JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PT XYZ DENGAN MENGGUNAKAN *FRAMEWORK* COBIT 2019 Pada Risk Profile (*Enterprise/IT Architecture, Hardware Incidents, IT Operational Infrastructure Incidents, dan IT-Investment Decision Making, Portfolio Definition and Maintenance*)

Suffy Aurora Khairunnisa*[1)], Widyatasya Agustika Nurtrisha[2)], Dhata Praditya[3)]
1. Telkom University, Indonesia
2. Telkom University, Indonesia
3. Telkom University, Indonesia

Article Info
Kata Kunci: Manajemen Risiko; Teknologi Informasi; ISO/IEC 27005; PT. XYZ; COBIT 2019

Keywords: *Risk Management; Information Technology; ISO/IEC 27005; PT. XYZ; COBIT 2019*

Article history:
Received 19 August 2024
Revised 5 September 2024
Accepted 2 October 2024
Available online 1 September 2025

DOI :
https://doi.org/10.29100/jipi.v10i3.6485

* Corresponding author.
Corresponding Author
E-mail address:
suffyaurora@student.telkomuniversity.ac.id

ABSTRAK
PT. XYZ, sebagai perusahaan yang bergerak di bidang perawatan pesawat, membutuhkan manajemen risiko teknologi informasi yang efektif untuk mendukung operasionalnya. Seiring dengan perkembangan pesat teknologi informasi dan internet, peran TI menjadi semakin penting. Saat ini, PT. XYZ belum memiliki kerangka kerja formal untuk manajemen risiko TI, sehingga penelitian ini bertujuan untuk menganalisisnya menggunakan *framework* ISO/IEC 27005:2018. Penelitian ini melibatkan proses identifikasi, analisis, evaluasi, dan penanganan risiko sesuai dengan panduan ISO/IEC 27005. Data dikumpulkan melalui kuesioner dan wawancara. Penilaian risiko dilakukan dengan mengacu pada COBIT 2019, mencakup aspek seperti *Enterprise/IT Architecture, Hardware Incidents, IT Operational Infrastructure Incidents, dan IT-Investment Decision Making, Portfolio Definition and Maintenance.* Implementasi manajemen risiko ini membantu mengatasi berbagai risiko yang ditemukan. Dari penilaian yang dilakukan, teridentifikasi 21 risiko, dengan delapan (8) di antaranya berisiko tinggi, lima (5) berisiko sedang, dan delapan (8) lainnya berisiko rendah. Mitigasi risiko dilakukan dengan mengikuti panduan dari COBIT 2019 untuk mendukung kelancaran operasional dan mengurangi dampak negatif dari risiko TI. Penelitian ini diharapkan dapat menjadi panduan bagi perusahaan dan peneliti di masa depan.

ABSTRACT
PT. XYZ, as an aircraft maintenance company, requires effective IT risk management to support its operations. With the rapid advancement of information technology and the internet, the role of IT has become increasingly crucial. Currently, PT. XYZ does not have a formal framework for IT risk management, so this study aims to analyze it using the ISO/IEC 27005:2018 framework. The research involves the process of identifying, analyzing, evaluating, and treating risks in accordance with ISO/IEC 27005 guidelines. Data was collected through questionnaires and interviews. The risk assessment is based on COBIT 2019, covering aspects such as Enterprise/IT Architecture, Hardware Incidents, IT Operational Infrastructure Incidents, and IT-Investment Decision Making, Portfolio Definition and Maintenance. The implementation of risk management helps in addressing the identified risks. The assessment results revealed 21 risks, with eight (8) classified as high risk, five (5) as medium risk, and eight (8) as low risk. Risk mitigation was carried out following COBIT 2019 guidelines to support operations and reduce the negative impact of IT risks. This study is expected to serve as a reference for the company and future researchers.

.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

I. PENDAHULUAN

Teknologi informasi (TI) kini menjadi salah satu faktor utama yang mendukung keberhasilan operasional organisasi modern. Pemanfaatan TI yang optimal memungkinkan organisasi untuk berkembang dengan cepat dan selaras dengan visi serta misi yang telah ditetapkan [1]. Namun, seiring dengan pesatnya perkembangan sistem informasi dan penggunaan jaringan internet, peran TI semakin vital, terutama dalam menjaga kelangsungan operasional perusahaan. PT. XYZ, yang sangat bergantung pada TI, saat ini belum memiliki kerangka kerja formal untuk manajemen risiko TI. Meskipun ada divisi *Enterprise Risk Management (ERM*), risiko TI, terutama yang terkait dengan Unit *Innovation & IT Project Management,* belum dikelola secara khusus. Hal ini berpotensi mengancam keberlangsungan operasional perusahaan [2]

Penelitian ini akan berfokus pada identifikasi dan penilaian risiko TI di PT. XYZ, terutama pada empat risk profile utama, yaitu *Enterprise/IT Architecture*, *Hardware Incidents*, *IT Operational Infrastructure Incidents*, dan *IT-Investment Decision Making Portfolio Definition and Maintenance*. Area-area ini dipilih karena berpotensi langsung mengganggu stabilitas operasional PT. XYZ. Misalnya, Arsitektur TI yang bermasalah bisa menghambat proses bisnis, perangkat keras yang rusak dapat menyebabkan downtime, kegagalan infrastruktur operasional TI dapat mengganggu layanan penting, dan keputusan investasi TI yang salah bisa mengurangi efisiensi perusahaan. Risiko-risiko ini, jika tidak dikelola dengan baik, dapat menghambat pencapaian tujuan bisnis PT. XYZ.

Framework ISO/IEC 27005 dan COBIT 2019 digunakan sebagai panduan dalam penelitian ini. ISO/IEC 27005 memberikan kerangka kerja yang terstruktur untuk menilai risiko melalui identifikasi, analisis, dan evaluasi. Namun, framework ini tidak menawarkan panduan terkait kontrol yang spesifik. Oleh karena itu, COBIT 2019 digunakan sebagai pelengkap, memberikan panduan manajemen TI yang dapat diimplementasikan sebagai kontrol yang efektif. Penelitian ini bertujuan untuk memberikan pemahaman yang lebih mendalam tentang bagaimana PT. XYZ dapat mengelola risiko TI dengan lebih efektif.

Penelitian ini juga bertujuan untuk mengatasi masalah yang ada di PT. XYZ dengan mengembangkan kerangka kerja yang tidak hanya mencakup identifikasi dan penilaian risiko, tetapi juga memberikan panduan praktis untuk manajemen risiko yang disesuaikan dengan kebutuhan perusahaan. Diharapkan, hasil penelitian ini akan memperkaya strategi manajemen risiko TI di industri ini dan menjadi acuan bagi perusahaan lain yang menghadapi tantangan serupa. Untuk menangani risiko-risiko tersebut, penelitian ini mengusulkan penerapan ISO/IEC 27005 yang sesuai dengan kondisi PT. XYZ, yang saat ini belum memiliki kerangka kerja formal. Integrasi ISO/IEC 27005 dengan COBIT 2019 diharapkan dapat menghasilkan kerangka kerja yang kuat dan terstruktur dalam manajemen risiko TI, yang pada akhirnya meningkatkan keamanan dan kelangsungan operasional perusahaan.

Dengan demikian, penelitian ini diharapkan dapat mengatasi kekurangan yang ada dan memperbaiki manajemen risiko TI di PT. XYZ, sekaligus menyajikan solusi serta panduan yang relevan bagi perusahaan lain yang menghadapi tantangan serupa.

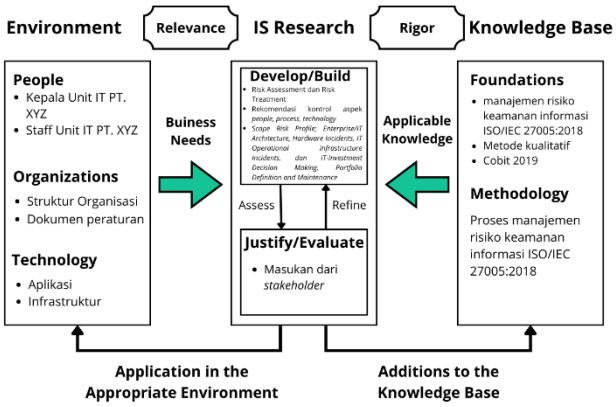
II. METODE PENELITIAN

Pada tahap pengumpulan data, penelitian ini menggunakan dua jenis data, yaitu data primer dan data sekunder. Data primer diperoleh langsung melalui wawancara dengan pekerja terkait serta melalui kuesioner yang dibagikan menggunakan *Google Forms* kepada 16 orang dari berbagai departemen, seperti *Innovation & Digital Transformation (TDI), ERP System & IT Service Delivery (TDO), Human Capital Management (TH),* dan lainnya. Kuesioner ini bertujuan untuk mengevaluasi risiko dan memahami kondisi eksisting perusahaan serta mengonfirmasi jenis risiko yang mungkin terjadi. Untuk memastikan validitas instrumen penelitian, kuesioner dan wawancara diuji melalui penilaian oleh para ahli di bidang manajemen risiko dan teknologi informasi. Selain itu, reliabilitas hasil penelitian diperiksa dengan pengujian berulang dan konsistensi jawaban dari responden. Sementara itu, data sekunder berasal dari informasi atau dokumen yang mencakup hasil identifikasi risiko dari kuesioner dan studi literatur. Studi literatur digunakan untuk menemukan informasi yang relevan terkait penilaian risiko teknologi informasi menggunakan *framework* ISO 27005 dan identifikasi serta kontrol risiko dengan *framework* COBIT 2019.

A. Model Konseptual

Model konseptual adalah rencana atau penjelasan tentang langkah-langkah yang terlibat dalam penelitian yang dilakukan. Model ini memberikan penjelasan tentang berbagai kerangka kerja yang disusun secara jelas untuk mencapai tujuan penelitian. Jalur penelitian desain sains adalah metode metodologis yang digunakan dalam penelitian desain sains untuk menciptakan dan menguji solusi inovatif untuk masalah nyata [3]. Metode ini menggabungkan prinsip-prinsip penelitian ilmiah dengan pendekatan kreatif untuk menghasilkan solusi yang dapat diterapkan di dunia nyata.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447



Gambar 1 Model Konseptual

Model Konseptual yang ditunjukkan pada Gambar 1 merujuk pada pedoman yang disajikan dalam "*Design Research in Information Systems*" [4]. Terdapat tiga elemen utama yang membentuk model konseptual penelitian ini, yaitu lingkungan, penelitian IS, dan sumber pengetahuan. Masing-masing elemen ini memiliki peran penting dalam penyusunan dan pelaksanaan penelitian.

B. Risiko

Ketidakpastian sering kali digunakan untuk menjelaskan risiko, yang tidak hanya dapat menimbulkan masalah tetapi juga menciptakan peluang. Risiko mengacu pada kemungkinan terjadinya kerugian yang tidak dapat diprediksi secara pasti dan dapat berdampak negatif pada tujuan organisasi [5]. Risiko didefinisikan sebagai konsekuensi negatif dari suatu tindakan. Risiko, menurut Kamus Besar Bahasa Indonesia, adalah kemungkinan terjadinya kerugian akibat ketidakpastian, termasuk dalam konteks bisnis sebagai potensi ancaman yang dapat menghambat operasi atau menggagalkan pencapaian tujuan perusahaan [6].

Risiko merupakan peluang terjadinya suatu peristiwa yang berdampak pada kelangsungan proses bisnis dan dapat menyebabkan kegagalan dalam mencapai tujuan organisasi [7] Ancaman dan kerentanan adalah faktor utama yang memicu risiko. Melalui manajemen risiko, organisasi dapat mengidentifikasi dan menangani ancaman serta kerentanan tersebut untuk mengurangi kemungkinan terjadinya kerugian [8] . Dalam konteks organisasi, risiko juga mencakup potensi ancaman atau serangan yang dapat mengganggu operasional atau menggagalkan tujuan organisasi [9]. Oleh karena itu, sangat penting bagi organisasi untuk memahami dan mengidentifikasi risiko agar dapat meminimalkan dampaknya dan mengambil tindakan pencegahan yang diperlukan [10].

C. Manajemen Risiko Teknologi Informasi

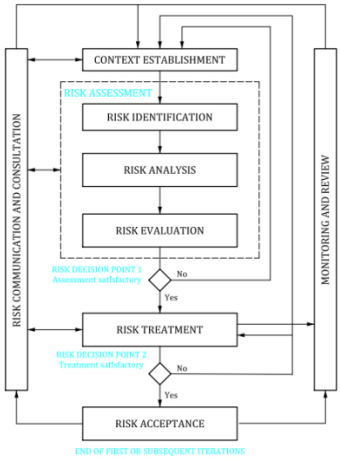
Manajemen risiko adalah proses yang bertujuan mengidentifikasi, mengevaluasi, dan mengelola ketidakpastian yang dapat memengaruhi pencapaian tujuan organisasi, dengan fokus pada perlindungan kelangsungan operasi [11].

Dalam konteks teknologi informasi, manajemen risiko TI melibatkan penerapan prinsip-prinsip ini untuk mengelola risiko yang timbul dari penggunaan teknologi, sebagai bagian penting dari keseluruhan sistem manajemen risiko perusahaan [12]. Proses ini mencakup perencanaan, pengorganisasian, dan pengawasan program penanganan risiko untuk meminimalkan dampak negatif pada operasi bisnis, keamanan data, serta pencapaian tujuan organisasi [13].

Manajer TI berperan penting dalam mengidentifikasi dan mengendalikan risiko teknologi guna memastikan keberlangsungan operasi dan keseimbangan antara risiko dan keuntungan perusahaan [14]. Dalam hal ini, identifikasi, evaluasi, dan pengendalian risiko yang terkait dengan penggunaan teknologi informasi dalam suatu organisasi menjadi sangat penting untuk mengurangi dampak negatifnya terhadap operasi bisnis, keamanan data, dan pencapaian tujuan organisasi.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

D. *Framework* ISO 27005



Gambar 2 *Framework* Iso 27005

Standar internasional ISO/IEC 27005:2018 memberikan pedoman untuk pengelolaan risiko keamanan informasi dalam suatu organisasi, terutama untuk organisasi yang mematuhi standar ISO/IEC 27001 untuk sistem manajemen keamanan informasi (ISMS) [15]. Standar ini menilai risiko yang terkait dengan aset informasi, data, sistem, dan jaringan. Sehingga selaras dengan scope risiko yang akan diidentifikasi pada penelitian ini.

Menurut ISO 27005 proses manajemen risiko keamanan informasi terdiri dari *Context Establishment, Risk Assessment, Risk Treatment, Risk Acceptance, Risk Communication, Risk Monitoring and Review* [16]. Dalam penelitian ini, framework ISO 27005 akan digunakan untuk memetakan hasil analisis risiko yang diperoleh dari wawancara dan kuesioner ke dalam elemen-elemen framework tersebut. Proses ini melibatkan pengidentifikasian konteks risiko, penilaian risiko, serta penanganan dan komunikasi risiko berdasarkan data yang dikumpulkan.

E. COBIT 2019

ISACA membuat kerangka kerja yang disebut COBIT *(Control Objectives for Information and Related Technology)* untuk mengatur dan mengelola informasi dan teknologi yang berkaitan di seluruh organisasi [17]. Konsep Enterprise I&T dalam COBIT mencakup semua teknologi dan proses informasi yang diterapkan oleh perusahaan untuk mencapai tujuan mereka, tidak hanya terbatas pada departemen TI, melainkan mencakup seluruh spektrum teknologi dan pemrosesan informasi di dalam perusahaan[18]. Framework COBIT 2019 akan digunakan untuk menganalisis data dengan cara memetakan hasil identifikasi risiko ke dalam elemen-elemen COBIT yang relevan dengan scope penelitian ini.

F. Perbandingan *Framework* ISO 27005 dengan ISO 31000

ISO/IEC 27005 dan ISO 31000 adalah standar manajemen risiko dengan fokus yang berbeda. ISO/IEC 27005, bagian dari ISO 27000, memberikan panduan untuk manajemen risiko keamanan informasi dan mendukung penerapan ISO 27001. Standar ini mencakup tahap-tahap seperti pembentukan konteks, penilaian risiko, dan perlakuan risiko terkait aset informasi, data, sistem, dan jaringan[19].

Sebaliknya, ISO 31000 adalah standar yang lebih luas yang mencakup semua jenis risiko yang dihadapi perusahaan, menyediakan kerangka kerja yang dapat diterapkan dan diadaptasi oleh berbagai jenis organisasi. Standar ini membantu organisasi mengidentifikasi, menilai, dan mengelola risiko secara sistematis, serta mendorong integrasi manajemen risiko ke dalam semua aspek organisasi untuk menghadapi ketidakpastian dan mencapai tujuan strategis [20] Kedua standar ini penting, namun dengan fokus yang berbeda: ISO/IEC 27005 untuk keamanan informasi, dan ISO 31000 untuk manajemen risiko secara umum..

III. HASIL DAN PEMBAHASAN

A. Analisis Data

1) Ruang lingkup dan Aset Teknologi Informasi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

TABEL I
ASET DIVISI IT PT XYZ

No	Komponen	Nama Aset
1.	Layanan	XPREAM IT Service Desk
2.	Infrastruktur	Server Laptop PC
3.	Aplikasi	SAP Swift XOPS AMS APPS HIL APPS

Divisi IT di PT. XYZ memiliki berbagai aset yang penting untuk mendukung operasional teknologi informasi. Aset-aset ini terbagi ke dalam tiga kategori utama, yaitu Layanan, Infrastruktur, dan Aplikasi. Dalam komponen Layanan, terdapat dua aset utama yaitu XPREAM dan IT Service Desk. XPREAM merupakan salah satu layanan unggulan yang dimiliki, sedangkan IT Service Desk berfungsi sebagai pusat bantuan untuk menangani berbagai masalah IT yang dihadapi oleh pengguna.

Selanjutnya, pada komponen Infrastruktur, terdapat tiga jenis perangkat keras yang digunakan, yaitu Server, Laptop, dan PC. Server berfungsi sebagai pusat pengolahan data dan penyimpanan yang mendukung berbagai aplikasi dan layanan IT. Laptop dan PC digunakan oleh karyawan untuk menyelesaikan pekerjaan sehari-hari, baik itu di kantor maupun di luar kantor.

Dan dalam komponen Aplikasi, terdapat beberapa aplikasi penting yang digunakan oleh perusahaan, yaitu SAP Swift, XOPS, AMS APPS, dan HIL APPS. Aplikasi-aplikasi ini dirancang untuk mendukung berbagai proses bisnis dan operasional, mulai dari manajemen sumber daya perusahaan hingga aplikasi spesifik yang mendukung operasional di bidang yang lebih teknis. Dengan keberadaan aset-aset ini, divisi IT PT. XYZ dapat menjalankan fungsinya dengan optimal, memastikan bahwa semua layanan dan infrastruktur teknologi informasi berjalan dengan lancar dan efisien.

2) Kriteria *Consequence*

Dalam mengelola risiko, penting untuk memahami dampak potensial jika suatu risiko terjadi. *Consequence criteria* ini didapatkan dari perusahaan langsung sehingga sangat membantu dalam mengidentifikasi dan menilai tingkat dampak yang mungkin terjadi dalam berbagai skenario.

TABEL 2
KRITERIA CONSEQUENCE

Consequence (C)		Score
Insignificant	Tidak ada efeknya atau pengaruhnya sangat kecil terhadap tujuan/objective	**1**
Minor	Terjadi penurunan keberhasilan pencapaian tujuan/objective	**2**
Moderate	Penurunan keberhasilan pencapaian tujuan/objective yang terjadi signifikan	**3**
Major	keberhasilan pencapaian tujuan/objective rendah dan dapat menimbulkan efek lain yang lebih parah	**4**
Catastropic	Efek yang ditimbulkan sangat tinggi dan menyebabkan tidak dapat tercapai tujuan organisasi	**5**

3) Kriteria *Likelihood*

Dalam proses pengelolaan risiko, kita juga perlu memperhitungkan seberapa besar kemungkinan suatu risiko terjadi. Faktor ini dikenal sebagai "*likelihood criteria*" atau kriteria kemungkinan. Memahami seberapa mungkin suatu risiko akan terjadi sangat penting untuk menentukan tingkat keparahan dan urgensi langkah-langkah mitigasi yang diperlukan

TABEL 3
KRITERIA LIKELIHOOD

	Likelihood (L)	Frekuensi Kemungkinan (dalam setahun)	Score
Rare	Kemungkinan terjadi risiko sangat kecil	X < 2 kali	**1**
Unlikely	Risiko jarang terjadi	2 ≤ X ≤ 5 kali	**2**
Possible	Risiko kadang-kadang terjadi	6 ≤ X ≤ 9 kali	**3**

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

Likely	Risiko tersebut terjadi berulang-ulang	$10 \leq X \leq 12$ kali	**4**
Certain	Risiko hampir tidak dapat dihindari	> 12 kali	**5**

4) Matriks Risiko

Matriks risiko adalah alat dalam manajemen risiko yang digunakan untuk mengidentifikasi, menganalisis, dan menilai kemungkinan risiko yang dapat mempengaruhi suatu organisasi atau proyek. Matriks ini menggambarkan tingkat dampak (*impact*) dan kemungkinan (*likelihood*) suatu risiko yang digambarkan dalam Tabel 4 yang mudah dipahami. Matriks risiko membantu manajer dan tim proyek menentukan prioritas penanganan risiko dan strategi mitigasi yang diperlukan dengan mengklasifikasikan risiko berdasarkan dua parameter ini. Risiko biasanya dikategorikan ke dalam beberapa tingkat, seperti rendah, sedang, tinggi, dan kritis. Orang dapat membuat keputusan yang lebih baik dan efektif dengan bantuan kategori ini

TABEL 4
MATRIKS RISIKO

Likelihood/ Consequence		***Insignificant***	***Minor***	***Moderate***	***Major***	***Catastrophic***
		1	**2**	**3**	**4**	**5**
Rare	1	1	2	3	4	5
Unlikely	*2*	2	4	6	8	10
Possible	*3*	3	6	9	12	15
Likely	*4*	4	8	12	16	20
Certain	*5*	5	10	15	20	25

Untuk menentukan tingkat risiko, dua faktor utama yang digunakan adalah tingkat kemungkinan terjadinya risiko dan tingkat dampak risiko. Tingkat kemungkinan terjadinya risiko, tingkat dampak risiko, dan masing-masing tingkat risiko harus digabungkan dan dipertimbangkan secara bersamaan.

TABEL 5
LEVEL RISIKO

Level Risiko	Besaran Risiko	Keterangan Risiko
Low	1 s.d 4	*Low*
Medium	5 s.d 8	*Medium*
High	9 s.d 15	*High*
Crisis	16 s.d 25	*Crisis*

B. Penilaian Risiko

1) Identifikasi Risiko

Identifikasi risiko yang mungkin dihadapi oleh organisasi adalah langkah pertama dalam penilaian risiko, yang bertujuan untuk mengidentifikasi sumber dan potensi efek dari setiap risiko yang diidentifikasi. Risiko yang ada pada Tabel 5 diambil dari referensi COBIT 2019 pada *Figure* 2.7—*Risk Profile Design Factor (IT Risk Categories),* yang kemudian diadopsi dan diprioritaskan dalam proses manajemen risiko teknologi informasi di perusahaan.

TABEL 6
IDENTIFIKASI RISIKO

Risk ID	Risk Profile	Risiko	Nilai *Consequence*	Nilai *Likelihood*
R5	*Enterprise/IT architecture* (5)	Jumlah pengecualian yang berlebihan terhadap standar arsitektur perusahaan dapat menyulitkan manajemen dan meningkatkan risiko operasional.	5	2
R6		Kegagalan dalam mengadopsi dan memanfaatkan infrastruktur baru dengan tepat waktu, atau mengabaikan infrastruktur yang sudah usang, bisa berdampak negatif.	5	1
R7		Kegagalan dalam mengadopsi dan memanfaatkan perangkat lunak baru dengan tepat waktu, baik dari segi fungsionalitas maupun pengoptimalan, atau meninggalkan aplikasi yang sudah usang, dapat menyebabkan masalah.	4	2
R8		Kekurangan dalam aspek keamanan arsitektur IT dapat meningkatkan risiko terhadap serangan siber dan kebocoran data yang dapat merugikan reputasi dan kepercayaan pelanggan.	4	1

R9		Arsitektur perusahaan itu rumit dan tidak fleksibel, menghalangi evolusi lebih lanjut dan ekspansi yang menyebabkan hilangnya bisnis peluang.	3	3
R10		Modifikasi perangkat lunak yang tidak disengaja yang menyebabkan hasil yang tidak akurat	1	1
R11		Sistem mungkin tidak mampu menangani volume transaksi ketika jumlah pengguna meningkat.	5	2
R12	*Hardware incidents*	Kegagalan utilitas seperti telekomunikasi atau listrik dapat menyebabkan gangguan sistem.	4	3
R13		Perangkat keras dapat mengalami kegagalan karena suhu yang berlebihan atau kondisi lingkungan lain seperti kelembaban	3	4
R14		Komponen perangkat keras yang rusak dapat mengakibatkan kehilangan data oleh staf internal.	3	1
R15		Sistem mungkin tidak mampu menangani beban ketika aplikasi atau inisiatif baru diterapkan.	3	4
R26		Kerusakan peralatan IT yang tidak disengaja	2	5
R27		Kesalahan yang dilakukan oleh staf TI (selama pencadangan, selama peningkatan sistem, selama pemeliharaan sistem, dll.)	2	1
R28	*IT operational infrastructure incidents*	Pencurian perangkat dengan data sensitive	4	2
R29		Penyalahgunaan hak akses dari peran sebelumnya untuk mengakses infrastruktur TI	3	1
R30		Penghancuran pusat data (sabotase, dll) oleh staf	3	1
R31		Adanya duplikasi atau tumpang tindih antara berbagai inisiatif investasi bisa menyebabkan pemborosan dan kesulitan koordinasi.	2	3
R32	*IT-investment decision making, portfolio definition and maintenance*	Pemilihan perangkat lunak yang tidak tepat, baik dari segi biaya, kinerja, fitur, kompatibilitas, redundansi, dan sebagainya, dapat mengganggu proses akuisisi dan implementasi.	4	2
R33		Kegagalan investasi dalam teknologi informasi dapat menghambat dukungan terhadap strategi digital perusahaan.	3	1
R34		Perangkat lunak yang berlebihan dibeli	2	1
R35		Kesalahan alokasi, pengelolaan yang tidak efisien, atau persaingan untuk mendapatkan sumber daya tanpa koordinasi yang baik dengan prioritas bisnis dapat merugikan kelancaran proyek.	3	3

2) Penanganan Risiko

Langkah terakhir adalah menentukan strategi penanganan risiko yang sesuai untuk mengelola risiko yang telah dievaluasi. Pada Tabel 7 berikut merangkum tindakan penanganan yang akan diambil untuk setiap risiko, memastikan bahwa setiap strategi terintegrasi dengan kebijakan dan tujuan perusahaan dalam mengelola risiko secara efektif.

TABEL 7
PENANGANAN RISIKO

Risk ID	Nilai Risiko	Level Risiko	Penanganan Risiko	Penanggung Jawab Risiko
R5	10	High	Modification	• MGR DIGITAL SOLUTION • MGR INNOVATION & IT PROJECT MANAGEMENT
R6	5	Medium	Modification	• MGR DIGITAL SOLUTION • MGR INNOVATION & IT PROJECT MANAGEMENT
R7	8	Medium	Modification	MGR DIGITAL SOLUTION
R8	4	Low	Retention	• SM ERP SYSTEM & IT SERVICE DELIVERY • SM INNOVATION & DIGITAL TRANSFORMATION
R9	9	High	Modification	• SM ERP SYSTEM & IT SERVICE DELIVERY • SM INNOVATION & DIGITAL TRANSFORMATION
R10	1	Low	Retention	ICT ANALYST (IT SECURITY OFFICER)
R11	10	High	Modification	• MGR IT SERVICE DELIVERY • ICT ANALYST (IT SECURITY OFFICER) • ICT ANALYST (IT BUSINESS ANALYST OFFICER)
R12	12	High	Sharing	• MGR FACILITY OPERATION

				• MGR IT SERVICE DELIVERY
R13	12	High	Modification	• MGR FACILITY OPERATION • MGR IT SERVICE DELIVERY
R14	3	Low	Retention	ICT ANALYST (IT BUSINESS ANALYST OFFICER)
R15	12	High	Modification	• MGR IT SERVICE DELIVERY • MGR DIGITAL SOLUTION
R26	10	High	Modification	• ICT ANALYST (IT ASET OFFICER) • ICT ANALYST (IT SECURITY OFFICER) • ICT ANALYST (IT BUSINESS ANALYST OFFICER)
R27	2	Low	Retention	• ICT ANALYST (IT BUSINESS ANALYST OFFICER) • ICT ANALYST (IT SECURITY OFFICER)
R28	8	Medium	Modification	ICT ANALYST (IT ASET OFFICER)
R29	3	Low	Retention	• ICT ANALYST (IT BUSINESS ANALYST OFFICER) • ICT ANALYST (IT SECURITY OFFICER)
R30	3	Low	Retention	• MGR IT SERVICE DELIVERY • ICT ANALYST (IT BUSINESS ANALYST OFFICER)
R31	2	Low	Retention	MGR INNOVATION & IT PROJECT MANAGEMENT
R32	8	Medium	Modification	• SM ERP SYSTEM & IT SERVICE DELIVERY • SM INNOVATION & DIGITAL TRANSFORMATION
R33	3	Low	Retention	• SM ERP SYSTEM & IT SERVICE DELIVERY • SM INNOVATION & DIGITAL TRANSFORMATION
R34	2	Low	Retention	MGR INNOVATION & IT PROJECT MANAGEMENT
R35	9	High	Modification	• SM ERP SYSTEM & IT SERVICE DELIVERY • SM INNOVATION & DIGITAL TRANSFORMATION

C. Penetapan Kontrol

Penetapan kontrol dilakukan untuk mengelola risiko dengan memastikan implementasi dan pemantauan prosedur yang sesuai dengan standar operasional perusahaan. Penggunaan kontrol yang disesuaikan dengan prinsip-prinsip COBIT 2019 diidentifikasi untuk meminimalkan dampak dan kejadian risiko yang tidak diinginkan.

TABEL 8
PENETAPAN KONTROL

Risk ID	Aspek	Judul Kontrol	Deskripsi	Dokumen Terkait
R5	*Process*	APO03.02 *Define reference architecture.*	Arsitektur referensi menggambarkan arsitektur dan tujuan saat ini untuk bisnis, data, informasi, aplikasi, dan teknologi.	-
	People	Membuat kelompok "*Architecture Board*"	Kelompok atau komite yang bertanggung jawab untuk mengawasi dan mengelola arsitektur enterprise dalam suatu organisasi	
R6	*Process*	APO04.03 *Monitor and scan the technology environment.*	Menetapkan prosedur pemantauan teknologi untuk mengawasi dan memindai lingkungan eksternal perusahaan guna mengidentifikasi teknologi baru yang dapat memberikan nilai, seperti dalam pengembangan strategi perusahaan, pengoptimalan biaya, pencegahan penuaan, serta peningkatan proses perusahaan dan R&D. Proses pemantauan ini juga melibatkan pengawasan pasar, sektor industri, lanskap kompetitif, serta tren hukum dan peraturan untuk mengidentifikasi teknologi baru.	-
	People	Membuat kelompok "*Architecture Board*"	Kelompok atau komite yang bertugas mengawasi dan mengelola arsitektur enterprise dalam suatu organisasi.	

R7	*Process*	APO03.05 *Provide enterprise architecture services.*	Menyediakan layanan arsitektur enterprise di dalam perusahaan, termasuk memberikan panduan dan pemantauan terhadap proyek implementasi, menetapkan metode kerja melalui kontrak arsitektur, serta mengukur dan mengomunikasik an nilai serta kepatuhan terhadap arsitektur tersebut.	-
	People	Membuat kelompok "*Architecture Board"*	Grup atau komite yang bertanggung jawab atas pengawasan dan pengelolaan arsitektur enterprise dalam sebuah organisasi.	
R8	*Process*	APO03.01 *Develop the Enterprise Architecture Vision*	Visi arsitektur memberikan gambaran komprehensif mengenai tujuan dan dasar arsitektur, meliputi domain bisnis, informasi, data, aplikasi, dan teknologi. Visi ini membantu sponsor mempresentasika n kemampuan yang diusulkan kepada pemangku kepentingan bisnis, serta menunjukkan bagaimana kemampuan baru, yang selaras dengan strategi dan tujuan penelitian dan pengembangan, dapat mencapai tujuan strategis perusahaan dan mengatasi kelemahan yang ada.	
		APO13.01 *Establish and maintain an information security management system (ISMS).*	Mengembangkan dan memelihara sistem manajemen keamanan informasi (ISMS) yang menawarkan pendekatan standar, formal, dan berkelanjutan untuk mengelola keamanan informasi, serta memastikan bahwa teknologi dan proses bisnis beroperasi dengan aman sesuai dengan kebutuhan bisnis.	-
	People	Membuat kelompok "*Architecture Board"*	Kelompok atau komite yang bertanggung jawab untuk mengawasi dan mengelola arsitektur enterprise dalam suatu organisasi.	
R9	*Process*	APO03.01 *Develop the Enterprise Architecture Vision*	Visi arsitektur memberikan pandangan mendalam tentang tujuan dan dasar-dasar arsitektur, mencakup domain bisnis, informasi, data, aplikasi, dan teknologi. Visi ini berfungsi sebagai alat penting bagi sponsor untuk mengkomunikasikan kemampuan yang diusulkan kepada pemangku kepentingan bisnis. Visi arsitektur menunjukkan bagaimana kemampuan baru yang selaras dengan strategi serta tujuan penelitian dan pengembangan dapat mencapai sasaran strategis perusahaan dan mengatasi kekurangan yang ada.	
		APO03.02 *Define Reference Architecture*APO03.03 *Select Opportunities and Solutions*	Arsitektur referensi menggambarkan arsitektur dan tujuan saat ini untuk bisnis, data, informasi, aplikasi, dan teknologi. Menjembatani perbedaan antara arsitektur saat ini dan yang diinginkan dengan mempertimbangkan perspektif bisnis dan teknis, lalu menggabungkannya dalam paket kerja proyek yang terstruktur. Proyek ini diintegrasikan dengan program investasi TI terkait untuk memastikan inisiatif arsitektur mendukung serta memfasilitasi perubahan keseluruhan perusahaan. Upaya ini dilakukan melalui kolaborasi dengan pemangku kepentingan utama dari bisnis dan IT untuk menilai kesiapan transformasi perusahaan, sekaligus mengidentifikasi peluang, solusi, dan kendala dalam implementasi.	-
	People	Membuat kelompok "*Architecture Board"*	Kelompok atau komite yang bertanggung jawab untuk mengawasi dan mengelola arsitektur enterprise dalam suatu organisasi.	
R10	*Process*	BAI03.07 *Prepare for solution testing*	Tentukan lingkungan dan rencana pengujian yang diperlukan untuk menguji komponen solusi secara terpisah dan terintegrasi. Ini mencakup proses bisnis, layanan pendukung, aplikasi, dan infrastruktur yang digunakan.	
		BAI06.01 *Evaluate, prioritize and authorize change requests.*	Meninjau setiap permintaan perubahan untuk menentukan dampaknya pada proses bisnis dan layanan R&D, serta mengevaluasi apakah perubahan tersebut dapat berdampak negatif pada lingkungan operasional dan memperkenalkan risiko yang tidak dapat diterima. Pastikan bahwa setiap perubahan dicatat, diprioritaskan, dikategorikan, dievaluasi, disetujui, direncanakan, dan dijadwalkan dengan baik.	Prosedur Perangkat Keras
R11	*Process*	BAI04.03 *Plan for new or changed service requirements.*	Merencanakan dan memprioritaskan dampak perubahan kebutuhan bisnis dan persyaratan layanan terhadap ketersediaan, kinerja, dan kapasitas.	Catatan Pemantauan Kinerja dan Kapasitas Sistem
R12	*Process*	DSS04.03 Develop and implement a business continuity response.	Dengan mempertimbangkan strategi, buat rencana kelangsungan bisnis (BCP) dan rencana pemulihan bencana (DRP). Dokumen yang mencakup semua prosedur yang diperlukan perusahaan untuk melakukan tugas penting dalam kasus insiden	Kontrak Layanan dengan vendor
R13	*Process*	BAI04.05 *Investigate and address availability, performance and capacity issues.*	Mengatasi penyimpangan dalam menyelidiki dan memecahkan masalah ketersediaan, kinerja, dan kapasitas yang teridentifikasi	Prosedur Perangkat Keras

R14	*Process*	BAI09.01 *Identify and record current assets.*	Memelihara catatan yang up-to-date dan akurat mengenai semua aset I&T yang diperlukan untuk menyediakan layanan, serta aset yang dimiliki atau dikendalikan oleh organisasi untuk menciptakan keuntungan di masa depan (termasuk sumber daya bernilai ekonomi, seperti perangkat lunak atau perangkat keras). Pastikan kepatuhan dengan keuangan dan manajemen konfigurasi.	Prosedur Perangkat Keras
		BAI09.03 *Manage the asset life cycle.*	Mengelola aset dari pembelian hingga penghapusan. Memastikan bahwa aset digunakan seefektif dan seefisien mungkin serta dihitung dan dilindungi secara fisik sampai saat penghapusan yang tepat.	
R15	*Process*	BAI04.05 *Investigate and address availability, performance and capacity issues.*	Menangani penyimpangan dengan menyelidiki dan menyelesaikan masalah ketersediaan, kinerja, dan kapasitas yang teridentifikasi.	
		APO03.01 *Develop the Enterprise Architecture Vision*	Visi arsitektur memberikan pemahaman yang mendalam tentang tujuan dan fondasi arsitektur, meliputi domain bisnis, informasi, data, aplikasi, dan teknologi. Visi ini menyediakan alat penting bagi sponsor untuk mengkomunikasikan kemampuan yang diusulkan kepada pemangku kepentingan bisnis. Visi arsitektur juga menunjukkan bagaimana kemampuan baru yang selaras dengan strategi dan tujuan penelitian dan pengembangan dapat memenuhi sasaran strategis perusahaan serta mengatasi kekurangan yang ada.	Catatan Pemantauan Kinerja dan Kapasitas Sistem
		APO03.02 *Define Reference Architecture*	Arsitektur referensi menggambarkan kondisi arsitektur saat ini serta target yang ingin dicapai untuk domain bisnis, informasi, data, aplikasi, dan teknologi.	
R26	*Process*	BAI04.01 *Assess current availability, performance and capacity and create a baseline*	Mengevaluasi ketersediaan, kinerja, dan kapasitas layanan serta sumber daya untuk memastikan bahwa kapasitas dan kinerja yang efisien tersedia guna mendukung kebutuhan bisnis dan memenuhi perjanjian tingkat layanan (SLAs). Membangun basis ketersediaan, kinerja, dan kapasitas sebagai acuan untuk perbandingan di masa depan.	Prosedur Pemeliharaan Perangkat Keras
	Technology	Menambahkan bantuan perangkat lunak otomatis *(tools)*	Bantuan perangkat lunak otomatis seperti alat atau tools untuk memantau kinerja peralatan atau perangkat IT	
R27	*Process*	DSS03.03 *Raise known errors*	Setelah penyebab masalah teridentifikasi, segera buat catatan kesalahan yang diketahui, dokumentasikan solusi yang sesuai, dan identifikasi solusi potensial.	
		DSS03.04 *Resolve and close problems.*	Mengidentifikasi dan menerapkan solusi berkelanjutan yang menangani akar masalah. Jika diperlukan, ajukan permintaan perubahan melalui proses manajemen perubahan. Pastikan karyawan yang terdampak mengetahui tindakan yang telah diambil dan rencana yang disusun untuk mencegah kejadian serupa di masa depan.	Prosedur Pemeliharaan Sistem
R28	*Process*	DSS05.05 *Manage physical access to I&T assets.*	Menetapkan dan menerapkan prosedur, termasuk prosedur darurat, untuk memberikan, membatasi, dan membatalkan akses ke fasilitas, bangunan, dan area sesuai dengan kebutuhan bisnis. Akses harus dibenarkan, disetujui, dicatat, dan dipantau. Persyaratan ini berlaku bagi semua orang yang memasuki fasilitas, termasuk karyawan, pekerja sementara, klien, vendor, pengunjung, atau pihak ketiga lainnya.	Prosedur Pemeliharaan Sistem
		DSS05.06 *Manage sensitive documents and output devices.*	Menyediakan jaminan fisik yang memadai, teknik akuntansi, dan manajemen persediaan untuk aset I&T yang sensitif, seperti formulir khusus, instrumen yang dapat diperdagangkan, printer khusus, atau token keamanan.	
R29	*Process*	DSS05.04 *Manage user identity and logical access.*	Untuk memastikan bahwa setiap pengguna memiliki hak akses informasi sesuai dengan persyaratan perusahaan, berkolaborasi dengan unit bisnis yang mengatur hak akses mereka sendiri selama proses operasi.	Prosedur Manajemen Akses
R30	*Process*	DSS01.04 *Manage the environment*	Mengambil tindakan untuk melindungi lingkungan, seperti memasang peralatan dan perangkat khusus untuk memantau dan mengontrol lingkungan.	
		DSS01.05 *Manage facilities*	Kontrol fasilitas, termasuk peralatan listrik dan komunikasi, sesuai dengan undang-undang dan peraturan, persyaratan teknis dan bisnis, kebutuhan pemasok, dan pedoman kesehatan dan keselamatan.	Kebijakan Keamanan Data
R31	*Process*	APO05.02 *Evaluate and select programs to fund.*	Berdasarkan persyaratan untuk kombinasi portofolio investasi secara keseluruhan, rencana strategis dan jalur R&T, evaluasi dan priorisasi kasus bisnis program, dan keputusan tentang proposal investasi Penyebaran dana dan pelaksanaan program.	
R32	*Process*	BAI03.04 *Procure solution components.*	Dalam rencana akuisisi, komponen solusi harus memenuhi persyaratan dan desain terperinci, prinsip arsitektur dan standar, persyaratan dan standar persetujuan, serta prosedur pembelian dan kontrak perusahaan. Penjual harus memastikan bahwa mereka menemukan dan menangani semua persyaratan hukum dan kontrak.	Prosedur Pengadaan
R33	*Process*	APO05.04 *Maintain portfolios.*	Memelihara portofolio program dan proyek investasi, aset penelitian dan pengembangan, dan produk dan layanan.	Prosedur Pengadaan
R34	*Process*	BAI09.03 *Manage the Asset Life Cycle*	Mengawasi aset mulai dari pembelian hingga penghapusan memastikan bahwa aset digunakan secara paling efisien dan efektif, serta disimpan dan dilindungi secara fisik sampai pensiun.	Catatan Inventaris

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2435-2447

R35	*Process*	APO06.02 *Prioritize resource allocation*	Menggunakan prosedur pengambilan keputusan untuk menentukan prioritas alokasi sumber daya dan menetapkan aturan untuk investasi bebas oleh unit bisnis individu, termasuk penggunaan penyedia layanan eksternal dan pertimbangan tentang pembelian, pengembangan, dan opsi sewa.	Prosedur Permintaan Solusi
		APO07.01 *Acquire and maintain adequate and appropriate staffing.*	Menetapkan dan mempertahankan cara untuk mengelola dan memperhitungkan semua biaya R&T, investasi, dan depreciasi sebagai komponen penting dari sistem keuangan dan akun perusahaan; laporan menggunakan sistem pengukuran keuangan perusahaan.	

D. Prioritas Rekomendasi

Dalam penelitian ini, Prioritas Rekomendasi digunakan sebagai landasan untuk mengembangkan roadmap implementasi selanjutnya. Hal ini memastikan bahwa langkah-langkah yang diambil sesuai dengan prioritas yang telah ditetapkan.

TABEL 9
PRIORITAS REKOMENDASI

Risk ID	Aspek	Judul Kontrol	Dokumen Terkait	Prioritas
R12	*Process*	DSS04.03 *Develop and implement a business continuity response.*	Kontrak Layanan dengan vendor	1
R13	*Process*	BAI04.05 *Investigate and address availability, performance and capacity issues.*	Prosedur Perangkat Keras	2
R15	*Process*	BAI04.05 *Investigate and address availability, performance and capacity issues.* APO03.01 *Develop the Enterprise Architecture Vision* APO03.02 *Define Reference Architecture*	Catatan Pemantauan Kinerja dan Kapasitas Sistem	3
R5	*Process*	APO03.02 *Define reference architecture.*	-	4
	People	Membuat kelompok *"Architecture Board"*		
R11	*Process*	BAI04.03 *Plan for new or changed service requirements.*	Catatan Pemantauan Kinerja dan Kapasitas Sistem	5
R26	*Process*	BAI04.01 *Assess current availability, performance and capacity and create a baseline*	Prosedur Pemeliharaan Perangkat Keras	6
	Technology	Menambahkan bantuan perangkat lunak otomatis *(tools)*		
R9	*Process*	APO03.01 *Develop the Enterprise Architecture Vision* APO03.02 *Define Reference Architecture* APO03.03 *Select Opportunities and Solutions*	-	7
	People	Membuat kelompok "*Architecture Board"*		
R35	*Process*	APO06.02 *Prioritize resource allocation* APO07.01 *Acquire and maintain adequate and appropriate staffing.*	Prosedur Pengadaan	8
R7	*Process*	APO03.05 *Provide enterprise architecture services.*	-	9
	People	Membuat kelompok "*Architecture Board"*		
R28	*Process*	DSS05.05 *Manage physical access to I&T assets.* DSS05.06 *Manage sensitive documents and output devices.*	Prosedur Pemeliharaan Sistem	10
R32	*Process*	BAI03.04 *Procure solution components.*	Prosedur Pengadaan	11
R31	*Process*	APO05.02 *Evaluate and select programs to fund.*	-	12
R6	*Process*	APO04.03 *Monitor and scan the technology environment.*	-	13
	People	Membuat kelompok "*Architecture Board"*	-	

E. Roadmap Implementasi

Penyusunan roadmap bertujuan untuk merencanakan jadwal implementasi rekomendasi, memastikan setiap langkah dilaksanakan tepat waktu dan sesuai prioritas.

TABEL 10
ROADMAP IMPLEMENTASI

No	Judul Kontrol	Q1	Q2	Q3	Q4
Aspek *People*					
1	Membuat kelompok "*Architecture Board"*				
Aspek *Technology*					

2	Menambahkan bantuan perangkat lunak otomatis *(tools)*	
Aspek *Process*		
3	DSS04.03 *Develop and implement a business continuity response.*	
4	BAI04.05 *Investigate and address availability, performance and capacity issues.*	
5	APO03.01 *Develop the Enterprise Architecture Vision* APO03.02 *Define Reference Architecture*	
6	BAI04.03 *Plan for new or changed service requirements.*	
7	BAI04.01 *Assess current availability, performance and capacity and create a baseline*	
8	APO03.03 *Select Opportunities and Solutions*	
9	APO06.02 *Prioritize resource allocation* APO07.01 *Acquire and maintain adequate and appropriate staffing.*	
10	APO03.05 *Provide enterprise architecture services.*	
11	DSS05.05 *Manage physical access to I&T assets.* DSS05.06 *Manage sensitive documents and output devices.*	
12	BAI03.04 *Procure solution components.*	
13	APO05.02 *Evaluate and select programs to fund.*	
14	APO04.03 *Monitor and scan the technology environment.*	

IV. KESIMPULAN

Berdasarkan identifikasi masalah, PT. XYZ menggunakan ISO/IEC 27005 untuk mengelola risiko teknologi informasi, melibatkan penentuan konteks organisasi, identifikasi risiko, dan analisis ancaman. Dengan referensi COBIT 2019, PT. XYZ menggunakan Matriks Pairwise Comparison untuk memprioritaskan risiko yang diidentifikasi, termasuk *Enterprise/IT Architecture, Hardware Incidents, IT Operational Infrastructure Incidents, dan IT-Investment Decision Making, Portfolio Definition and Maintenance*. Penilaian risiko mengikuti tahapan ISO/IEC 27005, mulai dari menetapkan konteks hingga evaluasi hasil. Dari 21 risiko yang diidentifikasi, ada delapan risiko *High*, lima risiko *Medium*, dan delapan risiko *Low*. Risiko *Low* dianggap dapat diterima, sedangkan risiko *Medium* dan *High* diberi tindakan pengendalian sesuai. Untuk penanganan risiko, kontrol dan rekomendasi diambil berdasarkan prinsip-prinsip COBIT 2019 dengan langkah seperti retention, modification, sharing, dan avoidance.

Disarankan agar PT. XYZ menerapkan manajemen risiko teknologi informasi secara berkelanjutan untuk memastikan risiko baru dapat diidentifikasi dan dikelola dengan tepat waktu. Selain itu, pembuatan dan pemeliharaan risk register yang komprehensif akan mempermudah proses identifikasi, penilaian, dan pengelolaan risiko serta monitoring secara periodik. Penting juga untuk menentukan narasumber yang tepat dan memberikan job description yang sesuai guna menghindari kesalahan dalam penilaian risiko.

DAFTAR PUSTAKA

[1] J. Rohman and E. Fadilah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Sistem Komputerisasi Haji Terpadu di Kantor Kementerian Agama Kabupaten Ogan Ilir," 2022.
[2] Jakaria, R. Fitriani, and J. N. Utamajaya, "Evaluasi Manajemen Risiko Teknologi Informasi Berbasis ISO 31000:2018," 2021.
[3] F. Z. Fahlevi, F. Dewi, and D. Praditya, "Analisis dan Perancangan Enterprise Architecture Menggunakan TOGAF ADM di Unit Koleksi Penagihan," *Media Online)*, vol. 4, no. 1, pp. 583–591, 2023, doi: 10.30865/klik.v4i1.1198.
[4] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science In Information Systems Research 1," 2004.
[5] A. I. K. E. B. H. M. P. S. Y. I. N. S. W. V. S. Eko Sudarmanto, "[III.A.1.a.2.9] FullBook Manajemen Risiko Perbankan," 2021.
[6] S. Sahira, R. Fauzi, and I. Santosa, "Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar Iso/Iec 27005:2018 Analysis Of Risk Management In E-Office Application Managed By Pt Telkom Indonesia Using ISO/IEC 27005:2018 Standard," 2020.
[7] G. J. Nofita Sari, K. Isnaini, and A. P. Kuncoro, "Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa," *Jurnal Eksplora Informatika*, vol. 13, no. 1, pp. 37–45, Sep. 2023, doi: 10.30864/eksplora.v13i1.696.
[8] E. Supristiowadi and Y. G. Sucahyo, "Manajemen Risiko Keamanan Informasi Pada Sistem Aplikasi Keuangan Tingkat Instansi (Sakti) Kementerian Keuangan," 2017.
[9] Asriyanik and Prajoko, "Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," 2018.
[10] M. Amirinnisa and R. Bisma, "Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun," 2023.
[11] R. Rambe, A. Gandhi, and M. K. Sabariah, "Implementasi Manajemen Risiko pada Aplikasi XYZ dengan Pendekatan SNI ISO/IEC 27005:2018," 2023.
[12] A. Subagyo, R. Simanjutak, and A. I. Bukit, *Dasar-Dasar Manajemen Risiko*. 2020. [Online]. Available: www.mitrawacanamedia.com
[13] N. Safaat, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 (Studi Kasus: Sistem Infrastruktur Ti Telkom Indonesia)," 2011.
[14] J. Sirajuddin, A. Rajjani, B. T. Hanggara, and Y. T. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12," 2021. [Online]. Available: http://j-ptiik.ub.ac.id
[15] E. J. Wibowo and K. Ramli, "Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute," 2022.
[16] ISO/IEC, "ISOIEC 27005:2018 Information technology — Security techniques — Information security risk management," 2018.

[17] R. A. Setiawan and W. Wasilah, "Evaluasi Tata Kelola Dan Manajemen Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung Selatan," 2022.
[18] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2018.
[19] A. P. Putra and B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," 2023. [Online]. Available: www.ijacsa.thesai.org
[20] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di PT Serasi Autoraya Menggunakan ISO 31000," 2019.