Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Analisis Manajemen Risiko Berbasis ISO 31000 pada Aspek Operasional Teknologi Informasi PT. Schlumberger Geophysics Nusantara

[1]Yogi Kamal, [2*]Andi Al-Ghifari, [3]M Afdhal H, [4]Fajar
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
*Email: *[1]anditriarusman@gmail.com*
(Naskah masuk: 3 Juni 2026, diterima untuk diterbitkan: 31 Juli 2026)

Abstrak: *PT. Schlumberger Geophysics Nusantara merupakan perusahaan multinasional terkemuka di bidang teknologi dan jasa terintegrasi untuk industri minyak dan gas bumi, berlokasi di Wisma Mulia Suite 45th Floor, Jakarta Selatan. Perusahaan ini mengandalkan platform DELFI berbasis cloud untuk mengelola seluruh kegiatan operasionalnya. Ketergantungan tinggi terhadap sistem teknologi informasi (TI) menimbulkan berbagai risiko operasional yang perlu dikelola secara sistematis. Penelitian ini menganalisis manajemen risiko operasional TI menggunakan kerangka kerja ISO 31000:2009 melalui pendekatan kualitatif deskriptif. Data dikumpulkan melalui wawancara terstruktur dengan Project Manager dan Account Manager Divisi Digital & Integration. Penilaian risiko menggunakan matriks likelihood × impact skala 1–5. Hasil penelitian mengidentifikasi 14 risiko operasional TI: 11 risiko (78,57%) pada tingkat Tinggi (skor ≥15) dan 3 risiko (21,43%) pada tingkat Menengah. Risiko tertinggi meliputi downtime sistem DELFI, serangan siber, dan kebocoran data. ISO 31000 terbukti mampu memberikan gambaran terstruktur mengenai tingkat risiko dan prioritas penanganannya untuk mendukung keberlanjutan operasional TI perusahaan.*

Kata Kunci – *Manajemen Risiko; ISO 31000; Teknologi Informasi; Risiko Operasional; Keamanan Siber*

Abstract: *PT. Schlumberger Geophysics Nusantara is a leading multinational company in integrated technology and services for the oil and gas industry, located at Wisma Mulia Suite 45th Floor, South Jakarta. The company relies on the cloud-based DELFI platform to manage all its operational activities. High dependence on information technology (IT) systems creates various operational risks that require systematic management. This study analyzes IT operational risk management using the ISO 31000:2009 framework through a qualitative descriptive approach. Data was collected through structured interviews with the Project Manager and Account Manager of the Digital & Integration Division. Risk assessment uses a likelihood × impact matrix on a 1–5 scale. The study identified 14 IT operational risks: 11 risks (78.57%) at High level (score ≥15) and 3 risks (21.43%) at Moderate level. The highest risks include DELFI system downtime, cyber attacks, and data breaches. ISO 31000 proved effective in providing a structured overview of risk levels and handling priorities to support the sustainability of the company's IT operations.*

Keywords – *Risk Management; ISO 31000; Information Technology; Operational Risk; Cybersecurity*

Pendahuluan

PT. Schlumberger Geophysics Nusantara merupakan perusahaan multinasional nomor satu di dunia di bidang penyediaan teknologi informasi dan jasa terintegrasi untuk industri minyak dan gas bumi. Perusahaan ini berlokasi di Wisma Mulia Suite 45th Floor, Jl. Jend. Gatot Subroto Kav. 42, Jakarta Selatan. Perusahaan menyediakan solusi teknologi canggih untuk kegiatan karakterisasi, pengeboran, produksi, dan pengolahan reservoir, serta bergerak di bidang konsultasi dan manajemen proyek terintegrasi [1].

Platform DELFI merupakan inovasi utama perusahaan, yaitu sistem penyimpanan dan pengelolaan data berbasis cloud yang mendukung seluruh kegiatan operasional dan penjualan. Ketergantungan tinggi terhadap sistem TI berbasis cloud membawa konsekuensi berupa meningkatnya eksposur risiko operasional [2]. Berbagai ancaman seperti downtime sistem, serangan siber, kehilangan

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

data, gangguan jaringan, kerusakan hardware, serta human error berpotensi mengganggu kelangsungan bisnis secara signifikan.

Penelitian sebelumnya oleh Manuputty et al. [5] pada perusahaan yang sama mengidentifikasi 14 risiko operasional TI dengan 11 risiko di level High dan 3 risiko di level Moderate, membuktikan tingginya kerentanan TI perusahaan. Penelitian ini hadir sebagai pembaruan dengan metode wawancara langsung kepada narasumber kunci. ISO 31000:2009 dipilih sebagai kerangka karena bersifat generik, fleksibel, dan tidak mensyaratkan sertifikasi [4]. Penelitian Atmojo & Manuputty [6], Kuncoro et al. [7], serta Herlambang et al. [8] juga membuktikan efektivitas ISO 31000 dalam analisis risiko TI berbagai organisasi.

Penelitian ini bertujuan: (1) mengidentifikasi seluruh risiko operasional TI PT. Schlumberger Geophysics Nusantara; (2) menganalisis tingkat kemungkinan dan dampak setiap risiko; (3) mengevaluasi tingkat dan prioritas risiko; serta (4) merumuskan usulan perlakuan risiko yang dapat diimplementasikan perusahaan.

Metode Penelitian

2.1 Jenis dan Pendekatan Penelitian

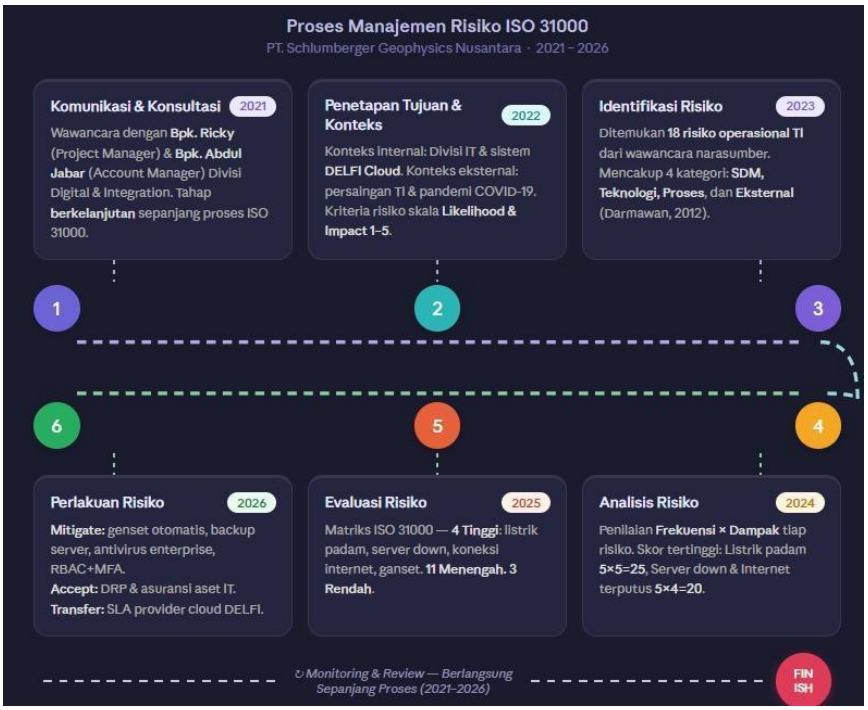
Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan mengadopsi kerangka kerja ISO 31000:2009 sebagai metode utama analisis risiko. Objek penelitian adalah aspek operasional teknologi informasi PT. Schlumberger Geophysics Nusantara, khususnya yang berkaitan dengan platform DELFI berbasis cloud. Pendekatan kualitatif dipilih karena penelitian ini berfokus pada eksplorasi mendalam terhadap kondisi aktual risiko operasional TI perusahaan [13].

2.2 Teknik Pengumpulan Data

Data primer diperoleh melalui wawancara terstruktur yang dilaksanakan pada 7 Mei 2026. Narasumber terdiri dari: (1) Project Manager PT. Schlumberger Geophysics Nusantara; dan (2) Account Manager Divisi Digital & Integration. Pemilihan narasumber dilakukan secara purposive karena keduanya memiliki pengetahuan langsung mengenai kondisi risiko operasional TI perusahaan.

2.3 Tahapan Analisis ISO 31000

Proses analisis risiko mengikuti tahapan ISO 31000:2009 seperti ditunjukkan pada Gambar 1.

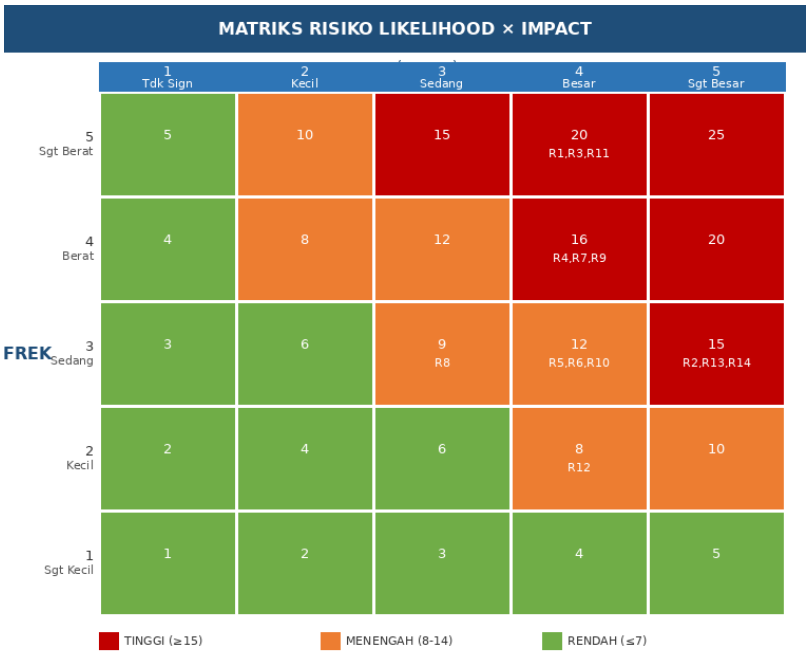


Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Gambar 1. Alur Proses Manajemen Risiko ISO 31000:2009

Tingkat risiko ditentukan dari skor Frekuensi (F) × Dampak (D) menggunakan skala 1–5 dengan kategori: Rendah (≤7), Menengah (8–14), dan Tinggi (≥15). Matriks penilaian risiko 5×5 ditunjukkan pada Gambar 2.



Gambar 2. Matriks Risiko Likelihood × Impact 5×5

Hasil dan Pembahasan

3.1 Penetapan Konteks

Penetapan konteks internal mencakup struktur Divisi IT perusahaan yang terdiri dari Project Manager, IT Development, IT Operations, IT Network & Infrastructure, dan Account Manager Divisi Digital & Integration. Perusahaan memiliki ketergantungan sangat tinggi terhadap platform DELFI berbasis cloud untuk seluruh kegiatan operasional harian di sektor minyak dan gas.

Penetapan konteks eksternal mencakup: (1) persaingan ketat antar penyedia teknologi informasi di industri energi global; (2) perkembangan teknologi digital yang pesat; (3) ancaman keamanan siber global yang terus meningkat; serta (4) regulasi pemerintah Indonesia terkait pengelolaan data dan cloud computing (PP No. 71/2019).

3.2 Identifikasi Risiko

Berdasarkan hasil wawancara dan analisis konteks, diperoleh 14 risiko operasional TI yang dikelompokkan ke dalam 4 kategori sebagaimana disajikan pada Tabel 1.

Tabel 1. Identifikasi Risiko Operasional TI PT. Schlumberger Geophysics Nusantara

No	Kode	Kemungkinan Risiko	Kategori
1	**R1**	Downtime / kegagalan sistem DELFI	Risiko Teknologi
2	**R2**	Kehilangan atau korupsi data perusahaan	Risiko Teknologi
3	**R3**	Serangan siber (hacking, malware, ransomware)	Risiko Eksternal
4	**R4**	Gangguan koneksi internet / jaringan	Risiko Teknologi
5	**R5**	Kesalahan konfigurasi sistem cloud	Risiko Proses

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

No	Kode	Kemungkinan Risiko	Kategori
6	**R6**	Kerusakan hardware (server, storage)	Risiko Teknologi
7	**R7**	Human error oleh operator TI	Risiko SDM
8	**R8**	Kurangnya kompetensi / pelatihan SDM TI	Risiko SDM
9	**R9**	Gangguan pasokan listrik / kegagalan UPS	Risiko Teknologi
10	**R10**	Ketergantungan berlebihan pada penyedia cloud	Risiko Eksternal
11	**R11**	Kebocoran data / pelanggaran keamanan data	Risiko Eksternal
12	**R12**	Perubahan regulasi pemerintah terkait data dan cloud	Risiko Eksternal
13	**R13**	Kegagalan sistem backup dan disaster recovery	Risiko Proses
14	**R14**	Serangan Distributed Denial of Service (DDoS)	Risiko Eksternal

3.3 Analisis dan Evaluasi Risiko

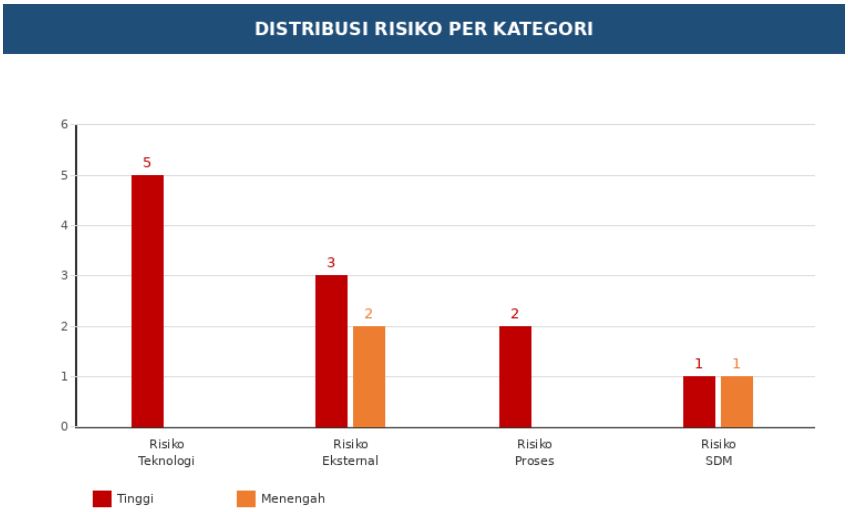
Hasil analisis dan evaluasi 14 risiko operasional TI berdasarkan penilaian F×D disajikan pada Tabel 2.

Tabel 2. Hasil Analisis dan Evaluasi Risiko Operasional TI

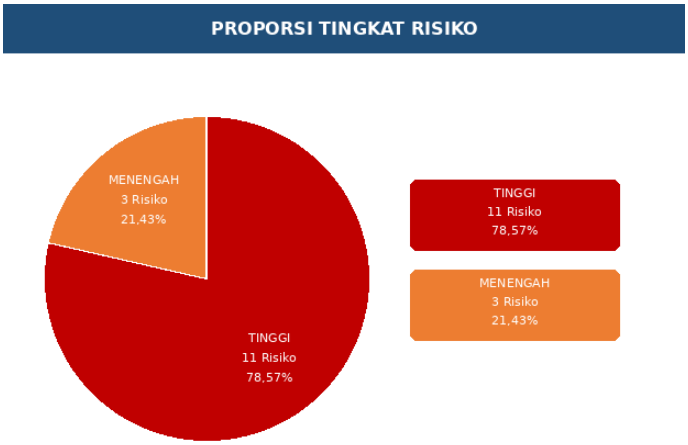
Kode	Kemungkinan Risiko	F	D	F×D	Level	Tindakan
R1	Downtime / kegagalan sistem DELFI	4	5	**20**	**Tinggi**	Segera
R2	Kehilangan atau korupsi data	3	5	**15**	**Tinggi**	Segera
R3	Serangan siber	4	5	**20**	**Tinggi**	Segera
R4	Gangguan koneksi jaringan	4	4	**16**	**Tinggi**	Segera
R5	Kesalahan konfigurasi cloud	3	4	**12**	**Tinggi**	Segera
R6	Kerusakan hardware	3	4	**12**	**Tinggi**	Segera
R7	Human error operator TI	4	4	**16**	**Tinggi**	Segera
R8	Kurangnya kompetensi SDM TI	3	3	**9**	**Menengah**	Direncanakan
R9	Gangguan listrik / kegagalan UPS	4	4	**16**	**Tinggi**	Segera
R10	Ketergantungan penyedia cloud	3	4	**12**	**Tinggi**	Segera
R11	Kebocoran data	4	5	**20**	**Tinggi**	Segera
R12	Perubahan regulasi data dan cloud	2	4	**8**	**Menengah**	Direncanakan
R13	Kegagalan sistem backup	3	5	**15**	**Tinggi**	Segera
R14	Serangan DDoS	3	5	**15**	**Tinggi**	Segera

Distribusi risiko per kategori ditunjukkan pada Gambar 3 dan proporsi tingkat risiko pada Gambar 4

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197



Gambar 3. Distribusi Risiko Operasional TI per Kategori



Gambar 4. Proporsi Tingkat Risiko Operasional TI

Berdasarkan Gambar 3 dan Gambar 4, Risiko Teknologi mendominasi dengan 5 risiko tingkat Tinggi (R1, R2, R4, R6, R9), diikuti Risiko Eksternal dengan 3 risiko Tinggi dan 2 Menengah. Secara keseluruhan, 78,57% risiko berada pada level Tinggi. Risiko dengan skor tertinggi (F×D = 20) adalah R1, R3, dan R11 yang menjadi prioritas utama. Temuan ini konsisten dengan penelitian Manuputty et al. [5] pada perusahaan yang sama.

3.4 Pengendalian / Perlakuan Risiko

Seluruh 11 risiko tingkat Tinggi memerlukan penanganan segera, sedangkan 3 risiko Menengah direncanakan secara berkala. Tabel 3 menyajikan usulan perlakuan risiko secara lengkap.

Tabel 3. Usulan Perlakuan Risiko Operasional TI

Kode	Level	Risiko	Usulan Perlakuan Risiko
R1	**Tinggi**	Downtime sistem DELFI	Menerapkan redundansi server (failover), monitoring real-time 24/7, serta menyusun dan menguji Disaster Recovery Plan (DRP) minimal setiap 6 bulan.
R2	**Tinggi**	Kehilangan/korupsi data	Backup otomatis harian dengan multi-location storage, enkripsi data end-to-end, dan asuransi data penting perusahaan.
R3	**Tinggi**	Serangan siber	Implementasi firewall, IDS/IPS, enkripsi end-to-end, dan pelatihan anti-phishing rutin setiap 3 bulan.
R4	**Tinggi**	Gangguan koneksi jaringan	Multi-ISP dengan automatic failover, peningkatan bandwidth, dan koneksi backup VPN/dedicated line.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

Kode	Level	Risiko	Usulan Perlakuan Risiko
R5	**Tinggi**	Kesalahan konfigurasi cloud	Standar konfigurasi cloud (hardening guide) dan double approval oleh tim senior sebelum perubahan diterapkan.
R6	**Tinggi**	Kerusakan hardware	Preventive maintenance bulanan, hardware redundancy (RAID, dual power), dan spare part kritis di gudang.
R7	**Tinggi**	Human error operator	SOP operasional detail, pelatihan rutin, double-check approval aktivitas kritis, dan audit log terpusat.
R8	**Menengah**	Kurangnya kompetensi SDM	Program sertifikasi tahunan (CompTIA, CISSP, AWS) dan knowledge sharing internal bulanan.
R9	**Tinggi**	Gangguan listrik/UPS	Peningkatan kapasitas UPS, generator cadangan dengan ATS, dan pemeliharaan perangkat listrik setiap 3 bulan.
R10	**Tinggi**	Ketergantungan cloud vendor	Negosiasi SLA (uptime 99,99%), implementasi multi-cloud strategy, dan contingency plan gangguan vendor.
R11	**Tinggi**	Kebocoran data	RBAC, DLP, audit log berkala, enkripsi database, dan compliance PP No. 71/2019.
R12	**Menengah**	Perubahan regulasi	Monitoring regulasi per kuartal dan penyesuaian kebijakan internal sesuai perubahan regulasi.
R13	**Tinggi**	Kegagalan sistem backup	Pengujian backup dan recovery setiap 3 bulan, dokumentasi hasil, dan backup offsite/cloud terenkripsi.
R14	**Tinggi**	Serangan DDoS	DDoS protection berbasis cloud (Cloudflare/AWS Shield), peningkatan bandwidth, dan prosedur respons insiden DDoS.

Kesimpulan

Berdasarkan analisis manajemen risiko operasional TI pada PT. Schlumberger Geophysics Nusantara menggunakan kerangka kerja ISO 31000:2009, diperoleh kesimpulan sebagai berikut:

1. Teridentifikasi 14 risiko operasional TI yang terbagi dalam 4 kategori: Teknologi (5 risiko Tinggi), Eksternal (3 risiko Tinggi, 2 Menengah), Proses (2 risiko Tinggi), dan SDM (1 risiko Tinggi, 1 Menengah). Tingginya proporsi risiko pada kategori Teknologi dan Eksternal mencerminkan kerentanan inheren dari model operasional berbasis cloud yang diadopsi perusahaan.
2. Dari total 14 risiko, 11 risiko (78,57%) berada pada tingkat Tinggi dengan skor $F \times D \geq 15$, dan 3 risiko (21,43%) pada tingkat Menengah dengan skor F×D antara 8–14. Distribusi ini konsisten dengan temuan Manuputty et al. [5] dan mengonfirmasi bahwa perusahaan berbasis platform cloud tunggal menghadapi eksposur risiko yang lebih tinggi dibandingkan perusahaan dengan infrastruktur hybrid.
3. Risiko dengan skor tertinggi ($F \times D = 20$) adalah downtime sistem DELFI (R1), serangan siber (R3), dan kebocoran data (R11), yang ketiganya menjadi prioritas utama penanganan segera. Ketiga risiko ini saling berkaitan karena kegagalan pada satu aspek dapat memicu kaskade risiko pada aspek lainnya.
4. Usulan perlakuan risiko yang dirumuskan mengikuti empat pendekatan ISO 31000: penghindaran, pengurangan, pemindahan, dan penerimaan risiko. Implementasi diprioritaskan dalam dua tahap: jangka pendek (0–3 bulan) untuk risiko skor 20, dan jangka menengah (3–6 bulan) untuk risiko skor 12–16.
5. Kerangka kerja ISO 31000:2009 terbukti efektif memberikan gambaran terstruktur mengenai tingkat risiko dan prioritas penanganannya untuk mendukung keberlanjutan operasional TI perusahaan berbasis cloud. Penelitian lanjutan disarankan melibatkan lebih banyak narasumber lintas divisi dan mengintegrasikan metode kuantitatif seperti simulasi Monte Carlo untuk estimasi risiko yang lebih presisi.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada PT. Schlumberger Geophysics Nusantara, khususnya kepada Bapak/Ibu Project Manager dan Account Manager Divisi Digital & Integration yang telah meluangkan waktu dan bersedia memberikan informasi serta data yang diperlukan dalam penelitian ini. Apresiasi juga disampaikan kepada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, [Universitas Muslim Indonesia] atas dukungan akademik yang diberikan selama proses penelitian berlangsung.

Daftar Pustaka

[1] R.R. Moeller, Brink's Modern Internal Auditing: A Common Body of Knowledge, 8th ed. Hoboken: Wiley, 2016.

[2] I. Grey, S. Manson, dan L. Crawford, The Audit Process: Principles, Practice and Cases, 6th ed. Cengage Learning, 2015.

[3] N.M. Sirait dan A. Susanty, "Analisis risiko operasional berdasarkan pendekatan Enterprise Risk Management (ERM) pada CV Mitra Dunia Palletindo," Industrial Engineering Online Journal, vol. 5, no. 4, 2016.

[4] International Organization for Standardization, ISO 31000:2009 Risk Management — Principles and Guidelines. Geneva: ISO, 2009.

[5] G.P. Manuputty, A. Abdul Azis, dan N.A. Nur Pratami, "Analisis manajemen risiko berbasis ISO 31000 pada aspek operasional teknologi informasi PT. Schlumberger Geophysics Nusantara," E-Prosiding Akuntansi Universitas Trilogi, 2022. https://trilogi.ac.id/journal/ks/index.php/EPAKT/article/view/1171

[6] S.A. Atmojo dan A.D. Manuputty, "Analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada aplikasi AHO Office," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 7, no. 3, hal. 546–558, 2020.

[7] S.D. Kuncoro, R.A. Ghaisan, M.U. Zaky, dan A. Wulansari, "Manajemen risiko pada teknologi informasi: Studi kasus pada perusahaan jasa," Prosiding Seminar Nasional Informatika, vol. 1, hal. 313–323, 2023.

[8] A.A. Herlambang, A.A. Gani, dan D.D. Alvianto, "Pendekatan ISO 31000:2018 dalam manajemen risiko teknologi informasi pada Tracer Study Universitas Sebelas April," Jurnal Teknologi Informasi dan Komunikasi, hal. 5651–5660, 2024.

[9] Jericho dan E. Haryani, "Penerapan ISO 31000:2018 dalam manajemen risiko teknologi informasi pada sistem penerbitan PT. X," Jurnal Informasi, Sains dan Teknologi (ISAINTEK), vol. 7, no. 2, 2024. https://isaintek.polinef.ac.id/index.php/isaintek/article/view/269

[10] A.M. Siregar et al., "Standarisasi manajemen risiko ISO 31000: Tantangan dan strategi implementasi pada PT. Telkom Indonesia," JERKIN: Jurnal Ekonomi, Riset, Kajian dan Inovasi, 2025. https://jerkin.org/index.php/jerkin/article/view/1564

[11] N. Safaat H, "Manajemen risiko teknologi informasi menggunakan framework ISO 31000 studi kasus sistem infrastruktur TI Telkom Indonesia," SITEKIN: Jurnal Sains, Teknologi dan Industri, vol. 12, no. 2, 2015.

[12] B. Prasetyo, A. Salsabila, dan W.E.Y. Retnani, "IT risk management analysis based on ISO 31000 and Bow Tie Analysis in higher education institution," Indonesian Journal of Information Systems, vol. 7, no. 1, hal. 84–96, 2024. https://doi.org/10.24002/ijis.v7i1.9673

[13] Iswajuni, A. Manasikana, dan S. Soetedjo, "The effect of enterprise risk management on firm value in manufacturing companies listed on Indonesian Stock Exchange," Asian Journal of Accounting Research, vol. 3, no. 2, hal. 224–236, 2018.

[14] H.A.M. Hani, D.R.I. Indah, dan P.E.S. Putri, "Analisis manajemen risiko pada teknologi informasi PT. Pos Indonesia menggunakan ISO 31000," Indonesian Journal of Computer Science, vol. 12, no. 6, hal. 3957–3974, 2023. https://doi.org/10.33022/ijcs.v12i6.3504

[15] S.D. Mulyati, R.A. Kuncoro, dan A. Wulansari, "Optimalisasi manajemen risiko teknologi informasi menggunakan framework ISO 31000 di era digital," JISAMAR, vol. 9, no. 1, 2025. https://journal.stmikjayakarta.ac.id/index.php/jisamar/article/view/1690