BAB I PENDAHULUAN

Bab Pendahuluan memuat latar belakang dari topik penelitian, perumusan masalah, tujuan penelitian, batasan-batasan, serta potensi manfaat dari penelitian.

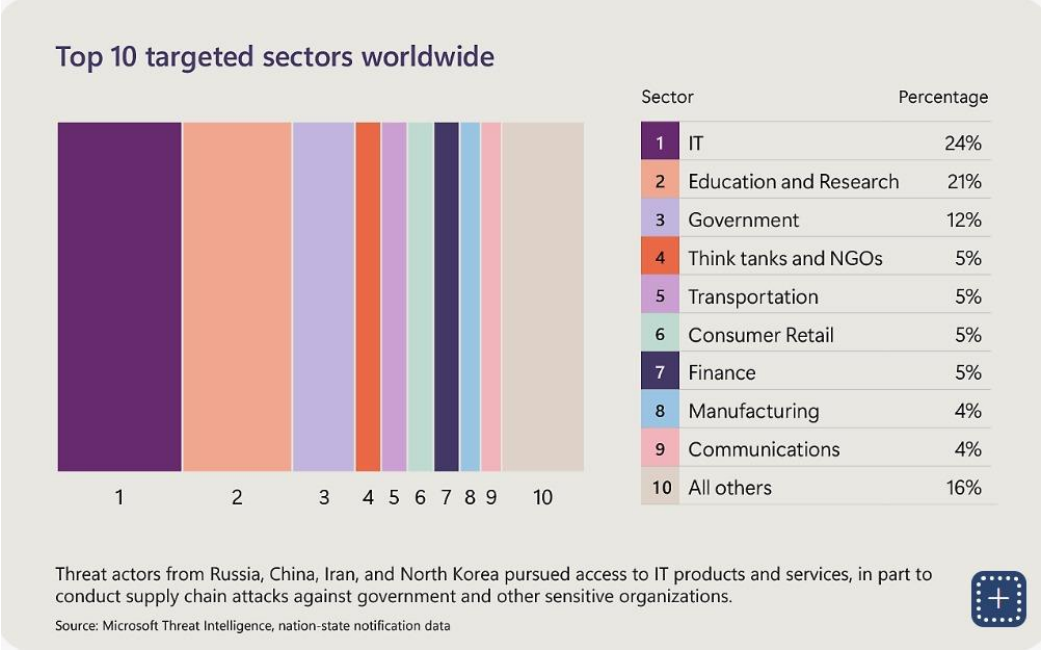
I.1 Latar Belakang

Dalam era transformasi digital yang kian pesat, instansi pemerintah dituntut untuk tidak hanya memanfaatkan teknologi informasi sebagai alat bantu operasional, tetapi sebagai pilar utama dalam penyelenggaraan tata kelola pemerintahan yang efektif, efisien, dan akuntabel (Syahindra dkk, 2022). Peran teknologi informasi telah beralih dari sekedar pendukung administratif menjadi penggerak utama dalam proses bisnis organisasi sektor publik termasuk dalam perancangan strategis, pengelolaan data publik, pelayanan publik, dan pengambilan keputusan berbasis data (Hidayatullah dkk, 2024). Namun, pemanfaatan teknologi informasi yang luas juga diiringi oleh meningkatnya kompleksitas pengelolaan dan pengendalian sumber daya teknologi informasi.

Transformasi digital ini, meskipun menjanjikan efisiensi dan peningkatan layanan, seringkali menghadapi tantangan dalam implementasinya, terutama dalam memastikan bahwa seluruh investasi teknologi informasi dapat memberikan nilai optimal dan terkendali. Kompleksitas pengelolaan sumber daya teknologi informasi di instansi pemerintah bukan hanya soal pengadaan perangkat lunak dan keras, tetapi juga mencakup pengelolaan data yang besar dan sensitif, pemeliharan infrastruktur yang vital, serta pengembangan kapasitas sumber daya manusia yang memadai. Menurut Purwanto dan Ismail (2024), manajemen risiko menjadi esensial untuk menghadapi kompleksitas ini untuk memastikan bahwa setiap langkah yang diambil dalam pemanfaatan teknologi informasi tidak menimbulkan kerugian yang tidak terduga atau menghambat pencapaian tujuan strategis organisasi.

Oleh sebab itu, tidak cukup bagi pemerintah hanya memiliki teknologi informasi yang canggih, tetapi dibutuhkan juga tata kelola teknologi yang sistematis dan terstruktur agar penggunaan teknologi informasi selaras dengan tujuan strategis organisasi dan mampu mengelola risiko yang muncul secara tepat (Hikam dkk,

2024). Tata kelola teknologi informasi yang baik memastikan bahwa semua komponen mulai dari sumber daya manusia, proses bisnis, kebijakan, hingga keamanan informasi berjalan dalam kerangkan akuntabilitas, transparansi, dan pengendalian risiko yang berkelanjutan (Syahindra dkk, 2022). Berdasarkan laporan Microsoft Digital Defense Report 2024 yang dirilis oleh microsoft terdapat beberapa sektor yang menjadi target penyerangan terhadap keamanan informasi (Microsoft, 2024).



Gambar I-1 Serangan Siber Internasiononal

(Sumber: Microsoft Digital Defence Report 2024)

Seiring dengan meningkatnya ketergantungan terhadap teknologi informasi, ancaman terhadap keamanan informasi pun semakin meningkat, baik dalam bentuk serangan siber, kehilangan data, maupun akses tidak sah terhadap sistem (Hikam dkk, 2024). Berdasarkan data pada Gambar I-1 diatas, dapat terlihat bahwa sektor pemerintahan menempati posisi ke – 3 dalam kasus serangan siber pada tahun 2024. Jenis serangan yang paling umum meliputi *ransomware*, *phishing*, dan serangan terhadap infrastruktur kritikal (Microsoft, 2024). Hasil data tersebut membuktikan bahwa sektor pemerintahan belum aman dan masih dapat diakses oleh pihak yang tidak bertanggung jawab. Oleh karena itu,

keamanan informasi merupakan suatu kebutuhan yang sangat penting dalam menjaga informasi (Syahindra dkk, 2022).

Ancaman siber yang terus berkembang tidak hanya mengancam operasional instansi pemerintah, tetapi juga dapat mengikis kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data dan menyediakan layanan esensial (Wibowo & Ramli, 2022). Insiden keamanan seperti kebocoran data pribadi atau gangguan layanan kritis dapat berdampak luas, mulai dari kerugian finansial hingga terganggunya fungsi pemerintahan secara signifikan. Oleh karena itu, upaya sistematis dalam mengidentifikasi, menilai, dan memitigasi risiko keamanan informasi bukan lagi pilihan, melainkan keharusan untuk menjaga keberlangsungan layanan publik dan kredibilitas instansi pemerintah di mata masyarakat (Sholikhatin & Isnaini, 2021).

Dalam konteks Indonesia, Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Jawa Barat memiliki peran sentral dalam menjaga keandalan dan keamanan sistem informasi pemerintahan sebagai tanggung jawab tata kelola teknologi informasi (Syahindra dkk, 2022). Setiap instansi pemerintahan diwajibkan menerapkan manajemen risiko yang baik berdasarkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020. Berdasarkan artikel berita "Gawat, Situs Judi Online Sekarang Sasar Website Resmi Pemerintah Kabupaten Kuningan" yang diunggah di portal berita Kabar Cirebon pada 27 Februari 2023, Kepala Bidang Persandian dan Statistik Diskominfo Kabupaten Kuningan menyampaikan bahwa terdapat 98 kasus situs web perangkat daerah dengan subdomain 'kuningankab.go.id' telah disusupi situs judi online. Oleh karena itu, analisis risiko menjadi langkah penting dalam menjaga keberlangsungan layanan dan pengambilan keputusan yang berbasis data (Hidayatullah dkk, 2024).

Informasi merupakan aset penting bagi organisasi, dan setiap informasi memiliki potensi risiko. Risiko ini tidak hanya berasal dari faktor eksternal, seperti ancaman siber, tetapi juga dari kerentanan internal, seperti kesalahan konfigurasi sistem atau kelalaian manusia (Hikam dkk, 2024). Untuk itu, organisasi perlu melakukan manajemen risiko yang efektif agar dapat mengidentifikasi, menganalisis, dan

mengevaluasi risiko secara sistematis (Hidayatullah dkk, 2024). Salah satu pendekatan dasar yang digunakan secara luas dalam mengevaluasi risiko keamanan informasi adalah prinsip *Confidentiality, Integrity, and Availability* (CIA), yang menjadi kerangkan utama dalam menentukan dampak dari insiden terhadap aset informasi (Hikam dkk, 2024). Pendekatan ini membantu organisasi dalam melindungi data dari akses yang tidak sah, menjaga keakuratan informasi, serta menjami ketersediaan layanan saat dibutuhkan.

Dalam konteks Diskominfo Provinsi Jawa Barat yang memiliki peran penting dalam pengelolaan infrastruktur layanan digital publik, pendekatan CIA dapat digunakan sebagai dasar dalam penilaian risiko yang timbul atas aset informasi yang mereka kelola. Untuk mendukung proses tersebut secara menyeluruh dan terstruktur, Divisi XYZ pada instansi ini dapat mengadopsi standar intersional ISO/IEC 27005:2022. Standar ini menyediakan panduan lengkap dalam proses manajemen risiko keamanan informasi, mulai dari penetapan konteks organisasi, identifikasi, analisis, dan evaluasi risiko hingga perlakuan risiko yang berkelanjutan (Hidayatullah dkk, 2024). Pentingnya pendekatan tesebut diperkuat oleh penelitian yang dilakukan oleh Syahindra dkk (2022), yang menunjukkan bahwa instansi Diskominfo masih menghadapi tantangan dalam menerapkan manajemen risiko keamanan informasi secara efektif dan terstruktur.

ISO/IEC 27005:2022 dipilih sebagai kerangka kerja dalam penelitian ini karena reputasinya sebagai standar internasional yang komprehensif dan mutakhir dalam manajemen risiko keamanan informasi (Hidayatullah dkk, 2024). Standar ini tidak hanya memberikan metodologi yang terstruktur untuk mengidentifikasi dan menganalisis risiko, tetapi juga panduan untuk mengevaluasi dampak dan mengusulkan perlakukan risiko yang tepat (Isnaini dkk, 2023). Pendekatan yang sistematis ini sangat relevan untuk organisasi sektor publik yang membutuhkan metode terukur dalam mengelola aset informasinya. Fleksibilitas ISO/IEC 27005:2022 juga memungkinkan penerapannya pada berbagai jenis konteks keamanan informasi, mulai dari sistem akademik yang dilakukan oleh Leasa dan Prassida (2024) hingga aspek manajemen risiko yang terkait tata kelola teknologi informasi secara keseluruhan seperti yang dilakukan oleh Hikam dkk (2024) dan

Hidayatullah dkk (2024), sehingga menjamin relevansi hasil analisis untuk pengambilan keputusan strategis.

Pada penelitian yang dilakukan oleh Nugraha dkk (2020) mengenai manajemen keamanan informasi menggunakan NIST 800-30. Penelitian tersebut bertujuan untuk menganalisis risiko yang terdapat pada sistem Tata Naskah Dinas Elektronik (TNDE) pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur dengan. Metode yang digunakan mencakup tahapan karakterisasi sistem, identifikasi ancaman dan celah, analisa kontrol, dan melakukan penilaian terhadap kemungkinan dan dampak dari setiap risiko yang diidentifikasi. Hasil penelitian tersebut menunjukkan sebagaian besar ancaman berada pada kategori risiko rendah, dengan beberapa ancaman strategis seperti pemadaman listrik, bencana alam, dan jaringan terputus yang tergolong dalam tidak dapat ditoleransi berdasarkan *risk appetite*.

Selain itu, Sari (2023) juga melakukan evaluasi manajemen risiko teknologi informasi di Diskominfo Kabupaten Magelang. Penelitian ini bertujuan untuk mengukur tingkat kapabilitas Diskominfo saat ini dan melakukan analisis *gap* untuk memberikan rekomendasi perbaikan tata kelola teknologi informasi terkait manajemen risiko tata kelola teknologi informasi. *Framework* yang digunakan adalah COBIT 2019 dengan fokus pada dua objektif yaitu EDM03 (*Evaluate, Direct, Monitor*) dan APO12 (*Align, Plan, and Organize*). Hasil penelitian menunjukkan bahwa tingkat kapabilitas Diskominfo untuk setiap objektifnya berada pada level 2. Rekomendasi yang diberikan berfokus pada pendokumentasian kegiatan manajemen risiko seperti pedoman risiko dan evaluasi manajemen risiko teknologi informasi secara berkala. Penelitian ini menunjukkan variasi pendekatan *framework* yang digunakan dalam evaluasi manajemen risiko di instansi pemerintahan daerah.

Berbeda dengan penelitian-penelitian sebelumnya yang berfokus pada sistem informasi spesifik atau menggunakan kerangka kerja seperti NIST 800-30 atau COBIT 2019. Penelitian ini mengadopsi standar internasional terbaru ISO/IEC 27005:2022 dalam menganalisa risiko keamanan informasi pada lingkup tata kelola TI pada divisi XYZ. Penerapan ISO/IEC 27005:2022 dalam konteks ini

dirancang untuk menghasilkan profil risiko yang lebih mendalam dan spesisfik, mencakup penentuan konteks organisasi, identifikasi risiko, evaluasi risiko, dan perlakuan risiko secara sistematis dan berkelanjutan. Pendekatan ini diharapkan dapat menjadi dasar yang kuat dalam perencanaan strategis keamanan informasi jangka panjang terutama pada Divisi XYZ, serta memberikan kontribusi signifikan dalam upaya peningkatan ketahanan siber dan keberlanjutan layanan digital pemerintah.

I.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah untuk penelitian ini adalah:

1. Bagaimana analisis ancaman risiko pada Diskominfo Provinsi Jawa Barat pada Divisi XYZ dengan mengunakan ISO 27005:2022?
2. Bagaimana Tingkat risiko pada Diskominfo Provinsi Jawa Barat Divisi XYZ?
3. Bagaimana penanganan risiko yang dapat diajukan berdasarkan hasil penilaian risiko pada Diskominfo Provinsi Jawa Barat Divisi XYZ?

I.3 Tujuan Penelitian

Adapun tujuan penelitian sebagai berikut:

1. Untuk mengetahui hasil identifikasi risiko pada Diskominfo Provinsi Jawa Barat di divisi XYZ dengan menggunakan ISO 27005:2022.
2. Untuk mengetahui dan menjelaskan hasil analisis risiko dengan menggunakan ISO 27005:2022 pada Diskominfo Provinsi Jawa Barat di divisi XYZ.
3. Untuk mengetahui dan menjelaskan mitigasi risiko dengan menggunakan ISO 27005:2022 pada Diskominfo Provinsi Jawa Barat di divisi XYZ.

I.4 Batasan Penelitian

Dalam penulisan penelitian ini, terdapat batasan-batasan penelitian yaitu:

1. Keterbatasan sumber daya, seperti akses informasi internal yang terbatas, waktu yang singkat, data wawancara yang tidak menyeluruh, serta analisis

yang dilakukan secara manual, menjadi kendala yang memengaruhi detail hasil penelitian ini.

2. Jumlah responden yang terbatas, karena tidak semua staf Divisi XYZ dapat diwawancarai secara langsung. Hal ini berdampak pada keterwakilan persepsi terhadap ancaman dan kerentanan yang mungkin belum sepenuhnya menggambarkan keseluruhan kondisi organisasi.
3. Keterbatasan waktu pelaksanaan penelitian, yang menyebabkan proses analisis risiko hanya dilakukan hingga tahap *risk treatment*, tanpa mencakup proses implementasi, evaluasi, dan monitoring efektivitas kontrol keamanan informasi secara berkelanjutan.
4. Penelitian ini memiliki keterbatasan dalam hal cakupan aset yang dianalisis. Karena keterbatasan waktu, data, dan akses, penelitian tidak mencakup identifikasi dan analisis risiko terhadap aset utama (*primary assets*) seperti informasi dan layanan inti yang dikelola oleh Divisi XYZ. Fokus penelitian dibatasi hanya pada aset pendukung (*supporting assets*), yakni perangkat keras (*hardware*), perangkat lunak (*software*), dan infrastruktur jaringan (*network*) yang secara teknis mendukung pengelolaan informasi. Aset lainnya seperti sumber daya manusia, layanan pihak ketiga, dan dokumen fisik tidak dianalisis lebih lanjut karena keterbatasan akses dan sumber daya dalam pelaksanaan penelitian ini.

I.5 Manfaat Penelitian

Dibawah ini terdapat manfaat penelitian yang diharapkan berguna bagi penulis dan masyarakat Indonesia dari segi aspek teoritis dan aspek praktis sebagai berikut:

1. Aspek Teoritis

   Hasil penelitian ini diharapkan menjadi masukan untuk mengkaji bagaimana melakukan evaluasi Tingkat risiko keamanan informasi pada suatu bisnis terhadap sistem informasi yang mengacu pada ISO 27005:2022 dan menambah referensi untuk penelitian berikutnya.
2. Aspek Praktis

Penelitian ini diharapkan dapat menjadi masukan bagi Perusahaan yang belum optimal dalam melaksanakan evaluasi Tingkat risiko keamanan informasi. Penerapan ini dapat menjadi langkah awal dalam keamanan informasi Perusahaan dalam menjaga aset yang dimiliki.

I.6 Sistematika Penulisan

Tugas akhir ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini menjelaskan latar belakang yang menjadi dasar dilakukannya penelitian, termasuk urgensi permasalahan keamanan informasi di lingkungan organisasi sektor publik, khususnya pada Divisi XYZ. Selain itu, bab ini menguraikan rumusan masalah yang menjadi fokus penelitian, tujuan yang ingin dicapai, batasan masalah yang memperjelas ruang lingkup penelitian, serta manfaat teoritis dan praktis dari penelitian ini. Di akhir bab, dijelaskan pula sistematika penulisan sebagai panduan pembaca dalam memahami isi tugas akhir secara keseluruhan.

Bab II Tinjauan Pustaka

Bab ini menyajikan landasan teori yang relevan dengan topik penelitian, mencakup konsep-konsep dasar seperti keamanan informasi, manajemen keamanan informasi, risiko, analisis risiko, dan ISO/IEC 27005:2022. Selain itu, bab ini juga membahas penelitian terdahulu yang berkaitan serta justifikasi pemilihan kerangka kerja dalam penelitian.

Bab III Metodologi Penelitian

Bab ini menguraikan secara rinci pendekatan dan metode penelitian yang digunakan untuk mencapai tujuan penelitian. Pembahasan mencakup kerangka berpikir, pendekatan penelitian yang digunakan, metode pengumpulan data (baik primer maupun sekunder), teknik analisis data, serta tahapan-tahapan dalam pelaksanaan analisis risiko berdasarkan ISO/IEC 27005:2022. Penjabaran metodologi dilakukan secara sistematis agar memudahkan dalam menelusuri proses pelaksanaan penelitian dari awal hingga akhir.

Bab IV Penetapan Konteks dan Analisa Data

Bab ini berisi proses pengumpulan, klasifikasi, dan analisis data untuk menetapkan konteks organisasi sebagai dasar dalam melakukan penilaian risiko. Penjelasan meliputi identifikasi objek penelitian, struktur organisasi, serta peran Divisi XYZ dalam pengelolaan keamanan informasi. Selanjutnya, dijabarkan pula proses identifikasi aset informasi, *supporting assets*, potensi ancaman, kerentanan, serta dampak yang mungkin timbul jika risiko terjadi. Analisis dilakukan dengan mengacu pada panduan ISO/IEC 27005:2022 dalam tahap "*Context Establishment*".

Bab V Analisis Hasil

Bab ini menyajikan hasil dari tahapan risk assessment yang telah dilakukan. Penjelasan mencakup proses *risk identification*, *risk analysis*, dan *risk evaluation* terhadap aset-aset yang telah ditentukan sebelumnya. Risiko-risiko yang ditemukan kemudian dianalisis untuk menentukan tingkat kemungkinan (*likelihood*) dan dampaknya (*impact*), serta dikalkulasikan untuk memperoleh tingkat risiko kualitatif. Selanjutnya, disajikan pula strategi penanganan risiko (*risk treatment*) yang sesuai dengan hasil evaluasi risiko serta kebijakan keamanan informasi organisasi.

Bab VI Kesimpulan dan Saran

Bab terakhir memuat kesimpulan dari keseluruhan hasil penelitian, yang mencerminkan pencapaian terhadap tujuan dan jawaban atas rumusan masalah. Selain itu, bab ini memberikan saran-saran yang bersifat konstruktif baik untuk instansi tempat penelitian dilakukan maupun untuk peneliti selanjutnya. Saran diberikan sebagai bentuk kontribusi penelitian dalam upaya peningkatan manajemen keamanan informasi secara berkelanjutan.