IONTech Vol. 07(02) : 18-28(Agustus 2026)
e-ISSN : 2745-7206
http://iontech.ista.ac.id/index.php/iontech

ANALISIS MANAJEMEN RISIKO BERBASIS ISO 31000 PADA ASPEK OPERASIONAL TEKNOLOGI INFORMASI PT. SCHLUMBERGER GEOPHYSICS NUSANTARA

RISK MANAGEMENT ANALYSIS BASED ON ISO 31000 ON THE OPERATIONAL ASPECTS OF INFORMATION TECHNOLOGY OF PT. SCHLUMBERGER GEOPHYSICS NUSANTARA

Yogi Kamal[1], Andi Al-Ghifari[2], M Afdhal H[3]*, Fajar[4]
[1,2,3,4]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
*Korespondensi: 13020230069@Student.umi.ac.id
Received: 12 Juli 2026, Revision: 07 Agustus 2026, Accepted: 16 Agusuts 2026

Abstrak

PT. Schlumberger Geophysics Nusantara merupakan perusahaan multinasional terkemuka di bidang teknologi dan jasa terintegrasi untuk industri minyak dan gas bumi, berlokasi di Jakarta Selatan. Perusahaan ini mengandalkan platform DELFI berbasis cloud dalam mendukung kegiatan operasionalnya. Ketergantungan yang 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 dengan skala 1–5. Hasil penelitian mengidentifikasi 14 risiko operasional TI, dengan 9 risiko (64,29%) berada pada tingkat Tinggi dan 5 risiko (35,71%) pada tingkat Menengah. Risiko tertinggi meliputi downtime sistem DELFI, serangan siber, dan kebocoran data, masing-masing dengan skor 20. ISO 31000:2009 memberikan kerangka terstruktur untuk mengidentifikasi, mengevaluasi, dan menentukan prioritas penanganan risiko guna mendukung keberlanjutan operasional TI perusahaan.

Kata kunci: ISO 31000:2009, Keamanan Siber, Manajemen Risiko, Risiko Operasional, Teknologi Informasi.

Abstract

PT. Schlumberger Geophysics Nusantara is a leading multinational company providing integrated technology and services to the oil and gas industry in Indonesia. The company relies on the cloud-based DELFI platform to support its operational activities. This 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 descriptive qualitative approach. Data were collected through structured interviews with the Project Manager and Account Manager of the Digital & Integration Division. Risk assessment was conducted using a likelihood × impact matrix on a 1–5 scale. The results identified 14 IT operational risks, with 9 risks (64.29%) classified as High and 5 risks (35.71%) classified as Moderate. The highest-rated risks were DELFI system downtime, cyberattacks, and data breaches, each with a risk score of 20. The ISO 31000:2009 framework provides a structured approach for identifying, evaluating, and prioritizing risk treatment to support the continuity of the company's IT operations.

Keywords: Cybersecurity, Information Technology, ISO 31000:2009, Operational Risk, Risk Management.

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 (Atmojo & Manuputty, 2020).

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 (Grey & Crawford, 2015). Berbagai ancaman seperti downtime sistem, serangan siber, kehilangan data, gangguan jaringan, kerusakan hardware, serta human error berpotensi mengganggu kelangsungan bisnis secara signifikan.

Penelitian sebelumnya oleh Manuputty et al. (Iswajuni & Soetedjo, 2018). 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 (International Organization for Standardization, 2009). ISO 31000:2009 Risk Management - Principles and Guidelines. ISO. Penelitian Atmojo & Manuputty , Kuncoro et al. , serta Herlambang et al. 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

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 (Prasetyo & Retnani, 2024).

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.

Tahapan Analisis ISO 31000

Proses analisis risiko dalam penelitian ini mengikuti tahapan kerangka kerja ISO 31000:2009 yang meliputi penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, serta perlakuan risiko.

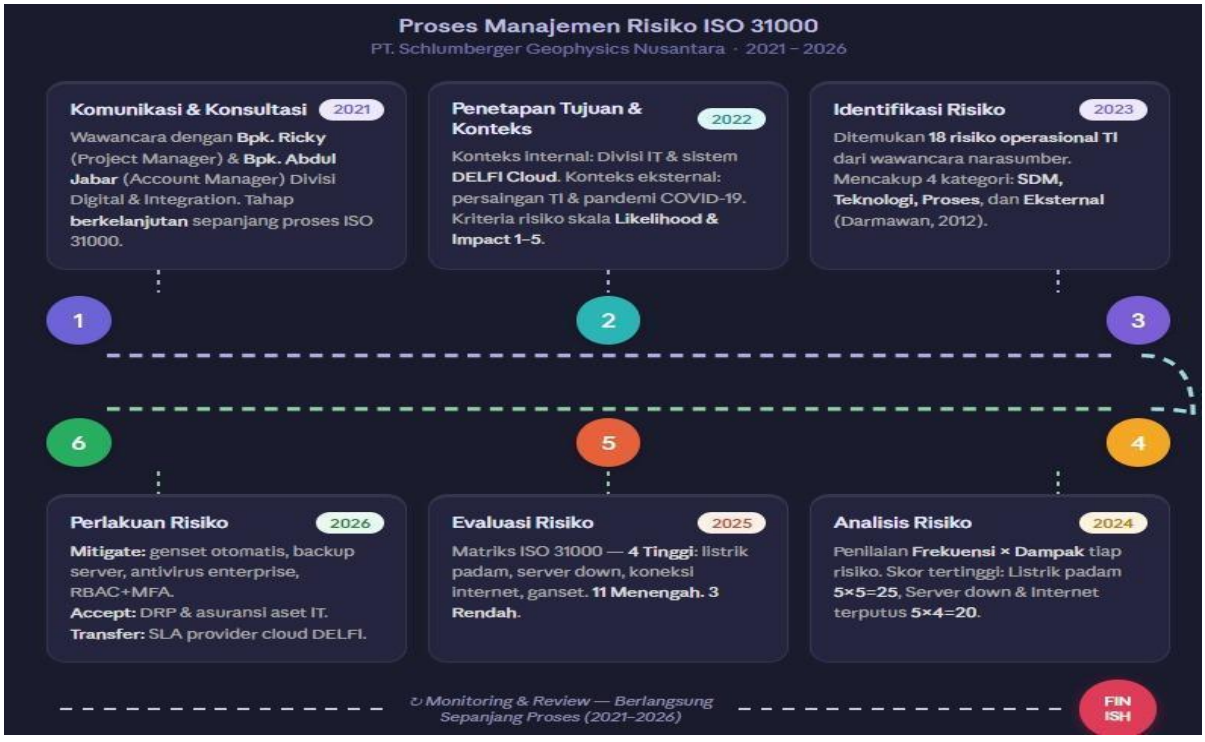
Data utama untuk mengisi tahapan tersebut digali melalui wawancara mendalam (*in-depth interview*) bersama narasumber kunci. Pemilihan narasumber dilakukan secara sengaja menggunakan teknik *purposive sampling* berdasarkan kriteria spesifik, yaitu:

1. Memiliki posisi struktural strategis dalam pengambilan keputusan teknologi di perusahaan.
2. Memiliki pengalaman kerja sekurang-kurangnya 3 (tiga) tahun di industri minyak dan gas bumi.
3. Terlibat langsung dalam tata kelola harian, integrasi, dan mitigasi kendala operasional platform berbasis *cloud*.

Berdasarkan kriteria tersebut, ditetapkan 2 (dua) narasumber utama, yaitu Project Manager dan Account Manager Divisi Digital & Integration. Penentuan narasumber ini sangat relevan dengan objek penelitian karena posisi mereka memberikan akses informasi tangan pertama mengenai dinamika risiko operasional, kerentanan sistem, serta dampak finansial maupun reputasi jika terjadi gangguan pada sistem TI perusahaan.

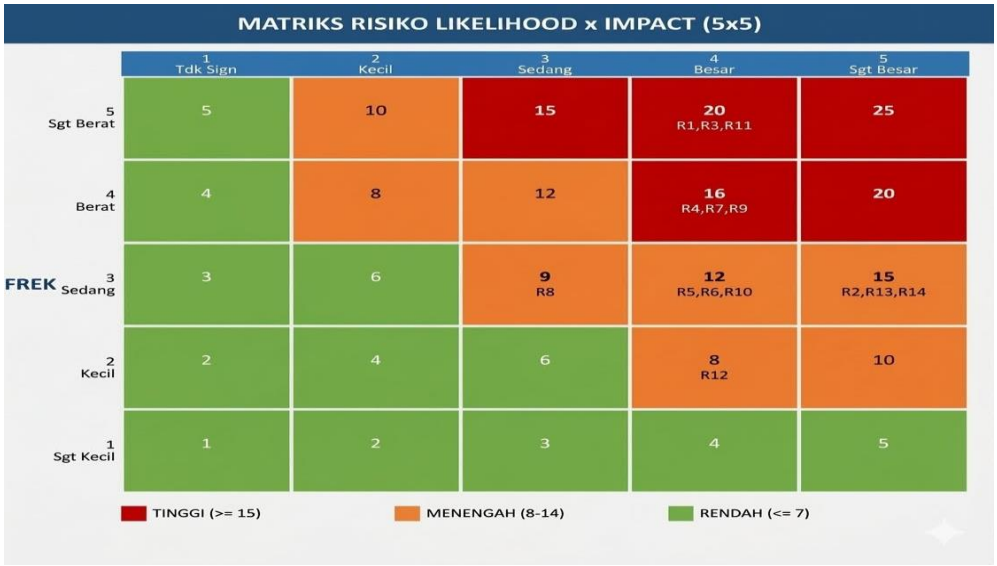
Selanjutnya, pengukuran tingkat risiko menggunakan metode semi-kuantitatif dengan mengalikan skor Frekuensi (F) dan Dampak (D). Penelitian ini mengadopsi skala ordinal 1–5 yang merujuk pada standar penilaian risiko umum industri teknologi informasi (AS/NZS 4360:2004) dan panduan praktis NIST SP 800-30 Rev 1. Alasan penggunaan skala 1–5 ini adalah untuk meminimalkan subjektivitas cx narasumber saat mengkuantifikasi temuan kualitatif, sekaligus memberikan rentang yang cukup sensitif dalam membedakan tingkat kegawatan risiko tanpa membingungkan pengambil keputusan.

Nilai hasil perkalian (skor 1–25) kemudian dikelompokkan ke dalam tiga kategori tingkatan berdasarkan sebaran area pada matriks risiko, yaitu: Rendah (skor ≤7), Menengah (skor 8–14), dan Tinggi (skor ≥15). Pembagian interval ini didasarkan pada prinsip prioritas penanganan risiko (*risk appetite*) organisasi, di mana skor \(\ge 15\) (Tinggi) memicu tindakan mitigasi segera, sedangkan skor 8–14 (Menengah) memerlukan pemantauan berkala. Sebuah matriks penilaian risiko (*risk matrix*) berukuran 5×5 digunakan sebagai instrumen visual untuk memetakan dan menentukan posisi akhir dari setiap risiko yang telah diidentifikasi. Proses analisis risiko mengikuti tahapan ISO 31000:2009 seperti ditunjukkan pada Gambar 1



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

Persetujuan Etik

Penelitian ini tidak melibatkan partisipan manusia sebagai subjek penelitian secara langsung; data diperoleh melalui wawancara profesional dengan pejabat perusahaan dalam kapasitas jabatan mereka, sehingga persetujuan etik formal tidak diperlukan.

HASIL DAN PEMBAHASAN

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).

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

Kode	Kemungkinan Risiko	Kategori
R1	*Downtime* / kegagalan akses platform DELFI	Risiko Teknologi
R2	Kehilangan atau korupsi data operasional	Risiko Teknologi
R3	Serangan siber (*malware / ransomware*)	Risiko Teknologi
R4	Gangguan koneksi internet / jaringan lokal	Risiko Teknologi
R5	Kesalahan konfigurasi (*misconfiguration*) sistem cloud	Risiko Proses
R6	Kerusakan perangkat keras (*workstation/device user*)	Risiko Teknologi
R7	*Human error* oleh administrator / operator TI	Risiko SDM
R8	Kurangnya kompetensi / pelatihan staf TI	Risiko SDM
R9	Gangguan pasokan daya listrik di kantor operasional	Risiko Teknologi
R10	Ketergantungan berlebihan pada penyedia cloud	Risiko Eksternal
R11	Kebocoran data (*data breach*) akibat celah keamanan	Risiko Teknologi
R12	Perubahan regulasi pemerintah terkait data dan cloud	Risiko Eksternal
R13	Kegagalan fungsi sistem *backup* dan *recovery*	Risiko Proses
R14	Serangan *Distributed Denial of Service* (DDoS)	Risiko Teknologi

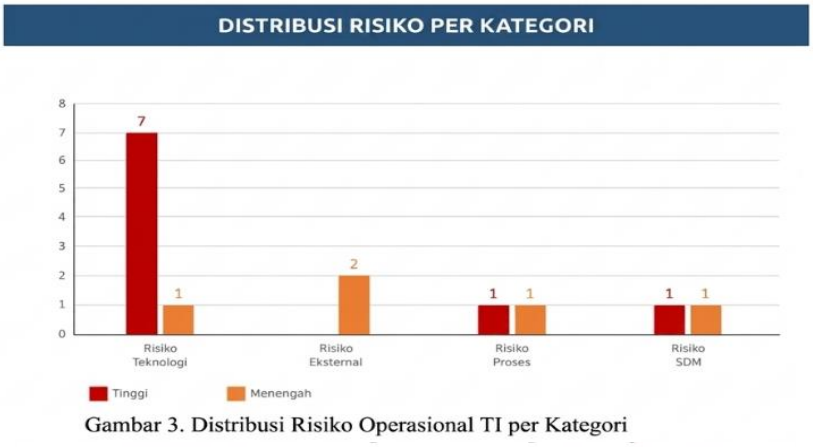
Analisis dan Evaluasi Risiko

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 akses platform DELFI	4	5	20	Tinggi	Segera
R2	Kehilangan atau korupsi data operasional	3	5	15	Tinggi	Segera
R3	Serangan siber (*malware / ransomware*)	4	5	20	Tinggi	Segera
R4	Gangguan koneksi internet / jaringan lokal	4	4	16	Tinggi	Segera
R5	Kesalahan konfigurasi (*misconfiguration*) sistem cloud	3	4	12	Menengah	Direncanakan
R6	Kerusakan perangkat keras (*workstation/device user*)	3	4	12	Menengah	Direncanakan
R7	*Human error* oleh administrator / operator TI	4	4	16	Tinggi	Segera
R8	Kurangnya kompetensi / pelatihan staf TI	3	3	9	Menengah	Direncanakan
R9	Gangguan pasokan daya listrik di kantor operasional	4	4	16	Tinggi	Segera
R10	Ketergantungan berlebihan pada penyedia cloud	3	4	12	Menengah	Direncanakan
R11	Kebocoran data (*data breach*) akibat celah keamanan	4	5	20	Tinggi	Segera
R12	Perubahan regulasi pemerintah terkait data dan cloud	2	4	8	Menengah	Direncanakan
R13	Kegagalan fungsi sistem *backup* dan *recovery*	3	5	15	Tinggi	Segera
R14	Serangan *Distributed Denial of Service* (DDoS)	3	5	15	Tinggi	Segera

Risiko Teknologi mendominasi dengan empat risiko tinggi (R1, R2, R4, R9), dengan total 57,14% risiko berada pada level tinggi dan 42,86% pada level menengah. Risiko utama (skor 20) mencakup R1, R3, dan R11, yang mendukung temuan kerentanan keamanan dan ketersediaan dari penelitian Manuputty et al [5]. Distribusi risiko per kategori ditunjukkan pada Gambar 3 dan proporsi tingkat risiko pada Gambar 4.



Gambar 3. Distribusi Risiko Operasional TI per Kategori

Gambar 4. Proporsi Tingkat Risiko Operasional TI

Berdasarkan pemetaan pada Gambar 3 dan Gambar 4, aspek operasional teknologi informasi PT. Schlumberger Geophysics Nusantara sangat didominasi oleh Risiko Teknologi. Dari total 14 risiko yang diidentifikasi, Risiko Teknologi mencakup 7 risiko tingkat Tinggi (*High*) (R1, R2, R3, R4, R9, R11, R14) dan 1 risiko tingkat Menengah (*Moderate*) (R6). Secara kumulatif, sebanyak 64,29% (9 risiko) dari keseluruhan ancaman operasional TI perusahaan berada pada level Tinggi, sedangkan 35,71% (5 risiko) sisanya berada pada level Menengah.

Risiko dengan skor tertinggi mencapai nilai kritis (F×D = 20) terfokus pada tiga poin utama, yaitu R1 (*Downtime* platform DELFI), R3 (Serangan siber berupa *malware/ransomware*), dan R11 (Kebocoran data akibat celah keamanan). Temuan dominasi level risiko ini sejalan dan memperkuat hasil penelitian terdahulu oleh Manuputty et al. [5] pada objek perusahaan yang sama, yang menegaskan bahwa ketergantungan penuh pada arsitektur jaringan *cloud* dan kerentanan keamanan siber global menempatkan ketersediaan (*availability*) serta kerahasiaan

(*confidentiality*) data operasional pada posisi yang paling rentan

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

Kode	Level	Risiko	Usulan Perlakuan Risiko
R1	Tinggi	*Downtime* sistem platform 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 atau korupsi data operasional	*Backup* otomatis harian dengan *multi-location storage*, enkripsi data *end-to-end*, dan asuransi data penting perusahaan.
R3	Tinggi	Serangan siber (*malware/ransomware*)	Implementasi *next-generation firewall*, IDS/IPS, enkripsi *end-to-end*, dan pelatihan *anti-phishing* rutin setiap 3 bulan bagi seluruh staf.
R4	Tinggi	Gangguan koneksi internet / jaringan lokal	Penggunaan layanan *Multi-ISP* dengan fitur *automatic failover*, peningkatan kapasitas *bandwidth*, dan koneksi cadangan melalui VPN/Dedicated Line.
R5	Menengah	Kesalahan konfigurasi (*misconfiguration*) cloud	Penyusunan standar konfigurasi cloud (*hardening guide*) serta menerapkan mekanisme *double approval* oleh tim senior sebelum perubahan konfigurasi diterapkan.
R6	Menengah	Kerusakan perangkat keras (*workstation user*)	Melakukan *preventive maintenance* bulanan pada aset komputer kerja staff lapangan/operasi, serta penyediaan unit cadangan (*spare part/device*) siap pakai di kantor lokal.
R7	Tinggi	*Human error* oleh administrator / operator TI	Standardisasi SOP operasional yang detail, pelatihan tim teknis secara berkala, pengawasan berlapis (*double-check approval*) untuk aktivitas kritis, dan audit log terpusat.
R8	Menengah	Kurangnya kompetensi / pelatihan staf TI	Program sertifikasi profesi tahunan (seperti CompTIA, CISSP, AWS) dan kegiatan *knowledge sharing* internal setiap bulan.
R9	Tinggi	Gangguan pasokan daya listrik di kantor	Peningkatan kapasitas UPS kantor operasional, penyediaan generator cadangan dengan ATS (*Automatic Transfer Switch*), dan pemeliharaan perangkat listrik setiap 3 bulan.
R10	Menengah	Ketergantungan berlebihan pada penyedia cloud	Negosiasi SLA ketat (garansi *uptime* minimal 99,99%), perencanaan arsitektur berbasis *multi-cloud strategy* di masa depan, dan menyusun *contingency plan*.
R11	Tinggi	Kebocoran data (*data breach*) celah keamanan	Penerapan *Role-Based Access Control* (RBAC), implementasi *Data Loss Prevention* (DLP), audit log akses berkala, enkripsi *database*, dan kepatuhan penuh pada PP No. 71/2019.
R12	Menengah	Perubahan regulasi pemerintah terkait data	Melakukan monitoring regulasi tata kelola data siber per kuartal dan melakukan penyesuaian kebijakan privasi internal secara responsif.
R13	Tinggi	Kegagalan fungsi sistem *backup* dan *recovery*	Melakukan simulasi pengujian restorasi data dari sistem *backup* setiap 3 bulan, dokumentasi hasil uji, dan penyimpanan salinan *backup offsite* terenkripsi.
R14	Tinggi	Serangan *Distributed Denial of Service* (DDoS)	Mengaktifkan proteksi DDoS berbasis cloud (seperti Cloudflare atau AWS Shield), mitigasi jalur trafik data, dan menyusun prosedur penanganan insiden DDoS.

KETERBATASAN PENELITIAN

Penelitian ini memiliki keterbatasan mendasar pada penggunaan kerangka kerja ISO 31000:2009 yang strukturnya cenderung kaku dan lebih berfokus pada proses formal birokrasi manajemen risiko secara linier. Model ini kurang adaptif

dalam menangkap dinamika perubahan infrastruktur teknologi digital berbasis *cloud* (seperti platform DELFI) yang berkembang sangat pesat. Selain itu, pengambilan data kualitatif yang bertumpu pada dua narasumber utama berpotensi menimbulkan bias subjektivitas sektoral. Untuk penelitian selanjutnya, disarankan untuk memigrasikan basis analisis risiko menggunakan standar ISO 31000:2018 yang lebih dinamis, serta memperluas cakupan narasumber dari sisi teknisi infrastruktur lokal korporasi.

KESIMPULAN

Berdasarkan analisis manajemen risiko operasional teknologi informasi pada PT. Schlumberger Geophysics Nusantara menggunakan kerangka kerja ISO 31000:2009, diperoleh kesimpulan sebagai berikut. Teridentifikasi 14 risiko operasional TI yang terbagi ke dalam 4 kategori utama, di mana Risiko Teknologi mendominasi mutlak dengan 7 risiko tingkat Tinggi dan 1 risiko tingkat Menengah. Secara keseluruhan, komposisi tingkat risiko menunjukkan bahwa 9 risiko (64,29%) berada pada tingkat Tinggi dengan skor F×D ≥ 15, dan 5 risiko (35,71%) berada pada tingkat Menengah dengan skor 8–14. Risiko dengan skor tertinggi mencapai nilai kritis (F×D = 20) terfokus pada *downtime* sistem platform DELFI (R1), serangan siber (R3), dan kebocoran data (R11) yang menjadi prioritas utama penanganan segera. Usulan perlakuan risiko dirumuskan secara terstruktur di mana seluruh risiko tingkat Tinggi wajib mendapatkan penanganan segera (*immediate action*), sedangkan risiko tingkat Menengah diatasi melalui rencana aksi berkala (*planned action*). Penggunaan kerangka kerja ISO 31000:2009 terbukti efektif memberikan gambaran terstruktur mengenai mitigasi operasional TI korporasi, meskipun disarankan untuk bermigrasi ke standar ISO 31000:2018 pada penelitian mendatang demi pendekatan tata kelola yang lebih dinamis.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada PT. Schlumberger Geophysics Nusantara, khususnya kepada 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.

DAFTAR PUSTAKA

Atmojo, S. A., & Manuputty, A. D. (2020). Analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada aplikasi AHO Office. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(3), 546–558.

Grey, I., Manson, S., & Crawford, L. (2015). The Audit Process: Principles, Practice and Cases (6th ed.). Cengage Learning.

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

International Organization for Standardization. (2009). ISO 31000:2009 Risk Management — Principles and Guidelines. ISO.

Iswajuni, Manasikana, A., & Soetedjo, S. (2018). The effect of enterprise risk management on firm value in manufacturing companies listed on Indonesian Stock Exchange. Asian Journal of Accounting Research, 3(2), 224–236.

Jericho, & Haryani, E. (2024). Penerapan ISO 31000:2018 dalam manajemen risiko teknologi informasi pada sistem penerbitan PT. X. Jurnal Informasi, Sains dan Teknologi (ISAINTEK), 7(2). https://isaintek.polinef.ac.id/index.php/isaintek/article/view/269

Kristiyanto, N. A., Safitri, N. H., & Slamet, N. I. (2024). Pengembangan sistem informasi berbasis web pada Klinik Apollo Spesialis Jakarta. Jicom: Journal Information & Computer, 2(1), 82–91.

Kuncoro, S. D., Ghaisan, R. A., Zaky, M. U., & Wulansari, A. (2023). Manajemen risiko pada teknologi informasi: Studi kasus pada perusahaan jasa. Prosiding Seminar Nasional Informatika, 1, 313–323.

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

Moeller, R. R. (2016). Brink's Modern Internal Auditing: A Common Body of Knowledge (8th ed.). Wiley.

Mulyati, S. D., Kuncoro, R. A., & Wulansari, A. (2025). Optimalisasi manajemen risiko teknologi informasi menggunakan framework ISO 31000 di era digital. JISAMAR, 9(1).

Nurhidayatuloh, Subariah, R., & Apandi, S. (2025). Analisis kualitas website sistem informasi Universitas Pamulang menggunakan karakteristik standar ISO/IEC 25010. Jicom: Journal Information & Computer, 3, 147–158.

Prasetyo, B., Salsabila, A., & Retnani, W. E. Y. (2024). IT risk management analysis based on ISO 31000 and Bow Tie Analysis in higher education institution. Indonesian Journal of Information Systems, 7(1), 84–96. https://doi.org/10.24002/ijis.v7i1.9673

Safaat H, N. (2015). Manajemen risiko teknologi informasi menggunakan framework ISO 31000 studi kasus sistem infrastruktur TI Telkom Indonesia. SITEKIN: Jurnal Sains, Teknologi dan Industri, 12(2).

Siregar, A. M., et al. (2025). Standarisasi manajemen risiko ISO 31000: Tantangan dan strategi implementasi pada PT. Telkom Indonesia. JERKIN: Jurnal Ekonomi, Riset, Kajian dan Inovasi.

Sirait, N. M., & Susanty, A. (2016). Analisis risiko operasional berdasarkan pendekatan Enterprise Risk Management (ERM) pada CV Mitra Dunia Palletindo. Industrial Engineering Online Journal, 5(4).

Hani, H. A. M., Indah, D. R. I., & Putri, P. E. S. (2023). Analisis manajemen risiko pada teknologi informasi PT. Pos Indonesia menggunakan ISO 31000. Indonesian Journal of Computer Science, 12(6), 3957–3974.