Analisis Manajemen Risiko TI Pada Bagian Konten Media Digital LPP TVRI Jabar Dengan *framework* ISO/IEC 27005:2022

1st Fairuz Ichsan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
fairuzichsan@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 Perkembangan teknologi informasi (TI) telah mengubah pola konsumsi informasi dan hiburan dari media konvensional ke digital. Sebagai media publik, LPP TVRI Jawa Barat perlu beradaptasi dengan perubahan ini, terutama dalam pengelolaan konten digital yang cepat, aman, dan andal. Namun, belum adanya kerangka manajemen risiko TI yang menyeluruh menunjukkan perlunya evaluasi dan pembenahan. Penelitian ini menggunakan *framework* ISO/IEC 27005:2022 untuk menganalisis manajemen risiko melalui tahapan identifikasi, analisis, evaluasi, dan penanganan. Selain itu, COBIT 2019 dan ISO/IEC 27001:2022 Annex A digunakan untuk menetapkan kontrol dan prioritas mitigasi berdasarkan klasifikasi risiko. Hasil studi mengidentifikasi 18 risiko TI: 1 risiko tinggi, 8 sedang, dan 9 rendah, yang masing-masing diberikan kontrol sesuai *framework*. Temuan ini diharapkan memperkuat sistem pengelolaan risiko LPP TVRI Jabar dan menjadi referensi bagi penerapan manajemen risiko TI di organisasi penyiaran dan digital lainnya.**

Kata kunci* — *manajemen risiko, teknologi informasi, ISO/IEC 27005:2022, COBIT 2019, ISO/IEC 27001:2022 Annex A

I. PENDAHULUAN

Transformasi teknologi informasi telah mengubah cara masyarakat mengakses informasi dan hiburan, dari media konvensional ke digital. Platform seperti YouTube, Instagram, dan layanan streaming kini menjadi pilihan utama *audiens*, menggeser dominasi televisi tradisional [1]. Kondisi ini menuntut LPP TVRI Jawa Barat untuk beradaptasi, khususnya dalam hal pengelolaan konten digital yang cepat, aman, dan relevan dengan perkembangan zaman. Data dari DataReportal (2025) menunjukkan bahwa sekitar 74,6% penduduk Indonesia menggunakan internet, dan 50,2% di antaranya aktif di media sosial [2]. Mayoritas pengguna internet menggunakan setidaknya satu platform media sosial. Hal ini menandakan bahwa masyarakat semakin terlibat dalam ruang digital untuk mengakses informasi, termasuk dari lembaga penyiaran publik.

Hasil pengamatan awal dan wawancara internal menunjukkan bahwa tata kelola risiko TI di LPP TVRI Jabar masih belum optimal. Pengelolaan risiko saat ini terbatas pada pelaporan manual kepada *person in charge* (PIC) di Bagian Konten Media, tanpa adanya sistem pencegahan dan prosedur yang terstruktur dalam mengidentifikasi serta menanggulangi risiko. Pendekatan reaktif ini menyebabkan keterlambatan dalam merespons ancaman seperti serangan siber, gangguan sistem, atau kegagalan distribusi konten digital, yang berisiko mengganggu operasional dan menurunkan kepercayaan publik. Ancaman terhadap media digital juga semakin meningkat. Laporan AJI (2024) mencatat 89 kasus serangan terhadap media di tahun 2023, dengan 16% di antaranya berupa serangan siber. Sementara itu, indeks keamanan digital media nasional hanya mencapai 19,71 dari 31, menunjukkan lemahnya praktik keamanan seperti audit sistem, SOP, dan pelatihan staf [3]. Untuk menjawab tantangan ini, penelitian ini menerapkan *framework* ISO/IEC 27005:2022 dalam proses manajemen risiko—meliputi identifikasi, analisis, evaluasi, dan penanganan. COBIT 2019 dan ISO/IEC 27001:2022 Annex A juga digunakan sebagai panduan dalam penetapan kontrol serta rekomendasi berbasis kategori risiko.

Diharapkan LPP TVRI Jabar dapat membangun sistem manajemen risiko TI yang proaktif dan menyeluruh, serta mendukung keberlangsungan pengelolaan konten digital yang aman dan terpercaya. Penelitian ini juga dapat menjadi rujukan bagi lembaga penyiaran lain dalam menghadapi tantangan digitalisasi secara strategis dan berkelanjutan.

II. KAJIAN TEORI

Menyajikan dan menjelaskan uraian teori-teori yang terkait dengan permasalahan, kerangka kerja, dan metode pada penelitian ini.

A. Teknologi informasi

Teknologi informasi (TI) memainkan peran penting dalam pengelolaan konten media digital, terutama di tengah percepatan transformasi digital. TI kini menjadi bagian strategis dalam proses produksi, manajemen, hingga

distribusi konten di berbagai platform seperti televisi daring, media sosial, dan situs web [4].

Penggunaan sistem TI memungkinkan pengelolaan konten yang terpusat, terdokumentasi, dan terkendali dengan baik. Ini membantu mempercepat penyampaian informasi, meningkatkan efisiensi operasional, dan menjaga kualitas konten yang dikonsumsi publik [5]. Selain itu, TI juga mendukung integrasi antara media konvensional dan digital dalam satu sistem terpadu yang bekerja secara real-time.

B. Manajemen risiko teknologi

Manajemen risiko teknologi informasi adalah pendekatan sistematis untuk mengenali, menganalisis, dan mengendalikan potensi ancaman terhadap sistem dan aset digital organisasi. Dalam konteks penyiaran publik yang semakin digital, ancaman seperti gangguan siaran, kehilangan data, kebocoran informasi, dan serangan siber dapat langsung memengaruhi kepercayaan publik dan kualitas layanan.

Penerapan manajemen risiko TI secara konsisten memungkinkan organisasi untuk mengantisipasi serta merespons insiden dengan lebih cepat dan efektif. Hal ini menjadi semakin penting seiring meningkatnya kompleksitas ancaman digital akibat pesatnya perkembangan teknologi. Lembaga penyiaran dituntut memiliki sistem pengelolaan risiko yang adaptif dan berfokus pada perlindungan aset informasi, khususnya dalam pengelolaan konten digital yang membutuhkan kecepatan dan akurasi tinggi [6].

Secara keseluruhan, manajemen risiko TI mendukung kelangsungan operasional dan perlindungan data dalam menghadapi dinamika dunia digital.

C. *Framework ISO/IEC 27005:2022*

Framework ISO/IEC 27005:2022 merupakan standar internasional yang memberikan panduan sistematis untuk mengelola risiko keamanan informasi. Standar ini mendukung ISO/IEC 27001 dengan menyediakan kerangka kerja yang terstruktur namun fleksibel, yang dapat diterapkan di berbagai sektor, termasuk lembaga penyiaran publik. Dalam pengelolaan konten media digital, *framework* ini membantu organisasi mengidentifikasi potensi ancaman terhadap sistem informasi, mengevaluasi tingkat risiko berdasarkan dampak dan kemungkinan, serta menetapkan langkah pengendalian yang tepat.

Penerapan ISO/IEC 27005 memberikan pemetaan risiko berbasis aset informasi yang lebih jelas, sekaligus meningkatkan kesiapsiagaan organisasi dalam menghadapi insiden keamanan [7].

D. *Framework COBIT 2019*

Framework COBIT 2019 adalah kerangka kerja tata kelola teknologi informasi yang dikembangkan oleh ISACA sebagai pembaruan dari COBIT 5. *Framework* ini memberikan panduan untuk memaksimalkan nilai TI sekaligus meminimalkan risiko yang ditimbulkan oleh penggunaan teknologi informasi [8]

COBIT 2019 menekankan pentingnya manajemen risiko, akuntabilitas, dan peningkatan kapabilitas TI melalui pendekatan berbasis proses dan domain. Setiap domain memiliki tujuan spesifik yang mendukung pengelolaan TI yang efektif dan efisien [9].

E. *Risk Profile Design Factor (IT Risk Categories) COBIT 2019*

Risk profile dalam COBIT 2019 merupakan elemen penting dalam desain tata kelola risiko, yang digunakan untuk mengelompokkan dan memahami jenis-jenis risiko yang dapat menghambat pencapaian tujuan bisnis, khususnya dalam konteks teknologi informasi [10].

Dalam penelitian ini, digunakan delapan kategori risiko (*risk profiles*) yang direkomendasikan oleh COBIT 2019, yaitu: *Data and Information Management, Noncompliance, Third-party/Supplier Incidents, Unauthorized Actions, IT Expertise, Skills and Behavior, IT Operational Infrastructure Incidents, Logical Attacks (Hacking, Malware, etc.).*

Kategori ini digunakan untuk mengklasifikasikan risiko dalam pengelolaan konten digital di LPP TVRI Jawa Barat agar dapat ditangani dengan kontrol yang sesuai berdasarkan panduan COBIT 2019.

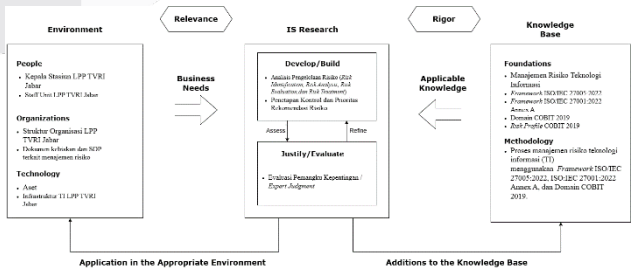
F. *Framework ISO/IEC 27001:2022*

Framework ISO/IEC 27001:2022 merupakan standar internasional yang menjadi rujukan utama dalam membangun dan mengelola Information Security Management System (ISMS) secara efektif. Standar ini dirancang untuk membantu organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi melalui pendekatan yang sistematis, terdokumentasi, dan dapat diaudit [11]. Pada edisi terbaru ini, ISO/IEC 27001:2022 memperkenalkan pembaruan pada Annex A, yang kini mencakup 93 kontrol keamanan informasi yang telah disusun ulang agar lebih sesuai dengan tantangan saat ini. Kontrol-kontrol tersebut meliputi aspek penting seperti struktur organisasi, perlindungan terhadap pengguna, keamanan fisik, hingga pemanfaatan teknologi.

III. METODE PENELITIAN

A. Model Konseptual

Penelitian ini menggunakan model konseptual sebagai panduan dalam merancang langkah-langkah sistematis untuk mencapai tujuan penelitian. Model ini mengacu pada pendekatan *Design Science Research* (DSR) yang dikembangkan oleh Alan Hevner, yang terdiri dari tiga komponen utama: Environment, Research, dan Knowledge Base. Gambar III.1 menyajikan ilustrasi model konseptual yang digunakan sebagai panduan dalam penelitian ini.



GAMBAR 1
Model Konseptual

Environment mencakup unsur People, Organizations, dan Technology. People merujuk pada individu yang terlibat dalam pengelolaan TI di TVRI Jawa Barat, Organizations mencakup struktur, kebijakan, dan prosedur organisasi,

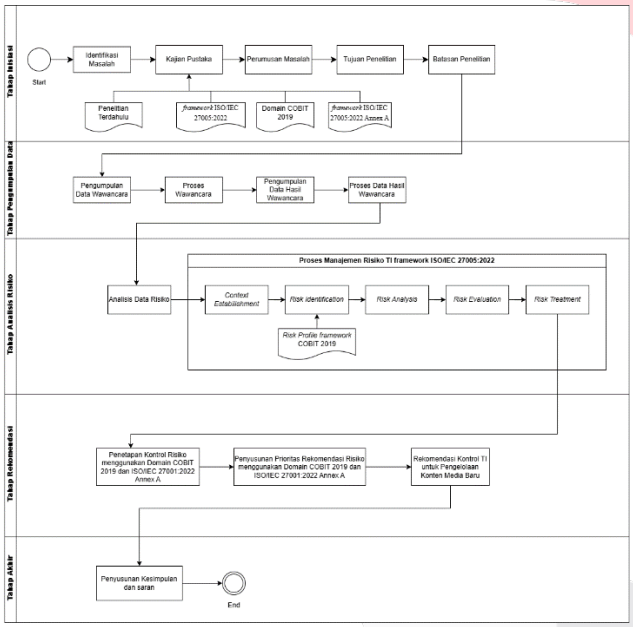
sementara Technology mengacu pada infrastruktur dan aset TI yang digunakan dalam mendukung konten media digital.

Research mencakup tahapan manajemen risiko berdasarkan ISO/IEC 27005:2022, yakni identifikasi, analisis, evaluasi, dan penanganan. Selanjutnya, ditentukan kontrol yang sesuai sebagai langkah mitigasi.

Knowledge Base menjadi landasan teoritis penelitian ini, terdiri dari aspek Foundations dan Methodology. Foundations melibatkan teori manajemen risiko TI serta prinsip dari ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A. Sementara Methodology mencakup pendekatan sistematis dalam pelaksanaan penelitian ini.

B. Sistematika penyelesaian masalah

Penomoran Penelitian ini mengacu pada pendekatan *Design Science Research* (DSR) yang dikembangkan oleh Alan Hevner sebagai dasar dalam menyusun model konseptual. Model ini digunakan untuk merancang langkah-langkah sistematis guna mencapai tujuan penelitian, sebagaimana digambarkan dalam Gambar III.2.



GAMBAR 2
Sistematika Penyelesaian Masalah

Model konseptual terdiri dari tiga komponen utama, yaitu *Environment, Research, dan Knowledge Base*. Komponen *Environment* meliputi *People, Organizations, dan Technology*. *People* merujuk pada pihak-pihak yang terlibat dalam pengelolaan TI di TVRI Jawa Barat, *Organizations* mencakup struktur serta kebijakan lembaga, sedangkan *Technology* mengacu pada infrastruktur digital yang mendukung manajemen konten.

Bagian Research merupakan inti dari proses penelitian, terdiri atas dua aktivitas utama: *Develop/Build* dan *Justify/Evaluate*. Tahap *Develop/Build* meliputi proses identifikasi, analisis, evaluasi, hingga penanganan risiko, sekaligus menetapkan kontrol dan rekomendasi mitigasi. Selanjutnya, *Justify/Evaluate* dilakukan dengan melibatkan pemangku kepentingan guna menilai efektivitas solusi yang dikembangkan.

Adapun *Knowledge Base* menjadi landasan keilmuan dalam penelitian ini, terdiri atas teori dasar manajemen risiko dan metodologi. *Foundations* mengacu pada *framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A, sedangkan *Methodology* mencakup pendekatan sistematis dalam penyusunan dan pelaksanaan penelitian.

C. Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui dua jenis sumber, yaitu data primer dan data sekunder, guna memperoleh informasi yang akurat dan mendalam untuk mendukung analisis manajemen risiko TI dalam pengelolaan konten media digital di TVRI Jawa Barat.

Data primer diperoleh melalui wawancara terstruktur dengan pihak-pihak internal yang terlibat langsung, seperti tim pengelola konten media digital. Wawancara difokuskan pada identifikasi risiko, tantangan yang dihadapi, serta upaya mitigasi yang sudah diterapkan atau direncanakan.

Sementara itu, data sekunder dikumpulkan dari studi pustaka, yang mencakup jurnal ilmiah, buku, laporan teknis, dokumen kebijakan, dan referensi digital lainnya yang sesuai dengan topik manajemen risiko TI. *Framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A juga digunakan untuk menetapkan kontrol dan menyusun rekomendasi prioritas berdasarkan risiko yang teridentifikasi. Pendekatan ini memberikan dasar teoritis yang kuat untuk mendukung analisis terhadap data primer yang diperoleh.

D. Pengumpulan Data

Data Pengolahan data dalam penelitian ini dilakukan dengan mengintegrasikan *framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A, yang difokuskan pada manajemen risiko TI di Bagian Konten Media Digital LPP TVRI Jawa Barat. Proses ini mencakup analisis menyeluruh terhadap risiko, diikuti dengan penyusunan kontrol dan rekomendasi prioritas untuk meminimalkan potensi dampak risiko, sehingga dapat meningkatkan efektivitas pengelolaan konten digital.

Langkah awal dimulai dengan mengidentifikasi dan mengklasifikasikan risiko berdasarkan kategori *Risk Profile Design Factor* (*IT Risk Categories*) dari COBIT 2019. Selanjutnya, dilakukan empat tahapan utama analisis risiko, yaitu *Risk Identification, Risk Analysis, Risk Evaluation, dan Risk Treatment*, guna memahami secara komprehensif potensi ancaman terhadap sistem TI dan menyiapkan langkah mitigasi yang sesuai.

Setelah analisis selesai, kontrol dan rekomendasi risiko disusun menggunakan acuan dari COBIT 2019 dan Annex A ISO/IEC 27001:2022. Kedua *framework* ini menyediakan panduan kontrol yang dapat diimplementasikan secara langsung, membantu menyusun strategi mitigasi yang terukur dan kontekstual untuk mendukung keamanan informasi dan meningkatkan kepercayaan publik terhadap layanan digital TVRI Jabar.

E. Metode Evaluasi

Penelitian ini menggunakan metode *Expert Judgment* sebagai pendekatan evaluasi. Tujuan dari metode ini adalah untuk mendapatkan *insight* dan *feedback* dari para ahli yang memiliki keahlian dan pengalaman dalam bidang Manajemen

Risiko TI. Evaluasi dilakukan melalui sesi wawancara dan diskusi bersama pakar yang memahami implementasi *framework* ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A dalam konteks pengelolaan risiko TI secara praktis.

F. Alasan Pemilihan Metode

Penelitian ini menggunakan pendekatan *Design Science Research* (DSR) sebagai metode utama karena dinilai paling sesuai dalam menyusun solusi berbasis desain yang terstruktur dan sesuai terhadap permasalahan pengelolaan risiko TI di Bagian Konten Media Digital LPP TVRI Jawa Barat. Pendekatan ini menggabungkan praktik desain dengan dasar ilmiah yang kuat, serta melibatkan tiga elemen inti, yaitu *Environment, IS Research*, dan *Knowledge Base*.

Aspek *Environment* digunakan untuk memahami secara menyeluruh konteks organisasi, termasuk struktur, proses kerja, infrastruktur teknologi, dan peran pengguna dalam ekosistem digital yang sedang diteliti. Sementara itu, IS *Research* memfasilitasi proses perancangan, pengembangan, dan evaluasi solusi yang ditawarkan agar sesuai dengan kondisi dan kebutuhan nyata organisasi. Terakhir, *Knowledge Base* berfungsi sebagai landasan keilmuan yang mencakup teori, metodologi, serta penggunaan *framework* seperti ISO/IEC 27005:2022, COBIT 2019, dan ISO/IEC 27001:2022 Annex A dalam mendukung analisis dan rekomendasi manajemen risiko yang tepat.

IV. HASIL DAN PEMBAHASAN

A. Matriks Risiko

Matriks risiko merupakan alat yang digunakan dalam manajemen risiko untuk memetakan potensi risiko berdasarkan dua aspek utama, yaitu tingkat kemungkinan (*likelihood*) dan dampak (*impact*). Matriks ini membantu mempermudah pemahaman visual tentang seberapa besar risiko yang mungkin terjadi, seperti yang ditunjukkan pada Tabel 1, dan mengacu pada referensi dari [12]. Dengan pengelompokan risiko ke dalam kategori seperti rendah, sedang, tinggi, dan kritis, organisasi dapat lebih mudah menetapkan prioritas serta menyusun strategi penanganan yang tepat.

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

Penentuan tingkat risiko dilakukan dengan mengevaluasi kemungkinan terjadinya risiko dan besarnya dampak yang ditimbulkannya. Kedua faktor ini harus dianalisis secara bersamaan agar hasil penilaian lebih akurat. Informasi lengkap terkait klasifikasi tingkat risiko disajikan pada Tabel 2.

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*

Respon terhadap risiko merupakan strategi untuk menangani risiko berdasarkan tingkat keparahan dan probabilitasnya. Tindakan ini bertujuan untuk mengurangi, menghindari, menerima, atau membagi risiko agar dampaknya dapat dikendalikan. Strategi penanganan ditentukan dari hasil analisis nilai risiko. Rangkuman jenis-jenis respon risiko ditampilkan pada Tabel 3[7] .

TABEL 3
Risk Response

Risk Response		
No	**Penanganan**	**Penjelasan**
1.	*Risk Retention* (Retensi risiko)	Risiko dibiarkan tanpa tindakan tambahan karena dianggap masih dalam batas yang dapat diterima. Misalnya, kerusakan kecil ditangani langsung tanpa prosedur panjang.
2.	*Risk Modification* (Modifikasi risiko)	Risiko dikurangi dengan menyesuaikan kontrol, seperti backup data rutin atau rencana pemulihan gangguan.
3.	*Risk Sharing* (Membagi risiko)	Risiko dibagi ke pihak lain seperti vendor, asuransi, atau melalui kerja sama pihak ketiga.
4.	*Risk Avoidance* (Mengurangi risiko)	Risiko dihindari sepenuhnya dengan menghentikan atau mengubah aktivitas yang berisiko tinggi

B. *Risk Analysis*

Tujuan dari tahap ini adalah untuk menilai tingkat keparahan setiap risiko berdasarkan kemungkinan terjadinya, dampak yang ditimbulkan, serta hasil evaluasi secara keseluruhan. Hasil analisis ini disajikan dalam Tabel 4.

TABEL 4
Risk Analysis

No	*Risk Profile*	*Risk* ID	Deskripsi Risiko	Nilai Risiko	Level Risiko
1	*Data and Information Management (19)*	R01	Penyebaran informasi *hoaks* atau tidak terverifikasi melalui akun media sosial resmi.	5	*Medium*
2		R02	Konten digital mendapatkan reaksi negatif dari masyarakat	5	*Medium*
3		R03	Ketidaksinkronan konten di berbagai platform digital menyebabkan inkonsistensi informasi yang diterima oleh publik.	3	*Low*

No	*Risk Profile*	*Risk* ID	Deskripsi Risiko	Nilai Risiko	Level Risiko
4		R04	Kehilangan arsip konten digital.	3	*Low*
5	*Noncompliance (13)*	R05	Konten Film/Dokumenter/Variety tidak lulus sensor.	4	*Low*
6		R06	Konten yang dianggap tidak netral atau berpihak.	3	*Low*
7		R07	Terjadinya Pelanggaran *Copyright.*	8	*Medium*
8	*Third-party/Supplier Incidents (12)*	R08	Laporan ketidakpuasan dari mitra kerja sama terkait konten media digital.	3	*Low*
9		R09	Akun media sosial bisa ditutup secara sepihak oleh platform jika melanggar pedoman komunitas.	4	*Low*
10	*Unauthorized Actions (7)*	R10	Pemalsuan akun media sosial (akun tiruan / palsu).	3	*Low*
11		R11	Pencurian Konten Digital untuk kepentingan pihak tertentu tanpa izin.	12	*High*
12	*IT Expertise, Skills and Behavior (4)*	R12	Konten yang diproduksi atau disebarkan tidak menarik bagi *audiens* karena tidak sesuai dengan tren dan kebutuhan mereka.	5	*Medium*
13		R13	Keterlambatan *respons* dalam menangani komentar, kritik, atau isu yang muncul secara tiba-tiba di media sosial resmi.	6	*Medium*
14		R14	Tidak tercapainya informasi publik di media sosial.	3	*Low*
15	*IT Operational Infrastructure Incidents (6)*	R15	Overload Server atau Gangguan Infrastruktur Teknologi.	6	*Medium*
16	*Logical Attacks (Hacking, Malware, etc.) (11)*	R16	Penggunaan *deepfake* dapat memanipulasi wajah atau suara dalam konten digital sehingga menimbulkan disinformasi.	4	*Low*
17		R17	Akun media sosial resmi bisa diretas dan disalahgunakan oleh pihak tidak bertanggung jawab.	5	*Medium*
18	*Technology-based Innovation (7)*	R18	Perubahan Algoritma platform yang dapat menurunkan visibilitas konten.	8	*Medium*

C. *Risk Treatment*

Tahap evaluasi risiko dilakukan untuk menetapkan prioritas penanganan berdasarkan tingkat keparahan risiko yang telah dianalisis. Risiko kemudian dikelompokkan agar organisasi dapat menentukan langkah penanganan yang sesuai. Hasil evaluasi ditampilkan pada Tabel 5.

TABEL 5
Risk Treatment

No	*Risk Profile*	*Risk* ID	Deskripsi Risiko	Level Risiko	Respon Risiko
1	*Data and Information Management (19)*	R01	Penyebaran informasi *hoaks* atau tidak terverifikasi melalui akun media sosial resmi.	*Medium*	*Modification*
2		R02	Konten digital mendapatkan reaksi negatif dari masyarakat	*Medium*	*Modification*
3		R03	Ketidaksinkronan konten di berbagai platform digital menyebabkan inkonsistensi informasi yang diterima oleh publik.	*Low*	*Retention*
4		R04	Kehilangan arsip konten digital.	*Low*	*Retention*
5	*Noncompliance (13)*	R05	Konten Film/Dokumenter/Variety tidak lulus sensor.	*Low*	*Retention*
6		R06	Konten yang dianggap tidak netral atau berpihak.	*Low*	*Retention*
7		R07	Terjadinya Pelanggaran *Copyright.*	*Medium*	*Modification*
8	*Third-party/Supplier Incidents (12)*	R08	Laporan ketidakpuasan dari mitra kerja sama terkait konten media digital.	*Low*	*Sharing*
9		R09	Akun media sosial bisa ditutup secara sepihak oleh platform jika melanggar pedoman komunitas.	*Low*	*Retention*
10	*Unauthorized Actions (7)*	R10	Pemalsuan akun media sosial (akun tiruan / palsu).	*Low*	*Retention*
11		R11	Pencurian Konten Digital untuk kepentingan pihak tertentu tanpa izin.	*High*	*Modification*
12	*IT Expertise, Skills and Behavior (4)*	R12	Konten yang diproduksi atau disebarkan tidak menarik bagi *audiens* karena tidak sesuai dengan tren dan kebutuhan mereka.	*Medium*	*Modification*
13		R13	Keterlambatan *respons* dalam menangani komentar, kritik, atau isu yang muncul secara tiba-tiba di media sosial resmi.	*Medium*	*Modification*
14		R14	Tidak tercapainya informasi publik di media sosial.	*Low*	*Retention*
15	*IT Operational Infrastructure Incidents (6)*	R15	Overload Server atau Gangguan Infrastruktur Teknologi.	*Medium*	*Modification*
16	*Logical Attacks (Hacking, Malware, etc.) (11)*	R16	Penggunaan *deepfake* dapat memanipulasi wajah atau suara dalam konten digital sehingga menimbulkan disinformasi.	*Low*	*Retention*
17		R17	Akun media sosial resmi bisa diretas dan disalahgunakan oleh pihak tidak bertanggung jawab.	*Medium*	*Modification*

No	*Risk Profile*	*Risk* ID	Deskripsi Risiko	Level Risiko	Respon Risiko
18	*Technology-based Innovation (7)*	R18	Perubahan Algoritma platform yang dapat menurunkan visibilitas konten.	*Medium*	*Modification*

D. Penetapan Kontrol Risiko

Penetapan kontrol dilakukan untuk memastikan bahwa risiko dapat dikelola melalui implementasi dan pemantauan prosedur yang sesuai dengan standar organisasi. Dalam penelitian ini, kontrol ditetapkan berdasarkan prinsip Domain COBIT 2019 dan ISO/IEC 27001:2022 Annex A sebagai strategi untuk mengurangi dampak dan kemungkinan risiko. Langkah ini bertujuan memperkuat efektivitas pengelolaan risiko serta menjaga keberlangsungan operasional di Bagian Konten Media Digital LPP TVRI Jabar. Tabel 6 merinci penetapan kontrol tersebut.

TABEL 6
Penetapan Kontrol Risiko

No	Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
1.	R01	APO12.01 - *Collect Data*	A.5.7 - *Threat intelligence*	Mengembangkan dan mengimplementasikan prosedur validasi fakta *(fact-checking)* konten sebelum dipublikasikan di akun media sosial resmi. Prosedur ini akan mencakup langkah-langkah validasi sumber, perbandingan informasi dari berbagai kanal terpercaya, dan verifikasi ulang fakta.
2	R07	BAI01.07 – *Manage program quality*	A.6.3 - *Information security awareness, education and training*	Melakukan analisis risiko terhadap konten sebelum produksi, terutama jika menyangkut isu-isu yang berpotensi sensitif (seperti agama, politik, atau budaya). Konten harus disusun secara seimbang, faktual, dan informatif. Setelah dipublikasikan, dilakukan pemantauan terhadap tanggapan publik serta disiapkan respons cepat jika muncul reaksi negatif.
3	R15	BAI03.01 - *Design high-level solutions*	A.8.9 - *Configuration management*	Mengembangkan sistem manajemen konten digital yang terintegrasi untuk memastikan semua konten direncanakan, ditinjau, dan didistribusikan secara konsisten di berbagai platform resmi. Menetapkan prosedur sinkronisasi dan koordinasi antar tim untuk memastikan informasi yang dipublikasikan konsisten dan tidak membingungkan publik.
4.	R16	DSS01.01 - *Perform operational procedures*	A.8.13 - *Information backup*	Menerapkan sistem *backup* otomatis dan berkala untuk seluruh arsip konten digital dengan penyimpanan di lokasi yang aman dan terpisah. Menyusun prosedur pengelolaan arsip digital yang terstruktur, termasuk klasifikasi dan pengindeksan konten agar mudah diakses dan dipulihkan jika diperlukan.
5.	R06	BAI03.06 *Perform quality assurance (QA)*	A.5.31 - *Legal, statutory, regulatory and contractual requirements*	Melakukan proses sensor yang ketat untuk memastikan bahwa konten yang akan disiarkan memenuhi standar yang berlaku dan tidak ada pelanggaran nilai, norma sosial, atau hukum di dalamnya.
6.	R08	APO12.01 - *Collect Data*	A.5.8 - *Information security in project management*	Menerapkan audit editorial secara berkala untuk memastikan konten disajikan secara netral dan berimbang. Analisis data dari berbagai platform digunakan untuk mendeteksi potensi bias. Sebelum dipublikasikan, setiap konten harus ditinjau menggunakan panduan netralitas dan formulir evaluasi editorial.
7.	R11	MEA03.01 -*Identify external compliance requirements* APO12.01 - *Collect Data*	A.5.31 - *Legal, statutory, regulatory and contractual requirements*	Melakukan identifikasi dan pemantauan secara berkala terhadap ketentuan hukum dan persyaratan kepatuhan eksternal terkait hak cipta. Menyusun dan menerapkan prosedur pengelolaan lisensi serta izin penggunaan konten secara resmi sebelum proses produksi dan distribusi dilakukan. Setiap konten eksternal wajib melalui tahap verifikasi legalitas dan pencatatan hak cipta guna memastikan kesesuaian dengan regulasi yang berlaku.
8.	R02	APO08.03 - *Manage the business relationship*	A.5.20 - *Addressing information security within supplier agreements*	Melakukan peninjauan konten secara berkala untuk memastikan seluruh program konten digital yang dipublikasikan telah sesuai dengan ketentuan dan standar yang tercantum dalam kontrak kerja sama. Mengkonfirmasi ulang terhadap konten bersama pihak terkait sebelum dipublikasikan untuk memastikan kesesuaian informasi yang disampaikan.
9.	R14	MEA03.01 - *Identify External Compliance Requirements*	A.5.31 - *Legal, statutory, regulatory and contractual requirements*	Menyusun panduan internal yang mengikuti pedoman komunitas masing-masing platform. Melakukan peninjauan konten sebelum tayang untuk memastikan tidak melanggar aturan yang berlaku di media sosial.

No	Risk ID	Judul Kontrol COBIT 2019	Judul Kontrol ISO/IEC 27001 Annex A	Deskripsi
10.	R03	DSS05.04 *Manage user identity and logical access*	A.5.16 - *Identity management* A.8.16 - *Monitoring activities*	Mengajukan permohonan verifikasi *(verified badge)* ke semua platform media sosial yang digunakan secara resmi. Melakukan monitoring berkala untuk akun tiruan, serta berkoordinasi dengan platform media sosial untuk melaporkan dan menghapus akun palsu.
11.	R12	DSS05.06 - *Manage sensitive documents and output devices*.	A.5.32 - *Intellectual property rights*	Menerapkan teknologi perlindungan hak cipta seperti digital *watermarking* pada semua konten yang diproduksi untuk menandai kepemilikan dan mencegah distribusi ilegal. Lakukan pemantauan aktif di ranah digital untuk mendeteksi penggunaan tanpa izin, dan segera lakukan tindakan hukum atau takedown jika terbukti.
12.	R05	BAI01.07 *Manage program quality*	A.6.3 - *Information security awareness, education and training*	Melakukan riset pasar dan analisis preferensi *audiens* secara berkala untuk menyesuaikan konten dengan tren dan kebutuhan terkini. Tim Konten Media juga harus cepat beradaptasi dengan perubahan tren dan kebutuhan *audiens*.
		Menambahkan aktivitas "*Audience Feedback*"	-	Menambahkan sistem *Audience Feedback* yang efektif untuk memungkinkan *audiens* memberikan masukan secara langsung terkait konten yang di inginkan.
13.	R18	DSS01.01 - *Perform operational procedures*	A.5.24 - *Information security incident management planning and preparation*	Menyusun dan menerapkan SOP respons cepat untuk menangani komentar, kritik, dan isu di media sosial secara *real-time.*
		APO07.03 - *Maintain the skills and competencies of personnel*	A.6.3 - *Information security awareness, education and training*	Menetapkan tim khusus untuk memantau dan merespons dalam waktu yang telah ditentukan. Hal ini penting agar *audiens* tetap percaya dan tidak beralih ke media lain yang lebih responsif.
14	R09	DSS01.01 - *Perform operational procedures*	A.5.14 - *Information transfer*	Menyusun rencana distribusi konten yang jelas berdasarkan waktu aktif *audiens* dan jenis platform. Tim media sosial berkoordinasi secara rutin agar penyebaran informasi lebih terarah, konsisten, dan tepat sasaran.
15.	R17	BAI04.01 - *Assess current availability, performance and capacity and create a baseline*	A.8.9 – *Configuration Management*	Melakukan penilaian kapasitas dan performa infrastruktur TI secara berkala untuk memastikan kesiapan dalam menangani trafik media digital yang tinggi. Kapasitas server perlu ditingkatkan sesuai kebutuhan operasional.
16.	R10	APO13.02 -*Define and manage an information security and privacy risk treatment plan*	A.8.25 - *Secure Development Life Cycle*	Menerapkan teknologi deteksi *deepfake* berbasis AI untuk mengidentifikasi konten yang dimanipulasi secara visual atau audio, serta menetapkan prosedur validasi konten digital yang ketat sebelum publikasi.
17	R13	DSS05.04 - *Manage user identity and logical access*	A.5.15 - *Access control*	Sistem keamanan harus memantau aktivitas akun, membatasi akses hanya pada personel yang berwenang, dan melakukan audit berkala terhadap penggunaan akun.
		Menambahkan aktivitas *"Multi-Factor Authentication Policy"*	A.8.5 - *Secure authentication*	Menerapkan kebijakan penggunaan password yang kuat dan unik, serta mengaktifkan autentikasi dua faktor (*Multi-Factor Authentication*) pada seluruh akun media sosial resmi.
18	R04	DSS01.01 - *Perform operational procedures*	A.8.16 - *Monitoring activities*	Melakukan pemantauan untuk mengikuti perubahan algoritma di platform seperti YouTube, Instagram, dan TikTok. Mengembangkan dan mengimplementasikan strategi distribusi konten seperti pemilihan kata kunci, format video, waktu unggah, dan tagar yang sesuai.

V. KESIMPULAN

Hasil penelitian menunjukkan bahwa Bagian Konten Media Digital LPP TVRI Jawa Barat membutuhkan sistem manajemen risiko TI yang menyeluruh untuk mengantisipasi berbagai ancaman terhadap operasional konten digital. Penelitian ini menggabungkan *framework* ISO/IEC 27005:2022 sebagai panduan utama dalam proses manajemen risiko (identifikasi, analisis, evaluasi, dan penanganan), serta COBIT 2019 dan ISO/IEC 27001:2022 Annex A sebagai pendukung dalam penetapan kontrol dan rekomendasi. Integrasi ketiga *framework* ini menghasilkan pendekatan yang sistematis dan terukur dalam pengelolaan risiko TI.

Proses manajemen risiko dilakukan sesuai tahapan ISO/IEC 27005:2022, dimulai dari penetapan konteks dan kriteria penilaian, dilanjutkan dengan identifikasi risiko berdasarkan *impact* dan *likelihood*, serta analisis untuk menghitung nilai risiko. Dari 18 risiko yang ditemukan, terdapat 1 risiko kategori tinggi, 8 sedang, dan 9 rendah. Risiko kategori rendah dinilai masih dapat ditoleransi, sedangkan risiko menengah dan tinggi memerlukan tindakan mitigasi yang lebih lanjut.

Untuk mengatasi berbagai risiko teknologi informasi yang telah diidentifikasi sebelumnya dietapkan strategi

penanganan yang tepat, yaitu *modification, retention, sharing*, dan *avoidance*. Dari 18 risiko yang dianalisis, 9 ditangani dengan modifikasi (*modification)*, 8 diterima (*retention*), dan 1 dibagi kepada pihak ketiga (*sharing*). Setiap risiko diberikan kontrol dan rekomendasi yang sesuai mengacu pada Domain COBIT 2019 dan ISO/IEC 27001:2022 Annex A untuk memastikan efektivitas penanganan.

REFERENSI

[1] A. M. Putra, A. Setia Gunawan, and N. Erlita, "From Conventional to Digital Media: Digital Transformation Strategies on METRO TV in Indonesia," *J Theor Appl Inf Technol*, vol. 15, no. 23, pp. 7640–7642, 2023, Accessed: Jun. 08, 2025. [Online]. Available: www.metrotvnews.com,

[2] Simon Kemp, "Digital 2025: Indonesia — DataReportal – Global Digital Insights," DataReportal. Accessed: Jun. 11, 2025. [Online]. Available: https://datareportal.com/reports/digital-2025-indonesia

[3] E. Wendratama, P. L. N. Suci, L. De Suriyani, and Masduki, "Laporan Riset Keamanan Digital Perusahaan Media di Indonesia," 2024. [Online]. Available: www.aji.or.id

[4] E. Mulyadi, "Industri Media Televisi Di Tengah Era Digitalisasi Dan Konvergensi Media Baru," *Journal Visioner: Journal of Television*, vol. 04, no. 1, pp. 1–10, 2019.

[5] Y. Harfiah, "Peran Media Online Terhadap Kinerja Lembaga Penyiaran Publik Di Era Konvergensi Media (Studi Kasus : LPP RRI Madiun)," *Jurnal Revitalisasi*, vol. 7, no. 2, pp. 144–161, Jan. 2018, doi: 10.32503/REVITALISASI.V7I2.796.

[6] M. H. Topan Nurdiansyah, "Analisis dan Penerapan Manajemen Risiko Aplikasi Pemantauan Serta Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013," *Universitas Langlangbuana*, vol. 33, no. 1, pp. 1–12, 2022.

[7] ISO/IEC 27005, "ISO/IEC 27005:2022, Information Security Risk Management," *ISO/IEC 27005:2022*, 2022.

[8] ISACA, *Designing an Information and Technology Governance Solution*. 2018.

[9] R. Afdhani and B. Soewito, "Perancangan Tata Kelola TI Menggunakan Framework COBIT 2019 pada Pusat Data dan Informasi Kementerian," *Jurnal Tata Kelola dan Kerangka Kerja TI*, vol. 10, no. 1, p. 22, 2024.

[10] ISACA, *Governance and Management Objectives*. 2018. [Online]. Available: https://www.isaca.org/resources/cobit

[11] ISO/IEC 27001, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements," *ISO/IEC Standard*, vol. 2022, pp. 11–18, 2022, doi: 10.2307/j.ctv30qq13d.

[12] Y. N. Qintharah, "Perancangan Penerapan Manajemen Risiko," *JRAK: Jurnal Riset Akuntansi dan Komputerisasi Akuntansi*, vol. 10, no. 1, pp. 67–86, Feb. 2019, doi: 10.33558/JRAK.V10I1.1645.