Journal of Production, Enterprise, and Industrial Applications
Vol. 4, Issue 1, pp. 65–72 (2026)
doi: http://doi.org/10.25124/logic.v4i1.6407

RESEARCH ARTICLE

Analisis Manajemen Risiko Teknologi Informasi Pada Bagian Teknik di Lembaga Penyiaran Publik Tvri Jawa Barat Dengan *Framework* Iso/Iec 27005:2022

Gede Dipta Narayana, Widyatasya Agustika Nurtrisha* and Ridha Hanafi

Fakultas Rekayasa Industri, Universitas Telkom, Bandung, 40257, Jawa Barat, Indonesia
*Corresponding author: widyatasya@telkomuniversity.ac.id

Abstrak

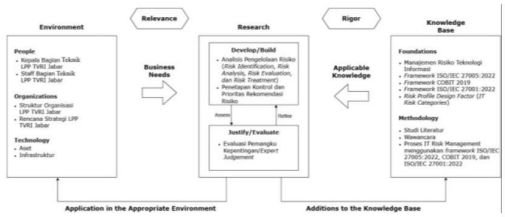
Lembaga Penyiaran Publik (LPP) TVRI Jawa Barat sangat bergantung pada keandalan infrastruktur teknologi informasi (TI) yang dikelola oleh Bagian Teknik untuk menjaga kontinuitas operasional di tengah era disrupsi digital. Namun, observasi internal menunjukkan bahwa Bagian Teknik belum memiliki proses manajemen risiko TI yang terstruktur dan masih mengandalkan mekanisme pelaporan manual kepada PIC (*person in charge*) yang bersifat reaktif. Kondisi ini dinilai tidak ideal dalam menghadapi ancaman siber dan teknis yang semakin kompleks. Penelitian ini bertujuan untuk merancang sebuah panduan manajemen risiko TI yang sistematis dengan mengadopsi pendekatan kualitatif yang mengintegrasikan *framework* ISO/IEC 27005:2022 untuk proses utama manajemen risiko, serta COBIT 2019 untuk identifikasi profil risiko dan penetapan kontrol. Hasil penelitian berhasil mengidentifikasi 20 risiko TI potensial, yang setelah melalui proses analisis diklasifikasikan menjadi satu (1) risiko dengan level *High*, sembilan (9) risiko dengan level Medium, dan sepuluh (10) risiko dengan level *Low*. Berdasarkan evaluasi, ditetapkan 10 risiko prioritas yang memerlukan penanganan lebih lanjut. Untuk risikorisiko tersebut, dirumuskan respon risiko berupa *modification* (9 risiko) dan *sharing* (1 risiko), serta penetapan kontrol relevan yang mengacu pada COBIT 2019 dan Annex A ISO/IEC 27001:2022, yang dikelompokkan ke dalam aspek *People, Process,* dan *Technology*.

Key words: Manajemen Risiko TI, TVRI Jawa Barat, ISO/IEC 27005:2022, COBIT 2019

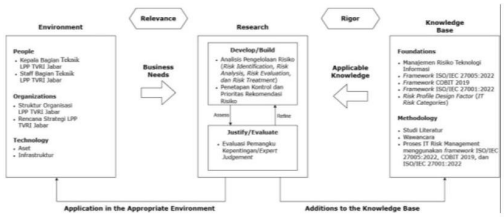
Pendahuluan

Perkembangan teknologi informasi (TI) telah menjadi komponen penting dalam industri jasa untuk mendorong inovasi dan daya saing [1]. Sebagai Lembaga Penyiaran Publik (LPP), Televisi Republik Indonesia (TVRI) Jawa Barat berperan penting menyajikan konten edukasi dan budaya [2]. Namun, TVRI menghadapi tantangan eksistensial akibat disrupsi media sosial yang mengubah preferensi audiens, terutama kaum muda. Penurunan minat menonton ini salah satunya disebabkan oleh anggapan bahwa kualitas teknis siaran TVRI belum modern [3]. Untuk tetap relevan, TVRI dituntut berevolusi dengan menyajikan konten berkualitas, yang sangat bergantung pada keandalan infrastruktur teknis yang dikelola oleh Bagian Teknik. Keandalan operasional penyiaran menjadikan tata kelola teknik sebagai salah satu komponen utama dalam keberlangsungan proses bisnis LPP TVRI Jawa Barat. Oleh karena itu, manajemen risiko TI memegang peranan vital untuk menjaga keamanan serta keandalan sarana dan prasarana pendukung operasional [4]. Lemahnya tata kelola risiko TI yang tidak terstruktur dan terdokumentasi dapat memicu berbagai dampak serius, mulai dari gangguan operasional, terhentinya layanan, hingga kerugian finansial yang signifikan. Oleh karena itu, kemampuan mengelola risiko operasional secara efisien menjadi kunci untuk meminimalkan kerugian dan memastikan keberhasilan proses bisnis perusahaan [5]. Namun, temuan awal melalui observasi dan wawancara internal mengindikasikan bahwa LPP TVRI Jabar belum mengadopsi proses manajemen risiko TI yang terstruktur serta belum menggunakan *framework* standar seperti ISO/IEC 27005:2022 atau COBIT 2019.

Sistem yang ada saat ini dinilai tidak memadai karena hanya bersifat reaktif, mengandalkan pelaporan manual tanpa standar kontrol yang proaktif untuk mengidentifikasi dan memitigasi risiko. Praktik ini dinilai tidak efektif dan berdampak luas sehingga memengaruhi kontinuitas operasional lembaga. Untuk merespons tantangan tersebut, penelitian ini mengusulkan pengembangan proses manajemen risiko TI yang terstruktur dengan mengadopsi *framework* ISO/IEC 27005:2022 sebagai acuan utama. Standar ini menyediakan pendekatan sistematis untuk pengelolaan risiko keamanan TI yang mencakup identifikasi, analisis, evaluasi, dan penanganan risiko. *Framework* COBIT 2019 juga diimplementasikan untuk mendukung penetapan kontrol yang relevan dan rekomendasi penanganan. Dengan demikian, penelitian ini bertujuan untuk menganalisis dan memetakan kondisi pengelolaan risiko existing, melaksanakan proses manajemen risiko TI secara mendalam pada



Gambar 1. Model Konseptual



Gambar 2. Sistematika Penyelesaian Masalah

operasional Bagian Teknik dengan mengacu pada kerangka kerja ISO-/IEC 27005:2022, serta merumuskan rekomendasi langkah-langkah penanganan risiko, termasuk kontrol yang sesuai untuk memitigasi risiko TI yang telah ditetapkan.

Metodologi Penelitian

Model Konseptual

Pendekatan Hevner digunakan sebagai kerangka acuan untuk rencana dan penjelasan tentang langkah - langkah yang akan diambil untuk mencapai tujuan penelitian ketika model konseptual ini dibuat, model konseptual ini dapat dilihat lebih rinci pada gambar 1. Dalam penelitian ini, *framework* ISO/IEC 27005:2022 digunakan untuk mengidentifikasi, menganalisis, dan menyusun solusi serta COBIT 2019 sebagai kontrol risiko dalam proses pengelolaan TI pada Bagian Teknik LPP TVRI Jawa Barat. Metode ini menggabungkan metode analisis teori dengan solusi praktis untuk menghasilkan rekomendasi kontrol risiko yang efektif dan dapat diterapkan di perusahaan [6].

Environment mencakup komponen *People*, *Organization*, dan *Technology*, yang secara kolektif membentuk konteks penelitian. *People* merujuk pada pemangku kepentingan yang berhubungan dengan LPP TVRI Jawa Barat, *Organization* meliputi struktur dan kebijakan yang ada, sedangkan *Technology* mencakup seluruh infrastruktur yang digunakan oleh organisasi yang didalam penelitian ini adalah LPP TVRI Jawa Barat. *Research* berfokus pada proses analisis dan pengembangan solusi yang mencakup perancangan, implementasi, dan evaluasi. Perancangan solusi melibatkan pengembangan strategi manajemen risiko berbasis ISO/IEC 27005:2022, yang kemudian diimplementasikan dan dievaluasi untuk menilai pencapaian tujuan serta dampak positifnya untuk lembaga. *Knowledge Base* terdiri dari landasan teori, metodologi, dan literatur relevan yang mendukung jalannya penelitian. Dasar teori utamanya mencakup manajemen risiko teknologi informasi *framework* ISO/IEC 27005:2022 dan COBIT 2019 sebagai kontrol, sementara metodologi merinci perancangan proses penelitian yang sistematis, termasuk metode yang digunakan.

Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah secara merupakan metode terstruktur untuk mengidentifikasi, menganalisis, dan menyelesaikan masalah secara efisien. Pendekatan ini terdiri dari beberapa proses penting yang dimaksudkan untuk memastikan bahwa masalah terselesaikan sepenuhnya dan solusi yang dihasilkan dapat diimplementasikan dengan baik. Dalam penelitian ini terdapat 5 tahapan utama proses penyelesaian sistematika penyelesaian masalah yang dapat dilihat pada gambar 2.

Pengumpulan Data

Proses pengumpulan data dalam penelitian ini dilakukan melalui dua metode pendekatan, yakni metode wawancara mendalam untuk pengambilan data primer dan studi literatur untuk peghimpunan data sekunder.Wawancara mendalam dilakukan dengan para *key stakeholder* di LPP TVRI Jabar, termasuk PIC (*person in charge*) utama manajemen risiko, kepala Bagian Teknik, dan *staff* Bagian Teknik. Wawancara ini bertujuan untuk mendapatkan wawasan langsung dan mendalam mengenai manajemen risiko teknologi informasi yang sedang diterapkan, tantangan yang dihadapi, dan kebutuhan spesifik dari organisasi. Kemudian kuesioner digunakan untuk mengumpulkan data kuantitatif mengenai kemungkinan dan dampak dari setiap risiko, yang kemudian dianalisis untuk menentukan tingkat serta prioritasnya.

Kuisioner hanya diisi oleh 1 (satu) orang narasumber dari Bagian Teknik di LPP TVRI Jawa Barat. Pengumpulan data sekunder melalui studi literatur membantu dalam memahami konteks teoretis dan praktik terbaik yang berkaitan dengan manajemen risiko IT dan penerapan *framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022. Selain itu jurnal ilmiah, buku, laporan industri, dan dokumen - dokumen internal LPP TVRI Jabar yang relevan dengan topik penelitian juga dijadikan sumber data sekunder dalam penelitian ini.

Pengolahan Data

Penelitian ini mengolah data secara sistematis untuk menganalisis tata kelola risiko TI pada operasional produksi, penyiaran, dan infrastruktur di Bagian Teknik TVRI Jawa Barat. Analisis dilakukan menggunakan kerangka kerja ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022. Proses diawali dengan identifikasi masalah melalui wawancara serta penyebaran kuisioner untuk menghimpun data primer, dan studi literatur (data sekunder) untuk memetakan risiko terkait penerapan TI. Proses pengolahan data diawali dengan identifikasi risiko menggunakan klasifikasi dari *framework* COBIT 2019.

Selanjutnya, risiko dianalisis secara mendalam melalui proses manajemen risiko ISO/IEC 27005:2022 (identifikasi, analisis, evaluasi, dan perlakuan). Kombinasi ini memastikan identifikasi ancaman komprehensif untuk merumuskan strategi penanganan yang efektif. Tahap selanjutnya adalah menetapkan kontrol dan prioritas rekomendasi berdasarkan analisis risiko sebelumnya. Penetapan kontrol mengacu pada *framework* COBIT 2019 dan Annex A pada ISO/IEC 27001:2022 untuk meningkatkan efektivitas manajemen risiko TI di Bagian Teknik LPP TVRI Jawa Barat.

Hasil dan Pembahasan

Matriks Risiko

Matriks Risiko digunakan pada tabel 1 untuk mengidentifikasi, menilai, dan menganalisis risiko yang terjadi pada perusahaan. Matriks risiko sendiri merupakan metode perhitungan skor manajemen risiko yang terdiri dari dua komponen penilaian yakni *impact* atau dampak dan *likelihood* atau kemingkinan, terjadinya suatu risiko yang mempengaruhi operasional dan tujuan bisnis suatu organisasi [7].

Penentuan level risiko didasarkan pada besaran skor yang dihitung dari komponen dampak (*impact*) dan kemungkinan (*likelihood*), dengan pemetaan skor level risiko yang terperinci pada Tabel 2.

Table 1. Matriks Risiko

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

Table 2. Matrixs Resiko

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	

Table 3. Risk Response

No	Penanganan Risiko	Penjelasan
1	*Risk Modification* (Mengurangi Risiko)	Tindakan untuk mengurangi kemungkinan dan/atau dampak risiko negatif hingga mencapai tingkat yang dapat diterima.
2	*Risk Retention* (Mitigasi Risiko)	Dilakukan ketika menerima risiko yang telah teridentifikasi tanpa mitigasi, karena risiko tersebut memiliki prioritas rendah.
3	*Risk Sharing* (Membagi Risiko)	Proses memindahkan tanggung jawab pengelolaan dan dampak suatu risiko kepada pihak ketiga.
4	*Risk Avoidance* (Menerima Risiko)	Diterapkan pada risiko dengan probabilitas kejadian tinggi untuk menghindari dampak yang signifikan..

Risk Response

Adapun beberapa bentuk respons terhadap risiko, seperti *Risk Modification, Risk Retention, Risk Avoidance,* dan *Risk Sharing*, yang digunakan sebagai langkah penanganan risiko yang telah teridentifikasi. Pemilihan strategi respons yang tepat ditentukan berdasarkan hasil analisis risiko.

Risk Analysis

Tahap analisis risiko 4 bertujuan untuk mengevaluasi tingkat signifikansi atau keparahan dari setiap risiko yang telah dikenali, yang penilaiannya didasarkan pada pertimbangan terhadap *likelihood* dan *impact* yang ditimbulkannya.

Risk Treatment

Penanganan risiko merupakan tahapan penetapan strategi untuk memitigasi kemungkinan dan dampak dari risiko yang telah diidentifikasi. Meskipun tidak mencakup tahap Monitoring & *Review* pada lingkup penelitian ini, tahapan ini sangat signifikan untuk memverifikasi efektivitas kerangka kerja jangka panjang serta mengidentifikasi dan mengevaluasi ancaman baru secara berkelanjutan. Adapun rincian strategi penanganan risiko yang diterapkan dalam penelitian ini, yang disesuaikan dengan klasifikasi kebutuhan perusahaan, disajikan pada Tabel 5.

Penetapan Kontrol Risiko

Penetapan kontrol adalah tahapan penting dalam manajemen risiko untuk memastikan prosedur operasional selaras dengan standar yang ditetapkan. Kontrol yang mengacu pada kerangka kerja COBIT 2019 dan Annex A ISO/IEC 27001:2022 diterapkan sebagai strategi untuk memitigasi dampak dan probabilitas risiko, yang bertujuan meningkatkan efektivitas pengelolaan risiko serta menjaga stabilitas operasional yang dapat dilihat pada 6,7 & 8.

Kesimpulan

Berdasarkan hasil observasi dan wawancara, kondisi manajemen risiko TI di Bagian Teknik LPP TVRI Jawa Barat saat ini belum terstruktur dan sangat terbatas pada mekanisme pelaporan manual yang sifatnya reaktif kepada *person in charge* (PIC). Menanggapi kelemahan ini, penelitian merancang sebuah panduan manajemen risiko TI yang komprehensif. Pendekatan yang digunakan mengintegrasikan dua *framework* yakni ISO/IEC 27005:2022 sebagai acuan utama proses manajemen risiko mulai dari identifikasi, analisis, evaluasi, hingga penanganan risiko, serta COBIT 2019 untuk identifikasi risk profile dan perumusan kontrol yang relevan. Kedua *framework* ini akan memfasilitasi LPP TVRI Jawa Barat dalam mengelola dampak dan kemungkinan risiko TI secara lebih terstruktur dan proaktif.

Proses manajemen risiko TI dalam penelitian ini dilaksanakan melalui beberapa tahapan yang mengacu pada standar ISO/IEC 27005:2022. Proses diawali dengan penetapan konteks serta kriteria risiko untuk membangun landasan penilaian. Tahap selanjutnya adalah identifikasi risiko, dengan mendapati risiko sebanyak 20 potensi risiko TI yang kemudian dinilai berdasarkan indeks *impact* dan *likelihood*. Hasil dari tahap analisis risiko menunjukkan klasifikasi tingkat risiko yang terdiri dari satu (1) risiko berkategori *High*, sembilan (9) risiko berkategori Medium, dan sepuluh (10) risiko berkategori *Low*. Berdasarkan hasil tersebut, tahap evaluasi menetapkan bahwa risiko dengan level *Low* dapat diterima oleh organisasi (retention), sedangkan risiko pada level *Medium* dan *High* memerlukan tindakan penanganan lebih lanjut.

Table 4. Risk Analysis

No	Risk Profile	Risk ID	Risiko	Nilai Risiko	Level Risiko
1	Program and projects lifecycle manageme nt (2)	R01	Gagalnya sistem pendukung produksi luar studio	3	*i*
2		R02	Server utama down	1	*Low*
3	IT operational infrastructu re incidents (6)	R03	Kehilangan aset IT	6	Medium
4		R04	Kegagalan sistem backup data	6	Medium
5	Data and Information Manageme nt (19)	R05	Dokumen penting atau sensitif hilang atau tidak ditemukan dalam sistem	8	Medium
6		R06	Pemadaman listrik menggangu produksi dan sistem IT	2	*Low*
7	Hardware Incidents (9)	R07	Malfungsi peralatan penyiaran luar studio	6	Medium
8		R08	Peralatan studio mengalami malfungsi	3	*Low*
9		R09	Kegagalan pengoperasian alat pendukung siaran	6	Medium
10		R10	Infrastruktur IT tidak layak digunakan	6	Medium
11	Enterprise/ IT Architectur e (5)	R11	Infrastruktur penyiaran tidak berfungsi	9	*High*
12		R12	Integrasi antar database gagal	1	*Low*
13		R13	Menurunya kualitas siaran karena sistem IT tidak optimal	2	*Low*
14	Software Failures (10)	R14	Sistem keamanan IT lemah	5	Medium
15		R15	Kerusakan database utama	1	*Low*
16		R16	Database tidak sesuai standar	1	*Low*
17	Unauthoriz ed Actions (7)	R17	Sabotase perangkat siaran	1	*Low*
18	*Logical attacks (hacking, malware, etc.)* (11)	R18	Akses tidak sah ke sistem	5	Medium
19		R19	Rusaknya database konten siaran	6	Medium
20	*IT Expertise, Skills and Behaviour* (4)	R20	Kecelakaan pegawai akibat kelalaian penggunaan teknologi produksi	3	*Low*

Penanganan risiko difokuskan pada 10 risiko prioritas yang termasuk dalam kategori *Medium* dan *High*. Dari pemilihan strategi respons risiko, ditetapkan bahwa sembilan (9) risiko akan ditangani melalui *modification* dan satu (1) risiko melalui *sharing*. Untuk kesepuluh risiko prioritas ini, dirumuskan serangkaian penetapan kontrol dan rekomendasi yang spesifik dengan mengacu pada panduan dari *framework* COBIT 2019 dan ISO/IEC 27001 Annex A. Seluruh rekomendasi yang diusulkan kemudian dikelompokkan ke dalam tiga aspek utama, yakni People, Process, dan Technology, guna memastikan implementasi yang komprehensif dan terstruktur di lingkungan LPP TVRI Jawa Barat, khususnya pada Bagian Teknik.

Daftar Pustaka

1. Nisa' FZ, Febrianti GD, Ajrina NN. Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa. Bulletin of Computer Science Research. 2023 Dec;4(1):66-74.
2. Pratama FY, Hasfi N, Sulistyani HD. Peran Produser dalam Produksi Berita Feature pada Segmen Mini Feature Program. Semarang; 2023. Accessed: 2024-12-28. Available from: `https://fisip.undip.ac.id/`.
3. Mutmainnah N, Triwibowo EW, Salamah U. Riset Khalayak Penonton Televisi: Pandangan Generasi Z Tentang TVRI; 2020.
4. Adiba MAM, Imansari NG. Analisis Reportase Media Massa di Era Digital: Tantangan, Peluang, dan Dampaknya pada Pandangan Khalayak. Journal of Media and Communication Studies. 2023 Nov;2(1):11-20.
5. Kramarz K, Korpysa J. The Evolution of the Concept of Risk Management in IT Organizations. In: Procedia Computer Science. Szczecin: Elsevier B.V.; 2023. p. 4843-9.
6. Hevner AR, March ST, Park J, Ram S. Design Science in Information Systems Research. MIS Quarterly. 2004;28(1):75-105.
7. Qintharah YN. Perancangan Penerapan Manajemen Risiko. JRAK: Jurnal Riset Akuntansi dan Komputerisasi Akuntansi. 2019 Feb;10(1):67-8.

Table 5. *Risk Treatment*

No	Risk Profile	Risk ID	Risiko	Level Risiko	Penanga nan Risiko
1	Program and projects lifecycle manageme nt (2)	R01	Gagalnya sistem pendukung produksi luar studio	*Low*	Retention
2	IT	R02	Server utama down	*Low*	Retention
3	operational infrastructu	R03	Kehilangan aset IT	Medium	Modificat ion
4	re incidents (6)	R04	Kegagalan sistem backup data	Medium	Modificat ion
5	Data and Information Management (19)	R05	Dokumen penting atau sensitif hilang atau tidak ditemukan dalam sistem	Medium	Modificat ion
6		R06	Pemadaman listrik menggangu produksi dan sistem IT	*Low*	Retention
7	Hardware Incidents (9)	R07	Malfungsi peralatan penyiaran luar studio	Medium	Modificat ion
8		R08	Peralatan studio mengalami malfungsi	*Low*	Retention
9		R09	Kegagalan pengoperasian alat pendukung siaran	Medium	Modificat ion
10		R10	Infrastruktur IT tidak layak digunakan	Medium	Modificat ion
11	Enterprise/ IT Architectur e (5)	R11	Infrastruktur penyiaran tidak berfungsi	*High*	*Sharing*
12		R12	Integrasi antar database gagal	*Low*	Retention
13		R13	Menurunya kualitas siaran karena sistem IT tidak optimal	*Low*	Retention
14	Software Failures (10)	R14	Sistem keamanan IT lemah	Medium	Modificat ion
15		R15	Kerusakan database utama	*Low*	Retention
16		R16	Database tidak sesuai standar	*Low*	Retention
17	Unauthoriz ed Actions (7)	R17	Sabotase perangkat siaran	*Low*	Retention
18	Logical attacks (hacking, malware, etc.) (11)	R18	Akses tidak sah ke sistem	Medium	Modificat ion
19		R19	Rusaknya database konten siaran	Medium	Modificat ion
20		R20	Kecelakaan pegawai akibat kelalaian penggunaan teknologi produksi	*Low*	Retention

Table 6. Penetapan Kontrol Risiko (a)

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
R01	BAI01.01 Maintain a standard approach for program management	A.5.30-ICT readiness f or business continuity	Merencanakan, mengimplementasikan, serta menguji kesiapan sistem pendukung produksi khususnya media komunikasi untuk keberlangsungan proyek. Prosedur pemulihan gangguan disiapkan untuk memastikan operasional produksi di luar studio dapat terus berjalan tanpa hambatan berarti saat terjadi insiden tak terduga.
R02	BAI04.01 Assess current availability, performance and capacity and create a baseline	A.8.9 Configuration management	Menerapkan manajemen konfigurasi dengan memantau, dan meninjau seluruh pengaturan hardware dan software. Mencegah kegagalan server akibat kesalahan konfigurasi atau perubahan yang tidak terkelola dengan baik dan terdokumentasi.
R03	BAI09.01 Identify and record current assets	A.5.9 Inventory of information and other associated assets	Mendata dan memelihara inventaris teknik secara akurat dan terkini untuk memastikan semua aset perusahaan tercatat, memiliki pemilik yang ditunjuk, dan dapat dilacak dengan mudah untuk mencegah kehilangan.
R04	DSS04.07 Manage backup arrangements	A.8.13 Information backup	Memelihara backup atau cadangan informasi, software, dan sistem serta mengujinya secara berkala. Prosedur ini dilakukan sesuai dengan kebijakan atau SOP pencadangan yang telah disepakati untuk menghindari kesalahan konfigurasi pencadangan data.
R05	APO14.09 Support data archiving and retention	A.5.33 Protection of records	Melindungi dokumen dari kehilangan, perusakan, pemalsuan, atau akses yang tidak sah. Ini mencakup menjalankan prosedur pengarsipan dan retensi yang aman dan terorganisir sesuai dengan persyaratan yang berlaku.
R06	DSS01.05 Manage facilities	A.7.11 Supporting utilities	Melakukan proteksi terhadap fasilitas pemrosesan informasi dan aset TI dari kegagalan daya dan gangguan utilitas pendukung lainnya. Menyediakan sumber daya listrik alternatif seperti UPS atau genset serta melakukan pemeliharaan rutin terhadap perangkat tersebut.
R07	BAI09.03 Manage the asset life cycle	A. 7.13 Equipment maintenance	Pemeliharaan peralatan secara rutin dan terjadwal untuk menjamin ketersediaan, keandalan, dan umur pakai yang optimal. Seluruh kegiatan \pemeliharaan harus terdokumentasi secara sistematis dalam log riwayat perawatan tiap-tiap aset peralatan penyiaran, terutama yang digunakan di luar studio dalam berbagai kondisi operasional.
R08	BAI09.03 Manage the asset life cycle	A. 7.13 Equipment maintenance	Menetapkan jadwal pemeliharaan untuk semua peralatan yang ada di studio, termasuk alat teknik pendukung siaran dalam studio. Setiap tindakan perbaikan dan pemeliharaan dicatat dalam logbook aset untuk melacak riwayat dan kondisi aset secara berkala guna meminimalisir terpakainya peralatan yang sedang malfungsi agar siaran tidak terhambat.

Table 7. Penetapan Kontrol Risiko (b)

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
R09	BAI09.02 Manage critical assets	A. 7.13 Equipment maintenance	Menyusun rencana pemeliharaan terjadwal bagi seluruhm perangkat pendukung siaran. Seluruh aktivitas pemeliharaan dan perbaikan dicatat dalam log riwayt aset guna memantau kondisi dan dapat mencegah penggunaan alat yang bermasalah sehingga proses produksi atau siaran tetp terlaksana dengan optimal.
	DSS01.01 Perform operational procedures	A.5.37 Documented operating procedures	Mendokumentasikan dan menyediakan prosedur operasional untuk semua fasilitas pemrosesan informasi dan aset pendukung produksi agar semua personel yang membutuhkan dan ingin menggunakan alat pendukung siaran dilakukan secara benardan konsisten sesuai dengan SOP penggunaan alat.
R10	BAI09.03 Manage the asset life cycle	A.7.13 Equipment maintenance	Mengembangkan dan melaksanakan rencana pemeliharaaninfrastruktur TI secara berkala untuk memantau kelayakan agar tidak mengganggu operasional produksi apabila rusak. Melakukan evaluasi kelaya an secara berkala untuk mengidentifikasi perangkat yang perlu diperbarui atau diganti.
R11	BAI09.02 Manage critical assets	A. 8.8 Management of technical vulnerabilities	Merancang jadwal pemeliharaan berkala untuk semua infrastruktur pendukung siaran baik hardware maupun software. Setiap kegiatan perawatan dan perbaikan dicatat dalam log riwayat aset untuk memantau kondisi peralatan. Melakukan evaluasi terhadap asset melalui log yang sudah dibuat dan mengambil tindakan yang sesuai, seperti penerapan patch, untuk mencegah kegagalan fungsi apabila ada.
R12	APO03.01 Develop the enterprise architecture vision	A.8.27 - Secure system architecture and engineering principles	Menetapkan dan menerapkan prinsip-prinsip ekayasa sistem yang aman pada seluruh aktivitas pengembangan sistem informasi. Arsitektur sistem dibuat untuk memastikan integrasi data antar database berjalan optimal.
R13	APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions	A. 8.8 Management of t echnical vulnerabilities	Melakukan peninjauan dan analisis terhadap potensi kelemahanteknis dalam sistem IT yang berperan dalam mendukung kegiatan siaran. Menerapkan tindakan korektif yang dibutuhkan guna mengatasi kelemahan tersebut serta mem astikan kualitas dan kinerja sistem tetap optimal secara menyeluruh.
	BAI09.02 Manage critical assets	A. 7.13 - Equipment maintenance	
R14	APO13.03 Monitor and *review* the information security management system (ISMS)	A.5.35 *Independent review* of information security	Melaksanakan tinjauan independen terhadap pengelolaan keamanan informasi secara berkala atau saat terjadi perubahan signifikan. Proses tinjauan mencakup evaluasi terhadap personel, proses, dan teknologi untuk menemukan celah keamanan secara objektif.
R15	APO14. 10 Manage data backup and restore arrangements	A.8.13 Information backup	Menjalankan prosedur backup database secara berkala. Melakukan pengujian restorasi secara rutin untuk memastikan database dapat dipulihkan jika terjadi kerusakan atau serangan siber.
	DSS05.01 Protect against malicious software	A.8.7 Protection against malware	Mengimplementasikan solusi perlindungan dari malware dengan instalasi antivirus dan firewall. Evaluasi atau pemindaian rutin untuk mengurangi kemungkinan serangan.

Table 8. Penetapan Kontrol Risiko (b)

Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/ IEC 27001 Annex A	Deskripsi
R16	APO11.04 Perform quality monitoring, control and reviews	A.8.27 - Secure system architecture and engineering principles	Menerapkan prinsip rekayasa arsitektur sistem yang aman dalam setiap pengembangan dan pemeliharaan database. Standar teknis dan keamanan untuk desain database didokumentasikan, diimplementasikan, dan diaudit secara berkala untuk memastikan kepatuhan.
R17	DSS05.05 Manage physical access to IT assets	A.5.15 - Access control	Mengimplementasikan aturan untuk mengontrol hak akses terhadap informasi dan aset terkait. Akses ke ruang studio atau perangkat siaran dan sistem pendukungnya dibatasi hanya untuk personel yang memiliki otorisasi sesuai dengan tugasnya.
R18	DSS05.04 Manage user identity and logical access	A.5.18 - Access rights	Menjalankan proses tertentu sesuai dengan SOP untuk memberikan, meninjau, memodifikasi, dan mencabut hak akses pengguna. Melaksanakan tinjauan hak akses secara berkala untuk memastikan setiap pengguna hanya memiliki akses yang relevan dengan tanggung jawab pekerjaannya.
	APO14. 10 Manage data backup and restore arrangements	A.8.13 Information backup	Melakukan backup secara berkala terhadap seluruh database konten siaran untuk memastikan ketersediaan data saat dibutuhkan.
R19	DSS05.01 Protect against malicious software	A.8.7 Protection against malware	Menerapkan atau instalasi tools anti-malware terbaru untuk mengamankan database dari potensi virus atau software yang terindikasi malware yang dapat mengganggu keutuhan data.
	APO07.03 Maintain the skills and competencies of personnel	A. 6.3 Information security awareness, education and training	Menyelenggarakan program pelatihan penggunaan alat kerja, edukasi teknis, serta peningkatan kesadaran akan pentingnya keamanan informasi secara rutin dan terstruktur kepada seluruh pekerja.
R20	DSS01.01 Perform operational procedures	A.5.37 Documented operating procedures	Mendokumentasikan prosedur operasional atau menerapkan SOP yang sudah ada untuk memastikan seluruh pekerja memahami cara aman mengoperasikan teknologi produksi dan mengurangi risiko kecelakaan.