Analisis *IT Risk Management* Pada Bagian Umum LPP TVRI Jabar Dengan *Framework* ISO/IEC 27005:2022

1st Al Ferdaus Leon Wagge
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
alferdausleon@student.telkomuniversity.ac.id

2nd Widyatasya Agustika Nurtrisha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
widyatasya@telkomuniversity.ac.id

3rd Ridha Hanafi
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ridhanafi@telkomuniversity.ac.id

***Abstrak* — Abstrak LPP TVRI Jabar belum menerapkan proses IT *Risk Management* yang terstruktur dengan bantuan *framework*, proses IT *Risk Management* di Bagian Umum pada LPP TVRI Jabar masih terbatas pada sistem pelaporan kepada *person in charge* (PIC) yang berada di Bagian Umum. Metode yang digunakan di penelitian dilakukan dengan menggabungkan metodologi pendekatan *framework* ISO/IEC 27005:2022 dan *framework* COBIT 2019. *Framework* ISO/IEC 27005:2022 berfokus pada proses IT *Risk Management* di Bagian Umum LPP TVRI Jabar, melalui analisis pengelolaan risiko IT yang tahapannya terdiri dari *Risk Identification, Risk Analysis, Risk Evaluation, dan Risk Treatment.* Sementara *framework* COBIT 2019 berfokus pada proses penetapan kontrol dan prioritas rekomendasi yang didasarkan pada hasil analisis pengelolaan risiko IT yang telah dilakukan melalui ISO/IEC 27005:2022. Selain itu *framework* COBIT 2019 juga digunakan sebagai alat bantu dalam mengidentifikasi risiko berdasarkan kategori *risk profile*, melalui *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)* [1]. Berdasarkan penelitian, terdapat 25 daftar risiko dengan satu (1) risiko level *High*, sebelas (11) risiko level *Medium*, dan tiga belas (13) risiko dengan level *Low*. Berdasarkan 25 daftar risiko yang telah diidentifikasi, risiko-risiko IT tersebut selanjutnya diberikan penanganan risiko serta penetapan kontrol yang mengacu pada *framework* COBIT 2019. Pada jurnal ini, untuk bagian Hasil dan Pembahasan hanya mencakup tahapan *Risk Analysis, Risk Treatment,* dan Penetapan Kontrol Risiko**

Kata kunci* — *IT Risk Management, ISO/IEC 27005:2022, COBIT 2019, LPP TVRI Jabar

I. PENDAHULUAN

Perkembangan *Information Technology* (IT) telah memberikan peranan penting hampir di seluruh aspek kehidupan manusia, terutama pada kemajuan di sektor instansi ataupun bisnis [2]. Penggunaan IT terdiri dari berbagai standar dan regulasi yang dibuat oleh suatu organisasi untuk memastikan bahwa informasi yang dimiliki dapat mencapai tujuan organisasi dan memenuhi kegiatan utama di dalamnya [3].

Berdasarkan proses wawancara dengan pihak LPP TVRI Jabar, diketahui bahwa saat ini LPP TVRI Jabar belum menerapkan proses IT *Risk Management* yang terstruktur dengan bantuan *framework* seperti COBIT 2019 ataupun ISO/IEC 27005:2022. Sehingga, dengan semakin berkembangnya implementasi dan kompleksitas IT yang dihadapi, menunjukkan bahwa pengelolaan risiko IT pada LPP TVRI Jabar belum sepenuhnya efektif. Berdasarkan hasil wawancara yang telah dilakukan, proses IT Risk Management yang ada saat ini dinilai masih bersifat reaktif dan belum terdokumentasi secara sistematis. Seluruh proses manajemen risiko IT hanya bergantung pada pelaporan manual dari pegawai kepada Person in Charge (PIC) saat terjadinya indikasi risiko, tanpa adanya dukungan standar atau pedoman internasional yang mengacu pada framework ISO/IEC 27005:2022 maupun COBIT 2019.

Ketiadaan pedoman dan standar acuan yang terstruktur tersebut pada IT *Risk Management* menimbulkan adanya gap dalam pengelolaan risiko. Kondisi ini mengakibatkan konsekuensi yang signifikan, karena Bagian Umum memiliki peran strategis dalam mendukung kelancaran operasional seluruh unit kerja di LPP TVRI Jabar, melalui pengelolaan sumber daya manusia, perlengkapan aset, serta infrastruktur IT. Meski peran Bagian Umum bersifat *supporting*, tugas dan fungsi dari bagian ini merupakan pondasi utama dalam menjamin keberlangsungan layanan di unit-unit lainnya.

Untuk mencapai solusi atas akar permasalahan tersebut, penelitian ini bertujuan untuk membantu perusahaan dalam menyusun standar dan prosedur yang jelas pada manajemen risiko IT di masa mendatang, dengan menggunakan pendekatan *framework* ISO/IEC 27005:2022. ISO/IEC 27005:2022 merupakan standar internasional yang dirancang khusus untuk pengelolaan risiko teknologi informasi, dengan fokusnya pada aspek keamanan, integritas, dan ketersediaan informasi, meskipun secara spesifik berfokus pada keamanan informasi, *framework* ini juga dapat digunakan untuk memetakan risiko-risiko bisnis yang memiliki keterkaitan langsung dengan risiko IT, melalui tahapan seperti, *risk identification, risk analysis, risk evaluation*, dan *risk treatment*. [4]. Selain menggunakan *framework* ISO/IEC 27005:2022, penelitian ini juga akan menerapkan *framework* COBIT 2019 sebagai alat bantu dalam mengidentifikasi risiko berdasarkan kategori *risk profile*, melalui referensi *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)* [1]. *framework* COBIT 2019 juga berperan sebagai alat bantu dalam menetapkan kontrol dan prioritas rekomendasi sesuai dengan risiko-risiko yang sebelumnya telah dianalisis.

Oleh karena itu, penelitian ini akan memberikan pedoman dan penilaian terbaru terhadap sejauh mana risiko

tersebut dapat diantisipasi dan dikelola dengan menggabungkan *framework* ISO/IEC 27005:2022 sebagai *framework* utama untuk analisis pengelolaan risiko IT (*risk identification, risk analysis, risk evaluation,* dan *risk treatment*), dan *framework* COBIT 2019 untuk identifikasi *risk profile*, penetapan kontrol risiko, dan prioritas rekomendasi atas risiko tersebut.

II. KAJIAN TEORI

Menyajikan dan menjelaskan uraian teori-teori yang terkait dengan permasalahan, kerangka kerja, dan metode pada topik IT Risk Management.

A. Manajemen Risiko Teknologi Informasi

Manajemen Risiko Teknologi Informasi (TI) merupakan metode pendekatan pada sebuah perusahaan untuk mengidentifikasi, menilai, dan mengurangi risiko-risiko yang berhubungan dengan TI. Manajemen Risiko TI digunakan untuk mengatasi aset strategis pada suatu permasalahan atau ancaman aspek teknologi informasi. Proses ini berperan dalam membantu perusahaan untuk menjaga kelangsungan bisnis dengan memastikan sistem operasional tetap berjalan dengan efektif terhadap berbagai potensi Risiko TI [7].

Menurut [8], proses ini juga merupakan langkah penerapan pada aspek Teknologi Informasi (TI) yang memungkinkan para manajer TI untuk melakukan penetapan langkah strategis terkait penyeimbangan pada biaya operasional dan biaya ekonomi, langkah ini dilakukan untuk melindungi aset krusial pada sistem TI dan data yang mendukung pencapaian target bisnis pada perusahaan.

Tahapan dari Manajemen Risiko TI mencakup identifikasi, mitigasi, serta penetapan kontrol terhadap dampak-dampak potensial pada sistem maupun infrastruktur operasional TI,

B. *Framework* ISO/IEC 27005:2022

Framework ISO/IEC 27005:2022 adalah kerangka kerja yang membahas standar internasional, yang digunakan sebagai panduan umum pada manajemen risiko [9]. *Framework* ini digunakan untuk membantu perusahaan yang ingin mengidentifikasi, menilai, dan mengelola risiko secara lebih terstruktur dan terdokumentasi dengan baik, guna menghindari adanya potensi risiko yang mengganggu tujuan strategis dan keberlangsungan operasional perusahaan.

Menurut [4] *framework* ini terdiri dari enam klausul proses, yang mencakup *context establishment, risk assessment, risk treatment, risk acceptance, communication and consultation,* dan *monitoring & review*. Pada penelitian ini, klausul yang akan digunakan dibatasi, hanya mencakup *context establishment, risk assessment, risk treatment (risk modification, risk retention, risk avoidance,* dan *risk sharing), risk acceptance,* dan *communication and consultation.*

C. *Framework* COBIT 2019

COBIT merupakan singkatan dari *Control Objectives for Information and Related Technology,* yang dikembangkan oleh organisasi ISACA. COBIT menyediakan kerangka kerja untuk proses audit, tata kelola, serta pengelolaan teknologi informasi yang mendukung implementasi strategi dan tujuan bisnis perusahaan. Tahapan dari *framework* ini berfungsi untuk memastikan sistem TI perusahaan mampu mendukung fungsi bisnis, mengoptimalkan risiko, dan memastikan nilai yang dihasilkan oleh penggunaan sistem informasi [10].

Penelitian ini menggunakan *framework* COBIT 2019, dikarenakan COBIT 2019 dapat mendukung penggunaan kustomisasi yang lebih fleksibel, serta penyesuaian pedoman tata kelola TI yang akurat, dan penyelarasan yang lebih erat dengan *framework* lainnya, seperti ITIL dan ISO.

Pada penelitian ini, *framework* COBIT 2019 digunakan sebagai alat bantu dalam menentukan penanganan risiko dengan penetapan judul kontrol melalui domain COBIT 2019 [11], sesuai dengan kebutuhan dari masing-masing risiko yang telah diidentifikasi.

D. Domain COBIT 2019

COBIT 2019 memiliki lima domain utama dalam fungsinya sebagai *framework* tata kelola dan manajemen teknologi informasi. Lima domain tersebut terdiri dari satu *Governance Objectives* dan empat *Management Objectives* yang dikelompokkan sesuai dengan tujuan utama dan aktivitas pada area dari setiap objektif [11].

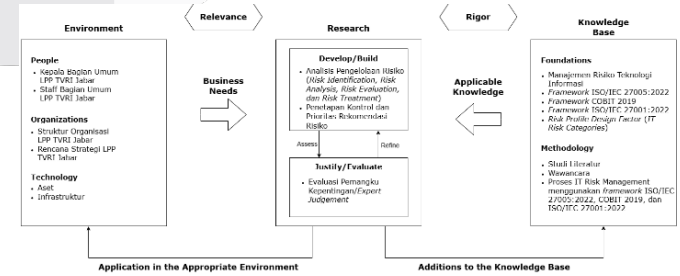
E. *Framework* ISO/IEC 27001:2022

ISO/IEC 27001:2022 adalah standar internasional yang menetapkan *framework* pada konteks praktik keamanan informasi di suatu organisasi. Standar ini membahas mengenai aturan dan prosedur yang diperlukan untuk membentuk, menetapkan, dan mengelola persyaratan dari *Information Security Management System* (ISMS). Pada penelitian ini [12], ISO/IEC 27001:2022 digunakan sebagai alat bantu tambahan dalam menetapkan kontrol, sebagai langkah lanjutan pada hasil analisis pengelolaan risiko IT yang telah dilakukan.

III. METODE PENELITIAN

A. Model Konseptual

Penyusunan model konseptual di penelitian ini menggunakan kerangka konseptual yang dibangun berdasarkan metode dari Alan Hevner [14], sebagai acuan terkait rencana atau penjelasan tentang langkah-langkah yang akan terlibat guna mencapai tujuan penelitian. Gambar 1, merupakan ilustrasi pada model konseptual yang digunakan pada penyusunan penelitian ini.



Gambar 1.
Model Konseptual

Gambar 1, Model Konseptual ini, menjelaskan mengenai tiga bagian utama yang membentuk model konseptual. Bagian *Environment* terdiri dari *People, Organizations*, dan,

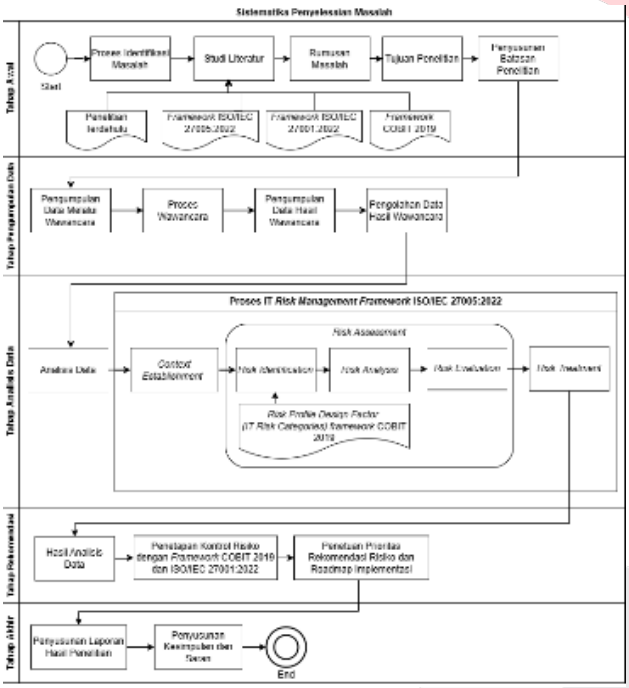
Technology. Ketiga komponen ini menjelaskan tentang lingkungan yang terdapat pada perusahaan atau objek dan pihak-pihak yang terlibat di proses penyusunan penelitian.

Bagian *IS Research* menjelaskan analisis proses penelitian, mulai dari perancangan hingga proses evaluasi. Bagian

Knowledge Base menjelaskan dasar ilmu, terdiri dari teori dasar dan metodologi yang mendukung proses penyusunan penelitian. Mencakup penjelasan dasar-dasar teori mengenai Teknologi Informasi, Manajemen Risiko Teknologi Informasi, *Framework* ISO/IEC 27005:2022, *Framework* COBIT 2019, Domain COBIT 2019, *Framework* ISO/IEC 27001:2022, dan *Risk Profile Design Factor (IT Risk Categories)*.

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah merupakan suatu proses yang disusun dalam bentuk alur dari suatu proses terstruktur untuk mempermudah setiap tahapan, fungsinya adalah sebagai panduan terhadap tahapan cara berpikir dalam menyelesaikan permasalahan yang diangkat pada penelitian ini. Gambar 2, merupakan ilustrasi dari sistematika yang digunakan pada penelitian ini.



Gambar 2.
Sistematika Penyelesaian Masalah

Pada Gambar 2, terdiri dari 5 tahapan terkait proses sistematika penyelesaian masalah, Berikut merupakan penjelasan secara lebih rinci mengenai 5 tersebut:

1. Tahap Awal: Tahap penelitian ini diawali dengan proses identifikasi terhadap penentuan masalah-masalah yang diangkat pada penelitian ini..
2. Tahap Pengumpulan Data: Tahap pengumpulan data dilakukan untuk mengetahui data-data yang dibutuhkan selama proses penelitian ini berlangsung.
3. Tahap Analisis Data: Pada tahap analisis data, akan dilakukan IT *Risk Management* menggunakan *Framework* ISO/IEC 27005:2022. Dan pada *Risk Identification* akan menggunakan referensi *Figure 2.7—Risk Profile Design Factor (IT Risk Categories) framework* COBIT 2019, untuk membantu proses identifikasi risiko berdasarkan *Risk Profile.*
4. Tahap Rekomendasi: Tahap ini, dilakukan untuk mengetahui rekomendasi terhadap penanganan risiko sebelumnya dilakukan menggunakan *framework* ISO/IEC 27005:2022, hasil analisis tersebut selanjutnya akan disusun berdasarkan proses penetapan kontrol dan prioritas rekomendasi risiko yang sesuai dengan *framework* COBIT 2019 dan ISO/IEC 27001:2022.
5. Tahap Akhir: Tahapan ini dilakukan setelah penulis memperoleh hasil analisis, sesuai dengan tujuan penelitian yang sebelumnya telah ditetapkan.

C. Pengumpulan Data

Proses pengumpulan data dalam penelitian ini dilakukan melalui dua metode kualitatif, yaitu wawancara semi-terstruktur dan studi literatur. Pada wawancara semi-terstruktur memanfaatkan proses wawancara secara langsung, dengan melakukan sesi interview dengan tiga perwakilan *staff* Bagian Umum LPP TVRI Jabar. Tujuannya adalah untuk memperoleh informasi secara mendalam mengenai kebutuhan, tantangan, dan permasalahan utama yang dihadapi terkait IT *Risk Management*.

Kemudian untuk studi literatur melibatkan informasi pada sumber-sumber terpercaya seperti, jurnal ilmiah, buku, laporan teknis yang berasal dari media dan internet, serta dokumen-dokumen resmi perusahaan yang berkaitan secara langsung dengan topik penelitian. Tujuannya adalah untuk mengetahui pemahaman yang mendalam mengenai praktik IT *Risk Management* pada Bagian Umum LPP TVRI Jabar.

D. Pengolahan Data

Pengolahan data pada penelitian ini dilakukan dengan menggunakan pendekatan *framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022. Penggunaan ketiga *framework* ini berfokus pada proses IT *Risk Management* di Bagian Umum LPP TVRI Jabar, melalui analisis pengelolaan risiko IT, serta proses penetapan kontrol dan prioritas rekomendasi risiko.

Langkah pertama pengolahan data pada dilakukan dengan melibatkan *framework* COBIT 2019 sebagai alat bantu dalam mengidentifikasi risiko berdasarkan kategori *risk profile*, melalui referensi pada *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)* [1]. Kemudian dilanjutkan dengan analisis pengelolaan risiko IT dengan *framework* ISO/IEC 27005:2022, tahapannya terdiri dari *Risk Identification, Risk Analysis, Risk Evaluation*, dan *Risk Treatment.*

Langkah selanjutnya adalah proses penetapan kontrol dan prioritas rekomendasi risiko dengan *framework* COBIT 2019 dan ISO/IEC 27001:2022, yang didasarkan pada hasil analisis pengelolaan risiko IT yang telah dilakukan sebelumnya, sesuai dengan kontrol dari bagian Domain COBIT 2019 dan ISO/IEC 27001:2022 Annex A.

IV. HASIL DAN PEMBAHASAN

Bagian ini akan menyajikan hasil dari analisis IT *Risk Management* di Bagian Umum LPP TVRI Jabar menggunakan *framework* ISO/IEC 27005:2022.

A. Matriks Risiko

Matriks Risiko merupakan metode perhitungan skor pada manajemen risiko yang fungsinya adalah untuk mengidentifikasi, menilai, serta menganalisis sebuah risiko yang terjadi pada organisasi. Matriks ini terdiri dari dua komponen penilaian, yaitu penilaian terhadap komponen dampak (*impact*) dan kemungkinan (*likelihood).* Penentuan matriks ini mengacu pada referensi [15]. Sehingga matriks ini akan menentukan prioritas dari penanganan suatu risiko berdasarkan besaran pengkategorian tingkat parameter pada komponen dampak (*impact*) dan kemungkinan (*likelihood*). Tabel 1, merupakan matriks risiko yang digunakan pada penelitian ini.

Tabel 1.
Matriks Risiko

			Impact				
			Insignificant	***Minor***	***Moderate***	***Major***	***Catastrophic***
			1	**2**	**3**	**4**	**5**
Likelihood	***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
	Very Likely	**5**	5	10	15	20	25

Kemudian, besaran skor suatu risiko ditentukan berdasarkan perhitungan dari komponen dampak (*impact*) dan kemungkinan (*likelihood*). Seperti yang ditunjukkan pada Tabel 2, jumlah dari besaran suatu risiko akan menentukan hasil dari level risiko tersebut

Tabel 2.
Level Risiko

No	Level Risiko	Besaran Risiko	Keterangan Risiko
1.	*Low*	1 s.d 4	
2.	*Medium*	5 s.d 8	
3.	*High*	9 s.d 15	
4.	*Very High*	16 s.d. 25	

B. *Risk Response*

Terdapat beberapa jenis risk response, yang digunakan untuk merespon tindakan penanganan dari suatu risiko, seperti *Risk Modification, Risk Retention, Risk Avoidance*, dan *Risk Sharing* [4]. Penentuan respon risiko ini ditentukan berdasarkan hasil dari identifikasi suatu risiko, yang diuraikan pada Tabel 3.

Tabel 3.
Risk Response

No	Penanganan Risiko	Keterangan
1.	*Risk Modification* (Modifikasi Risiko)	*Risk Modification* dilakukan ketika organisasi akan melakukan penanganan risiko untuk mengurangi kemungkinan terjadinya risiko, maupun dampak yang akan ditimbulkan oleh risiko negatif. Hingga risiko tersebut nantinya dapat dikendalikan dan diterima.
2.	*Risk Retention* (Retensi Risiko)	*Risk Retention* dilakukan ketika suatu risiko yang telah diidentifikasi, tidak dilakukan proses mitigasi terhadap risiko tersebut. Hal ini dilakukan apabila risiko tersebut memiliki tingkat prioritas yang rendah dan tidak berdampak negatif.
3.	*Risk Avoidance* (Menghindari Risiko)	*Risk Avoidance* dilakukan apabila organisasi berencana untuk menghindari suatu aktivitas akibat dampak signifikan yang akan ditimbulkan, serta probabilitas terjadinya risiko yang tinggi pada aktivitas tersebut.
4.	*Risk Sharing* (Berbagi Risiko)	*Risk Sharing* merupakan proses membagi suatu risiko kepada third party/pihak lain yang akan bertanggung jawab untuk mengelola serta menanggung terjadinya dampak negatif pada risiko tersebut.

C. *Risk Analysis*

Tahapan ini dilakukan untuk membantu penelitian dalam menentukan tingkatan risiko berdasarkan pengkategorian pada kemungkinan, dampak, dan penilaian dari setiap risiko tersebut. Tabel 4, akan menguraikan hasil dari analisis risiko pada penelitian ini.

Tabel 4.
Risk Analysis

Risk Profile	***Risk ID***	Risiko	Nilai Risiko	Level Risiko
IT Expertise, Skills, and Behavior (4)	R01	Tidak tersedianya data operasional yang diperlukan	8	Medium
	R02	Ketergantungan berlebihan pada sistem terkait pelaksanaan evaluasi	6	Medium
	R03	Kinerja pegawai IT yang tidak optimal	2	Low
	R04	Kualitas dan kuantitas pegawai IT tidak kompeten	2	Low
	R05	Kesalahan pengguna dalam mengoperasikan aplikasi	1	Low
	R06	Pelatihan kepada pegawai terhadap pemahaman sistem informasi yang tidak berhasil	2	Low
Program and Projects Lifecycle Management (2)	R07	Keterlambatan pengelolaan data keuangan proyek IT	3	Low
	R08	Komplain atau masalah yang muncul dari mitra kerja sama, terkait kualitas sistem atau layanan IT yang diberikan	6	Medium
Noncompliance (13)	R09	Kegagalan dalam mematuhi 17 standar LPSE pada proses dokumentasi pengelolaan layanan pengadaan secara elektronik	1	Low
Hardware Incidents (9)	R10	Gangguan pada sistem pengadaan barang/jasa	1	Low
	R11	Server *down*	1	Low
IT-Investment Decision Making, Portfolio Definition and Maintenance (1)	R12	Kegagalan penggunaan dan pengembangan sistem informasi	1	Low
	R13	Maintenance website yang kurang efektif	2	Low
	R14	Ketersediaan fasilitas perangkat jaringan yang belum memadai	6	Medium

Risk Profile	*Risk* ID	Risiko	Nilai Risiko	Level Risiko
Logical Attacks (hacking, malware, etc.) (11)	R15	Kebocoran atau penyalahgunaan keamanan informasi pada data sensitif perusahaan	5	Medium
	R16	Kegagalan mengatasi serangan malware terhadap sistem informasi LPP TVRI oleh pihak yang tidak bertanggung jawab	1	Low
Software Failures (10)	R17	Pengelolaan data pada aplikasi manajemen pelelangan yang belum terintegrasi secara menyeluruh	6	Medium
	R18	Aplikasi tidak dapat digunakan	6	Medium
Unauthorized Actions (7)	R19	Manipulasi data pada sistem perusahaan yang dapat mendukung praktik Korupsi, Kolusi, dan Nepotisme (KKN)	4	Low
IT Operational Infrastructure Incidents (6)	R20	Pemindahan aset IT tanpa persetujuan	1	Low
	R21	Kerusakan aset hardware BMN (Barang Milik Negara)	8	Medium
	R22	Kesalahan pencatatan aset hardware BMN (Barang Milik Negara)	8	Medium
	R23	Data pada database tidak akurat	5	Medium
	R24	Infrastruktur IT rusak/tidak bisa digunakan/usang	10	High
	R25	Terdapat bug dan kesalahan minor atau major pada website LPP TVRI	6	Medium

D. *Risk Treatment*

Risk Treatment merupakan langkah untuk menentukan strategi penanganan risiko untuk mengurangi terjadinya kemungkinan dan dampak yang ditimbulkan dari risiko-risiko, tahapan ini akan memastikan setiap risiko yang dilakukan asesmen, dapat diberikan penanganan yang tepat.

Meskipun pada penelitian ini tidak mencakup tahap *Monitoring & Review*, tahapan ini penting untuk dilakukan bagi perusahaan dalam mengetahui dan memastikan efektivitas IT *Risk Management* yang telah diterapkan tetap efektif dan relevan seiring dengan berjalannya waktu. Tahapan ini akan membantu perusahaan dalam mengidentifikasi, menilai, dan mengevaluasi risiko secara berkelanjutan terhadap adanya ancaman terbaru. Tabel 5, akan menguraikan hasil dari penanganan risiko yang sesuai dengan klasifikasi kebutuhan perusahaan.

Tabel 5.
Risk Treatment

Risk Profile	*Risk* ID	Risiko	Level Risiko	Respon Risiko
IT Expertise, Skills, and Behavior (4)	R01	Tidak tersedianya data operasional yang diperlukan	Medium	*Modification*
	R02	Ketergantungan berlebihan pada sistem terkait pelaksanaan evaluasi	Medium	*Modification*
	R03	Kinerja pegawai IT yang tidak optimal	Low	*Retention*
	R04	Kualitas dan kuantitas pegawai IT tidak kompeten	Low	*Retention*
	R05	Kesalahan pengguna dalam mengoperasikan aplikasi	Low	*Retention*
	R06	Pelatihan kepada pegawai terhadap pemahaman sistem informasi yang tidak berhasil	Low	*Retention*
Program and Projects Lifecycle Management (2)	R07	Keterlambatan pengelolaan data keuangan proyek IT	Low	*Retention*
	R08	Komplain atau masalah yang muncul dari mitra kerja sama, terkait kualitas sistem atau layanan IT yang diberikan	Medium	*Modification*
Noncompliance (13)	R09	Kegagalan dalam mematuhi 17 standar LPSE pada proses dokumentasi pengelolaan layanan pengadaan secara elektronik	Low	*Retention*
Hardware Incidents (9)	R10	Gangguan pada sistem pengadaan barang/jasa	Low	*Retention*
	R11	Server *down*	Low	*Retention*
IT-Investment Decision Making, Portfolio Definition and Maintenance (1)	R12	Kegagalan penggunaan dan pengembangan sistem informasi	Low	*Retention*
	R13	Maintenance website yang kurang efektif	Low	*Retention*
	R14	Ketersediaan fasilitas perangkat jaringan yang belum memadai	Medium	*Modification*
Logical Attacks (hacking, malware, etc.) (11)	R15	Kebocoran atau penyalahgunaan keamanan informasi pada data sensitif perusahaan	Medium	*Avoidance*
	R16	Kegagalan mengatasi serangan malware terhadap sistem informasi LPP TVRI oleh pihak yang tidak bertanggung jawab	Low	*Retention*
Software Failures (10)	R17	Pengelolaan data pada aplikasi manajemen pelelangan yang belum terintegrasi secara menyeluruh	Medium	*Modification*
	R18	Aplikasi tidak dapat digunakan	Medium	*Sharing*
Unauthorized Actions (7)	R19	Manipulasi data pada sistem perusahaan yang dapat mendukung praktik Korupsi, Kolusi, dan Nepotisme (KKN)	Low	*Retention*
IT Operational Infrastructure Incidents (6)	R20	Pemindahan aset IT tanpa persetujuan	Low	*Retention*
	R21	Kerusakan aset *hardware* BMN (Barang Milik Negara)	Medium	*Modification*
	R22	Kesalahan pencatatan aset *hardware* BMN (Barang Milik Negara)	Medium	*Modification*
	R23	Data pada database tidak akurat	Medium	*Avoidance*
	R24	Infrastruktur IT rusak/tidak bisa digunakan/usang	High	*Sharing*
	R25	Terdapat bug dan kesalahan minor atau major pada website LPP TVRI	Medium	*Sharing*

E. Penetapan Kontrol Risiko

Tahapan ini merupakan langkah untuk mengelola risiko dengan memberikan penanganan kontrol dan prosedur yang sesuai dengan standar operasional perusahaan, melalui

penyesuaian yang mengacu pada prinsip kontrol dari Domain COBIT 2019 dan ISO/IEC 27001:2022 Annex A. Tahapan ini difokuskan untuk meminimalisir dampak dan kemungkinan yang ditimbulkan dari terjadinya risiko pada perusahaan. Tabel 6, menjelaskan penetapan kontrol risiko pada Bagian Umum LPP TVRI Jabar.

Tabel 6.
Penetapan Kontrol Risiko

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
R01	DSS01.01 - *Perform operational procedures*	A.5.37 - *Documented Operating Procedures*	Menerapkan prosedur operasional yang terdokumentasi untuk memastikan penerimaan, pengolahan, dan penyampaian data dari *stakeholder* secara tepat waktu, serta pemantauan terhadap performa dari aktivitas guna mengidentifikasi hambatan yang dapat menyebabkan keterlambatan pengolahan data.
R02	APO07.03 - *Maintain the skills and competencies of personnel*	A.6.3 – *Information Security Awareness, Education and Training*	Menetapkan dan mengelola pengembangan kompetensi serta keterampilan personel yang diperlukan untuk memahami, mengelola, dan mengevaluasi proses secara manual maupun otomatis, melalui asesmen terhadap kemampuan pegawai dalam menggunakan sistem otomasi, sekaligus memastikan adanya pelatihan berkelanjutan untuk mempertahankan pengetahuan kritis dan pengambilan keputusan secara manual, guna mencegah ketergantungan berlebihan pada sistem otomatis.
	Menambahkan Role "*Evaluation Process Facilitator*"	A.5.2 – *Information Security Roles and Responsibilities*	Memastikan jalannya proses evaluasi secara terstruktur, efektif, dan fokus pada tujuan evaluasi.
R03	APO07.03 - *Maintain the skills and competencies of personnel*	A.6.3 – *Information Security Awareness, Education and Training*	Mengembangkan pelatihan secara berkelanjutan pada penggunaan dan pemeliharaan sistem IT melalui peningkatan pada pengetahuan, keterampilan, dan kompetensi yang dibutuhkan.
R04	APO07.01 - *Acquire and maintain adequate and appropriate staffing*	A.5.2 – *Information Security Roles and Responsibilities*	Menetapkan proses rekrutmen dan perencanaan pegawai IT yang terstruktur untuk memperoleh kualitas pegawai IT yang sesuai dengan kebutuhan strategis dan operasional perusahaan.
	Menambahkan Role "*Evaluation Process Facilitator*"	A.5.2 – *Information Security Roles and Responsibilities*	Memastikan jalannya proses pengambilan keputusan secara terstruktur, efektif, dan fokus pada tujuan evaluasi.
R05	APO07.03 - *Maintain the skills and competencies of personnel*	A.6.3 – *Information Security Awareness, Education and Training*	Meningkatkan dan mengelola keterampilan pegawai IT melalui pelatihan secara berkelanjutan dalam mengoperasikan aplikasi, sesuai dengan tingkat yang dibutuhkan.
R06	APO07.01 - *Acquire and maintain adequate and appropriate staffing*	A.5.4 – *Management Responsibilities*	Menyusun rencana program pelatihan yang strategis pada sumber daya manusia di bidang IT, melalui penetapan jadwal pelatihan yang terstruktur dan diselaraskan dengan kebutuhan operasional serta beban kerja pegawai.
R07	DSS01.01 - *Perform operational procedures*	A.5.37 - *Documented Operating Procedures*	Menetapkan dan menjalankan prosedur operasional standar untuk memastikan pengelolaan data keuangan yang akurat, lengkap, dan tepat waktu, dalam mendukung alokasi pendanaan anggaran pada kebutuhan teknologi informasi.
R08	APO08.03 - *Manage the business relationship*	A.5.6 – *Contact with Special Interest Groups*	Membangun dan memelihara mekanisme komunikasi secara terbuka pada mitra kerja sama dalam membahas evaluasi layanan, penanganan insiden, serta perbaikan berkelanjutan guna menjaga kesesuaian layanan IT terhadap standar yang disepakati.
R09	MEA03.01 - *Identify external compliance requirements*	A.5.36 – *Compliance with Policies, Tules and Standards for Information Security*	Mengidentifikasi dan membangun mekanisme pemantauan terhadap seluruh persyaratan pada 17 standar LPSE yang berlaku, dipatuhi secara berkala untuk menjamin kesesuaian dengan standar tersebut.
R10	BAI04.03 - *Plan for new*	A.8.6 – *Capacity Management*	Merencanakan layanan baru pada sistem pengadaan barang/jasa

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
	or changed service requirements		untuk menangani volume data dan transaksi, dengan memprioritaskan ketersediaan, kinerja, dan kapasitas yang sesuai dengan kebutuhan bisnis.
R11	BAI04.01 - *Assess current availability, performance and capacity and create a baseline*	A.8.9 – *Configuration Management*	Melakukan penilaian rutin terhadap ketersediaan, kinerja, dan kapasitas server, untuk memastikan kesiapan dan keandalannya dalam mendukung operasional bisnis, melalui pengembangan *baseline* pada setiap komponen server. Sebagai perbandingan untuk pemantauan dan deteksi awal atas potensi terjadinya gangguan.
	Mengembangkan aktivitas "*Maintenance Planning*"	A.8.25 – *Secure Development Life Cycle*	Merencanakan bagaimana dan kapan proses *maintenance* aset perlu untuk dilakukan.
R12	BAI03.10 - *Maintain solutions*	A.5.9 – *Inventory of Information and Other Associated Assets*	Mengembangkan dan melaksanakan rencana untuk investasi sistem informasi secara jangka panjang berdasarkan komponen solusi dan infrastruktur, yang mencakup tinjauan secara berkala terhadap kebutuhan bisnis dan persyaratan operasional.
R13	BAI03.10 - *Maintain solutions*	A.8.6 – *Capacity Management*	Mengembangkan dan melaksanakan rencana untuk pemeliharaan website secara rutin, berdasarkan komponen solusi dan infrastruktur, yang mencakup tinjauan secara berkala terhadap kebutuhan bisnis dan persyaratan operasional.
R14	APO05.04 - *Maintain portfolios*	A.5.24 – *Information Security Incident Management Planning and Preparation*	Melakukan pengelolaan portofolio proyek investasi pada aset perangkat jaringan yang baru.
R15	DSS05.07 - *Manage vulnerabilities and monitor the infrastructure for security-related events*	A.8.12 – *Data Leakage Prevention*	Mengelola dan mengidentifikasi kerentanan pada insiden keamanan informasi menggunakan *tools* pendeteksi ancaman keamanan terhadap akses yang tidak sah pada data sensitif perusahaan.
	Mengembangkan *tools* deteksi ancaman keamanan	A.8.12 – *Secure Authentication*	Mengembangkan *tools* tambahan untuk mendeteksi ancaman pada data sensitif perusahaan secara otomatis.
R16	DSS05.01 - *Protect against malicious software*	A.8.7 – *Protection Against Malware*	Menerapkan dan memelihara tindakan pencegahan dari serangan *malware*, untuk melindungi sistem informasi perusahaan akibat serangan perangkat lunak yang berbahaya oleh pihak yang tidak bertanggung jawab.
	Mengembangkan *tools* deteksi ancaman keamanan	A.8.12 – *Secure Authentication*	Mengembangkan tools tambahan untuk mendeteksi ancaman pada data sensitif perusahaan secara otomatis.
R17	BAI03.05 - *Build solutions*	A.5.37 – *Documented Operating Procedures*	Melakukan integrasi menyeluruh antara data pada aplikasi manajemen pelelangan, dengan sistem database proses bisnis terkait, untuk memastikan data dapat diakses dan dimanfaatkan secara tepat dan konsisten, serta memastikan data pada aplikasi diperbarui secara berkala untuk mencerminkan solusi yang dilakukan.
R18	BAI03.10 - *Maintain solutions*	A.8.6 – *Capacity Management*	Mengembangkan dan melaksanakan rencana untuk pemeliharaan fungsionalitas aplikasi secara rutin, berdasarkan komponen solusi dan infrastruktur, yang mencakup tinjauan secara berkala terhadap pengoperasian sistem aplikasi dalam mengakses informasi yang dibutuhkan.
R19	DSS05.04 - *Manage user identity and logical access*	A.8.2 – *Privileged Access Rights*	Memastikan seluruh pegawai memiliki hak akses data/informasi yang disesuaikan berdasarkan posisinya pada perusahaan.
R20	BAI09.02 - *Manage critical assets*	A.5.10 – *Acceptable Use of Information and Other Associated Assets*	Menetapkan dan menerapkan kebijakan pada pengelolaan aset IT yang mencakup proses identifikasi, klasifikasi, pencatatan, serta kontrol akses terhadap aset penting perusahaan, melalui prosedur yang terdokumentasi.

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
R21	BAI09.03 - *Manage the asset life cycle*	A.5.9 – *Inventory of Information and Other Associated Assets*	Menerapkan dan mengelola manajemen siklus hidup aset yang komprehensif terhadap BMN, mulai dari tahap perencanaan pengadaan, pemakaian, pemeliharaan, hingga pembuangan, serta memastikan bahwa aset dapat digunakan secara efektif, efisien, dan dipertanggungjawabkan.
R22	BAI09.01 - *Identify and record current assets*	A.5.33 – *Protection of Records*	Menerapkan sistem pencatatan aset *hardware* yang akurat, terkini, dan terdokumentasi dengan baik, untuk mendukung keselarasan layanan dengan manajemen konfigurasi dan keuangan yang ada di perusahaan.
R23	DSS03.04 - *Resolve and close problems*	A.8.8 – *Management of Technical Vulnerabilities*	Melakukan analisis pada akar penyebab (*root cause analysis*) permasalahan atas ketidakakuratan data dalam database dan menetapkan tindakan penanganan yang berkelanjutan, melalui proses manajemen perubahan. Memastikan pegawai yang terkena dampak, mengetahui tindakan yang dilakukan untuk mencegah terjadinya pengulangan insiden serupa di masa mendatang.
R24	BAI04.01 - *Assess current availability, performance and capacity and create a baseline*	A.8.6 – *Capacity Management*	Melakukan penilaian rutin terhadap ketersediaan, kinerja, dan kapasitas Infrastruktur IT, untuk memastikan kesiapan dan keandalannya dalam mendukung operasional bisnis, melalui pengembangan *baseline* pada setiap komponen Infrastruktur IT. Sebagai perbandingan untuk pemantauan dan deteksi awal.
	Mengembangkan aktivitas "*Maintenance Planning*"	A.8.25 – *Secure Development Life Cycle*	Merencanakan bagaimana dan kapan proses *maintenance* aset perlu untuk dilakukan.
R25	BAI04.05 - *Investigate and address availability, performance and capacity issues*	A.8.9 – *Configuration Management*	Menangani permasalahan ketersediaan dan kinerja, melalui pemantauan terhadap fungsionalitas dan performa website secara *real-time,* pada masalah teknis yang terjadi.

V. HASIL DAN PEMBAHASAN

Berdasarkan hasil dari penelitian yang dilakukan, diketahui bahwa Bagian Umum LPP TVRI Jabar, saat ini belum menerapkan proses IT *Risk Management* yang terstruktur dengan bantuan *framework* seperti COBIT 2019 ataupun ISO/IEC 27005:2022. Untuk mengatasi solusi atas permasalahan tersebut, penulis melakukan penelitian pada analisis IT *Risk Management* untuk memberikan penilaian terbaru terhadap sejauh mana risiko IT pada Bagian Umum LPP TVRI Jabar dapat dikelola, dengan menggabungkan *framework* ISO/IEC 27005:2022 sebagai *framework* utama untuk analisis pengelolaan risiko IT (*risk identification, risk analysis, risk evaluation*, dan *risk treatment*), dan *framework* COBIT 2019 untuk identifikasi *risk profile*, penetapan kontrol dan rekomendasi atas risiko tersebut.

Dengan hasil analisis pengelolaan risiko IT tersebut, diketahui terdapat 25 risiko IT yang perlu diidentifikasi melalui penilaian indeks risiko (level *impact* dan level *likelihood*). Dari hasil analisis risiko yang dilakukan terhadap 25 daftar risiko, tercatat sebanyak satu (1) risiko dengan level *High*, sebelas (11) risiko dengan level *Medium*, dan tiga belas (13) risiko dengan level *Low*, dengan hasil ini risiko-risiko IT dengan level *Medium* dan *High*, akan diberikan penanganan dan pengendalian yang sesuai, untuk mengurangi dampak yang signifikan dan kemungkinan yang akan ditimbulkan.

Langkah berikutnya adalah pemberian *risk response* yang sesuai dengan *framework* ISO/IEC 27005:2022, tercatat sebanyak tujuh (7) risiko dengan respon *modification,* tiga belas (13) risiko dengan respon *retention*, dua (2) risiko dengan respon *avoidance,* dan tiga (3) risiko dengan respon *sharing.* Risiko-risiko IT tersebut selanjutnya akan diberikan penetapan kontrol dan rekomendasi yang mengacu pada *framework* COBIT 2019, serta kontrol dari *framework* ISO/IEC 27001:2022 Annex A, yang disesuaikan dengan urgensinya pada masing-masing risiko IT.

REFERENSI

[1] C. 2019 Design Guide, *Designing an Information and Technology Governance Solution*. 2018.

[2] D. Darmawan and A. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," *J. Comput. Inf. Syst. Ampera*, vol. Vol. 3, No, pp. 1–4, 2022, [Online]. Available: https://www.researchgate.net/publication/358815508_Analisis_dan_Desain_Tata_Kelola_Teknologi_Informasi_Menggunakan_Framework_COBIT_2019_pada_PT_XYZ

[3] R. Abdul Aziz, Kusrini, and Sudarmawan, "Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan BUMN Menggunakan Standar COBIT 5 (Studi Kasus: PT TASPEN PERSERO)," *J. Ilm. IT Cida Disem. Teknol. Inf.*, pp. 2–3, 2018, [Online]. Available: https://journal.amikomsolo.ac.id/index.php/itcida/art

icle/view/80/59
[4] ISO/IEC 27005, "ISO/IEC 27005:2022, Information Security Risk Management," vol. 2022, 2022.
[5] F. A. Zahwa and I. Syafi'i, "Pemilihan pengembangan media pembelajaran berbasis teknologi informasi," *Equilib. J. Penelit. Pendidik. dan Ekon.*, vol. 19, no. 01, pp. 61–78, 2022.
[6] Z. Nuryana, "Pemanfaatan teknologi informasi dalam pendidikan agama islam," *TAMADDUN J. Pendidik. dan Pemikir. Keagamaan*, vol. 19, no. 1, pp. 75–86, 2019.
[7] H. Iin and A. Tjahyanto, "Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOK, Dan ISO 31000," *J. Ilm. Teknol. Dan Rekayasa*, vol. 9, no. 2, pp. 43–50, 2017.
[8] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Tek. Inform. Dan Sist. Informasi)*, vol. 7, no. 3, pp. 546–558, 2020.
[9] Meilita Karenda Putri and A. R. Hakim, "Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005:2018 dan NIST SP 800-30 Revisi 1," *Info Kripto*, vol. 15, no. 3, pp. 134–141, 2021, doi: 10.56706/ik.v15i3.34.
[10] J. S. 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," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 5, no. 5, pp. 1734–1744, 2021.
[11] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2018.
[12] ISO/IEC 27001, "ISO/IEC 27001:2022," *ISO/IEC 27001:2022*, vol. 2022, 2022, doi: 10.2307/j.ctv30qq13d.
[13] D. D. A. Efe, "A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT," *J. Audit. Assur. Serv.*, vol. 3, no. 2, pp. 185–205, 2023.
[14] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q. Manag. Inf. Syst.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.
[15] Y. N. Qintharah, "Perancangan Penerapan Manajemen Risiko," *JRAK J. Ris. Akunt. dan Komputerisasi Akunt.*, vol. 10, no. 1, pp. 67–86, 2019, doi: 10.33558/jrak.v10i1.1645.