BAB I
PENDAHULUAN

1.1 Latar Belakang

Pemerintah Indonesia saat ini sudah mulai menerapkan sistem pemerintahan berbasis elektronik atau biasa disingkat SPBE, tercantum dalam PERPRES nomor 95 tahun 2018 bahwa dalam kegiatan mewujudkan pemerintahan yang efektif, terbuka dan memberikan layanan umum yang lebih baik dan dapat dipercaya, maka dibuatnya peraturan untuk penerapan SPBE[1]. Dengan sistem elektronik dalam sistem pemerintahan maka, akan muncul permasalahan baru, yaitu permasalahan terkait keamanan aset/data yang diproses secara elektronik.

Menurut data dari laporan BSSN tahun 2022 sektor administrasi pemerintahan adalah bidang paling banyak serangan dan aduan, yaitu sejumlah 885 serangan *web defacement* dari 2.348 kasus dan adanya aduan siber sebanyak 110 diantaranya 72 aduan terkait kesalahan konfigurasi yang menyebabkan kerentanan pada sistem elektronik. Administrasi pemerintahan juga menjadi paling banyak terjadi serangan *darknet exposure* sebesar 76.20% dengan jumlah data kredensial akun yang terekspos, yaitu 21.302 tersebar di *darknet*[2]. Instansi XYZ termasuk dalam bagian tersebut karena bergerak dibidang yang mengurus administrasi pemerintahan dengan mengalami serangan yaitu, serangan *web defacment* yang terlampir pada lampiran 1.

Instansi XYZ bertanggung jawab dalam merencanakan, mengoordinasikan, dan menilai pengembangan dan pelaksanaan kebijakan daerah di bidang teknologi dan sistem informasi, Instansi XYZ memiliki kurang lebih 165 *subdomain* dalam lingkup SPBE yang terlampir pada lampiran 3. Saat ini di instansi XYZ hanya menerapkan standar sistem manajemen keamanan informasi indeks keamanan informasi (Indeks KAMI) versi 4.2 yang masih mengacu pada ISO 27001:2013 dalam lingkup satu buah sistem elektronik yang tertera pada lampiran 3. Permasalahan yang terjadi pada instansi XYZ masih kurangnya terkait penanganan keamanan terhadap

SPBE yaitu kurangnya SDM, sarana dan prasarana, penerapan SPBE dan pedoman yang masih mengacu pada ISO/IEC 27001 versi tahun 2005 dan ISO/IEC 27002 versi tahun 2008 yang terlampir pada lampiran 2. Instansi XYZ perlu memiliki sistem keamanan yang baik dalam menjaga aset dan data yang ada, maka perlunya standar untuk sistem manajemen keamanan informasi yang terbaru dan lingkup yang menyeluruh.

Sistem manajemen keamanan informasi (SMKI) berfungsi untuk mengamankan kerahasiaan, integritas dan ketersediaan informasi/aset dengan melakukan kegiatan mengelola risiko dan memberikan kepercayaan kepada pihak yang bersangkutan bahwa risiko telah dijalankan sesuai prosedur[3]. SMKI memiliki standar yang diterbitkan oleh ISO (*International Organization for* Standardization) dan IEC (*the Internasional Electrotechnical Commission*) yaitu bernama ISO/IEC 27001 tentang sistem manajemen keamanan informasi yang berfungsi untuk mengamankan aset organisasi. Tata tertib SMKI dijelaskan dalam Peraturan Menteri Komunikasi dan Informatika nomor 4 Tahun 2016, pada pasal 7 ayat 1 menyatakan bahwa pengelola sistem elektronik diwajibkan menerapkan standar SNI ISO/IEC 27001[4]. Kemudian pada peraturan Badan Siber dan Sandi Negara nomor 8 tahun 2020 pada pasal 9 menjelaskan pengelola sistem elektronik wajib menerapkan SNI ISO/IEC 27001[5]. SNI ISO/IEC 27001 adalah Standar Nasional Indonesia ISO/IEC 27001 yaitu adopsi langsung dari ISO/IEC 27001 dengan tambahan terjemahan bahasa Indonesia[6].

Tujuan dari penelitian ini adalah untuk meningkatkan sistem manajemen keamanan informasi instansi XYZ dengan melaksanakan standar yang terbaru yaitu SNI ISO/IEC 27001:2022 sebagai tolok ukur SMKI dan SNI ISO/IEC 27002:2022 referensi pengendalian keamanan informasi. Maka aset informasi di instansi XYZ akan lebih terjamin aman dengan adanya SMKI yang terorganisir dan terlaksana.

1.2 Perumusan Masalah

Perumusan masalah membantu menetapkan arah penelitian dan memperjelas maksud dan tujuan penelitian. Berikut ini rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana tingkat kematangan SMKI instansi XYZ pada kondisi saat ini berdasarkan standar SNI ISO/IEC 27001:2022?
2. Bagaimana kesenjangan pada tingkat kematangan SMKI instansi XYZ saat ini dengan yang diharapkan?
3. Apa saja rekomendasi untuk meningkatkan kematangan SMKI instansi XYZ berdasarkan SNI ISO/IEC 27002:2022?

1.3 Batasan Masalah

Penelitian ini berfokus pada objek yaitu instansi XYZ terkait sistem manajemen keamanan informasi dan untuk metode yang digunakan yaitu kualitatif untuk pengumpulan data dengan cara wawancara dan observasi, lampiran A SNI ISO/IEC 27001:2022 sebagai acuan tolok ukur penerapan SMKI, *maturity level* COBIT 2019 sebagai penentu tingkat kematangan SMKI dan rancangan rekomendasi yang diberikan untuk meningkatkan tingkat kematangan kontrol pengendalian SMKI yaitu dengan SNI ISO 27002:2022 pada instansi XYZ.

1.4 Tujuan

Berlandaskan rumusan masalah pada penelitian ini, maka tujuan dari penelitian ini yaitu sebagai berikut:

1. Mengetahui tingkat kematangan pengimplementasian sistem manajemen keamanan informasi pada instansi XYZ.
2. Mengetahui kesenjangan tingkat kematangan yang terjadi pada sistem manajemen keamanan informasi yang saat ini terjadi dengan yang diharapkan pada instansi XYZ.
3. Penjelasan rekomendasi yang berisi cara dan kebutuhan yang dibutuhkan untuk meningkatkan tingkat kematangan sistem manajemen keamanan informasi saat ini menuju yang diharapkan pada instansi XYZ.

1.5 Ide Solusi

Kondisi saat ini instansi XYZ hanya menerapkan standar manajemen keamanan informasi yaitu indeks KAMI yang mengacu ISO/IEC 27001:2013 dan pedoman yang masih mengacu pada ISO/IEC 27001:2005 dengan lingkup satu sistem elektronik, yang membuat kurangnya keamanan yang ada dan tidak terarahnya dalam mencegah maupun mengatasi penyerangan

terhadap aset informasi yang ada. Dengan menggunakan SNI ISO/IEC 27001:2022 sebagai manajemen keamanan sistem informasi terbaru, sistem keamanan memiliki standarisasi yang lebih aman dan memiliki kerangka kerja untuk acuan mengelola aset dari ancaman yang terbaru.

Metode yang digunakan yaitu kualitatif dengan cara mewawancara dan observasi pihak terkait terhadap pengimplementasian keamanan informasi untuk menemukan tingkat kematangan manajemen keamanan sistem informasi dan kekurangan atau kesenjangannya. Kemudian dari data tersebut menghasilkan saran perbaikan untuk meningkatkan kematangan pengimplementasian agar aset yang ada tetap aman.