BAB I PENDAHULUAN

I.1 Latar Belakang

Keamanan informasi merupakan aspek yang sangat penting pada era digitalisasi saat ini, terutama terhadap instansi atau organisasi yang menggunakan teknologi informasi (Utomo dkk., 2012). Di tengah transformasi digital yang pesat, ancaman terhadap data dan sistem informasi semakin meningkat, seiring dengan semakin kompleksnya teknologi yang diadopsi. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia pada tahun 2022 meningkat sebesar 22% dibandingkan tahun sebelumnya. Serangan siber tersebut terdiri dari berbagai jenis, mulai dari serangan *phishing*, *malware*, *ransomware*, hingga serangan *DDoS* (integrasolusi, 2023).

Sektor Terdampak	Jumlah
Adm. Pemerintahan	186
Lainnya	60
Keuangan	38
Transportasi	24
ESDM	18
TIK	5
Kesehatan	5
Pangan	5
Pertahanan	2

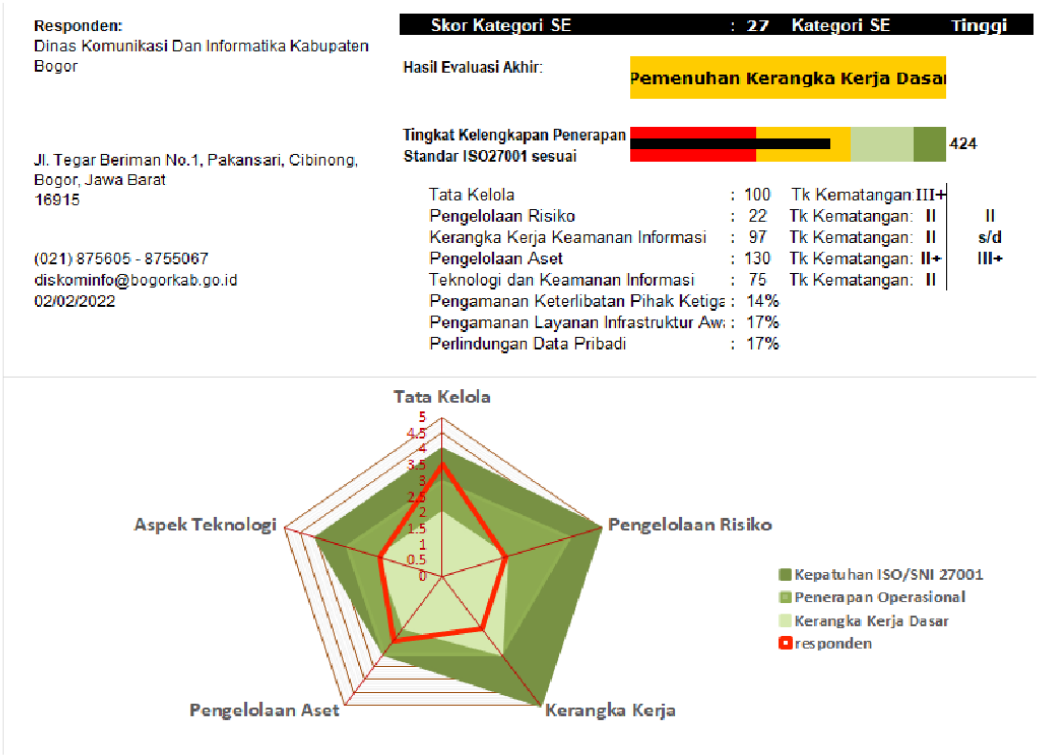
Gambar I.1 Laporan Lanskap Keamanan Siber Indonesia
Sumber (BSSN, 2023)

Berdasarkan Gambar I.1, menurut laporan lanskap keamanan siber Indonesia tahun 2023, total terdapat 347 dugaan insiden siber di berbagai sektor, termasuk administrasi pemerintahan, keuangan, transportasi, kesehatan, dan teknologi informasi dan komunikasi (TIK). Dari seluruh insiden, sektor administrasi pemerintahan tercatat paling terdampak dengan jumlah 186 kasus, yang

menunjukkan kerentanan sektor pemerintahan terhadap ancaman siber. Fakta bahwa sektor ini menjadi target utama menunjukkan pentingnya perlindungan dan pengelolaan risiko keamanan informasi secara lebih efektif (Aurabillah dkk., 2024).

Sebagai contoh nyata dari konsekuensi risiko tersebut, pada Juni 2024 terjadi sebuah insiden siber berskala nasional berupa serangan ransomware yang berhasil melumpuhkan Pusat Data Nasional Sementara (PDNS) (Prasetyo, 2024). Serangan ini mengakibatkan gangguan pada berbagai layanan publik dan menjadi bukti betapa rentannya infrastruktur digital pemerintah jika tidak dilindungi oleh manajemen risiko yang kuat. Kasus ini mengekspos kelemahan kritis dalam keamanan informasi dan menunjukkan urgensi bagi setiap instansi pemerintah untuk membangun pertahanan yang sistematis dan proaktif.

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Bogor merupakan sebuah instansi pemerintah yang berperan penting dalam pemanfaatan teknologi informasi dan komunikasi (TIK) (Diva Ramadhani dkk., 2020). Diskominfo bertanggung jawab untuk memastikan informasi dan data digital pemerintah tetap aman serta bebas dari ancaman siber yang dapat mengganggu operasional dan pelayanan kepada masyarakat. Untuk menghadapi berbagai ancaman keamanan siber, Diskominfo Kabupaten Bogor menerapkan manajemen risiko keamanan informasi secara sistematis. Namun, efektivitas pengelolaan ini masih memerlukan penguatan, agar keamanan informasi yang ada semakin kuat.



Gambar I.2 Indeks KAMI

Sumber (Dinas Komunikasi dan Informatika Kabupaten Bogor, 2023)

Indeks KAMI (Keamanan Informasi) merupakan alat yang dirancang oleh Badan Siber dan Sandi Negara (BSSN) Indonesia untuk menilai dan meningkatkan kesiapan serta ketahanan keamanan informasi di instansi pemerintah maupun organisasi lainnya (Indah Dwi Octaviani & Dwi Herlambang, 2019). Berdasarkan Gambar I.2, memberikan gambaran terkait tingkat kesiapan Diskominfo Kabupaten Bogor dalam pengelolaan keamanan informasi berdasarkan standar ISO/SNI 27001. Berdasarkan skor yang tercantum, Diskominfo Kabupaten Bogor berada pada tahap "Pemenuhan Kerangka Kerja Dasar" dengan skor kategori Sistem Elektronik (SE) sebesar 27, yang mengindikasikan bahwa institusi ini masih memiliki banyak ruang untuk peningkatan, terutama dalam penerapan standar yang lebih tinggi terkait keamanan informasi. Beberapa area penting seperti pengelolaan risiko hanya memperoleh skor 22 dan tingkat kematangan II, menunjukkan bahwa terdapat kebutuhan mendesak untuk meningkatkan penilaian dan manajemen risiko keamanan informasi di instansi ini.

Upaya yang dapat dilakukan oleh Diskominfo Kabupaten Bogor adalah mengimplementasikan standar internasional seperti ISO 27005:2022 menjadi

pedoman yang sangat relevan (Nasher, 2018). ISO/IEC 27005:2022 memberikan panduan komprehensif untuk manajemen risiko keamanan informasi. Standar ini mendukung penerapan persyaratan dalam Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/IEC 27001:2022 dengan menyediakan kerangka kerja untuk mengidentifikasi, menilai, dan mengelola risiko yang berkaitan dengan keamanan informasi (Hikam dkk., 2024). Dalam konteks organisasi pemerintah, seperti Diskominfo, penerapan ISO/IEC 27005:2022 dapat membantu menciptakan pendekatan yang lebih sistematis dan berkelanjutan untuk mengelola risiko keamanan informasi, memastikan bahwa perlindungan data dan layanan publik dapat terus ditingkatkan. Penyelenggara layanan publik sangat dianjurkan untuk mengimplementasikan pengamanan informasi berdasarkan standar ISO 27000, sebagaimana yang tercantum dalam Panduan Penerapan Tata Kelola Keamanan Informasi (Asriyanik & Prajoko, 2018).

Hingga saat ini, Diskominfo Kabupaten Bogor belum sepenuhnya menerapkan standar yang mengatur Manajemen Risiko Keamanan Informasi seperti ISO 27005:2022. Menurut Peraturan Pemerintah (PP) Republik Indonesia No. 71 Tahun 2019, Peraturan ini mengatur penyelenggaraan sistem dan transaksi elektronik, termasuk aspek keamanan informasi dan manajemen risiko yang wajib diterapkan oleh penyelenggara sistem elektronik (Peraturan Pemerintah Republik Indonesia, 2019). Peraturan ini memberikan dasar hukum bagi instansi pemerintah dalam menerapkan langkah-langkah keamanan untuk melindungi data dan informasi. Selain itu, Peraturan Presiden (Perpres) No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) juga menjadi acuan penting dalam upaya meningkatkan kualitas tata kelola pemerintahan digital (Peraturan Presiden Republik Indonesia, 2018). Perpres ini mengharuskan instansi pemerintah, termasuk Diskominfo, untuk mematuhi prinsip-prinsip keamanan informasi dalam rangka mendukung implementasi SPBE secara optimal. Kepatuhan terhadap Perpres SPBE tidak hanya meningkatkan efisiensi layanan publik tetapi juga memastikan perlindungan data yang lebih baik bagi masyarakat. Sebagai upaya memperkuat pengelolaan risiko di lingkungan pemerintah daerah, Pemerintah Kabupaten Bogor menerbitkan Peraturan Bupati Bogor Nomor 24 Tahun 2024 tentang Pedoman Pengelolaan Risiko di Lingkungan Pemerintah

Daerah (Peraturan Bupati Bogor, 2024). Peraturan ini bertujuan untuk memberikan panduan dalam mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat menghambat pencapaian tujuan pemerintah daerah.

Berdasarkan permasalahan yang dihadapi Diskominfo Kabupaten Bogor, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis risiko keamanan informasi yang ada di instansi terkait. Penelitian ini juga bertujuan untuk memberikan rekomendasi yang berbasis pada kerangka kerja ISO 27005:2022 dalam rangka meningkatkan perlindungan terhadap aset TI dan memitigasi potensi ancaman yang dapat mengganggu operasional maupun kepercayaan publik terhadap layanan Diskominfo.

I.2 Perumusan Masalah

Rumusan masalah yang akan dibahas dalam penulisan ini yang telah dipaparkan berdasarkan latar belakang adalah sebagai berikut:

a. Bagaimana penerapan ISO 27005:2022 untuk mengidentifikasi dan menilai risiko keamanan informasi di Diskominfo Kabupaten Bogor?
b. Bagaimana rancangan solusi terkait peningkatan keamanan informasi yang dapat diterapkan di Diskominfo Kabupaten Bogor berdasarkan hasil identifikasi dan penilaian risiko?

I.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

a. Mengidentifikasi dan menilai risiko keamanan informasi di Diskominfo Kabupaten Bogor menggunakan ISO 27005:2022.
b. Memberikan rancangan solusi untuk meningkatkan keamanan informasi yang dapat diterapkan di Diskominfo Kabupaten Bogor berdasarkan hasil identifikasi dan penilaian risiko.

I.4 Batasan Penelitian

Dari sisi cakupan aset, analisis tidak mencakup aset teknologi informasi (TI) yang dikelola oleh Organisasi Perangkat Daerah (OPD) lain, melainkan hanya aset yang

berada di bawah pengelolaan langsung Diskominfo Kabupaten Bogor. Selain itu, penelitian ini tidak sampai pada tahap implementasi teknis, pengadaan teknologi, maupun evaluasi terhadap efektivitas dari solusi yang telah dirancang.

I.5 Manfaat Penelitian

Manfaat yang bisa didapat dari penelitian ini, yaitu:

1. Bagi Diskominfo Kabupaten Bogor dan organisasi sejenis, seperti instansi pemerintah daerah atau lembaga publik lainnya yang mengelola TI, Penelitian ini diharapkan membantu dalam mengidentifikasi dan mengelola risiko keamanan informasi, serta dapat memberikan rekomendasi kebijakan keamanan yang lebih efektif untuk mendukung transformasi digital dan meningkatkan keamanan informasi.
2. Bagi lembaga akademik dan peneliti lain, Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan ilmu pengetahuan, khususnya di bidang manajemen risiko keamanan informasi. Penelitian ini melengkapi knowledge base mengenai penerapan standar ISO 27005:2022 dan memberikan wawasan yang relevan untuk penelitian serupa, pengembangan kurikulum, serta studi lanjutan yang mendukung inovasi di bidang keamanan informasi.

I.6 Sistematika Laporan

Sistematika penulisan laporan tugas akhir berfungsi sebagai panduan bagi mahasiswa dalam menyusun laporan sebagai bentuk pertanggungjawaban atas kegiatan penelitian yang telah dilaksanakan. Sistematika ini memberikan struktur yang jelas untuk memastikan laporan disusun dengan baik dan mencakup semua aspek penting dari tugas akhir. Berikut adalah sistematika penulisan laporan tugas akhir adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi mengenai latar belakang, rumusan masalah, tujuan, manfaat, serta batasan penelitian. Bab ini memberikan gambaran umum mengenai alasan dilakukannya penelitian, arah dan fokus penelitian, serta ruang lingkup yang

dibatasi agar pembahasan tetap terarah dan sesuai dengan konteks yang telah ditentukan, serta dapat memahami dasar dan arah penelitian secara menyeluruh sebelum masuk ke pembahasan yang lebih teknis pada bab-bab selanjutnya.

BAB II LANDASAN TEORI

Bab ini menjelaskan secara mendalam mengenai kajian literatur dan teori-teori yang relevan dengan topik penelitian. Di dalamnya dibahas berbagai konsep dasar, definisi, serta penjelasan mengenai *framework* yang digunakan dalam penelitian. Selain itu, bab ini juga mencakup penelitian terdahulu yang selaras sebagai bahan perbandingan dan penguat dalam menyusun landasan teoritis. Tujuannya adalah agar solusi atau analisis yang dibangun dalam penelitian memiliki dasar ilmiah yang kuat.

BAB III METODE PENYELESAIAN MASALAH

Bab ini menguraikan tentang sistematika yang digunakan untuk menyelesaikan masalah yang telah didasarkan pada rumusan masalah secara rinci untuk mencapai tujuan penelitian, termasuk apa yang dilakukan sehingga *framework* yang digunakan dapat menjadi solusi dari permasalahan yang ada. Bab ini bersifat konseptual dan memberikan gambaran bagaimana metode akan dijalankan, serta disajikan kerangka berpikir yang menjelaskan mengapa pendekatan tersebut dianggap paling tepat untuk konteks permasalahan yang dihadapi.

BAB IV PENYELESAIAN MASALAH

Bab ini berisi uraian mengenai proses pengumpulan dan pengolahan data dari pelaksanaan metode yang telah ditetapkan pada bab sebelumnya. Di dalamnya, menyajikan data yang diperoleh dari berbagai sumber dikumpulkan secara sistematis, kemudian diolah dan dianalisis untuk menghasilkan informasi yang relevan dan mendukung penyusunan solusi terhadap permasalahan yang telah dirumuskan. Proses disusun secara runtut yang bertujuan untuk menunjukkan tahapan penyelesaian masalah secara menyeluruh sehingga pembaca dapat memahami jalannya proses secara utuh dan terarah.

BAB V VALIDASI, ANALISIS HASIL, DAN IMPLIKASI

Bab ini berisi hasil dari proses pengolahan data yang telah dilakukan, disertai dengan analisis untuk menilai sejauh mana dalam menjawab permasalahan yang ada. Di dalamnya, ditampilkan temuan-temuan utama dari penelitian, termasuk identifikasi kesenjangan antara kondisi eksisting dan kondisi ideal. Berdasarkan hasil tersebut, disusun rekomendasi perbaikan. Selain itu, bab ini proses validasi terhadap hasil yang diperoleh guna memastikan keakuratan dan relevansinya.

BAB VI KESIMPULAN DAN SARAN

Pada bab ini merangkum hasil utama yang telah dicapai, menjawab rumusan masalah, serta mengambil kesimpulan berdasarkan hasil analisis. Selain itu, disampaikan juga saran-saran yang bersifat konstruktif, baik untuk penerapan hasil penelitian di masa depan, perbaikan pada proses yang berjalan, maupun untuk penelitian lanjutan yang relevan dengan topik yang diangkat.