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. 2448-2458

ANALISIS *IT RISK MANAGEMENT* DENGAN MENGGUNAKAN *FRAMEWORK* COBIT 2019 Pada Risk Profile *Logical Attacks, Program and Projects Lifecycle Management, Software Adoption/Usage Problems,* dan *Unauthorized Actions* (Studi Kasus: PT XYZ)

Raif Fawwazdzaky*[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; COBIT 2019; ISO 27005; NIST SP 800-53

Keywords: *Risk Management; Information Technology; COBIT 2019;, ISO 27005;* NIST SP 800-53

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:
raifwzdky@student.telkomuniversity.ac.id

ABSTRAK
PT XYZ adalah perusahaan yang beroperasi di bidang *Maintenance, Repair, and Overhaul* (MRO). PT XYZ memiliki divisi ERM yang mengelola risiko, namun belum ada pendekatan khusus untuk mengelola risiko di unit IT. Hal ini dapat menyebabkan risiko terkait teknologi informasi belum terkelola dengan baik dan berpotensi mengganggu kegiatan operasional perusahaan. Penelitian ini memiliki tujuan untuk mengevaluasi potensi risiko yang mungkin muncul dalam kegiatan operasional unit IT PT XYZ, serta memberikan rekomendasi untuk menerapkan rekomendasi untuk penerapan manajemen risiko yang efektif. Dalam penelitian ini, *framework* ISO 27005 dipilih sebagai standar untuk pengelolaan risiko, sementara identifikasi risiko dilakukan dengan mengadopsi COBIT 2019 sebagai referensi daftar risiko. Data diperoleh melalui kuesioner dan wawancara dengan *stakeholder* terkait. Hasil penelitian ini mengidentifikasi 23 risiko, terdiri dari 8 risiko yang memiliki tingkat risiko *Low*, 7 risiko yang memiliki tingkat risiko *Medium*, 5 risiko yang memiliki tingkat risiko *High*, dan 3 risiko yang memiliki tingkat risiko *Crisis*. Dari total 23 risiko tersebut, 15 diantaranya akan diprioritaskan untuk penanganan dengan kontrol yang sesuai menggunakan *framework* COBIT 2019 dan NIST SP 800-53 sebagai panduan tambahan. Langkah-langkah ini diambil untuk memastikan bahwa risiko-risiko tersebut dapat dikelola secara efektif, sehingga diharapkan dapat meningkatkan efisiensi operasional unit IT di PT XYZ, meminimalkan potensi gangguan, dan mendukung keberlanjutan bisnis perusahaan.

ABSTRACT
PT XYZ operates in the Maintenance, Repair, and Overhaul (MRO) sector and has an Enterprise Risk Management (ERM) division responsible for managing risks. However, there is currently no specific approach for managing risks within the IT unit. This gap may result in inadequately managed IT-related risks, potentially disrupting the company's operational activities. This study aims to evaluate potential risks arising from the IT unit's operational activities at PT XYZ and to provide recommendations for implementing effective risk management practices. ISO 27005 has been selected as the standard for risk management, while risk identification is conducted using COBIT 2019 as a reference. Data was collected through questionnaires and interviews with relevant stakeholders. The study identifies 23 risks, categorized as 8 Low, 7 Medium, 5 High, and 3 Crisis. Of these, 15 risks are prioritized for management with appropriate controls, guided by COBIT 2019 and NIST SP 800-53. These steps are intended to ensure effective management of these risks, enhancing operational efficiency in PT XYZ's IT unit, minimizing potential disruptions, and supporting the company's business continuity.

.

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. 2448-2458

I. PENDAHULUAN

RISIKO adalah aspek yang tak terhindarkan dan selalu dihadapi oleh setiap perusahaan [1]. Tanpa persiapan yang matang, perusahaan berisiko menghadapi konsekuensi serius yang dapat berakibat fatal dan menimbulkan kerugian signifikan [2]. Dalam era teknologi informasi, banyak faktor yang dapat menimbulkan risiko bagi perusahaan. Oleh karena itu, diperlukan langkah-langkah untuk mendeteksi risiko baik di dalam maupun di luar perusahaan, yang mengharuskan adanya sistem untuk menemukan risiko tersebut, sehingga penerapan manajemen risiko pada suatu perusahaan harus dilakukan [3].

Manajemen risiko adalah sistem komprehensif yang melibatkan kebijakan, prosedur, dan praktik untuk mengendalikan dan meminimalkan risiko, dengan tujuan akhir meningkatkan nilai perusahaan [4]. Manajemen risiko melibatkan proses identifikasi risiko, menilai besarannya, dan menerapakan langkah-langkah yang sesuai untuk mengurangi risiko hingga mencapai tingkat yang dapat diterima oleh perusahaan [5]. Manajemen risiko membantu perusahaan untuk mengambil langkah-langkah yang tepat dalam meminimalkan dampak yang mungkin terjadi [6]. Dengan menerapkan manajemen risiko, perusahaan dapat mempengaruhi kinerjanya secara signifikan. Dalam dunia Teknologi Informasi (TI) yang penuh ketidakpastian, manajemen risiko membantu perusahaan untuk mengantisipasi, mengelola, dan merespons risiko dengan cara yang mengurangi potensi kerugian serta memaksimalkan peluang [7].

PT XYZ merupakan perusahaan yang bergerak di bidang pemeliharaan dan perbaikan pesawat, atau yang dikenal dengan *Maintenance, Repair, and Overhaul* (MRO). Di samping fokus pada MRO, PT XYZ juga memiliki unit Teknologi Informasi (TI) yang berperan penting dalam menunjang operasional bisnisnya. Teknologi informasi sangat diperlukan untuk mewujudkan rencana jangka panjang perusahaan. Namun, tanpa manajemen risiko yang tepat di unit TI, potensi masalah dapat mengganggu pencapaian tujuan perusahaan. Meskipun PT XYZ sudah memiliki divisi *Enterprise Risk Management* (ERM), unit TI belum memiliki pendekatan khusus dalam mengelola risikonya. Divisi *Innovation & IT Project Management* menyadari pentingnya peran TI, tetapi risiko-risiko TI masih berpotensi tidak tertangani dengan baik. Penelitian ini bertujuan untuk mengevaluasi risiko yang mungkin muncul di unit TI PT XYZ dan memberikan rekomendasi manajemen risiko yang lebih efektif, sehingga mendukung rencana jangka panjang perusahaan serta meminimalkan dampak risiko.

Penelitian ini menggunakan framework ISO 27005 sebagai acuan utama dalam pengelolaan risiko di unit TI PT XYZ, dengan fokus pada analisis risiko keamanan informasi. Selain itu, framework COBIT 2019 akan digunakan untuk menentukan kontrol yang diperlukan, sementara standar NIST SP 800-53 diterapkan sebagarisiko *Logical Attack*. Perbandingan ketiga framework ini dilakukan untuk menilai efektivitasnya, di mana ISO 27005 fokus pada penilaian risiko, COBIT 2019 memberikan panduan luas untuk kontrol manajemen TI, dan NIST SP 800-53 menawarkan kontrol yang lebih terperinci. COBIT 2019 juga digunakan dalam proses identifikasi risiko, dengan mengacu pada *Figure 2.7 — Risk Profile Design Factor (IT Risk Categories)*. Untuk mendukungnya, penelitian ini akan mengumpulkan data melalui penyebaran kuesioner dan wawancara. Kuesioner akan memberikan data yang diperlukan untuk penilaian risiko, sementara wawancara akan dilakukan untuk mengevaluasi hasil kuesioner serta mengumpulkan informasi tambahan yang diperlukan. Dengan menerapkan ISO 27005, COBIT 2019, dan NIST SP 800-53, penelitian ini menerapkan identifikasi risiko berdasarkan kategori *risk profile* yang disediakan dalam COBIT *2019*. Fokus utama yang berbeda adalah penggunaan pendekatan ini, yaitu menggunakan pengelompokan risiko yang memungkinkan analisis mendalam serta praktis dalam manajemen risiko TI yang memberikan wawasan baru dan relevan tentang pengelolaan risiko yang lebih terstruktur dan terperinci.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif yang mendalam untuk pengumpulan dan pengolahan data. Setelah data dari kuesioner dan wawancara terkumpul, langkah selanjutnya adalah menganalisis tanggapan responden dengan mengidentifikasi setiap jawaban responden. Setiap risiko kemudian dievaluasi lebih lanjut untuk memahami perspektif responden terhadap risiko yang dihadapi, sehingga dapat terdapat gambaran yang jelas mengenai persepsi risiko di perusahaan. Pengumpulan data primer dilakukan dengan menyebarkan kuesioner kepada 16 narasumber dari berbagai departemen di PT XYZ, termasuk *Innovation & Digital Transformation*. Tujuannya adalah untuk mendapatkan pandangan mengenai risiko dari pihak yang memahami secara mendalam potensi risiko yang dihadapi perusahaan. Setelah semua kuesioner terkumpul, dilakukan wawancara lanjutan guna memverifikasi dan memperdalam hasil yang diperoleh.

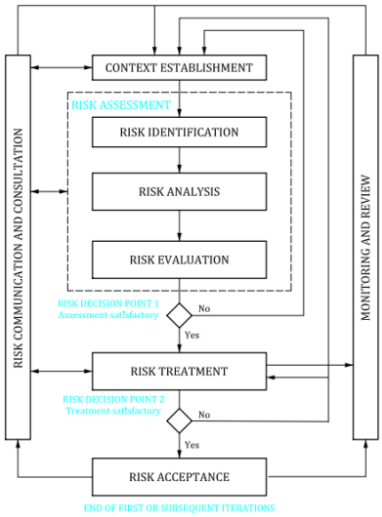
Data yang telah terkumpul kemudian dianalisis dengan menggunakan framework ISO 27005 yang secara khusus berfokus pada manajemen risiko keamanan informasi, yang disesuaikan dengan topik utama penelitian ini, yaitu manajemen risiko TI. Proses analisis mencakup beberapa tahap, mulai dari identifikasi, analisis, hingga evaluasi risiko. Hasil dari analisis kualitatif tersebut akan diimplementasikan ke dalam elemen-elemen yang terdapat dalam ISO 27005. Dengan cara ini, setiap risiko yang teridentifikasi dapat dianalisis secara sistematis sesuai dengan

metode yang disarankan oleh framework. Selanjutnya, dilakukan tahap *risk treatment* untuk menentukan langkah-langkah pengendalian yang paling tepat. COBIT 2019 dan NIST SP 800-53 dipilih karena terdapat relevansi kontrol terhadap risiko yang telah diidentifikasi, efektivitasnya dalam mengurangi dampak risiko, serta kecocokannya dengan konteks penelitian ini. Rekomendasi kontrol kemudian diprioritaskan berdasarkan analisis risiko, dengan mempertimbangkan seberapa besar risiko tersebut dan pengaruhnya terhadap tujuan bisnis. Proses prioritisasi ini menggunakan pendekatan berbasis risiko, sehingga kontrol yang paling efektif dalam mengurangi risiko besar mendapatkan prioritas lebih tinggi.

A. Manajemen Risiko Teknologi Informasi

Manajemen risiko melibatkan proses identifikasi, analisis, dan penanganan risiko dengan tujuan mengurangi dampaknya pada proses bisnis organisasi, sehingga melalui analisis ini perusahaan dapat melindungi aset informasi dari berbagai ancaman, seperti kebocoran data, penggunaan akses *user*, dan lainnya [8]. Manajemen risiko teknologi informasi penting bagi perusahaan dikarenakan dapat mengindentifikasi, menilai, mengelola risiko seperti serangan malware dan kerusakan perangkat keras yang pada akhirnya mendukung pencapaian tujuan bisnis perusahaan [9]. Manajemen Risiko Teknologi Informasi memiliki pendekatan sistematis untuk mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan penggunaan teknologi informasi dalam organisasi, yang berfungsi sebagai dasar perencanaan, pengambilan keputusan, serta untuk meminimalkan potensi kerugian yang dapat timbul dari ancaman terhadap sistem TI [10].

B. *Framework* ISO 27005



GAMBAR 1
Framework ISO 27005

Menurut [11], *framework* ISO 27005 memiliki proses penilaian dan penanganan risiko dilakukan secara berulang, dimulai dengan evaluasi konteks awal dan penilaian risiko. Jika informasi yang diperoleh belum cukup untuk menentukan tindakan yang diperlukan guna mencapai tingkat risiko yang dapat diterima, proses tersebut diulangi dengan konteks yang direvisi. Keefektifan penanganan risiko bergantung pada hasil penilaian risiko, dan jika tingkat risiko yang tersisa belum memadai, siklus penilaian risiko dilakukan kembali. Pada akhirnya, risiko yang tersisa harus disetujui secara eksplisit oleh direksi organisasi. Menurut [12], Penggunaan *framework* ISO 27005 dapat digunakan untuk mengatasi permasalahan dalam penelitian untuk menjawab permasalahan dalam sistem informasi dan pemeliharaan sekaligus pengukuran pada suatu perusahaan yang belum mempertimbangkan penilaian risiko dalam penggunaannya. ISO 27005 merupakan bagian dari keluarga ISO 27000 yang memiliki fokus utama pada manajemen risiko keamanan informasi yang memiliki tahapan *risk assessment, risk treatment, monitoring and consulting* [13]. ISO 27005 membantu organisasi dalam mengidentifikasi, menilai, mengevaluasi, dan menangani kerentanan keamanan, serta menekankan pentingnya pemahaman aset meskipun tidak menyediakan metode spesifik untuk menghitung nilai aset, dan menyadari bahwa penilaian risiko dapat bersifat subjektif dan dipengaruhi oleh penilaian evaluator [14].

C. COBIT 2019

COBIT 2019 adalah kerangka kerja terkait tata kelola teknologi informasi yang dirancang untuk seluruh organisasi yang mencakup semua proses yang melibatkan teknologi dan informasi untuk mencapai tujuan organisasi [15]. Melakukan implementasi kontrol COBIT 2019 berguna untuk mencapai tujuan organisasi dengan memaksimalkan nilai dari manajemen TI, COBIT 2019 juga membantu perusahaan untuk mengelola sistem TI secara

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. 2448-2458

efektif dan seimbang serta diharapkan dapat mengurangi potensi risiko yang mengoptimalkan penggunaan sumber daya organisasi [16]. COBIT 2019, sebagai versi terbaru dari COBIT 5, menawarkan panduan yang lebih lengkap untuk mengidentifikasi serta mengelola aktivitas kontrol risiko TI dalam organisasi [17].

D. NIST SP 800-53

NIST SP 800-53 adalah dokumen atau buku pedoman yang merangkum berbagai kontrol untuk membantu organisasi mengamankan informasi dengan panduan menyeluruh dalam menilai dan mengelola risiko, penerapan kontrol menggunakan NIST SP 800-53 diharapkan untuk memanfaatkan teknologi informasi agar menjadi efektif dan efisien [15]. NIST SP 800-53 merupakan standar yang mencakup prosedur untuk menilai keamanan informasi serta kontrol keamanan yang dapat diterapkan pada sistem informasi dan dalam organisasi [18].

E. Perbandingan *Framework* ISO 27005 dengan COSO ERM

Framework ISO 27005 berfokus kepada manajemen risiko keamanan informasi, memberikan panduan rinci untuk identifikasi, analisis, evaluasi, dan pengelolaan risiko dalam suatu organisasi [19]. Sedangkan untuk COSO ERM berfokus mengelola risiko perusahaan secara keseluruhan yang memiliki langkah yang kompleks dan berlapis-lapis dan menangkap konsep yang penting bagi perusahaan secara efektif untuk mencapai tujuan [20]. ISO 27005 dipilih sebagai *framework* yang digunakan pada penelitian ini terkait manajemen risiko TI, sementara COSO ERM dapat digunakan sebagai pelengkap untuk mengelola risiko lain yang mempengaruhi tujuan perusahaan.

III. HASIL DAN PEMBAHASAN

A. Analisis Data

1) Ruang lingkup dan Aset Teknologi Informasi

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

Pada Tabel 1, Dijelaskan bahwa penelitian ini mencakup sejumlah aset yang dibagi menjadi tiga komponen utama, yaitu layanan, infrastruktur, dan aplikasi. Dalam komponen layanan, terdapat XPREAM, yaitu sebuah sistem manajemen kinerja perusahaan dan IT Service Desk yang menyediakan layanan IT bagi user. Pada komponen infrastruktur, terdapat server yang mendukung berbagai aplikasi dan layanan IT perusahaan, serta laptop dan PC yang digunakan oleh karyawan untuk operasional sehari-hari. Sedangkan dalam komponen aplikasi, terdapat SAP Swift, sistem ERP yang mengelola berbagai aspek bisnis, serta aplikasi operasional internal seperti XOPS, AMS APPS, dan HIL APPS.

2) Kriteria *Likelihood*

Kriteria likelihood digunakan untuk menilai seberapa besar kemungkinan suatu risiko akan terjadi, sehingga penilaian risiko yang dihasilkan sesuai dengan ketentuan yang diharapkan. Berikut dijelaskan pada Tabel 2.

TABEL 2
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**
Likely	Risiko tersebut terjadi berulang-ulang	10 ≤ X ≤ 12 kali	**4**
Certain	Risiko hampir tidak dapat dihindari	> 12 kali	**5**

3) Kriteria Dampak/*Consequennce*

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. 2448-2458

Kriteria dampak atau consequence adalah panduan untuk menilai sejauh mana risiko dapat memengaruhi perusahaan, sehingga besaran risiko yang telah diidentifikasi dapat diukur sesuai dengan standar yang ditetapkan. Berikut dijelaskan pada Tabel 3.

TABEL 3
KRITERIA LIKELIHOOD

Consequence (C)		Score
Insignificant	Tidak ada efeknya atau pengaruhnya sangat kecil ter-hadap 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 menyebab-kan tidak dapat tercapai tujuan organisasi	**5**

4) Matriks Risiko

Matriks risiko digunakan untuk menentukan besaran risiko dengan mempertimbangkan *likelihood* dan *consequence*. Dari matriks risiko ini, akan dihasilkan ukuran risiko untuk setiap *risk register*, yang kemudian menunjukkan tingkat risiko yang perlu ditangani oleh perusahaan.

TABEL 4
MATRIKS RISIKO

Matriks Risiko					
5 (*Certain*)	5 (*Medium*)	10 (*High*)	15 (*High*)	20 (*Crisis*)	25 (*Crisis*)
4 (*Likely*)	4 (*Low*)	8 (*Medium*)	12 (*High*)	16 (*Crisis*)	20 (*Crisis*)
3 (*Possible*)	3 (*Low*)	6 (*Medium*)	9 (*High*)	12 (*High*)	15 (*High*)
2 (*Unlikely*)	2 (*Low*)	4 (*Low*)	6 (*Medium*)	8 (*Medium*)	10 (*High*)
1 (*Rare*)	1 (*Low*)	2 (*Low*)	3 (*Low*)	4 (*Low*)	5 (*Medium*)
Likelihood/ Consequence	1 (*Insignificant*)	2 (*Minor*)	3 (*Moderate*)	4 (*Major*)	5 (*Catastropic*)

B. Penilaian Risiko

Penilaian risiko merupakan langkah pertama dalam proses manajemen risiko. Tahap ini meliputi tiga proses inti, yaitu mengidentifikasi risiko, menganalisis risiko, dan mengevaluasi risiko. Setelah proses penilaian risiko selesai, tahap selanjutnya adalah penanganan risiko, di mana setiap risiko yang telah dianalisis akan diberikan tindakan yang sesuai berdasarkan hasil penilaian tersebut.

1) Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengidentifikasi potensi risiko yang mungkin terjadi, sehingga perusahaan dapat memahami frekuensi dan dampak dari risiko tersebut. Hal ini penting agar perusahaan dapat menentukan fokus penanganan risiko secara tepat. Pada Tabel 5, daftar risiko diadaptasi dari COBIT 2019 Design Guide, tepatnya *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)*. Penetapan dan pemilihan *risk profile* ini dilakukan oleh perusahaan dan kemudian disesuaikan dengan prioritas yang telah ditetapkan.

TABEL 5
IDENTIFIKASI RISIKO

Risk ID	Risk Profile	Risiko	Nilai *Consequence*	Nilai *Likelihood*
R36	*Logical attacks (hacking, malware, etc.)*	Spionase industri	3	2
R37		Pengguna tidak sah (internal) yang mencoba membobol sistem	2	1
R38		Gangguan layanan akibat serangan *denial-of-service* (DoS)	1	1
R39		Serangan malware	2	4
R40		Hacktivisme	5	1

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. 2448-2458

R41		Perusakan situs web	5	2
R42		Karyawan yang tidak puas mengimplementasikan bom waktu yang mengakibatkan hilangnya data	2	1
R43		Data perusahaan dicuri melalui akses tidak sah yang diperoleh melalui serangan phishing	2	1
R44		Serangan pemerintah asing terhadap sistem penting	2	3
R45	*Program and projects lifecycle management*	Melebihi anggaran untuk proyek I&T.	4	5
R46		Kegagalan dari senior manajemen untuk menghentikan proyek-proyek yang gagal (karena biaya melonjak, penundaan berlebihan, *scope creep*, perubahan prioritas bisnis)	4	1
R47		Kurangnya kualitas pada proyek-proyek I&T	3	2
R48		Keterlambatan pada proyek-proyek I&T	4	5
R49		Kegagalan pihak ketiga (*outsourcer*) untuk men-deliver proyek sesuai dengan perjanjian kontrak (kombinasi anggaran yang melebihi, masalah kualitas, fungsionalitas yang hilang, keterlambatan pengiriman)	5	3
R50	*Software adoption/usage problems*	Tidak diadopsinya perangkat lunak aplikasi baru oleh pengguna	4	3
R51		Ketidaksesuaian perangkat lunak dengan kebutuhan bisnis	4	3
R52		Penggunaan perangkat lunak baru yang tidak efisien oleh pengguna	2	5
R53		Ketidakcocokan dengan sistem yang sudah ada	4	2
R61	*Unauthorized actions*	Modifikasi atau manipulasi perangkat lunak yang disengaja sehingga menghasilkan data yang salah	3	1
R62		Modifikasi atau manipulasi perangkat lunak yang disengaja yang mengarah pada tindakan penipuan	3	1
R63		Modifikasi perangkat lunak yang tidak disengaja yang menyebabkan hasil yang tidak akurat	3	3
R64		Merusak perangkat lunak	4	1
R65		Kesalahan konfigurasi dan manajemen perubahan yang tidak disengaja	3	2

2) Penanganan Risiko

Tahap penanganan risiko dilakukan untuk menentukan jenis penanganan dan pemilik risiko berdasarkan level risiko pada masing-masing daftar risiko. Pada Tabel 6, dijelaskan bagaimana penentuan penanganan risiko pada masing-masing risiko yang sudah dinilai.

TABEL 6
PENANGANAN RISIKO

Risk ID	Level Risiko	Penanganan Risiko	Penanggung Jawab Risiko
R36	***MEDIUM***	*MODIFICATION*	SM INNOVATION & DIGITAL TRANSFORMATION
R37	***LOW***	*RETENTION*	ICT ANALYST (IT SECURITY OFFICER)
R38	***LOW***	*RETENTION*	ICT ANALYST (IT SECURITY OFFICER)
R39	***MEDIUM***	*MODIFICATION*	ICT ANALYST (IT SECURITY OFFICER)
R40	***MEDIUM***	*MODIFICATION*	ICT ANALYST (IT SECURITY OFFICER)
R41	***HIGH***	*SHARING / TRANSFER*	MGR DIGITAL SOLUTION
R42	***LOW***	*RETENTION*	ICT ANALYST (IT SECURITY OFFICER)
R43	***LOW***	*RETENTION*	ICT ANALYST (IT SECURITY OFFICER)
R44	***MEDIUM***	*MODIFICATION*	ICT ANALYST (IT SECURITY OFFICER)
R45	***CRISIS***	*MODIFICATION*	• SM INNOVATION & DIGITAL TRANSFORMATION • SM ERP SYSTEM & IT SERVICE DELIVERY
R46	***LOW***	*RETENTION*	• SM INNOVATION & DIGITAL TRANSFORMATION • SM ERP SYSTEM & IT SERVICE DELIVERY
R47	***MEDIUM***	*MODIFICATION*	• SM INNOVATION & DIGITAL TRANSFORMATION • SM ERP SYSTEM & IT SERVICE DELIVERY

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. 2448-2458

R48	***CRISIS***	*MODIFICATION*	• SM INNOVATION & DIGITAL TRANSFORMATION • SM ERP SYSTEM & IT SERVICE DELIVERY
R49	***HIGH***	*MODIFICATION*	• SM INNOVATION & DIGITAL TRANSFORMATION • SM ERP SYSTEM & IT SERVICE DELIVERY • MGR PROCUREMENT CONTRACT
R50	***HIGH***	*MODIFICATION*	• MGR DIGITAL SOLUTION • MGR IT SERVICE DELIVERY • ICT ANALYST (IT ASET OFFICER) ICT ANALYST (IT BUSINESS ANALYST OFFICER)
R51	***HIGH***	*MODIFICATION*	• MGR DIGITAL SOLUTION MGR IT SERVICE DELIVERY
R52	***HIGH***	*MODIFICATION*	• MGR DIGITAL SOLUTION MGR IT SERVICE DELIVERY
R53	***MEDIUM***	*MODIFICATION*	• MGR DIGITAL SOLUTION MGR IT SERVICE DELIVERY
R61	***LOW***	*RETENTION*	MGR DIGITAL SOLUTION
R62	***LOW***	*RETENTION*	MGR DIGITAL SOLUTION
R63	***HIGH***	*MODIFICATION*	• MGR DIGITAL SOLUTION ICT ANALYST (IT WEB QA OFFICER)
R64	***LOW***	*RETENTION*	• MGR DIGITAL SOLUTION ICT ANALYST (IT WEB QA OFFICER)
R65	***MEDIUM***	*MODIFICATION*	• MGR DIGITAL SOLUTION • MGR IT SERVICE DELIVERY • ICT ANALYST (IT BUSINESS ANALYST OFFICER)

C. Penetapan Kontrol

Penetapan kontrol proses ditetapkan kepada risiko yang dinilai membutuhkan tahapan kontrol. Penentuan kontrol sudah melalui tahap evaluasi dan validasi terhadap *stakeholder* dan penanggung jawab risiko terkait untuk memastikan bahwa kontrol yang diterapkan selaras dengan situasi yang sedang dihadapi perusahaan saat ini. Berikut dijelaskan bagaimana penetapan kontrol dari masing-masing risiko yang telah dinilai pada Tabel 7.

TABEL 7
PENETAPAN KONTROL

Risk ID	Judul Kontrol	Deskripsi	Dokumen Terkait
R36	**DSS05.07** - *Manage vulnerabilities and monitor the infrastructure forsecurity-related events.*	Menggunakan portofolio alat dan teknologi, kelola kerentanan dan pantau infrastruktur dari akses tidak sah. Pastikan bahwa alat, teknologi, dan deteksi keamanan terintegrasi dengan pemantauan umum kejadian dan manajemen insiden.	SOP keamanan infrastruktur
R37	**APO13.01** - *Establish and maintain an information security management system (ISMS).* **APO13.03** - *Monitor and review the information security managementsystem (ISMS).*	Bangun dan pelihara *information security management system* (ISMS) yang standar, formal. Komunikasikan dan mengumpulkan analisis data ISMS untuk meningkatkan efektivitasnya dan memperbaiki ketidaksesuaian agar tidak terulang kembali.	-
R38	**DSS05.01** – *Protect against malicious software*	Menerapkan dan mempertahankan langkah-langkah pencegahan, deteksi, dan perbaikan, termasuk pembaruan patch keamanan dan kontrol virus, untuk melindungi sistem informasi perusahaan dari perangkat lunak berbahaya.	-
R39	**DSS05.01** – *Protect against malicious software.*	Menerapkan dan mempertahankan langkah-langkah pencegahan, deteksi, dan perbaikan, termasuk pembaruan patch keamanan dan kontrol virus, untuk melindungi sistem informasi perusahaan dari perangkat lunak berbahaya.	SOP *Internet Policy*

R40	**DSS05.04** – *Manage user identity and logical access*. **SI-3** – *Malicious code(malware) protection.* **SA-15** – *Development process, standards, and tools.*	Memastikan hak akses informasi sesuai kebutuhan bisnis dan koordinasikan dengan unit terkait. Melindungi sistem dari malware dengan teknologi yang tepat dan terapkan kontrol konfigurasi ketat untuk menjaga integritas alat dan proses pengembangan.	SOP *Internet Policy*, Kebijakan *user access*
R41	**DSS05.04** – *Manage user identity and logical access*. **AC-22** – P*ublicly accessible content.* **SI-3** – *Malicious code(malware) protection.* **SA-15** – *Development process, standards, and tools.*	Mengelola hak akses pengguna sesuai kebutuhan bisnis, melindungi sistem dari malware, dan kontrol integritas alat pengembangan. Pastikan publik tidak mengakses informasi non-publik sesuai hukum dan kebijakan organisasi.	SOP kerentanan aplikasi/web
R42	**DSS05.07** – *Manage vulnerabilities and monitor the infrastructure forsecurity-related events.*	Mengelola kerentanan dan pantau infrastruktur dengan alat deteksi. Integrasikan alat keamanan dengan pemantauan acara dan manajemen insiden.	-
R43	**BAI08.03** – *Use and share knowledge* **DSS05.01** – *Protect against malicious software*	Menerapkan langkah pencegahan dan kontrol virus terbaru untuk melindungi sistem dari perangkat lunak berbahaya. *Sharing knowledge* kepada pihak terkait untuk mendukung berbagai kebutuhan, seperti pemecahan masalah dan perencanaan strategis.	-
R44	**DSS05.07** – *Manage vulnerabilities and monitor the infrastructure forsecurity-related events*	Mengelola kerentanan dan pemantauan infrastruktur untuk mengidentifikasi dan merespons kejadian keamanan secara efektif.	SOP keamanan infrastruktur
R45	**APO06.04** – Model and allocate costs **AP006.05** – Manage costs. **APO02.06** – Communicate the I&T strategy and direction.	Menentukan dan mengalokasikan biaya proyek, pemantauan biaya proyek, serta mengembangkan strategi komunikasi I&T yang efektif.	Kebijakan penganggaran proyek
R46	**APO05.01** – *Determine the availability and sources of funds* **BAI01.09** – *Close a program.*	Menentukan sumber dana serta dampaknya terhadap pengembalian investasi. Menghapus program dari portofolio jika nilai yang diinginkan tercapai atau tidak mungkin tercapai.	-
R47	**BAI11.07** - *Monitor and control projects.*	Memantau dan mengendalikan proyek dengan menerapkan kriteria proyek, pelaporan kemajuan proyek, mengelola perubahan, dan menilai kinerja setiap proyek.	Prosedur penyediaan TI
R48	**BAI01.06** - *Monitor, control and report on the program outcomes.* **BAI01.05** - *Launch and execute the program.* **BAI01.04** - *Develop and maintain the program plan.*	Mengawasi dan kontrol kinerja proyek dengan melaporkan hasil secara komprehensif kepada manajemen terkait untuk menghindari keterlambatan pengerjaan proyek.	Prosedur penyediaan TI
R49	**APO10.04** - *Manage vendor risk.* **APO10.05** - *Monitor vendor performance and compliance.*	Mengelola risiko terkait vendor dan memantau kinerja serta mendukung kepatuhan vendor untuk mendukung manajemen *lifecycle* terkait program dan proyek.	Kontrak perjanjian dengan vendor
R50	**BAI07.01** - *Establishing an Implementation Plan.* **BAI11.01** - *Maintain a standard approach for project management.*	Mengatur rencana implementasi yang terstruktur serta memelihara standar untuk manajemen proyek.	-
R51	**APO03.01** – *Develop the Enterprise Architecture Vision.* **BAI03.02** – *Design detailed solution components.*	Mengembangkan *enterprise architecture vision* perusahaan dan merancang komponen solusi secara terperinci untuk memastikan kesesuaian dengan proses bisnis perusahaan.	-
R52	**BAI08.03** - *Use and share knowledge.*	Mengadakan kegiatan untuk berbagi pengetahuan terkait penggunaan perangkat lunak terkait.	-
R53	**BAI03.06** - *Perform quality assurance (QA).* **APO03.05** - *Provide enterprise architecture services.*	Memastikan adanya peran *quality assurance* serta keselarasan layanan *enterprise architecture* dengan tujuan strategis dan nilai bisnis.	-
R61	**APO01.05** – *Establish roles and responsibilities.* **APO01.07** – *Define information (data) and system ownership*	Menentukan dan komunikasikan peran serta tanggung jawab untuk I&T perusahaan, termasuk tingkat wewenang dan akuntabilitas. Menetapkan tanggung jawab kepemilikan informasi dan sistem, serta pastikan pemilik mengklasifikasikan dan melindungi informasi sesuai klasifikasinya.	-
R62	**APO14.01** - *Define and communicate the organization's data management strategy and roles and responsibilities.*	Menentukan strategi manajemen dan organisasi sesuai dengan tujuan dan strategi perusahaan. Komunikasikan strategi tersebut kepada semua pihak terkait dan tetapkan peran serta tanggung	-

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. 2448-2458

		jawab untuk memastikan data dikelola sebagai aset penting dan strategi tersebut diterapkan secara efektif.	
R63	**BAI03.06** - *Perform quality assurance (QA).* **BAI03.12** - *Design solutions based on the defined development methodology.*	Memastikan adanya peran *quality assurance* dan merancang solusi sesuai dengan metodelogi pengembangan yang sesuai.	-
R64	**BAI09.03** – *Manage the aset life cycle.*	Mengelola lifecycle aset dari pengadaan hingga pembuangan. Memastikan aset digunakan secara efektif dan efisien, serta terlindungi dan tercatat dengan baik.	-
R65	**DSS06.04** - *Manage errors and exceptions.* **BAI06.01** - *Evaluate, prioritize and authorize change requests.*	Mengelola kesalahan serta mengevaluasi dan mendokumentasikan setiap permintaan perubahan untuk memastikan kepatuhan.	*Change management policy*

D. Prioritas Rekomendasi

Pada Tabel 8, dijelaskan bagaimana penetapan prioritas digunakan untuk melihat risiko yang memiliki besaran risiko tertinggi sampai dengan terkecil.

TABEL 8
PRIORITAS REKOMENDASI

Risk ID	Judul Kontrol	Besaran Risiko	Prioritas
R45	**APO06.04** – Model and allocate costs **AP006.05** – Manage costs. **APO02.06** – Communicate the I&T strategy and direction.	20	1
R48	**BAI01.06** – *Monitor, control and report on the program outcomes.* **BAI01.05** – *Launch and execute the program.* **BAI01.04** – *Develop and maintain the program plan.*	20	2
R49	**APO10.04 –** *Manage vendor risk.* **APO10.05 –** *Monitor vendor performance and compliance.*	15	3
R50	**BAI07.01** – *Establishing an Implementation Plan.* **BAI11.01** – *Maintain a standard approach for project management.*	12	4
R53	**APO03.01** – *Develop the Enterprise Architecture Vision.* **BAI03.02** – *Design detailed solution components.*	12	5
R41	**DSS05.04 –** *Manage user identity and logical access*. **AC-22 –** P*ublicly accessible content.* **SI-3** – *Malicious code(malware) protection.* **SA-15** – *Development process, standards, and tools.*	10	6
R52	**BAI08.03** – *Use and share knowledge.*	10	7
R63	**BAI03.06** – *Perform quality assurance (QA).* **BAI03.12 –** *Design solutions based on the defined development methodology.*	9	8
R39	**DSS05.01** – *Protect against malicious software.*	8	9
R53	**BAI03.06** – *Perform quality assurance (QA).* **APO03.05** – *Provide enterprise architecture services.*	8	10
R36	**DSS05.07** - *Manage vulnerabilities and monitor the infrastructure forsecurity-related events.*	6	11
R44	**DSS05.07** - *Manage vulnerabilities and monitor the infrastructure forsecurity-related events.*	6	12
R47	**BAI11.07** - *Monitor and control projects.*	6	13
R65	**DSS06.04** - *Manage errors and exceptions.* **BAI06.01** - *Evaluate, prioritize and authorize change requests.*	6	14
R40	**DSS05.04** - *Manage user identity and logical access*. **SI-3** - *Malicious code(malware) protection.* **SA-15** - *Development process, standards, and tools.*	5	15

E. *Roadmap* Implementasi

Dalam memberikan rekomendasi kepada perusahaan, roadmap implementasi disusun untuk membantu memprioritaskan risiko yang perlu ditangani terlebih dahulu guna mendukung kesuksesan strategi perusahaan. Tabel 9 menjelaskan bahwa *roadmap* ini dirancang untuk memastikan prioritas risiko yang sesuai dengan pelaksanaan strategi perusahaan.

TABEL 9
ROADMAP IMPLEMENTASI

No.	Judul Kontrol	Q1	Q2	Q3	Q4
1	**APO06.04** - *Model and allocate costs*				
	AP006.05 - *Manage costs.*				
	APO02.06 - *Communicate the I&T strategy and direction.*				
2	**BAI01.06** - *Monitor, control and report on the program outcomes.*				
	BAI01.05 - *Launch and execute the program.*				
	BAI01.04 - *Develop and maintain the program plan.*				
3	**APO10.04** - *Manage vendor risk.*				
	APO10.05 - *Monitor vendor performance and compliance.*				
4	**BAI07.01** - *Establishing an Implementation Plan.*				
	BAI11.01 - *Maintain a standard approach for project management.*				
5	**APO03.01** - *Develop the Enterprise Architecture Vision.*				
	BAI03.02 - *Design detailed solution components.*				
6	**DSS05.04** - *Manage user identity and logical access*.				
	AC-22 - P*ublicly accessible content.*				
	SI-3 - *Malicious code(malware) protection.*				
	SA-15 - *Development process, standards, and tools.*				
7	**BAI08.03** - *Use and share knowledge.*				
8	**BAI03.06** - *Perform quality assurance (QA).*				
	BAI03.12 - *Design solutions based on the defined development methodology.*				
9	**DSS05.01** - *Protect against malicious software.*				
10	**APO03.05** - *Provide enterprise architecture services.*				
11	**DSS05.07** - *Manage vulnerabilities and monitor the infrastructure forsecurity-related events.*				
12	**BAI11.07** - *Monitor and control projects.*				
13	**DSS06.04** - *Manage errors and exceptions.*				
	BAI06.01 - *Evaluate, prioritize and authorize change requests.*				

Pada Tabel 8, tercantum 15 risiko yang diurutkan dari yang tertinggi hingga terendah tetapi masih di atas batas toleransi manajemen risiko perusahaan. Namun, Tabel 9 hanya mencantumkan 13 roadmap implementasi karena beberapa kontrol berlaku untuk beberapa prioritas risiko. Dengan demikian, meskipun ada 15 risiko yang diprioritaskan, implementasi kontrol yang sama dapat menangani beberapa risiko, sehingga hanya diperlukan 13 roadmap.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan pada PT. XYZ, dapat disimpulkan bahwa terdapat 23 identifikasi risiko yang diadopsi dari COBIT 2019, *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)* dengan empat *risk profile* dan dilakukan penetapan oleh perusahaan. Dari penilaian risiko tersebut, 8 risiko dikategorikan berisiko rendah (*Low*), 7 risiko berisiko sedang (*Medium*), 5 risiko berisiko tinggi (*High*), dan 3 risiko berisiko krisis (*Crisis*). Evaluasi lebih lanjut menunjukkan bahwa risiko berisiko rendah tidak memerlukan pengelolaan kontrol lebih lanjut, sementara 15 risiko lainnya yang berkisar dari tingkat risiko sedang hingga krisis akan dikelola dengan kontrol yang sesuai.

Dari 15 risiko tersebut, 14 risiko akan ditangani melalui respon *Modification*, sementara satu risiko yaitu "perusakan situs web" akan dikelola melalui respon *Sharing/Transfer*. Untuk mengelola risiko-risiko ini, *framework* COBIT 2019 digunakan dengan kontrol-kontrol seperti DSS05.07 untuk mengelola kerentanan dan memantau infrastruktur, DSS05.01 untuk melindungi terhadap perangkat lunak berbahaya, serta berbagai kontrol lainnya yang terkait dengan manajemen identitas pengguna, alokasi biaya, dan evaluasi risiko vendor. Selain itu, beberapa kontrol dari NIST SP-800-53 juga diterapkan, termasuk AC-22 untuk konten yang dapat diakses publik, SI-3 untuk perlindungan terhadap kode berbahaya, dan SA-15 untuk proses pengembangan dan standar yang digunakan. Pemilihan kontrol ini bertujuan untuk memberikan rekomendasi yang komprehensif dalam mengelola risiko di divisi IT PT XYZ untuk mendukung keberhasilan operasional perusahaan.

DAFTAR PUSTAKA

[1] I. Setiawan, A. R. Sekarini, R. Waluyo, dan F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, hlm. 389–396, Mei 2021, doi: 10.30812/matrik.v20i2.1093.

[2] J. Ecleas dan A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," 2021. [Daring]. Tersedia pada: http://jurnal.mdp.ac.id

[3] A. P. Putra dan B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," 2023. [Daring]. Tersedia pada: www.ijacsa.thesai.org

[4] Zainal Putra, S. Chan, dan M. Iha, "Desain Manajemen Risiko Berbasis ISO 31000 pada PDAM Tirta Meubaloh," 2017.

[5] T. George Abisay dan Nurhadi, "Manajemen Risiko Pada Bandara Soekarno Hatta Berbasis ISO 31000," 2013.
[6] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, hlm. 128–146, Agu 2020, doi: 10.36596/jcse.v1i2.76.
[7] D. L. Ramadhan, R. Febriansyah, dan R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, hlm. 91, Feb 2020, doi: 10.30865/jurikom.v7i1.1791.
[8] S. Sahira, R. Fauzi, dan 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.
[9] V. P. P. Wijaya dan A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," vol. 9, no. 2, hlm. 1295–1307, 2022.
[10] A. Kurniati, L. Edi Nugroho, dan M. Nur Rizal, "Manajemen Risiko Teknologi Informasi pada e-Government: Ulasan Literatur Sistematis," *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, vol. 22, no. 2, hlm. 207–222, 2020, doi: 10.33164/iptekkom.22.2.2020.207-222.
[11] S. Patino, E. F. Solis, S. G. Yoo, dan R. Arroyo, "ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005," dalam *2018 5th International Conference on eDemocracy and eGovernment, ICEDEG 2018*, Institute of Electrical and Electronics Engineers Inc., Jun 2018, hlm. 75–82. doi: 10.1109/ICEDEG.2018.8372361.
[12] A. Wibowo, "RISK ASSESSMENT RELATED TO PRIVACY INFORMATION ON ELECTRONIC MONEY SERVER-BASED USING ISO 27001 ISO 27005, ISO 27701," *J Theor Appl Inf Technol*, vol. 15, no. 3, 2023, [Daring]. Tersedia pada: www.jatit.org
[13] M. Al Fikri, F. A. Putra, Y. Suryanto, dan K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," dalam *Procedia Computer Science*, Elsevier B.V., 2019, hlm. 1206–1215. doi: 10.1016/j.procs.2019.11.234.
[14] B. Metin, S. Duran, E. Telli, M. Mutlutürk, dan M. Wynn, "IT Risk Management: Towards a System for EnhancingObjectivity in Asset Valuation That Engenders a Security Culture," *Information (Switzerland)*, vol. 15, no. 1, hlm. 9, Jan 2024, doi: 10.3390/info15010055.
[15] H. Ghozie Afiansyah dan A. Amiruddin, "Perancangan Rencana Tata Kelola dan Manajemen Teknologi Informasi Menggunakan COBIT 2019 dan NIST SP 800-53 Rev 5 (Studi Kasus: Instansi Pemerintah ABC)," 2022.
[16] S. Tangprasert, "A Study of Information Technology Risk Management of Government and Business Organizations in Thailand using COSO-ERM based on the COBIT 5 Framework," *J Appl Sci (Thailand)*, vol. 19, no. 1, hlm. 13–24, Jun 2020, doi: 10.14416/j.appsci.2020.01.002.
[17] H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat, dan C. U. Putri, "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk," dalam *Procedia Computer Science*, Elsevier B.V., 2017, hlm. 569–576. doi: 10.1016/j.procs.2017.12.191.
[18] E. Supristiowadi, P. Yudho, dan G. Sucahyo, "Manajemen Risiko Keamanan Informasi Pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," 2018.
[19] ISOIEC, "ISOIEC 270052018 Information technology — Security techniques — Information security risk managem," 2018.
[20] R. R. Moeller, "COSO enterprise risk management: establishing effective governance, risk, and compliance processes (Vol. 560)," 2011.