BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digitalisasi, keamanan informasi menjadi prioritas utama, khususnya bagi institusi pemerintahan. Ketergantungan pada sistem informasi menghadirkan efisiensi, namun juga meningkatkan risiko terhadap serangan siber. IBM Security X-Force (2024) melaporkan bahwa sektor pemerintahan menempati posisi ketiga target serangan siber global dengan persentase sekitar 17%, menegaskan bahwa transformasi digital harus diiringi dengan penerapan sistem manajemen keamanan informasi yang tangguh [1]. Tanpa perlindungan yang memadai, data publik dan negara akan rentan disalahgunakan. Kondisi inilah yang mendorong perlunya standar pengelolaan keamanan informasi yang terstruktur dan diakui secara global.

Oleh karena itu ISO/IEC 27001:2022 hadir sebagai standar global yang menyediakan pendekatan sistematis dalam manajemen risiko keamanan informasi. Pembaruan versi 2022 menekankan fleksibilitas dalam pengelolaan aset digital, termasuk cloud dan sistem kerja jarak jauh [2]. Hal ini sangat relevan dengan kebutuhan instansi publik yang mulai mengadopsi teknologi terbuka, seperti smart city. Pendekatan berbasis risiko yang diatur dalam standar ini juga selaras dengan prinsip manajemen risiko ISO 31000, sehingga memungkinkan kontrol diterapkan secara adaptif. Tidak hanya aspek teknis, ISO/IEC 27001 juga menekankan tata kelola, dokumentasi, serta komitmen organisasi, sehingga menjadikannya tepat diterapkan di lingkungan birokrasi pemerintahan. Namun, meskipun standar ini menyediakan kerangka kerja yang komprehensif, penerapannya di sektor publik masih menghadapi tantangan nyata.

Implementasi ISO/IEC 27001:2022 di sektor publik, khususnya pemerintah daerah, masih menghadapi berbagai kendala. Keterbatasan SDM, minimnya pelatihan, serta belum adanya pemetaan risiko yang memadai menjadi tantangan besar [3]. Selain itu, budaya keamanan informasi belum terbentuk secara menyeluruh, sehingga kontrol cenderung bersifat formalitas administratif. Kepatuhan terhadap kebijakan keamanan juga sangat bergantung pada pemahaman

dan sikap pegawai [4]. Jika kondisi ini tidak ditangani dengan pendekatan strategis dan berbasis data, maka penerapan ISO berisiko hanya menjadi formalitas tanpa implementasi nyata. Permasalahan ini juga dapat ditemui dalam konteks lokal, salah satunya di Dinas Komunikasi dan Informatika (Diskominfo) Provinis DIY.

Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Daerah Istimewah Yogyakarta (DIY) memegang peran penting dalam pengelolaan sistem informasi daerah melalui inisiatif *Jogja Smart Province* yang mendorong pemanfaatan TIK untuk layanan publik [5]. Transformasi digital ini meningkatkan ketergantungan pada sistem TIK yang kompleks, namun hingga kini belum ada studi sistematis mengenai pengelolaan keamanan informasinya. Identifikasi aset seperti data kependudukan, aplikasi layanan publik, infrastruktur jaringan, dan perangkat keras belum terdokumentasi dengan baik. Demikian pula, penilaian risiko terkait kerahasiaan, integritas, dan ketersediaan informasi belum dilakukan secara menyeluruh. Kondisi ini membuat potensi ancaman, seperti kebocoran data, downtime aplikasi, serangan DDoS, maupun kerusakan perangkat, sulit dievaluasi secara objektif [6], [7]. Oleh karena itu, kesenjangan tersebut menegaskan perlunya penelitian yang tidak hanya memetakan aset dan risiko secara sistematis, tetapi juga menghasilkan dasar yang kuat bagi peningkatan keamanan informasi di Diskominfo Provinsi DIY.

Penelitian ini diharapkan dapat memberikan manfaat praktis bagi Diskominfo Prov DIY dalam merancang kontrol yang lebih efektif. Selain itu, peta risiko yang tersusun dapat dijadikan pedoman dalam pelatihan staf dan penyusunan SOP keamanan informasi. Tøndel et al. menekankan bahwa manajemen insiden akan berjalan optimal jika ditopang oleh hasil penilaian risiko yang terdokumentasi. Dengan hasil penelitian ini, institusi lain juga bisa menggunakan pendekatan serupa sebagai model awal implementasi ISO/IEC 27001. Dengan demikian, kontribusi penelitian ini tidak hanya terbatas pada Diskominfo, tetapi juga relevan secara nasional [8].

Sejalan dengan manfaat tersebut, penelitian ini secara khusus bertujuan mendalami ISO/IEC 27001:2022 secara sistematis dan berbasis data untuk menyusun peta risiko keamanan informasi di Diskominfo Provinsi DIY. Hasilnya

akan memberikan dasar bagi rekomendasi kontrol dan kebijakan keamanan yang lebih terarah. Selain itu, studi ini diharapkan dapat memperkaya literatur akademik tentang penerapan ISO di sektor publik di Indonesia. Mengingat pentingnya perlindungan data di era digital, penelitian ini menjadi kontribusi nyata dalam meningkatkan ketahanan informasi pemerintahan di tingkat lokal maupun nasional.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, dapat dirumuskan permasalahan utama dalam penelitian ini sebagai berikut:

1. Bagaimana proses identifikasi aset informasi penting yang dilakukan di Dinas Komunikasi dan Informatika (Diskominfo) Provinsi DIY ?
2. Bagaimana proses penilaian risiko terhadap keamanan informasi dilakukan sesuai dengan standar ISO/IEC 27001:2022 ?

1.3 Batasan Masalah

Agar penelitian ini terarah dan fokus, maka ruang lingkup penelitian dibatasi pada aspek-aspek berikut:

1. Penelitian difokuskan pada identifikasi risiko keamanan informasi internal yang berkaitan dengan aset informasi strategis di lingkungan Dinas Komunikasi dan Informatika (Diskominfo) Provinsi DIY.
2. Unit analisis terbatas pada bidang atau bagian yang secara langsung mengelola dan melindungi aset informasi, tidak mencakup seluruh Organisasi Perangkat Daerah (OPD) atau instansi lain di luar Diskominfo Prov DIY.
3. Penilaian risiko dilakukan berdasarkan kerangka kerja ISO/IEC 27001:2022, khususnya Annex A, serta mengacu pada pedoman manajemen risiko ISO 31000:2018.
4. Penelitian ini tidak mencakup pengujian atau pengukuran efektivitas kontrol keamanan informasi yang saat ini telah diterapkan oleh organisasi.
5. Data penelitian diperoleh melalui observasi checklist kontrol, dan dokumentasi internal dari Diskominfo Prov DIY.

6. Dari total 93 kontrol yang tercantum dalam Annex A ISO/IEC 27001:2022 penelitian ini hanya mengevaluasi kontrol yang relevan dengan lingkup, aset informasi, dan risiko yang telah teridentifikasi di Diskominfo Prov DIY. Kontrol yang tidak relevan dengan lingkup penelitian tidak dianalisis lebih lanjut.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk memberikan gambaran sistematis dan terukur mengenai manajemen risiko keamanan informasi di Diskominfo Prov DIY. Adapun tujuan khusus dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi aset-aset informasi utama yang dimiliki oleh Diskominfo Provinsi DIY dan memiliki nilai strategis bagi kelangsungan layanan publik.
2. Menganalisis tingkat risiko terhadap aset informasi tersebut dengan mempertimbangkan dua parameter utama, yaitu tingkat dampak dan kemungkinan terjadinya insiden keamanan informasi.
3. Memberikan rekomendasi peningkatan keamanan informasi berdasarkan kontrol dan praktik terbaik yang tercantum dalam Annex A dari standar ISO/IEC 27001:2022.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dalam dua aspek, yaitu secara teoritis dan praktis.

1. Secara Teoritis

   Penelitian ini berkontribusi pada pengembangan literatur akademik terkait penerapan ISO/IEC 27001:2022 di sektor pemerintahan daerah Indonesia. Studi ini menjadi rujukan bagi peneliti yang mengkaji manajemen keamanan informasi di institusi publik dan adaptasi standar internasional dalam birokrasi lokal. Selain itu, penelitian ini memperkaya kajian identifikasi dan evaluasi risiko informasi berbasis pendekatan kuantitatif yang masih jarang diterapkan di sektor publik.

2. Secara Praktis

   Penelitian ini bermanfaat bagi Diskominfo Prov DIY dalam mengidentifikasi aset informasi strategis, mengevaluasi risiko keamanan, dan merekomendasikan kontrol berbasis ISO/IEC 27001:2022. Peta risiko yang tersusun sistematis membantu meningkatkan kesiapan menghadapi ancaman siber serta menyusun kebijakan dan SOP yang tepat. Hasilnya juga dapat menjadi acuan awal bagi lembaga pemerintah lain yang ingin mengimplementasikan sistem manajemen keamanan informasi berstandar internasional.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari lima bab yang disusun secara sistematis sebagai berikut:

- BAB I PENDAHULUAN : berisi uraian mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan skripsi.
- BAB II TINJAUAN PUSTAKA : memuat studi literatur dan dasar teori yang relevan dengan topik penelitian, termasuk konsep ISO/IEC 27001:2022 dan metode penilaian risiko.
- BAB III METODE PENELITIAN : menjelaskan pendekatan kuantitatif yang digunakan, objek dan alur penelitian, alat dan bahan, teknik pengumpulan, serta analisis data.
- BAB IV HASIL DAN PEMBAHASAN : menyajikan hasil identifikasi dan penilaian risiko informasi serta pembahasan yang mengacu pada teori dan standar ISO/IEC 27001:2022.
- BAB V PENUTUP : memuat kesimpulan dari hasil penelitian dan saran untuk pengembangan lebih lanjut di masa mendatang.