Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan Metode *Failure Mode and Effects Analysis* (FMEA) dan Kontrol ISO/IEC 27001:2022 (Studi Kasus: Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ)

Alda Risma Harjian, Raden Venantius Hari Ginardi, dan Henning Titi Ciptaningtyas
Departemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
e-mail: hari@its.ac.id

***Abstrak*—Teknologi informasi merupakan salah satu kebutuhan penting sebuah organisasi untuk menunjang kegiatan operasional serta membantu meningkatkan efisiensi dan efektifitas proses kegiatan organisasi. Namun, penggunaan TI melibatkan risiko keamanan informasi, sehingga bisnis atau lembaga pemerintah harus mengelola aset informasi mereka. Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ bertanggung jawab atas pengelolaan informasi dan statistik di wilayah tersebut, tetapi belum memiliki kebijakan manajemen risiko yang mengatur tentang keamanan informasi. Penelitian ini bertujuan untuk mengidentifikasi, menilai, dan memberikan rekomendasi mitigasi risiko pada DISKOMINFOTIK. Data dikumpulkan melalui observasi, wawancara, kuesioner, dan peninjauan dokumen. Metode *Failure Mode and Effect Analysis* (FMEA) digunakan untuk mengidentifikasi proses bisnis, penyebab, dampak kegagalan, serta menilai tingkat keparahan, kejadian, deteksi, dan *Risk Priority Number* (RPN). ISO/IEC 27001 memberikan rekomendasi mitigasi risiko. Dalam penelitian ini diperoleh 37 *potential cause* dan 29 risiko terkait aset *hardware, software, people, network*, dan data. Berdasarkan RPN, terdapat 3 risiko kategori *very low*, 11 *low*, 6 *moderate*, 11 *high*, dan 6 *very high*. Standar Nasional Indonesia (SNI) ISO/IEC 27001:2022 digunakan untuk mengurangi risiko dengan 9 kontrol keamanan.**

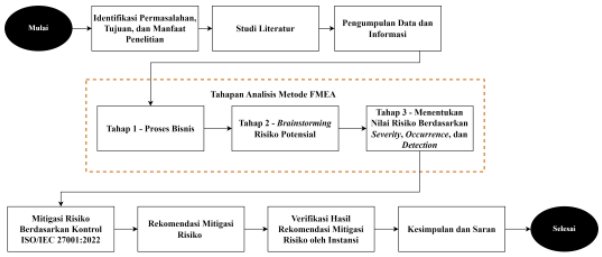
***Kata Kunci*—*Failure Mode and Effect Analysis* (FMEA), ISO/IEC 27001:2022, Keamanan Informasi, Manajemen Risiko.**

I. PENDAHULUAN

TEKNOLOGI informasi (TI) adalah bagian penting dalam operasional dan proses bisnis organisasi, meningkatkan efisiensi dan efektivitas [1]. Tidak dapat dipungkiri bahwa penggunaan TI membawa risiko keamanan informasi seperti kebocoran data dan serangan siber [2]. Oleh karena itu, pengelolaan aset informasi harus dilakukan dengan tepat melalui penilaian dan mitigasi risiko, yaitu manajemen risiko keamanan informasi.

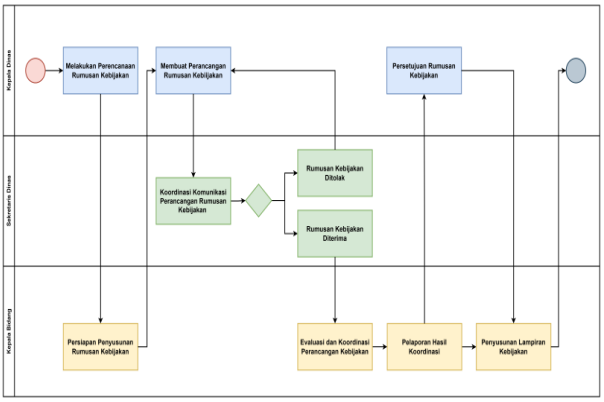
Metode *Failure Mode and Effect Analysis* (FMEA) digunakan untuk mengidentifikasi dan menilai risiko TI dengan 4 penilaian: *severity*, *occurrence*, *detection*, dan *Risk Priority Number* (RPN) [3]. Nilai RPN tetinggi menentukan prioritas tindakan perbaikan. ISO/IEC 27001:2022 memberikan rekomendasi mitigasi dengan praktik terbaik dalam keamanan informasi dan pendekatan berbasis risiko [4].

Pemilihan Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ didasari oleh riwayat insiden keamanan informasi, seperti kebocoran data dan kerusakan perangkat keras akibat ketidakstabilan tegangan listrik. Instansi belum memiliki kebijakan manajemen keamanan informasi yang memadai. Oleh karena itu, diperlukan manajemen risiko untuk mencegah dan meminimalisir risiko.



Gambar 1. Alur metode penelitian.

Gambar 2. Skema pengisian kuesioner.



Gambar 3. Penentuan kebijakan.

Penelitian audit keamanan informasi di Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ menggunakan metode *Failure Mode and Effect Analysis* (FMEA) dan mitigasi dengan *framework* ISO 27001:2022. Penelitian ini bertujuan mengidentifikasi dan meminimalisir risiko terhadap aset informasi serta memberikan mitigasi sesuai dengan hasil identifikasi dan kebutuhan instansi.

II. TINJAUAN PUSTAKA

Upaya dalam mengembangkan keamanan informasi pada instansi sudah banyak dilakukan dalam beberapa tahun

Tabel 1.
Skala Tingkat Keparahan

Dampak	Kriteria	Peringkat
Berbahaya: Tanpa Peringatan	Mengakibatkan proses organisasi berhenti > 1 minggu.	10
Berbahaya: Dengan Peringatan	Mengakibatkan proses organisasi berhenti > 1 hari.	9
Sangat Tinggi	Menimbulkan proses organisasi terhenti <1 hari.	8
Tinggi	Menimbulkan proses organisasi terhenti dalam 1 hari.	7
Sedang	Menyebabkan layanan gagal berfungsi sebagaimana mestinya.	6
Rendah	Menimbulkan komplain.	5
Sangat Rendah	Menimbulkan gangguan yang cukup berpengaruh/menyebabkan sedikit kerugian.	4
Sedikit	Menyebabkan sedikit terjadinya gangguan maupun tanpa adanya kehilangan sesuatu.	3
Sangat Sedikit	Tanpa disadari dan memberikan dampak kecil pada kinerja.	2
Tidak ada	Tanpa disadari dan tidak mempengaruhi kinerja	1

Tabel 2.
Skala Tingkat Kejadian

Probobilitas Risiko	Periode Waktu	Peringkat
Sangat Tinggi	Lebih dari satu kali tiap harinya	10
Tinggi: tingkat kegagalan tidak terelakan	Satu kali dalam 4 hari	9
Tinggi: secara umum terkait dengan proses yang sebelumnya sering kali gagal	Satu kali dalam seminggu	8
Proses yang sering kali gagal	Satu kali dalam sebulan	7
Moderate	Satu kali setiap 3 bulan	6
Proses yang sebelumnya memiliki kegagalan tidak terlalu sering	Satu kali setiap 6 bulan	5
Kegagalan yang pernah terjadi, tapi tidak dalam proporsi yang besar	Satu kali dalam setahun	4
Rendah	Satu kali dalam 1-3 tahun	3
Sangat rendah	Satu kali dalam 3-6 tahun	2
Remote: kegagalan tidak mungkin terjadi	Satu kali dalam 6 tahun lebih	1

Tabel 3.
Skala Tingkat Deteksi

Deteksi	Kriteria	Peringkat
Hampir Tidak Mungkin	Potensi penyebab tidak dapat diidentifikasi.	10
Sangat Sulit	Sangat sulit untuk mendeteksi risiko.	9
Sulit	Sulit terdeteksi atau sulit terkontrol.	8
Cukup Sulit	Cukup sulit untuk dideteksi.	7
Normal	Bisa dideteksi dengan usaha ekstra.	6
Sedang / Moderat	Dapat dideteksi.	5
Cukup Mudah	Cukup mudah untuk dideteksi.	4
Mudah	Mudah untuk dideteksi.	3
Sangat Mudah	Sangat mudah untuk dideteksi.	2
Hampir Pasti	Terlihat jelas, sangat mudah pengendaliannya.	1

Tabel 4.
Kontrol Keamanan ISO/IEC 27001:2022 yang Digunakan

Keterangan	Kontrol Organisasi
A.5.2	Peran dan Tanggung Jawab Keamanan Informasi
A.5.15	Kontrol Akses
7	Kontrol Fisik
A.7.4	Pemonitoran Keamanan Fisik
A.7.5	Memproteksi dari Ancaman Fisik dan Lingkungan
A.7.8	Penempatan dan Proteksi Peralatan
8	Kontrol Teknologi
A.8.6	Manajemen Kapasitas
A.8.9	Manajemen Konfigurasi
A.8.12	Pencegahan Kebocoran Data
A.8.15	Membuat Log

terakhir. Faktor yang mempengaruhi risiko aset keamanan informasi, mengidentifikasi, menilai serta memberikan rekomendasi mitigasi risiko pada Diskominfo Kabupaten Sambas [4]. Keamanan informasi umumnya didefinisikan dalam hal properti atau karakteristik yang seharusnya dimiliki oleh informasi yang aman [5]. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) [6]. Metode *Failure Mode and Effect Analysis* digunakan untuk melakukan identifikasi proses bisnis, penyebab kegagalan, dampak kegagalan, dan pencegahan terjadinya kegagalan berdasarkan tingkat keparahan (*severity*), tingkat kejadian (*occurrence*), dan tingkat deteksi (*detection*). Tiga variabel utama dalam FMEA adalah *severity*, *occurrence*, dan *detection*, yang digunakan untuk menentukan nilai keseriusan kegagalan [7]. Sedangkan ISO/IEC 27001:2013 digunakan untuk memberikan rekomendasi mitigasi resiko berdasarkan dengan klausul objektif serta memberikan keyakinan kepada pihak berkepentingan (Gambar 1) [8].

Selain itu, mengukur dan mengidentifikasi risiko menggunakan metode *Failure Mode and Effect Analysis* (FMEA) dan standar ISO/IEC 27001:2013 [3]. Metode

Tabel 5.
Penilaian Risiko

Aset	*Potential Cause*	Risiko	*Severity*	*Occurrence*	*Detection*	RPN
Hardware	*Maintenance* yang tidak teratur	*Hardware failure*	9	5	5	225
	Sever *overload*		5	3	3	45
	Pemadaman listrik	*Power failure*	7	8	8	448
	Kapasitas memori server yang sudah tidak memenuhi kebutuhan	Memori server full	8	6	4	192
	Listrik tidak stabil	Kerusakan server	9	5	7	315
	Gangguan jaringan	Router mati	7	7	5	245
	Ruang server tidak memiliki kunci	Server dapat dimatikan	9	3	5	135
	Kurangnya penggunaan CCTV	Tidak ada akses fisik yang terotorisasi	7	6	4	168
Software dan Website SIHAWA	Bug atau kekurangan dalam kode	Terjadinya kesalahan dalam *software*	6	3	4	72
	Kesalahan konfigurasi		2	3	3	18
	Serangan DoS	Aplikasi tidak bisa diakses	7	7	5	245
	Aplikasi bajakan	Pencurian data	7	6	4	168
	SQL *Injection*	Bocornya informasi	7	4	6	168
	Broken Access Control	Mengizinkan seseorang melihat atau mengedit akun orang lain	7	3	8	168
	Plaintext Storage of a Password	Peningkatan hak akses dan pengalihan Pengguna tak terotentikasi ke halaman yang seharusnya tidak diakses	7	5	4	140
	Weak Password Policy	Dapat mengakses database	7	5	4	140
	Stored Cross-Site Scripting (XSS)	Pencurian *cookie* dan *defacement.*	7	5	5	175
	Exposure of sensitive information to an unauthorized actor	Aplikasi menampilkan informasi sensitif kepada pihak yang tidak berwenang	3	5	3	45
People	Serangan virus atau malware	Kebocoran data	5	4	5	100
	Kurangnya keamanan pada perangkat lunak		3	2	3	18
	Adanya *share login*	Penyalahgunaan hak akses	1	9	1	9
	Kurangnya training prosedur penggunaan TI yang diberikan		5	3	4	60
	Kesalahan pengimputan dan penghapusan data	*Human* atau *technician error*	6	4	4	96
	Staff tidak *logout* ketika meninggalkan komputer		6	5	4	120
	Pengolahan data illegal oleh karyawan	Modifikasi dan pencurian database	5	2	5	50
	Kurangnya mekanisme pemantauan para pegawai	Pencurian media atau informasi penting	5	3	3	45
	Lemahnya keamanan sistem internal TI	Serangan *hacker*	6	3	4	72
	Jaringan LAN Putus	Kehilangan koneksi internet	5	6	1	30
	Kerusakan pada infrastruktur jaringan	*Network failure*	5	4	4	80
Network	Kurangnya mekanisme pemantauan terhadap jaringan		7	2	6	84
	Kesalahan dalam melakukan konfigurasi *access point*		6	2	6	72
	Kabel digigit oleh hewan		7	8	4	224
	Koneksi jaringan putus	Rusaknya perangkat jaringan	6	2	7	84
	Pencurian data atau modifikasi data	Penyalahgunaan hak akses	4	3	4	48
	Gangguan listrik	Data *corrupt* atau *error*	4	3	4	48
Data	Kehilangan data akibat tidak melakukan *backup* data	*Backup* data *failure*	7	5	5	175
	Kesalahan dalam pengimputan dan penghapusan data	Kehilangan data	6	3	4	72

pengumpulan data yang digunakan dalam penelitian ini yaitu *stud y literature* digunakan sebagai rujukan atau acuan dalam penelitian. Hasil dari analisis penelitian ini menunjukan terdapat 22 *cause failure* yang akan menyebabkan terjadinya risiko pada keamanan asset TI di Bidang Perdagangan Dalam Negeri (PDN) Dinas Perdagangan dan Perindustrian Pemerintah Provinsi XYZ. Risiko TI bisa berdampak pada operasional perusahaan dan menciptakan tantangan dalam mencapai tujuan dan pencapaian strategis [8].

Terdapat 11 *cause failure* yang memiliki level tinggi dengan rentan nilai 400-175. ISO 27001:2022 berfokus pada perlindungan informasi penting, membantu organisasi mengelola risiko keamanan informasi melalui pembangunan dan pemeliharaan sistem manajemen keamanan informasi.

Tabel 6.
Mitigasi Berdasarkan ISO/IEC 27001:2022

Jenis Risiko	Kontrol Keamanan	Rekomendasi
[Hardware] Pemadaman listrik - *Power failure*	A.7.5 Memproteksi dari Ancaman Fisik dan Lingkungan	DISKOMINFOTIK perlu menyediakan generator listrik untuk meminimalisir server atau PC mati mendadak akibat pemadaman listrik.
[Hardware] Listrik tidak stabil - Kerusakan server	A.7.5 Memproteksi dari Ancaman Fisik dan Lingkungan	Instansi dapat menggunakan stabilizer untuk menjaga tegangan listrik stabil dan UPS (*Uninterruptible Power Supply*) sebagai daya cadangan untuk memastikan server tetap beroperasi, sehingga mencegah kerusakan akibat kehilangan daya tiba-tiba.
[Hardware] Gangguan jaringan - Router mati	A.7.5 Memproteksi dari Ancaman Fisik dan Lingkungan	Instansi harus merancang dan menerapkan langkah perlindungan terhadap ancaman fisik pada infrastruktur DISKOMINFOTIK. ini dapat diatasi dengan menggunakan UPS atau generator listrik sebagai cadangan daya selama pemadaman.
	A.7.8 Penempatan dan Proteksi Peralatan	Instansi harus menempatkan peralatan dengan aman dari akses tidak sah dan ancaman fisik atau lingkungan.
[Software] Serangan DoS - Aplikasi tidak bisa diakses	A.8.9 Manajemen Konfigurasi	Instansi harus mengamankan digital dengan menggunakan *firewall* untuk mencegah serangan keamanan.
	A.8.15 Membuat Log	Instansi disarankan untuk mencatat, menyimpan, dan menganalisis aktivitas jaringan dan server menggunakan SIEM untuk mendeteksi dan menganalisis serangan keamanan pada digital.
[Hardware] Maintenance yang tidak teratur - *Hardware failure*	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Pegawai harus menyadari tanggung jawab mereka dalam pemeliharaan berkala *hardware* untuk menghindari kegagalan. Selain itu, seluruh pihak DISKOMINFOTIK perlu diberikan *awareness* tentang pentingnya pemeliharaan *hardware*.
[Network] Kabel digigit oleh hewan - *Network failure*	A.7.5 Memproteksi dari Ancaman Fisik dan Lingkungan	Instansi harus merancang dan menerapkan perlindungan terhadap ancaman fisik, baik disengaja maupun tidak, pada infrastruktur DISKOMINFOTIK seperti pemasangan pelindung kabel yang tahan gigitan hewan dan pemantauan infrastruktur secara berkala.
	A.7.8 Penempatan dan Proteksi Peralatan	Instansi dapat melakukan penempatan kabel pada tempat yang tertutup seperti lemari kaca dan melakukan manajemen kabel.
[Hardware] Kapasitas memori server full	A.8.6 Manajemen Kapasitas	Penggunaan sumber daya harus terus dimonitor dan disesuaikan dengan kapasitas saat ini.
[Software] *Stored Cross-Site Scripting* (XSS) - Pencurian *cookie* dan *defacement*	A.8.9 Manajemen Konfigurasi	Instansi harus menggunakan *firewall* pada digital yang dimiliki.
	A.8.12 Pencegahan Kebocoran Data	Menerapkan prosedur *secure coding* untuk memvalidasi setiap input pengguna, mencegah penginputan *payload* berbahaya yang dapat menyebabkan kebocoran data.
	A.8.15 Membuat Log	Instansi disarankan untuk mencatat, menyimpan, dan menganalisis aktivitas abnormal pada jaringan dan server menggunakan SIEM.
[Data] Kehilangan data akibat tidak melakukan *backup* data - *Backup* data *failure*	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Instansi perlu menyadari bahwa pegawai memiliki tanggung jawab masing-masing terkait keamanan informasi. Diperlukan pelatihan tentang praktik keamanan informasi (backup data secara teratur)
[Hardware] Kurangnya penggunaan CCTV - Tidak ada akses fisik yang terotorisasi	A.5.15 Kontrol Akses	Instansi harus membuat dan mengimplementasikan aturan untuk mengontrol akses fisik ke kritis di DISKOMINFOTIK, berdasarkan persyaratan bisnis dan keamanan informasi.
	A.7.4 Pemonitoran Keamanan Fisik	Instansi harus menggunakan CCTV atau alarm penyusup di setiap area penting untuk mencegah akses tak terotorisasi di DISKOMINFOTIK.
[Software] Aplikasi bajakan - Pencurian data	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Instansi dapat memberikan pelatihan untuk meningkatkan kesadaran, termasuk pemahaman tentang penggunaan perangkat lunak ilegal dan konsekuensinya.
[Software] SQL *Injection* - Bocornya informasi	A.8.12 Pencegahan Kebocoran Data	Instansi harus mengidentifikasi informasi sensitif yang memerlukan perlindungan seperti menggunakan DLP (*Data Loss Prevention*) untuk mencegah kehilangan data akibat serangan siber atau kesalahan sistem.
	A.8.15 Membuat Log	Instansi disarankan untuk mencatat, menyimpan, dan menganalisis aktivitas abnormal pada jaringan dan server menggunakan SIEM.
[Software] *Broken access control* - Mengizinkan seseorang melihat atau mengedit akun orang lain	A.5.15 Kontrol Akses	Instansi harus menetapkan aturan untuk mengontrol akses fisik dan logis ke informasi dan , termasuk menerapkan *Role-Based Access Control* sesuai tanggung jawab pengguna dan melakukan peninjauan berkala terhadap hak akses.
	A.8.15 Membuat Log	Instansi harus mencatat, menyimpan, dan menganalisis log untuk mendeteksi aktivitas abnormal yang dapat menunjukkan gangguan keamanan pada jaringan koneksi atau server.
[Software] *Plaintext storage of a password* - Peningkatan hak akses dan pengalihan pengguna tak terotentikasi	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Instansi harus menetapkan SOP dan peran yang bertanggung jawab atas manajemen dan keamanan informasi, termasuk perlindungan data sensitif dengan pengelolaan kata sandi menggunakan fungsi *hash*.
	A.5.15 Kontrol Akses	Instansi harus menetapkan aturan untuk mengontrol atau membatasi akses ke data sensitif seperti mengakses database.
[Software] *Weak password policy* - Masuk akun pengguna lain	A.8.12 Pencegahan Kebocoran Data	Instansi harus menerapkan kebijakan kriteria *password* yang aman, menggunakan kombinasi huruf besar, huruf kecil, karakter spesial, dan batas panjang *password*.
[Hardware] Ruang server tidak memiliki kunci - Server dimatikan	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Instansi perlu memastikan pegawai menyadari tanggung jawab mereka terhadap keamanan informasi, termasuk kontrol akses ruang server.
	A.7.4 Pemonitoran Keamanan Fisik	Instansi harus menggunakan alat pemantau seperti CCTV, penjaga, atau koordinator server untuk terus memonitor premis dan mendeteksi akses fisik yang tidak terotorisasi.
[People] Staff tidak *logout* ketika meninggalkan komputer – *Human Technician Error*	A.5.2 Peran dan Tanggung Jawab Keamanan Informasi	Pegawai harus menyadari tanggung jawab mereka terhadap keamanan data sensitif yang dikelola di DISKOMINFOTIK.

aset, analisis risiko, pengendalian, manajemen insiden, dan tinjauan berkelanjutan [9]. Penelitian terkait pengimplementasian standar ISO/IEC 27001:2022 pada bidang industri MRO (*maintenance, repair, and overhaul*). Pengimplementasian ISO/IEC 27001:2022 memberikan banyak manfaat seperti perlindungan data pelanggan, meningkatkan reputasi dan membantu menjaga kepatuhan terhadap peraturan dan persyaratan hukum yang berlaku [10]. Penelitian ini berfokus pada klausa utama yaitu klausa 4 sampai 10 dan kontrol-kontrol *annex*.

Kesenjangan yang teridentifikasi kemudian dibuatkan perancangan rekomendasi berdasarkan aspek *people, process*, dan *technology* yang mencakup pilihan sertifikasi, pilihan kelompok minat khusus, penambahan peran dan tanggung jawab, prosedur, kebijakan dan pemilihan perangkat. Hasil dari penelitian ini dapat digunakan sebagai referensi untuk meningkatkan efisiensi keamanan informasi dan memberi beberapa rekomendasi jika perusahaan ingin mengajukan sertifikasi ISO/IEC 27001:2022.

ISO/IEC 27001 adalah standar yang diterbitkan oleh *The International Organization for Standardization* untuk membangun Sistem Manajemen Keamanan Informasi (SMKI). Penelitian terkait pengimplementasian ISO 27001:2013 pada Universitas Airlangga dengan cara mengukur tingkat risiko dan potensi kerugian biaya pada aset-aset yang dimiliki oleh Institusi dari segi keamanan informasi [11]. Langkah pertama dari penelitian dilakukan dengan mengidentifikasi asset-aset yang dimiliki dan mengukur nilai dari asset tersebut berdasarkan *Confidentiality*, *Integrity*, dan *Availability* (CIA).

Kemudian, aset-aset tersebut diidentifikasi menggunakan metode OCTAVE sehingga diperoleh perkiraan kalkulasi dari kerugian pada setiap kerentanan dan kontrol ISO terkait sebagai bentuk mitigasi risiko yang mungkin terjadi. Risiko merupakan konsekuensi yang tidak diharapkan terjadi dalam proses langsung atau tidak langsung [12].

Terkait pengukuran kondisi dan kesiapan PT.JPK terhadap *Business Continuity Management Systems* berbasis ISO 22301 dengan pendekatan *control objective* mengenai Information *Security Aspects of Business Continuity Management* dari ISO 27001, kemudian dilanjutkan dengan strategi pemenuhan gap dan menyempurnakan *Standard Operarting Procedure* (SOP) hingga bisa digunakan perusahaan untuk sertifikasi ISO 22301 [13].

III. METODOLOGI

Pada bab ini, dijelaskan mengenai alur metode, alat dan bahan yang digunakan pada penelitian, serta implementasi.

A. Metode

Metode pada penelitian ini meliputi:

1) Identifikasi Permasalahan, Tujuan & Manfaat

Pada tahapan ini dilakukan kegiatan untuk menemukan permasalahan yang ada. Setelah menemukan masalah, langkah selanjutnya adalah mencari solusi yang dapat digunakan untuk memperbaiki masalah tersebut.

2) Studi Literatur

Tahap ini melibatkan pencarian referensi teoritis untuk mendukung tugas akhir, termasuk data dari buku, jurnal, dan laporan penelitian terkait analisis dan manajemen risiko, keamanan informasi, teknologi informasi, metode *Failure Mode and Effects Analysis* (FMEA), dan kontrol ISO/IEC 27001:2022.

3) Pengumpulan Data dan Informasi

Pada tahap ini dilakukan pengumpulan data dan informasi yang dilakukan melalui observasi, wawancara, kuisioner, dan peninjauan dokumen.

Pengambilan data dilakukan dengan metode deskriptif kuantitatif untuk menjawab pertanyaan penelitian yang berkaitan dengan siapa, apa, di mana, mengapa dan bagaimana peristiwa atau pengalam itu terjadi (Gambar 2).

Metode ini difokuskan pada pengumpulan data secara mendalam dan detail, dengan tujuan untuk menemukan pola-pola yang muncul pada peristiwa tersebut [14].

4) Tahapan Analisis Metode FMEA

Adapun tahapan analisis metode FMEA, meliputi:

a. Tahap 1 – Proses Bisnis

Langkah pertama dalam *Failure Mode and Effects Analysis* (FMEA) adalah membuat alur proses bisnis organisasi menggunakan Business *Process Model and Notation* (BPMN). Analisis BPMN dilakukan berdasarkan tugas pokok dan fungsi (tupoksi) Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ.

b. Tahap 2 – Brainstorming Risiko Potensial

Tahap ini melibatkan brainstorming risiko dengan pemangku kepentingan untuk mengidentifikasi potensi ancaman, kerentanan, dan dampak keamanan informasi dari proses bisnis di Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ.

c. Tahap 3 – Menentukan Nilai Risiko Berdasarkan Severity, Occurrence, Detection dan Hasil RPN

Setelah *brainstorming* risiko, dilakukan penilaian risiko berdasarkan tingkat keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*). Langkah berikutnya adalah menghitung *Risk Priority Number* (RPN).

Parameter *severity*, *occurrence*, dan *detection* dapat dilihat pada Tabel 1, Tabel 2, dan Tabel 3.

5) Mitigasi Risiko dengan Kontrol ISO 27001:2022

Pada tahapan ini dilakukan mitigasi risiko berdasarkan penerapan dari metode *Failure Mode and Effects Analysis* (FMEA) terhadap aset keamanan informasi yang memiliki tingkat kerentanan risiko tinggi dan mempunyai ancaman. Mitigasi ini dilakukan berdasarkan standar kontrol ISO/IEC 27001:2022 pada Tabel .

6) Rekomendasi Mitigasi Risiko

Tahapan mitigasi risiko dilakukan untuk memberikan rekomendasi mitigasi risiko yang disesuaikan dengan karakteristik, kebutuhan, dan lingkungan operasional yang berkaitan dengan Dinas Komunikasi, Informatika, dan Statistik pada Kabupaten XYZ yang ditunjukkan melalui Gambar 3.

7) Verifikasi Hasil Rekomendasi Mitigasi Risiko oleh Instansi

Pada tahap ini, hasil rekomendasi mitigasi risiko akan diverifikasi oleh instansi untuk memastikan kesesuaian dengan kondisi lapangan. Selain itu, DISKOMINFOTIK akan mempertimbangkan implementasi mitigasi risiko berdasarkan saran yang direkomendasikan.

8) Kesimpulan dan Saran

Pada tahapan terakhir dari penelitian ini adalah perumusan kesimpulan sebagai jawaban dari masalah yang telah dirumuskan sebelumnya serta saran bagi peneliti berikutnya yang akan melakukan penelitian serupa.

B. Implementasi

Pengumpulan Data dan Informasi

1) Observasi

Observasi yang dilakukan dalam penelitian ini, bertujuan untuk melihat kondisi, keadaan dan proses bisnis yang terjadi di lingkungan DISKOMINFOTIK melalui *survey* langsung ke lapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya yang digunakan pada DISKOMINFOTIK Kabupaten XYZ.

2) Wawancara

Pada penelitian ini, wawancara memiliki peran penting dalam hal pengumpulan data. Untuk mengurangi perbedaan pendapat terkait kuesioner dan memastikan data valid serta dapat diandalkan, perlu dilakukan wawancara mendalam dengan materi *in-depth interview*.

3) Kuesioner

Penulis mengajukan kuesioner kepada pegawai DISKOMINFOTIK untuk mengumpulkan data penelitian. Kuesioner ini dirancang untuk mendapatkan informasi tentang profil DISKOMINFOTIK, identifikasi risiko aset (*hardware*, *software*, *people*, *network*, dan data), serta implementasi praktik keamanan informasi berdasarkan ISO 27001:2022. Skema kuesioner ini terdiri dari beberapa bagian yang dapat dilihat pada Gambar .

4) Peninjauan Dokumen

Dokumen terkait praktik SMKI ditinjau untuk memvalidasi implementasi keamanan di DISKOMINFOTIK. Metode ini membantu mengetahui dokumentasi dan implementasi aset-aset kritis. Beberapa dokumen yang ditinjau untuk mendukung data dan informasi penelitian adalah sebagai berikut:

a. Dokumen mengenai struktur organisasi, tugas, fungsi, dan uraian tugas dari setiap jabatan pada DISKOMINFOTIK.
b. SOP Akses Ruang Server.
c. SOP *Backup* data *Restore* Data.
d. SOP Hak Akses TI.

IV. HASIL DAN PEMBAHASAN

A. Tahapan Metode Failure Mode and Effect Analysis (FMEA)

Tahapan metode *failure mode dan effect analysis* (FMEA) meliputi:

1) Proses Bisnis Analisis

Proses bisnis organisasi dilakukan menggunakan *Business Process Model and Notation* (BPMN) untuk menggambarkan logika dan model setiap langkah proses bisnis. Tujuannya adalah mengenali semua aspek dan tahap proses bisnis untuk mengidentifikasi potensi kegagalan. Analisis ini mencakup 4 proses bisnis: Proses Bisnis Penentuan Kebijakan, Proses Bisnis Penyusunan Penyelenggaraan Kegiatan, Proses Bisnis Pelaksanaan Kegiatan Dinas, dan Proses Bisnis Pengawasan Kegiatan. Proses Bisnis Penentuan Kebijakan dapat dilihat pada Gambar .

2) Brainstorming Risiko Potensial

Pada tahap ini, dilakukan brainstorming untuk mengidentifikasi risiko potensial dan kegagalan dalam sistem yang diterapkan. Hasilnya adalah daftar *potential cause* dan risiko pada aset di Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ.

Risiko ini mencakup kejadian dengan probabilitas tinggi, baik dari kondisi eksternal seperti bencana alam dan gangguan fasilitas umum, maupun kondisi internal seperti sosial dan operasional. Terdapat 37 *potential cause* dan 29 risiko teridentifikasi yang meliputi kategori aset *hardware*, *software*, *people*, *network*, dan data.

3) Menentukan Nilai Risiko Berdasarkan Severity, Occurrence, Detection, dan Hasil RPN

Penentuan nilai risiko berdasarkan *severity*, *occurrence*, *detection*, dan Hasil RPN ditunjukkan pada Tabel 5.

B. Mitigasi Risiko Berdasarkan Kontrol ISO 27001:2022

Setelah mengidentifikasi dan menilai risiko menggunakan *Failure Mode and Effect Analysis* (FMEA) di DISKOMINFOTIK, dilakukan pemetaan kontrol keamanan untuk mitigasi risiko berdasarkan standar ISO/IEC 27001:2022. Mitigasi risiko ini diurutkan dari tingkat risiko yang sangat tinggi hingga tinggi, seperti yang terlihat pada Tabel .

Berdasarkan mitigasi sesuai dengan kontrol keamanan ISO/IEC 27001:2022, instansi mengalami penurunan *Risk Priority Number* (RPN), menunjukkan efektivitas langkah-langkah pengurangan risiko keamanan informasi. Contoh yang diterapkan adalah *backup* data secara berkala (A.5.2) yang mengurangi tingkat keparahan dan frekuensi. Penerapan kontrol akses (A.5.15) dan pemantauan keamanan fisik (A.7.4) efektif mengurangi keparahan dan frekuensi serta meningkatkan deteksi risiko.

Gangguan jaringan akibat router mati dimitigasi dengan perlindungan fisik dan lingkungan (A.7.5) serta penempatan peralatan (A.7.8), menurunkan RPN dengan keparahan rendah, frekuensi sangat rendah, dan risiko mudah dideteksi. Manajemen kapasitas (A.8.6) mengurangi risiko kapasitas memori tidak mencukupi dengan pemantauan berkala. Risiko *Stored Cross-Site Scripting* (XSS) dikurangi dengan manajemen konfigurasi (A.8.9), pencegahan kebocoran data (A.8.12), dan pembuatan log (A.8.15), menurunkan RPN dengan keparahan dan frekuensi rendah serta deteksi melalui log.

C. Rekomendasi Mitigasi Risiko

Dalam memastikan efektivitas manajemen risiko keamanan informasi, telah disusun rekomendasi mitigasi risiko yang sesuai dengan karakteristik, kebutuhan, dan lingkungan operasional DISKOMINFOTIK.

D. Verifikasi Hasil Rekomendasi Mitigasi Risiko oleh Instansi

Setelah evaluasi SMKI pada instansi, langkah selanjutnya adalah justifikasi hasil evaluasi dengan kondisi sebenarnya. Instansi kemudian menentukan tindakan mitigasi yang akan diimplementasikan dan bagaimana tindak lanjutnya.

V. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa: (1) Identifikasi risiko keamanan informasi pada Dinas Komunikasi, Informatika, dan Statistika Kabupaten XYZ menggunakan metode *Failure Mode and Effect Analysis* (FMEA) dilakukan melalui observasi, wawancara, kuesioner, peninjauan dokumen, dan brainstorming risiko potensial. (2) Berdasarkan ancaman risiko yang ditemukan di instansi, untuk meningkatkan keamanan informasi pada Dinas Komunikasi, Informatika, dan Statistika Kabupaten XYZ, dapat diterapkan kontrol keamanan sesuai standar ISO/IEC 27001:2022. Terdapat 9 kontrol keamanan pada ISO/IEC 27001:2022 yang digunakan sebagai sarana mitigasi risiko ancaman yang ditemukan. (3) Berdasarkan analisis manajemen risiko keamanan informasi pada Dinas Komunikasi, Informatika, dan Statistik Kabupaten XYZ diperoleh 37 *potential cause* dan 29 identifikasi risiko dari kategori aset *hardware*, *software*, *people*, *network*, dan data. (4) Berdasarkan hasil *Risk Priority Number* (RPN) terdapat ancaman risiko dengan kategori *very low*, 11 ancaman risiko dengan kategori *low*, 6 ancaman risiko dengan kategori *moderate*, 11 ancaman risiko dengan kategori *high*, dan 6 ancaman risiko dengan kategori *very high*. (5) Seluruh mitigasi risiko berdasarkan ISO 27001:2022 dan rekomendasi mitigasi risiko secara umum diterima oleh instansi, walaupun tidak langsung diimplementasikan.

DAFTAR PUSTAKA

[1] M. R. Slamet, M. Ikhlash, and F. Wulandari, "Analisis penilaian keamanan informasi dengan menggunakan penilaian mandiri keamanan informasi (Paman kami)," *J. Appl. Bus. Adm.*, vol. 6, no. 1, pp. 41–50, 2022, doi: 10.30871/jaba.v6i2.3604.

[2] F. Wirayudha, "Evaluasi Keamanan Informasi Menggunakan Indeks Kami pada Organisasi Pemerintah (Kasus Dinas Kominfo Kabupaten Penukal Abab Lematang Ilir)," Departemen Sistem Informasi, Yogyakarta: Universitas Atma Jaya Yogyakarta, 2022.

[3] L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran risiko keamanan aset TI menggunakan Metode FMEA dan Standar ISO/IEC 27001: 2013," *Technomedia J.*, vol. 5, no. 2 Februari, pp. 167–181, 2021, doi: 10.33050/tmj.v5i2.1377.

[4] T. Tutik, N. Mutiah, and I. Rusi, "Analisis dan manajemen risiko keamanan informasi menggunakan metode failure mode and effects analysis (fmea) dan kontrol iso/iec 27001: 2013 (studi kasus: dinas komunikasi dan informatika Kabupaten Sambas)," *Coding J. Komput. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022, doi: 10.26418/coding.v10i02.55082.

[5] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[6] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security.," *J. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 21–45, 2014, https://api.semanticscholar.org/CorpusID:215838643

[7] Y. Syarifudin and A. Pusakaningwati, "Analisis pengendalian kualitas produk stan kontainer dengan metode fmea (failure mode and effect analysis) di bengkel las Mulia Utama Perkasa," *J. Cakrawala Ilm.*, vol. 2, no. 11, pp. 4177–4188, 2023, doi: 10.53625/jcijurnalcakrawalailmiah.v2i11.6129.

[8] K. Harsanto and D. HIdayat, "Sistem informasi manajemen risiko dengan menggunakan framework national institute of standards and technology pada lembaga pendidikan," *Insa. Pembang. Sist. Inf. dan Komput.*, vol. 6, no. 1, pp. 1–9, 2018, http://www.lppm.ipem.ac.id

[9] R. Sinaga, "Pengembangan model penilaian kepatuhan salah satu perguruan tinggi terhadap standar ISO 27001: 2022," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 3, pp. 381–394, 2023, doi: 10.28932/jutisi.v9i3.6850.

[10] M. R. Aditama, F. Dewi, and D. Praditya, "Perancangan proses keamanan informasi berdasarkan framework ISO27001: 2022," *SEIKO J. Manag. & Bus.*, vol. 6, no. 2, 2023, doi: 10.37531/sejaman.v6i2.5550.

[11] I. Sulistyowati, "Manajemen Risiko Keamanan Informasi Dengan Metode Octave Dan ISO/EIC 27001: 2013 (Studi Kasus: Universitas Airlangga)," Departemen Manajemen Teknologi, Surabaya: Institut Teknologi Sepuluh Nopember, 2019.

[12] D. Sirait, R. D. E. Putra, and Y. Kuncoro, "Manajemen risiko penumpang kapal PT (Persero) Pelayaran Nasional Indonesia Cabang Tanjung Priok Jakarta," *J. Manaj. Bisnis Transp. dan Logistik*, vol. 3, no. 1, pp. 95–110, 2016, doi: 10.54324/j.mbtl.v3i1.924.

[13] E. H. Prakasita and R. V. H. Ginardi, "Tinjauan kesiapan terhadap implementasi Business Continuity Management Systems (BCMS) berbasis ISO 22301 dan ISO 27001 (Studi kasus: PT. JPK)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 13, no. 2, pp. 76–83, 2018, doi: 10.30872/jim.v13i2.902.

[14] H. Kim, J. S. Sefcik, and C. Bradway, "Characteristics of qualitative descriptive studies: A systematic review," *Res. Nurs. Health*, vol. 40, no. 1, pp. 23–42, 2017, doi: 10.1002/nur.21768.