BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era transformasi digital, keamanan informasi menjadi aspek strategis bagi setiap instansi pemerintahan. Informasi tidak lagi hanya berfungsi sebagai pendukung operasional, tetapi telah menjadi aset yang memiliki nilai penting sehingga harus dijaga kerahasiaan, integritas, dan ketersediaannya. Ancaman seperti serangan siber, kebocoran data, dan penyalahgunaan hak akses dapat mengganggu keberlangsungan layanan publik serta menurunkan kepercayaan masyarakat terhadap penyelenggaraan pemerintahan digital [1]. Oleh karena itu, audit risiko sistem informasi diperlukan untuk memastikan keamanan, efektivitas, dan efisiensi pengelolaan sistem informasi dalam organisasi [2].

Di Indonesia, peningkatan penggunaan internet hingga mencapai 221,56 juta pengguna atau 79,5% dari total populasi turut meningkatkan ancaman siber. Data Badan Siber dan Sandi Negara (BSSN) menunjukkan rata-rata 768 juta anomali lalu lintas jaringan setiap tahun dalam lima tahun terakhir [3]. Kondisi tersebut menuntut instansi pemerintah untuk menerapkan tata kelola keamanan informasi yang efektif. Salah satu instansi yang memiliki peran strategis adalah Dinas Komunikasi dan Informatika (Diskominfo) Kota Lhokseumawe sebagai pengelola infrastruktur teknologi informasi, layanan pemerintahan berbasis elektronik, serta data sektoral pemerintah daerah [4]. Peran tersebut menjadikan keamanan informasi sebagai faktor penting dalam menjamin keberlangsungan pelayanan publik.

Dalam penerapan tata kelola keamanan informasi, terdapat beberapa standar dan kerangka kerja yang umum digunakan, yaitu ISO/IEC 27001:2022, COBIT 2019, dan NIST Cybersecurity Framework (NIST CSF) 2.0. COBIT 2019 berfokus pada tata kelola dan manajemen teknologi informasi secara menyeluruh [5]. NIST CSF 2.0 berfokus pada pengelolaan risiko keamanan siber melalui fungsi *Govern, Identify, Protect, Detect, Respond,* dan *Recover*, sehingga lebih banyak digunakan sebagai pedoman peningkatan ketahanan siber organisasi [6]. Sementara itu, ISO/IEC 27001:2022 secara khusus mengatur penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis risiko sebagai standar internasional yang digunakan untuk membangun, menerapkan, memelihara, dan meningkatkan keamanan informasi secara berkelanjutan [4]. Oleh

karena itu, penelitian ini menggunakan ISO/IEC 27001:2022 karena paling sesuai dengan tujuan penelitian, yaitu mengevaluasi tata kelola keamanan informasi pada instansi pemerintah. Selain itu, standar ini memiliki keterkaitan yang kuat dengan Indeks Keamanan Informasi (KAMI) versi 5.0 sehingga hasil evaluasi dapat dipetakan terhadap persyaratan ISO/IEC 27001:2022 [7],[8].

Meskipun ISO/IEC 27001:2022 telah menjadi acuan internasional dalam penerapan SMKI, berbagai penelitian menunjukkan bahwa tingkat kesiapan instansi pemerintah dalam menerapkan tata kelola keamanan informasi masih relatif rendah. Permasalahan yang umum ditemukan meliputi keterbatasan sumber daya manusia, belum terintegrasinya kebijakan keamanan informasi, rendahnya komitmen manajemen, serta kurangnya budaya kesadaran keamanan informasi [9]. Selain itu, sebagian besar penelitian terdahulu hanya berfokus pada pengukuran tingkat kematangan menggunakan satu kerangka kerja, baik ISO/IEC 27001 maupun Indeks KAMI. Penelitian yang mengintegrasikan hasil evaluasi Indeks KAMI 5.0 dengan analisis kesenjangan terhadap ISO/IEC 27001:2022 serta menyusun roadmap implementasi sebagai tindak lanjut hasil evaluasi, khususnya pada instansi pemerintah daerah, masih relatif terbatas.

Indeks Keamanan Informasi (KAMI) versi 5.0 merupakan instrumen evaluasi yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) untuk menilai tingkat kematangan penerapan keamanan informasi berdasarkan standar ISO/IEC 27001:2022. Menurut Firmansyah dan Nugroho [7], Indeks KAMI 5.0 dapat membantu instansi pemerintah menilai tingkat kematangan keamanan informasi secara objektif sebagai langkah awal menuju penerapan ISO/IEC 27001:2022. Oleh karena itu, kombinasi Indeks KAMI 5.0 dan ISO/IEC 27001:2022 memberikan pendekatan yang lebih komprehensif karena tidak hanya mengukur tingkat kematangan, tetapi juga menghasilkan arah perbaikan berdasarkan standar internasional [8].

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk menganalisis tata kelola keamanan informasi pada Dinas Komunikasi dan Informatika Kota Lhokseumawe berdasarkan standar ISO/IEC 27001:2022 dengan menggunakan Indeks KAMI versi 5.0 sebagai instrumen evaluasi. Penelitian ini mengintegrasikan hasil evaluasi tingkat kematangan, analisis kesenjangan (*gap analysis*) terhadap persyaratan ISO/IEC 27001:2022, serta penyusunan roadmap implementasi sebagai rekomendasi peningkatan

tata kelola keamanan informasi. Hasil penelitian diharapkan dapat menjadi acuan bagi Diskominfo Kota Lhokseumawe maupun instansi pemerintah daerah lainnya dalam meningkatkan penerapan Sistem Manajemen Keamanan Informasi secara bertahap, terukur, dan berkelanjutan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat kesesuaian dan kesiapan tata kelola keamanan informasi di Dinas Komunikasi dan Informatika (Diskominfo) Kota Lhokseumawe terhadap standar ISO/IEC 27001:2022 berdasarkan analisis kesenjangan (*gap analysis*)?
2. Apa saja faktor penghambat dan pendukung dalam penerapan tata kelola keamanan informasi di Diskominfo Kota Lhokseumawe?
3. Rekomendasi apa yang dapat disusun untuk meningkatkan efektivitas dan keberlanjutan penerapan tata kelola keamanan informasi sesuai standar ISO/IEC 27001:2022?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menganalisis tingkat kesesuaian dan kesiapan tata kelola keamanan informasi di Dinas Komunikasi dan Informatika (Diskominfo) Kota Lhokseumawe berdasarkan standar ISO/IEC 27001:2022.
2. Mengidentifikasi faktor-faktor penghambat dan pendukung dalam penerapan tata kelola keamanan informasi di Diskominfo Kota Lhokseumawe.
3. Menyusun rekomendasi strategis untuk meningkatkan efektivitas dan keberlanjutan penerapan keamanan informasi sesuai standar ISO/IEC 27001:2022.

1.4 Batasan Penelitian

Untuk menjaga ruang lingkup agar tetap fokus dan terarah, penelitian ini dibatasi pada hal-hal berikut:

1. Penelitian hanya dilakukan pada Dinas Komunikasi dan Informatika (Diskominfo) Kota Lhokseumawe sebagai objek studi.

2. Standar acuan yang digunakan adalah ISO/IEC 27001:2022, dengan fokus pada elemen manajemen, kebijakan, risiko, dan kontrol keamanan informasi, bukan pada aspek teknis seperti konfigurasi sistem, perangkat keras, atau enkripsi.
3. Data penelitian diperoleh melalui wawancara, kuesioner, dan observasi terhadap pegawai dan pejabat yang berperan dalam pengelolaan keamanan informasi di lingkungan Diskominfo.
4. Penilaian terhadap kondisi aktual dilakukan dengan metode analisis kesenjangan (*gap analysis*) antara penerapan saat ini dan standar ISO/IEC 27001:2022.
5. Penelitian tidak membahas aspek implementasi teknis sertifikasi ISO/IEC 27001:2022, melainkan sebatas analisis kesiapan dan tata kelola organisasi terhadap standar tersebut.

1.5 Manfaat Penelitian

1. Menambah wawasan ilmiah mengenai tata kelola keamanan informasi di sektor publik, khususnya dalam konteks pemerintahan daerah.
2. Memberikan kontribusi akademik terhadap pengembangan kajian penerapan ISO/IEC 27001:2022 dalam organisasi pemerintah.
3. Menjadi referensi bagi peneliti berikutnya yang mengkaji topik serupa, terutama terkait analisis kesiapan keamanan informasi dan faktor penghambat implementasinya.
4. Memberikan gambaran komprehensif kepada Diskominfo Kota Lhokseumawe mengenai tingkat kesesuaian tata kelola keamanan informasinya terhadap standar internasional.
5. Mengidentifikasi faktor-faktor penghambat dan pendukung yang dapat menjadi dasar penyusunan kebijakan peningkatan keamanan informasi di masa mendatang.
6. Menjadi acuan bagi pemerintah daerah lain dalam merancang strategi dan kebijakan keamanan informasi yang selaras dengan regulasi nasional dan standar global.
7. Mendukung upaya pemerintah dalam mewujudkan layanan publik digital yang aman, efisien, dan terpercaya bagi masyarakat.