JuSiTiK
Jurnal Sistem dan Teknologi Informasi Komunikasi
P-ISSN 2579-4116 | E-ISSN 2579-5570 Vol. 9 No. 2 – Juli 2026

Analisis Manajemen Risiko TI Menggunakan ISO31000 Pada PT ABC

Ayu Elisya Natama Sianturi[1], Wianti Maharani[2], Sri Andayani[3*]
[1-3]Sistem Informasi, Universitas Katolik Musi Charitas
[1-3]Jalan Bangau No. 60, Palembang, Sumatera Selatan
Email: ayuelisyans@gmail.com[1], maharaniwianti@gmail.com[2], andayani_s@ukmc.ac.id[3]

Abstract

PT ABC is a pawn-based financial service company that heavily relies on information technology (IT) to support its operational activities across head and branch offices. This study aims to analyze IT risk management within the company using the ISO 31000 framework. A qualitative case study approach was employed, utilizing data collection methods such as interviews, field observations, and internal document reviews. The risk management process followed the standard stages: establishing scope and criteria, risk assessment, risk treatment, recording, and continuous monitoring. The research identified 21 IT risks associated with hardware, software, network infrastructure, security, and operational procedures. Based on the risk evaluation matrix, 4 risks were classified as High, including server downtime, slow system performance, 502 gateway errors, and server overload, while the remaining 17 risks fell into the Medium category. Recommended risk treatments involve increasing server capacity, implementing rigorous system performance monitoring, strengthening network security, and refining Standard Operating Procedures (SOPs). Furthermore, managing access rights and conducting regular risk reviews are essential to ensure business continuity. These findings provide a strategic roadmap for PT ABC to mitigate technical disruptions and enhance its overall IT resilience.

Key Words*: *Information Technology, ISO31000, Qualitative Study, Risk Management, Risk Treatment

Abstrak

PT ABC merupakan perusahaan jasa keuangan berbasis gadai yang sangat bergantung pada teknologi informasi (TI) untuk mendukung aktivitas operasional di kantor pusat maupun cabang. Penelitian ini bertujuan untuk menganalisis manajemen risiko TI pada PT ABC dengan mengacu pada kerangka kerja ISO 31000. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus melalui teknik wawancara, observasi, dan telaah dokumen internal. Proses manajemen risiko dijalankan secara sistematis, meliputi tahapan penetapan lingkup, penilaian risiko, hingga pemantauan dan pelaporan. Hasil penelitian berhasil mengidentifikasi 21 risiko TI yang mencakup aspek perangkat keras, perangkat lunak, jaringan, keamanan, dan prosedur operasional. Berdasarkan matriks evaluasi risiko, ditemukan 4 risiko dalam kategori *High*, yaitu *server down*, sistem lambat, *502 gateway*, dan *server overload*, sementara 17 risiko lainnya masuk dalam kategori *Medium*. Sebagai langkah mitigasi, penelitian ini merekomendasikan beberapa perlakuan risiko, antara lain peningkatan kapasitas server, pemantauan performa sistem secara intensif, penguatan keamanan jaringan, penyempurnaan standar operasional prosedur (SOP), serta pengelolaan hak akses. Implementasi rekomendasi ini diharapkan dapat meminimalisir dampak gangguan TI terhadap keberlangsungan bisnis perusahaan secara keseluruhan.

Kata Kunci: ISO31000, Manajemen Risiko, Penelitian Kualitatif, Perlakuan Risiko, Teknologi Informasi

Pendahuluan

Transformasi digital telah mengubah cara organisasi menjalankan operasionalnya, di mana teknologi informasi (TI) kini menjadi faktor utama dalam mempercepat proses bisnis sekaligus meningkatkan efisiensi kerja [1]. Pemanfaatan TI yang tepat memungkinkan perusahaan merespons perubahan pasar dengan lebih cepat dan memberikan nilai tambah yang lebih kompetitif bagi para pemangku kepentingan [2]. Kondisi serupa juga terjadi pada PT ABC sebagai perusahaan jasa keuangan berbasis gadai yang sangat bergantung pada sistem informasi dalam menjalankan layanan operasionalnya. Namun demikian, ketergantungan yang tinggi terhadap teknologi juga menimbulkan risiko baru yang semakin kompleks. Penggunaan TI tidak terlepas dari potensi gangguan, baik berupa kegagalan teknis maupun ancaman keamanan siber yang dapat terjadi sewaktu-waktu [3] sehingga kemampuan organisasi dalam mengidentifikasi dan mengelola risiko menjadi hal yang krusial untuk menjaga stabilitas dan keberlanjutan kinerja perusahaan di era digital [1]. Pentingnya pengelolaan risiko kemudian mendorong berbagai penelitian untuk mengkaji kerangka kerja yang tepat, salah satunya

*) Corresponding Author: Sri Andayani

adalah ISO31000 yang merupakan standar internasional yang menyediakan prinsip, kerangka kerja, dan proses dalam pengelolaan risiko, serta dapat diterapkan oleh organisasi mana pun tanpa terbatas pada ukuran, jenis kegiatan, maupun sektornya [4].

Berbagai penelitian sebelumnya telah mengkaji penerapan kerangka kerja ISO31000 pada beragam sektor. Studi pada PT Trust Lerinvital Timur menunjukkan bahwa penerapan ISO31000 dapat mengurangi risiko pada sistem ERP yang sering mengalami gangguan jaringan [3]. Di sektor perbankan, kerangka kerja ini membantu Bank ABC dalam memetakan tingkat risiko pada layanan *mobile banking* guna mencegah potensi kebocoran data [5]. Selain itu, pada lingkungan pendidikan seperti Universitas ABC, ISO31000 terbukti efektif dalam mengidentifikasi koneksi internet sebagai salah satu risiko kritis dalam sistem informasi akademik [6] [7]. Penelitian lain juga mengombinasikan ISO31000 dengan metode *Failure Mode and Effects Analysis* (FMEA) untuk meningkatkan keamanan aset TI dengan hasil identifikasi risiko yang bervariasi dari tingkat sangat rendah hingga sangat tinggi [8]. Temuan-temuan ini menunjukkan bahwa ISO31000 bersifat fleksibel dan dapat diterapkan pada berbagai jenis organisasi.

Implementasi manajemen risiko berbasis ISO31000 juga memberikan dampak positif di sektor industri dan logistik. Penelitian pada PT Eterindo Nusa Graha menunjukkan bahwa sebagian besar risiko yang teridentifikasi masih dapat dikendalikan melalui strategi mitigasi yang tepat [2]. Sementara itu, pada PT Pos Indonesia, penerapan standar ini menghasilkan identifikasi puluhan risiko yang mayoritas berada pada tingkat menengah dan dapat dijadikan dasar dalam upaya pencegahan ke depan [9]. Di sektor manufaktur, penerapan ISO31000 bahkan dikembangkan dengan visualisasi data berbasis *dashboard* untuk meningkatkan pemahaman manajemen terhadap risiko [10]. Selain itu, pada perusahaan penerbitan, standar ini terbukti mampu meningkatkan kesadaran risiko serta melindungi aset TI dari ancaman seperti peretasan dan kerusakan server [11]. Beberapa studi terbaru juga menunjukkan bahwa ISO31000:2018 dapat digunakan untuk menganalisis risiko pada beragam objek bisnis dan sistem informasi. Penelitian pada CV Tunas Mandiri menggunakan ISO31000:2018 untuk mengevaluasi risiko operasional, bencana, dan pemasaran, sedangkan penelitian pada Bengkel Mobil XYZ mengidentifikasi risiko aset digital seperti *server down*, pencurian data, dan penyalahgunaan hak akses [12][13]. Penerapan ISO31000:2018 pada sistem informasi akuntansi PT Batu Bara XYZ juga menunjukkan bahwa pengelompokan risiko berdasarkan *likelihood* dan *impact* dapat membantu perusahaan menyusun strategi pengelolaan risiko yang lebih tepat [14]. Selain itu, studi pada XYZ *Boutique* menemukan risiko IS/IT dengan tingkat *high*, *medium*, dan *low* yang kemudian diberikan solusi penanganan sesuai tingkat risikonya [15]. Meskipun demikian, keberhasilan tersebut belum tentu dapat langsung diterapkan tanpa penyesuaian pada setiap organisasi, termasuk pada PT ABC yang memiliki karakteristik risiko operasional yang berbeda.

Pada praktiknya, implementasi manajemen risiko masih menghadapi berbagai kendala. Studi pada salah satu anak perusahaan BUMN di DKI Jakarta menunjukkan bahwa meskipun kesadaran terhadap risiko sudah ada, proses dokumentasi dan mitigasi masih belum optimal dan belum sepenuhnya sesuai dengan standar ISO31000 [16]. Selain itu, aspek tata kelola serta komitmen manajemen puncak sering menjadi tantangan dalam mengintegrasikan manajemen risiko ke dalam aktivitas operasional [17]. Hal ini sejalan dengan penelitian di sektor asuransi yang menegaskan bahwa keberhasilan manajemen risiko sangat bergantung pada sejauh mana prinsip-prinsipnya diterapkan dalam struktur organisasi dan proses pengambilan keputusan [17]. Integrasi ISO31000 dengan kerangka kerja lain seperti COBIT 5 juga dinilai mampu memberikan pendekatan yang lebih menyeluruh dalam menjaga keberlangsungan bisnis dan meningkatkan kepercayaan pemangku kepentingan [18]. Berbagai kendala tersebut menunjukkan adanya kesenjangan antara konsep dan implementasi di lapangan. Kondisi tersebut juga relevan dengan situasi yang dihadapi oleh PT ABC, di mana pengelolaan risiko TI belum dilakukan secara terstruktur dan terdokumentasi dengan baik.

Berdasarkan hasil observasi dan wawancara pada PT ABC, ditemukan beberapa permasalahan seperti ketidakstabilan server, gangguan pada *gateway*, serta penurunan performa sistem yang berdampak pada aktivitas operasional ribuan pengguna di kantor pusat maupun cabang [1]. Oleh karena itu, penelitian ini bertujuan untuk merancang manajemen risiko TI yang sistematis pada PT ABC. Berbeda dengan penelitian sebelumnya yang banyak berfokus pada sektor manufaktur atau pendidikan, penelitian ini

menitikberatkan pada pengelolaan risiko TI pada perusahaan jasa keuangan berbasis gadai dengan karakteristik operasional yang kompleks [19][20][21]. Penelitian ini bersifat terbarukan karena memetakan profil risiko TI pada usaha pegadaian dengan banyak cabang, sehingga mengungkap pola risiko yang berbeda dari sektor-sektor yang telah diteliti sebelumnya. Dengan demikian, penelitian ini memiliki tujuan agar dapat menghasilkan rekomendasi penanganan risiko yang lebih tepat guna untuk mendukung keberlangsungan sistem informasi perusahaan di masa mendatang [3][11].

Metode Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus di PT ABC. Data dikumpulkan melalui wawancara langsung, pengamatan pada sistem web perusahaan, serta pemeriksaan dokumen aturan internal yang berkaitan dengan aset TI. Validasi data dilakukan melalui triangulasi sumber, yaitu dengan membandingkan hasil wawancara, observasi langsung pada sistem, dan telaah dokumen internal (SOP dan laporan gangguan). Hasil identifikasi serta penilaian risiko kemudian dikonfirmasi kembali kepada pihak IT PT ABC untuk memastikan kesesuaian dengan kondisi operasional aktual.

Langkah-langkah dalam melaksanakan kerangka kerja ISO31000 adalah sebagai berikut:

1. Komunikasi dan Konsultasi: Melakukan diskusi dengan pihak manajemen TI untuk memastikan tujuan penelitian sesuai dengan masalah yang dihadapi perusahaan [8].
2. Penetapan Lingkup dan Kriteria: Menentukan batasan penelitian pada sistem internal PT ABC dan menetapkan standar penilaian risiko berdasarkan kemungkinan terjadi dan dampak kerugiannya [8].
3. Penilaian Risiko (*Risk Assessment*):
    a. Identifikasi Risiko: Mencari dan mencatat semua potensi masalah pada aset TI, baik karena faktor alam, kesalahan orang, maupun kerusakan sistem [3][6] [7].
    b. Analisis Risiko: Menghitung tingkat bahaya risiko dengan melihat seberapa sering risiko itu muncul dan seberapa besar dampaknya bagi bisnis perusahaan [3][11].
    c. Evaluasi Risiko: Membandingkan hasil analisis dengan standar perusahaan untuk menentukan mana risiko yang harus didahulukan penanganannya, mulai dari level rendah, sedang, hingga tinggi [3][21].
4. Perlakuan Risiko (*Risk Treatment*): Membuat usulan tindakan untuk mengatasi risiko, seperti mengurangi dampak risiko, membagi risiko ke pihak lain, atau menerima risiko tersebut jika masih dalam batas aman [3][19].
5. Pencatatan dan Pelaporan: Mendokumentasikan semua hasil penilaian risiko agar bisa dipelajari oleh internal perusahaan [8][16].
6. Pemantauan dan Peninjauan: Melakukan evaluasi rutin untuk memastikan bahwa cara-cara penanganan risiko yang diusulkan tetap efektif dan bisa terus dikembangkan [18][10].

Hasil dan Pembahasan

A. Komunikasi dan Konsultasi

Tahap komunikasi dan konsultasi dilakukan melalui wawancara dengan pihak internal PT ABC untuk memahami penggunaan teknologi informasi dan permasalahannya. Hasil wawancara menunjukkan PT ABC menggunakan sistem internal terintegrasi lintas unit dengan pengaturan akses berdasarkan peran, unit, dan jabatan, serta sistem khusus unit gadai untuk pemantauan operasional. Karena sistem ini penting bagi kantor pusat dan cabang, gangguan seperti *server down*, *502 gateway*, sistem lambat, dan kendala pembaruan dapat menghambat proses bisnis. Pelaporan gangguan saat ini melalui IT unit bisnis yang diteruskan ke IT lintas unit, namun dokumentasi risiko masih perlu disusun lebih sistematis sesuai tahapan ISO31000.

B. Penetapan Lingkup, Konteks, dan Kriteria

Lingkup penelitian difokuskan pada aset teknologi informasi yang mendukung operasional PT ABC, khususnya aset yang berkaitan dengan sistem internal, perangkat keras, perangkat lunak, serta jaringan dan keamanan.

Kriteria risiko ditetapkan berdasarkan dua parameter utama, yaitu kemungkinan terjadinya risiko (*Likelihood*) dan dampak risiko (*Impact*) terhadap operasional perusahaan. Kemungkinan digunakan untuk menilai frekuensi suatu risiko muncul, sedangkan dampak digunakan untuk menilai tingkat gangguan terhadap proses bisnis, keamanan data, kualitas layanan, dan efektivitas kerja pengguna.

Tabel 1 Kriteria *Likelihood*

Nilai	Kriteria	Deskripsi
1	*Rare*	Risiko sangat jarang terjadi atau belum pernah terjadi, namun tetap memiliki kemungkinan muncul.
2	*Unlikely*	Risiko jarang terjadi dan tidak menjadi gangguan rutin.
3	*Possible*	Risiko dapat terjadi dalam periode tertentu dan perlu dipantau.
4	*Likely*	Risiko cukup sering terjadi dan berpotensi mengganggu proses kerja.
5	*Almost Certain*	Risiko sering terjadi, misalnya dalam frekuensi mingguan atau berulang pada jam operasional.

Tabel 2 Kriteria *Impact*

Nilai	Kriteria	Deskripsi
1	*Insignificant*	Risiko tidak berdampak signifikan terhadap proses bisnis.
2	*Minor*	Risiko menimbulkan hambatan kecil, tetapi proses bisnis tetap berjalan.
3	*Moderate*	Risiko mengganggu sebagian proses bisnis atau menurunkan efektivitas kerja.
4	*Major*	Risiko menghambat sebagian besar aktivitas operasional dan membutuhkan penanganan segera.
5	*Catastrophic*	Risiko menyebabkan penghentian layanan utama, kerugian besar, atau ancaman serius terhadap keamanan data.

C. Penilaian Risiko (*Risk Assessment*)

a. Identifikasi Aset

Identifikasi aset dilakukan untuk menentukan komponen SI/TI yang berpotensi terdampak risiko. Aset yang diidentifikasi dikelompokkan menjadi perangkat keras, perangkat lunak, serta jaringan dan keamanan.

Tabel 3 Identifikasi Aset SI/TI PT ABC

Komponen SI/TI	Aset
Hardware	Komputer, CPU, *mouse*, *keyboard*, laptop, *printer*, Wi-Fi, server
Software	Website Internal Group Perusahaan, Sistem Internal Gadai, Microsoft Word, Microsoft Excel, Google Spreadsheet, Google Docs, Draw.io, Figma
Jaringan dan Keamanan	VPN, Mikrotik

b. Identifikasi Kemungkinan Risiko

Berdasarkan hasil wawancara, observasi, dan pengelompokan aset, risiko TI pada PT ABC dapat diklasifikasikan ke dalam tiga faktor utama, yaitu faktor manusia, faktor sistem dan infrastruktur, serta faktor lingkungan.

Tabel 4 Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Sistem dan Infrastruktur	R01	*Server down*
	R02	502 *gateway* pada sistem internal
	R03	Sistem lambat atau *lag* saat diakses banyak pengguna
	R04	*Overload* karena kapasitas server belum memadai
	R05	Kegagalan *update* sistem
	R06	Gangguan integrasi API pada sistem internal gadai
	R07	Koneksi jaringan tidak stabil atau terputus
	R08	Gangguan VPN
	R09	Gangguan konfigurasi atau kinerja mikrotik

	R10	Kerusakan perangkat *hardware* pengguna
	R11	Kegagalan *backup* data
	R12	Serangan *malware* atau virus
Manusia dan Prosedur	R13	*Human error* dalam penggunaan sistem
	R14	Penyalahgunaan hak akses
	R15	Keterlambatan eskalasi dan persetujuan perbaikan infrastruktur
	R16	SOP belum dipahami atau belum terdokumentasi secara optimal
	R17	Tampilan sistem kurang mendukung operasional dan analisis data
Keamanan Informasi	R18	Potensi kebocoran data
Lingkungan	R19	Listrik padam
	R20	*Overheat* pada perangkat atau ruang server
	R21	Bencana fisik, seperti banjir, petir, atau kebakaran

Risiko yang paling dominan berdasarkan hasil wawancara adalah gangguan server dan penurunan performa sistem ketika diakses oleh banyak pengguna. Risiko ini menjadi penting karena sistem digunakan oleh banyak pihak dalam rentang waktu operasional yang panjang.

c. Identifikasi Dampak Risiko

Tabel 5 Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
R01	*Server down*	Pengguna tidak dapat mengakses sistem sehingga proses operasional terhambat.
R02	502 *gateway*	Sistem tidak dapat dibuka atau layanan gagal merespons permintaan pengguna.
R03	Sistem lambat atau *lag*	Aktivitas *input*, *monitoring*, dan analisis data menjadi tidak efisien.
R04	*Overload* server	Kinerja sistem menurun dan berpotensi menyebabkan *crash*.
R05	Kegagalan *update* sistem	Fitur tidak berjalan optimal dan dapat menimbulkan gangguan lanjutan.
R06	Gangguan integrasi API	*Monitoring* interaksi operasional tidak berjalan maksimal.
R07	Koneksi jaringan tidak stabil atau terputus	Akses terhadap sistem internal terganggu.
R08	Gangguan VPN	Pengguna tertentu tidak dapat mengakses sistem dari jaringan yang membutuhkan koneksi aman.
R09	Gangguan Mikrotik	Distribusi jaringan dan pengaturan konektivitas terganggu.
R10	Kerusakan *hardware*	Pengguna tidak dapat bekerja secara optimal menggunakan perangkat kerja.
R11	Kegagalan *backup* data	Risiko kehilangan data meningkat apabila terjadi gangguan sistem.
R12	Serangan *malware* atau virus	Data dan perangkat dapat terganggu, rusak, atau tidak dapat digunakan.
R13	*Human error*	Kesalahan input atau penggunaan fitur dapat memengaruhi akurasi data.
R14	Penyalahgunaan hak akses	Data dapat diakses atau diubah oleh pihak yang tidak berwenang.
R15	Keterlambatan eskalasi dan persetujuan perbaikan	Penyelesaian masalah infrastruktur menjadi lebih lama.
R16	SOP belum optimal	Penanganan risiko tidak seragam dan sulit dievaluasi.
R17	Tampilan sistem kurang mendukung	Pengguna cabang dan *head office* dapat memiliki interpretasi berbeda terhadap data.
R18	Potensi kebocoran data	Kerahasiaan data perusahaan dan pengguna dapat terganggu.

R19	Listrik padam	Perangkat dan koneksi sistem dapat berhenti sementara.
R20	*Overheat*	Kinerja perangkat menurun dan berpotensi terjadi kerusakan.
R21	Bencana fisik	Infrastruktur TI dapat mengalami kerusakan dan menghambat proses bisnis.

d. Analisis Risiko

Analisis risiko dilakukan dengan memberikan nilai *likelihood* dan *impact* pada setiap risiko. Penilaian *likelihood* dan *impact* diperoleh dari staf IT unit gadai yang dipilih secara *purposive* karena terlibat langsung dalam penanganan gangguan sistem. Skor 1–5 ditentukan melalui wawancara semi-terstruktur dengan merujuk pada frekuensi gangguan aktual pada *log*/laporan insiden perusahaan serta penilaian dampak terhadap proses bisnis PT ABC.

Tabel 6 Penilaian *Likelihood* dan *Impact*

ID	Kemungkinan Risiko	*Likelihood*	*Impact*
R01	*Server down*	5	5
R02	502 *gateway*	4	4
R03	Sistem lambat atau lag	5	4
R04	*Overload* server	4	4
R05	Kegagalan *update* sistem	3	4
R06	Gangguan integrasi API	3	4
R07	Koneksi jaringan tidak stabil atau terputus	3	4
R08	Gangguan VPN	2	4
R09	Gangguan Mikrotik	2	4
R10	Kerusakan *hardware*	3	2
R11	Kegagalan *backup* data	1	5
R12	Serangan *malware* atau virus	2	3
R13	*Human error*	3	3
R14	Penyalahgunaan hak akses	2	4
R15	Keterlambatan eskalasi dan persetujuan perbaikan	3	4
R16	SOP belum optimal	3	3
R17	Tampilan sistem kurang mendukung	4	3
R18	Potensi kebocoran data	1	5
R19	Listrik padam	2	4
R20	*Overheat*	2	3
R21	Bencana fisik	1	4

Berdasarkan Tabel 6, risiko dengan nilai *likelihood* dan *impact* tertinggi terdapat pada R01, yaitu *server down*, dengan nilai 5 pada kedua aspek. Hal ini menunjukkan bahwa gangguan server menjadi risiko utama karena memiliki kemungkinan terjadi yang tinggi dan berdampak besar terhadap proses operasional. Selain itu, risiko R02, R03, dan R04 juga memiliki nilai tinggi karena berkaitan langsung dengan ketersediaan dan performa sistem internal. Nilai *likelihood* dan *impact* pada tabel ini selanjutnya digunakan sebagai dasar dalam penyusunan matriks evaluasi risiko.

e. Evaluasi Risiko

Tahap evaluasi risiko dilakukan untuk menentukan tingkat prioritas penanganan terhadap risiko-risiko yang telah dianalisis pada tahap sebelumnya. Pada tahap ini, setiap risiko dipetakan ke dalam matriks evaluasi risiko berdasarkan kombinasi nilai *likelihood* dan *impact*. Hasil pemetaan tersebut kemudian digunakan untuk mengelompokkan risiko ke dalam tiga level, yaitu *Low*, *Medium*, dan *High*. Dengan demikian, perusahaan dapat mengetahui risiko mana yang harus segera diprioritaskan penanganannya dan risiko mana yang cukup dipantau secara berkala.

Tabel 7 Matriks Evaluasi Risiko

Likelihood							
	Certain	5	*Medium*	*Medium*	*High*	*High*	*High*
	Likely	4	*Medium*	*Medium*	*Medium*	*High*	*High*
	Possible	3	*Low*	*Medium*	*Medium*	*Medium*	*High*
	Unlikely	2	*Low*	*Low*	*Medium*	*Medium*	*Medium*

	Rare	1	*Low*	*Low*	*Low*	*Medium*	*Medium*
	Impact		1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Berdasarkan matriks pada Tabel 7, setiap risiko kemudian ditempatkan sesuai dengan nilai *likelihood* dan *impact* yang telah diperoleh. Pemetaan tersebut menghasilkan sebaran risiko sebagaimana ditunjukkan pada Tabel 8.

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

Likelihood	*Certain*	5				R03	R01
	Likely	4			R17	R02, R04	
	Possible	3		R10	R13, R16	R05, R06, R07, R15	
	Unlikely	2			R12, R20	R08, R09, R14, R19	
	Rare	1				R21	R11, R18
	Impact		1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Berdasarkan Tabel 8, terdapat 4 risiko kategori *High*, yaitu *server down* (R01), sistem lambat atau *lag* (R03), 502 *gateway* (R02), dan *overload server* (R04). Risiko tersebut menjadi prioritas utama karena berkaitan langsung dengan performa dan ketersediaan sistem internal perusahaan. Selain itu, terdapat 17 risiko kategori *Medium* yang tetap perlu dikelola karena dapat mengganggu proses bisnis, kualitas layanan, dan keamanan informasi. Hasil evaluasi menunjukkan bahwa risiko TI PT ABC didominasi kategori *Medium* dan *High*, sehingga hasil ini menjadi dasar dalam penyusunan strategi perlakuan risiko.

Sebaran risiko TI PT ABC yang didominasi kategori *Medium* sejalan dengan temuan pada PT Pos Indonesia [22]dan PT Eterindo Nusa Graha [23], yang juga menunjukkan mayoritas risiko berada pada tingkat menengah dan masih dapat dikendalikan melalui mitigasi yang tepat. Namun, terdapat perbedaan karakteristik yang menonjol, yaitu pada XYZ Boutique risiko tersebar merata [15] dan pada Bengkel Mobil XYZ didominasi risiko keamanan data [13], risiko kategori *High* pada PT ABC justru terkonsentrasi pada aspek ketersediaan dan performa sistem (*server down*, sistem lambat, *502 gateway*, dan *overload server*). Hal ini menegaskan bahwa karakteristik perusahaan jasa keuangan berbasis gadai dengan sistem terintegrasi lintas cabang menjadikan risiko infrastruktur sebagai prioritas utama, berbeda dari sektor yang banyak diteliti sebelumnya.

D. Perlakuan Risiko

Setelah risiko dikelompokkan berdasarkan tingkatannya, tahap berikutnya adalah perlakuan risiko atau *risk treatment* untuk mengurangi kemungkinan maupun dampak risiko. Perlakuan disusun berdasarkan hasil evaluasi pada Tabel 8, sehingga risiko kategori *High* menjadi prioritas utama. Keempat risiko *High* (*server down*, sistem lambat, *502 gateway*, dan *overload server*) memiliki implikasi bisnis langsung karena dapat menghentikan atau memperlambat transaksi gadai di seluruh cabang sehingga menimbulkan kerugian pendapatan, menambah antrean nasabah, dan menurunkan kepercayaan pelanggan. Risiko dengan kategori *Medium* tetap diberikan tindakan pengendalian agar tidak berkembang menjadi risiko yang lebih besar.

Tabel 9 Usulan Perlakuan Risiko

ID	Kemungkinan Risiko	*Risk Level*	Usulan Perlakuan Risiko
R01	*Server down*	*High*	Melakukan peningkatan kapasitas server sesuai jumlah pengguna aktif, menerapkan pemantauan performa server secara berkala, serta menyiapkan server cadangan atau mekanisme *failover* untuk layanan yang bersifat kritis.
R03	Sistem lambat atau *lag*	*High*	Melakukan optimasi performa sistem, evaluasi penggunaan *database*, penerapan *load balancing*, serta pengujian beban sistem untuk mengetahui kapasitas maksimal ketika banyak pengguna mengakses sistem secara bersamaan.
R02	502 *gateway*	*High*	Melakukan pengecekan konfigurasi *gateway* dan web server, menyiapkan prosedur *troubleshooting*, serta memastikan

			proses pembaruan sistem tidak dilakukan tanpa pengujian pada lingkungan percobaan.
R04	*Overload* server	*High*	Melakukan *capacity planning*, penambahan sumber daya server, pengaturan jadwal *maintenance* di luar jam operasional utama, serta pemantauan trafik pengguna secara *real time*.
R17	Tampilan sistem kurang mendukung operasional	*Medium*	Melakukan evaluasi UI/UX dengan melibatkan pengguna kantor pusat dan cabang, menyusun daftar kebutuhan fitur, serta memperbaiki tampilan data agar lebih mendukung proses operasional dan analisis data.
R05	Kegagalan *update* sistem	*Medium*	Menyediakan lingkungan *testing* sebelum pembaruan diterapkan, membuat *rollback plan*, menyusun jadwal pembaruan sistem, serta mendokumentasikan perubahan sistem secara terstruktur.
R06	Gangguan integrasi API	*Medium*	Melakukan pemantauan koneksi API, pengecekan *log* integrasi, validasi data yang dikirim dan diterima, serta menyiapkan prosedur penanganan apabila API tidak merespons.
R07	Koneksi jaringan tidak stabil atau terputus	*Medium*	Mengevaluasi kualitas jaringan dan ISP, menyediakan jalur koneksi cadangan, melakukan pemantauan jaringan, serta memastikan perangkat jaringan berada dalam kondisi optimal.
R15	Keterlambatan eskalasi dan persetujuan perbaikan infrastruktur	*Medium*	Menetapkan SLA penanganan insiden, memperjelas alur eskalasi dari unit bisnis ke tim IT terkait, serta menyusun kategori prioritas agar gangguan kritis dapat segera ditangani.
R13	*Human error*	*Medium*	Memberikan pelatihan penggunaan sistem kepada pengguna, menyusun panduan operasional, menerapkan validasi input pada fitur penting, serta menyediakan mekanisme konfirmasi sebelum perubahan data dilakukan.
R16	SOP belum optimal	*Medium*	Menyusun dan memperbarui SOP penanganan gangguan TI, melakukan sosialisasi kepada pengguna dan tim terkait, serta melakukan evaluasi berkala terhadap efektivitas SOP.
R10	Kerusakan *hardware*	*Medium*	Melakukan inventarisasi perangkat, pemeliharaan berkala, penyediaan perangkat cadangan, serta penggantian perangkat yang sudah tidak layak digunakan.
R08	Gangguan VPN	*Medium*	Melakukan pengecekan konfigurasi VPN, pembaruan kredensial secara berkala, pembatasan akses hanya kepada pengguna yang berwenang, serta pemantauan aktivitas *login*.
R09	Gangguan Mikrotik	*Medium*	Melakukan backup konfigurasi Mikrotik, audit konfigurasi jaringan, pembatasan akses administrator, serta pengecekan perangkat secara berkala.
R14	Penyalahgunaan hak akses	*Medium*	Menerapkan prinsip *least privilege*, melakukan evaluasi hak akses secara berkala, menonaktifkan akun yang tidak digunakan, serta mencatat aktivitas pengguna melalui *log* sistem.
R19	Listrik padam	*Medium*	Menyediakan UPS untuk perangkat penting, memastikan ketersediaan sumber listrik cadangan, serta menetapkan prosedur pemadaman aman agar perangkat dan data tidak mengalami kerusakan.

R12	Serangan *malware* atau virus	*Medium*	Mengaktifkan antivirus dan firewall, melakukan pembaruan sistem secara rutin, membatasi penggunaan perangkat eksternal, serta memberikan edukasi keamanan informasi kepada pengguna.
R20	*Overheat*	*Medium*	Menjaga suhu ruang perangkat, menyediakan pendingin yang memadai, membersihkan perangkat secara berkala, serta memantau suhu server dan perangkat jaringan.
R21	Bencana fisik	*Medium*	Menempatkan perangkat penting pada lokasi yang aman, menyediakan alat pemadam kebakaran, menyusun rencana pemulihan bencana, serta memastikan data penting memiliki salinan cadangan di lokasi berbeda.
R11	Kegagalan *backup* data	*Medium*	Menetapkan jadwal *backup* otomatis, melakukan uji pemulihan data secara berkala, menyimpan salinan backup pada media atau lokasi berbeda, serta mendokumentasikan hasil proses *backup*.
R18	Potensi kebocoran data	*Medium*	Menerapkan enkripsi data, audit akses, pembaruan kata sandi secara berkala, penggunaan autentikasi berlapis, serta pengawasan terhadap aktivitas akses data yang tidak wajar.

Setelah usulan perlakuan risiko diterapkan, diharapkan terjadi penurunan tingkat risiko (*residual risk*). Pada risiko kategori *High*, penambahan kapasitas dan *failover server*, optimasi performa, serta pemantauan trafik secara berkala diperkirakan dapat menurunkan nilai *likelihood* sehingga sebagian besar risiko *High* seperti *server down*, sistem lambat, *502 gateway*, dan *overload server* dapat turun ke kategori *Medium*. Adapun risiko kategori *Medium* diharapkan menurun ke tingkat yang lebih terkendali. Estimasi *residual risk* ini perlu diverifikasi kembali melalui pemantauan dan peninjauan berkala untuk memastikan efektivitas mitigasi yang diterapkan.

E. Pencatatan dan Pelaporan

Tahap pencatatan dan pelaporan dilakukan dengan mendokumentasikan hasil identifikasi, analisis, evaluasi, dan perlakuan risiko. PT ABC telah memiliki alur pelaporan gangguan melalui IT unit bisnis yang diteruskan kepada IT lintas unit. Namun, proses tersebut perlu diperkuat melalui *risk register* yang memuat jenis risiko, aset terdampak, dampak, tingkat risiko, tindakan penanganan, dan status penyelesaian agar dapat menjadi dasar evaluasi serta pengambilan keputusan.

F. Pemantauan dan Peninjauan

Tahap pemantauan dan peninjauan dilakukan secara berkala untuk memastikan perlakuan risiko tetap efektif. Fokus utama pemantauan adalah risiko kategori *High*, yaitu *server down*, 502 *gateway*, sistem lambat atau *lag*, dan *overload server*. Selain itu, SOP, alur eskalasi, jadwal *maintenance*, hak akses, serta risiko kategori *Medium* juga perlu ditinjau agar manajemen risiko TI dapat berjalan berkelanjutan.

Kesimpulan

Berdasarkan hasil analisis manajemen risiko TI menggunakan ISO31000 pada PT ABC, ditemukan 21 risiko yang berkaitan dengan aset *hardware*, *software*, jaringan, keamanan, serta prosedur operasional. Hasil evaluasi menunjukkan terdapat 4 risiko dengan level *High*, yaitu *server down*, sistem lambat atau *lag*, 502 *gateway*, dan *overload* server, sedangkan 17 risiko lainnya berada pada level *Medium*. Risiko tertinggi berhubungan dengan stabilitas dan kapasitas sistem internal yang digunakan oleh kantor pusat dan cabang, sehingga perlakuan risiko perlu diprioritaskan pada peningkatan kapasitas server, pemantauan performa sistem, penguatan jaringan, penyempurnaan SOP, pengelolaan hak akses, serta pencatatan dan peninjauan risiko secara berkala agar operasional perusahaan tetap berjalan stabil dan aman.

Daftar Pustaka

[1] S. K. Fadiyah and Ilham, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA PT XYZ," *Jurnal Mahasiswa Teknik Informatika (JATI)*, vol. 9, no. 1, pp. 1613–1618, 2025.

[2] U. S. Oktavia, I. G. Anugrah, and W. P. P. Witra, "ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI PT . ETERINDO NUSA GRAHA MENGGUNAKAN FRAMEWORK ISO31000:2018," *JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK)*, vol. 16, no. 1, pp. 100–119, 2025.

[3] D. Y. Andika and A. F. Wijaya, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR," *Jurnal MNEMONIC*, vol. 5, no. 2, pp. 111–118, 2022.

[4] International Organization for Standardizatio, "Risk management — Guidelines," Geneva, Switzerland, 2018.

[5] H. C. Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan Framework ISO 31000," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 1, 2022.

[6] E. Ardius, A. Isroqmi, N. Nurdiana, D. Irawan, and S. Hastini, "Manajemen risiko penggunaan sistem informasi akademik di universitas abc menggunakan iso," *Jurnal Digital Teknologi Informasi*, vol. 08, no. 02, pp. 57–63, 2025.

[7] F. S. Lubis, V. S. Praditha, M. Lubis, M. F. Safitra, and Y. Z. Ramadhan, "IT Risk Analysis Based on Risk Management Using ISO 31000: Case study Registration Application at University XYZ," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2023, pp. 522–528. doi: 10.1145/3629378.3629464.

[8] I. C. Dewi and G. S. Palupi, "Risk Management Analysis of Information Technology (IT) Asset Security Using ISO 31000 and FMEA," *Journal of Education Technology and Information System*, vol. 01, no. 02, pp. 88–97, 2025.

[9] H. A. Mattjik, D. R. Indah, and P. E. Sevtiyuni, "Analisis Manajemen Risiko Pada Teknologi Informasi PT. Pos Indonesia Menggunakan ISO 31000," *Indonesian Journal of Computer Science*, vol. 12, no. 6, pp. 3957–3974, 2023.

[10] M. F. Fahlevi, A. H. Nasution, R. Riski, and A. F. Chrisnadeva, "Production Division Risk Management Analysis Using ISO 31000 : 2018 at PT Bangkit Laksana Jaya Ban," *Jurnal Ilmiah Sistem Informasi (JUSI)*, vol. 5, no. 1, pp. 372–387, 2026.

[11] M. Aprikasari, L. Benedicta, N. A. Adrielvino, and A. T. Ayunda, "Penerapan ISO 31000 : 2018 untuk Manajemen Risiko IT pada Sistem Penerbitan PT . X," *Jurnal Informasi, Sains dan Teknologi*, vol. 7, no. 2, pp. 154–167, 2024.

[12] S. Adtiya, Y. A. Apriyanto, and S. Andayani, "Analisis Manajemen Risiko Pada CV. Tunas Mandiri," *Jurnal Sains Sistem Informasi*, vol. 2, no. 2, p. 54, May 2024, doi: 10.31602/jssi.v2i2.14620.

[13] E. Effendy and S. Andayani, "Identifikasi dan Pengelolaan Risiko Aset Digital di Bengkel Mobil XYZ Menggunakan Framework ISO 31000:2018," *Jurnal Sistem & Teknologi Informasi Komunikasi*, vol. 8, no. 2, pp. 83–1, Jul. 2025.

[14] A. Azzahra, P. Aditya, and S. Andayani, "ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI AKUNTANSI PADA PT. BATU BARA XYZ ISO 31000:2018," *Jurnal Sistem Informasi (JuSIN)*, vol. 5, no. 1, pp. 41–50, 2024.

[15] Crecia, M. J. Aguswan, and S. Andayani, "ANALISIS RISIKO INFORMATION SYSTEM (IS)/INFORMATION TECHNOLOGY (IT) DENGAN FRAMEWORK ISO 31000:2018 PADA XYZ BOUTIQUE," *Jurnal Informatika Progres*, vol. 16, no. 1, Apr. 2024.

[16] D. Al Kautsar and C. D. Djakman, "Evaluation of Iso 31000 Risk Implementation in in DKI Jakarta Provincial Government-Owned Enterprises (BUMN) Subsidiaries (Case Study on PT B , A Subsidiary of PTX)," *Jurnal LOCUS: Penelitian dan Pengabdian*, vol. 4, no. 10, pp. 10085–10097, 2025.

[17] A. P. Singgih and F. A. Alijoyo, "A Study on the Implementation of ISO 31000 in the Insurance Industry Through the Application of Integrated Risk Management Principles," *American Journal of Economic and Management Business*, vol. 4, no. 12, pp. 2140–2151, 2025.

[18] F. F. Ahkmad and Ilham, "Manajemen Risiko dalam Optimalisasi Keberhasilan Proyek Teknologi Informasi Menggunakan Framework ISO 31000," *Jurnal Telematika*, vol. 19, no. 2, pp. 60–64, 2025.

[19] C. H. Pamungkas and A. H. Prasetyo, "Rancangan Manajemen Risiko pada Perusahaan Startup PT . Haruka Evolusi Digital Utama," *Journal of Emerging Business Management and Entrepreneurship Studies*, vol. 2, no. 1, pp. 50–66, 2022.

[20] S. G. Asmarawati and A. M. Dewi, "Asesmen Manajemen Risiko Berdasarkan ISO 31000 dalam Pengukuran Risiko Operasional dan Risiko Keuangan pada Perusahaan XYZ Abstrak ISO 31000-Based Risk Management : Assessment of a XYZ Company ' s Operational Risk and Financial Risk Abstract," *JEBDEKER*, vol. 4, no. 2, pp. 365–388, 2024.

[21] G. K. Geofanny and A. R. Tanaamah, "Sistem Manajemen Risiko Berbasis ISO 31000 : 2018 Di PT . Bawen Mediatama," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 4, pp. 2870–2878, 2022.

[22] H. A. Mattjik, D. R. Indah, and P. E. Sevtiyuni, "Analisis Manajemen Risiko Pada Teknologi Informasi PT. Pos Indonesia Menggunakan ISO 31000," *Indonesian Journal of Computer Science*, vol. 12, no. 6, pp. 3957–3974, 2023.

[23] U. S. Oktavia, I. G. Anugrah, and W. P. P. Witra, "ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI PT . ETERINDO NUSA GRAHA MENGGUNAKAN FRAMEWORK ISO31000:2018," *JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK)*, vol. 16, no. 1, pp. 100–119, 2025.