigasi (*Mitigate*) menjadi strategi yang paling dominan diterapkan, disusul kombinasi penghindaran dan pembagian risiko untuk ancaman tertentu.

Prioritas penanganan diberikan pada tiga risiko berkategori Sangat Tinggi (kritis), yaitu listrik padam (R04), peretasan (R09), dan kegagalan *backup* data (R18), karena ketiganya berpotensi menghentikan operasional bisnis secara total. Penanganan ketiganya diarahkan pada penyediaan infrastruktur redundansi daya, penguatan keamanan siber, dan pencadangan otomatis berbasis awan. Risiko berkategori Tinggi, yaitu serangan virus (R06) dan akses data oleh mantan karyawan (R16), ditangani melalui penguatan *endpoint protection* serta pengetatan tata kelola hak akses. Rincian strategi penanganan untuk seluruh risiko signifikan disajikan pada Tabel 3.

Tabel 3. Strategi Penanganan Risiko (*Risk Treatment*)

ID Risiko	Level Risiko	Opsi Penanganan	Rekomendasi Tindakan
R04	Sangat Tinggi	*Mitigate*	Pengadaan infrastruktur redundansi daya mandiri berupa UPS dan generator (*genset*) otomatis, serta pemasangan stabilizer untuk melindungi server.
R09	Sangat Tinggi	*Mitigate* & *Share*	Penguatan *firewall*, penerapan IDS/IPS, dan uji penetrasi (*penetration testing*) berkala; sebagian risiko dialihkan melalui layanan keamanan terkelola dan asuransi siber.
R18	Sangat Tinggi	*Mitigate*	Implementasi pencadangan (*backup*) otomatis terjadwal berbasis awan (*cloud*) dengan skema 3-2-1 disertai uji pemulihan (*restore test*) secara periodik.
R06	Tinggi	*Mitigate*	Pemasangan antivirus dan *endpoint protection* terpusat, pembaruan *signature* otomatis, serta edukasi keamanan bagi seluruh pengguna.
R16	Tinggi	*Avoid* & *Mitigate*	Penerapan prosedur *offboarding* ketat dengan pencabutan hak akses segera saat karyawan keluar, serta audit akun pengguna secara berkala.
R05	Sedang	*Mitigate*	Pemantauan beban server secara berkala dan peningkatan kapasitas (*scaling*) sesuai pertumbuhan transaksi.
R11	Sedang	*Mitigate*	Penerapan redundansi penyimpanan (RAID) dan enkripsi data untuk menjaga integritas serta ketersediaan data.
R12	Sedang	*Mitigate*	Validasi proses penyimpanan dan pemantauan kapasitas storage untuk mencegah kegagalan penyimpanan data.
R13	Sedang	*Mitigate* & *Share*	Penyediaan jalur internet cadangan (ISP redundan) dan kontrak tingkat layanan (SLA) dengan penyedia jaringan.
R15	Sedang	*Mitigate*	Pelatihan SOP secara rutin dan penerapan kontrol validasi input untuk menekan kesalahan manusia (*human error*).
R17	Sedang	*Mitigate*	Penerapan prinsip hak akses minimum (*least privilege*) dan pencatatan (*logging*) aktivitas pengguna.
R19	Sedang	*Mitigate*	Pemeliharaan terjadwal dan penyediaan server cadangan (*failover*) untuk menjaga ketersediaan layanan.

Adapun risiko dengan level Rendah dan Sangat Rendah, seperti debu pada perangkat (R01), kebakaran (R20), dan rambatan petir (R21), pada dasarnya ditangani dengan opsi penerimaan (*Accept*) yang disertai pemantauan rutin dan pemeliharaan preventif, mengingat probabilitas kejadiannya yang rendah dan biaya mitigasi yang tidak sebanding. Dengan demikian, kerangka penanganan risiko ini menghasilkan rekomendasi tata kelola yang terukur dan dapat dijadikan landasan penyusunan Standar Operasional Prosedur (SOP) keamanan aset informasi bagi PT ABC.

4. KESIMPULAN

Penelitian ini telah berhasil menganalisis dan mengevaluasi ekosistem sistem informasi pada PT ABC dengan instrumen yang terstruktur menggunakan standar acuan ISO 31000:2018. Melalui identifikasi secara definitif, ditemukan total 21 komponen kerentanan yang mengancam stabilitas manajemen data komputasi. Evaluasi silang antara probabilitas ancaman dan implikasi destruktifnya merumuskan konklusi bahwa ancaman keamanan paling dominan (seperti gangguan utilitas kelistrikan masif, kegagalan prosedur pencadangan data, dan infiltrasi siber berupa peretasan) terkategori berada pada zona risiko Sangat Tinggi (kritis), sementara serangan virus dan lemahnya tata kelola kewenangan akun sisa mantan pekerja berada pada zona Tinggi. Berdasarkan hasil evaluasi tersebut, strategi penanganan risiko (*risk treatment*) dirumuskan dengan proporsi dominan pada tindakan mitigasi (*Mitigate*), disusul oleh penghindaran (*Avoid*), penerimaan (*Accept*), dan pembagian risiko (*Share*). Untuk risiko kritis, mitigasi diarahkan pada pengadaan infrastruktur redundansi daya mandiri (UPS dan *genset*), fasilitas pencadangan otomatis berbasis awan (*cloud*), serta penguatan keamanan siber pada perimeter jaringan dan tata kelola hak akses pengguna. Konklusi akhir dari laporan investigasi manajemen risiko ISO 31000 ini krusial untuk dijadikan tonggak pedoman strategis (SOP tata kelola) oleh jajaran manajemen PT ABC guna memperkuat keandalan basis datanya serta menjamin kelancaran layanan transaksi properti di masa mendatang.

DAFTAR PUSTAKA

[1] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko dengan menggunakan Framework ISO 31000:2018 pada Sistem Informasi Gudang," Jurnal Teknik Informatika dan Sistem Informasi (JUTIF), vol. 9, no. 1, pp. 407–420, 2022.

[2] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," Jurnal Sistem Informasi Bisnis (JSINBIS), vol. 10, no. 1, pp. 28–35, 2020.

[3] DI. P. A. S. Putra and I. K. R. Hendrawan, "Analisis Manajemen Risiko SIMRS pada Rumah Sakit Ganesha Menggunakan ISO 31000," JATI (Jurnal Teknologi dan Informasi), vol. 14, no. 1, pp. 88–96, 2024.

[4] A. R. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi menggunakan ISO 31000 dan Standar Pengendalian ISO/IEC 27001 di Tripio Purwokerto," MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 20, no. 2, pp. 389–396, 2021.

[5] E. Ardius, A. Isroqmi, N. Nurdiana, D. Irawan, and S. Hastini, "Manajemen Risiko Penggunaan Sistem Informasi Akademik di Universitas ABC Menggunakan ISO 31000," Jurnal Digital Teknologi Informasi, vol. 9, no. 1, pp. 27–36, 2022.

[6] M. I. Fachrezi, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018," Klik - Jurnal Ilmu Komputer, vol. 4, no. 2, pp. 115–125, 2023.

[7] A. Sulistiawati and K. D. Hartomo, "Analisis Manajemen Risiko pada Aplikasi Sistem Informasi Manajemen Sekolah Menggunakan ISO 31000:2018," Sistemasi: Jurnal Sistem Informasi, vol. 13, no. 2, pp. 430–441, 2024.

[8] L. Febriyanti, M. Febrinazahra, Kraugusteeliana, and I. G. S. Masdiyasa, "Manajemen Risiko Sistem Informasi Unit Organisasi BPIW Kementerian PUPR Menggunakan Framework ISO 31000:2018," Jurnal Sistem Informasi dan Aplikasi (JSIA), vol. 2, no. 2, pp. 75–84, 2024.

[9] M. R. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC menggunakan Framework ISO 31000," Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 1, pp. 735–748, 2022.

[10] A. C. Salsabila, Ilham, and M. A. Izzudin, "ANALISIS RISIKO MENGGUNAKAN ISO 31000 : 2018 DALAM PENGELOLAAN APLIKASI PADA KECAMATAN DAN OPD KABUPATEN SIDOARJO," JATI (Jurnal Teknologi dan Informasi), vol. 14, no. 2, pp. 120–129, 2024.

[11] ISO, "ISO 31000:2018 Risk management - Guidelines," International Organization for Standardization, Geneva, Switzerland, Standard, 2018.

[12] N. N. Putri and C. Rudianto, "Penerapan Framework ISO 31000:2018 dalam Menganalisis Manajemen Risiko pada Aplikasi e-Poin," Sistemasi: Jurnal Sistem Informasi, vol. 13, no. 3, pp. 510–521, 2024.

[13] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko menggunakan ISO 31000 pada Smart Canteen SMA XYZ," JURIKOM (Jurnal Riset Komputer), vol. 7, no. 1, pp. 91–96, 2020.

[14] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo menggunakan ISO 31000," JCSE (Journal of Computer Science and Engineering), vol. 1, no. 2, pp. 129–145, 2020.

[15] O. D. Pebriani and D. H. Zulfikar, "Analisis Manajemen Risiko Teknologi Informasi menggunakan ISO 31000 Pada Website SIMPEG di Kantor Kementerian Agama Kota Palembang," dalam Prosiding SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika, 2022, pp. 183–190.

[16] T. Filikano, A. Gunawan, and S. Andayani, "ANALISIS RISIKO SISTEM INFORMASI AKUNTANSI MENGGUNAKAN ISO 31000:2018 DI PT. XYZ," Jurnal Ilmiah Sistem Informasi, vol. 4, no. 1, pp. 31–45, Jun. 2024.