

BAB I PENDAHULUAN

I.1 Latar Belakang

Saat ini, pemanfaatan teknologi di Indonesia semakin meluas untuk mempermudah komunikasi, baik dalam ranah pribadi maupun publik. Hal ini membawa risiko terjadinya kebocoran data dan ancaman serangan siber, yang bisa mempengaruhi sektor pemerintah maupun swasta. Menurut Eset Indonesia, sebuah perusahaan keamanan siber global, Indonesia mengalami serangan siber setiap hari, di mana serangan *malware* masih menjadi ancaman utama. Selain itu, *ransomware* diperkirakan akan tetap menjadi tantangan besar dalam menjaga keamanan informasi bagi organisasi atau perusahaan serta instansi pemerintah di Indonesia (Ipungkarti, 2023).

Keamanan informasi dan kesadaran terhadap potensi kebocoran informasi menjadi hal yang krusial dalam penggunaan teknologi informasi, khususnya bagi informasi yang memiliki nilai strategis dan bersifat rahasia. Seluruh informasi wajib dilindungi dan dijaga kerahasiaannya dari berbagai ancaman, seperti akses ilegal, penyalahgunaan, pengungkapan tanpa izin, gangguan, perubahan, maupun perusakan oleh pihak yang tidak memiliki wewenang. Oleh sebab itu, seluruh bentuk informasi baik yang disimpan maupun yang disebarkan harus senantiasa dijamin keamanannya. Seiring dengan meningkatnya jumlah informasi yang disediakan oleh instansi pemerintah untuk keperluan layanan publik, tantangan terhadap keamanan informasi pun menjadi semakin kompleks. Keamanan informasi mencakup tiga komponen utama, yakni kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Oleh karena itu, seluruh pemangku kepentingan, perlu memahami urgensi perlindungan informasi serta menyadari risiko yang mungkin timbul dalam sistem informasi dan komunikasi (Pratiwi & Wulandari, 2021).

Untuk dapat mengelola, menjaga dan juga menerapkan prinsip-prinsip keamanan sistem informasi pemerintah dapat menggunakan ISO (*International Organization for Standardization*) 27001. ISO 27001 merupakan sistem manajemen keamanan informasi (SMKI) yang berstandarkan internasional dapat

membantu untuk kebutuhan keamanan informasi dari sebuah Lembaga pemerintah (Aurabillah et al., 2024).

ISO 27001 merupakan standar internasional yang telah mendapatkan pengakuan luas dan dirancang guna membantu organisasi dalam proses identifikasi serta mitigasi risiko yang berkaitan dengan keamanan informasi. Standar ini juga menetapkan pedoman dan prosedur keamanan yang bersifat ketat. ISO 27001 kerap dimanfaatkan untuk menentukan kebutuhan dalam penerapan sistem keamanan informasi secara tepat. Sebagai sebuah kerangka kerja, ISO 27001 mendukung perusahaan dalam membangun serta menerapkan SMKI secara optimal. Penerapan kerangka kerja ini dapat meningkatkan kepercayaan pelanggan serta menunjang performa bisnis melalui strategi mitigasi risiko, sekaligus memastikan bahwa sistem informasi terlindungi dari ancaman keamanan. Lebih lanjut, ISO 27001 juga berperan penting dalam membantu organisasi memenuhi ketentuan hukum dan regulasi yang berkaitan dengan keamanan informasi (Aditama et al., 2023).

I.2 Perumusan Masalah

Rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana kondisi *eksisting* sistem manajemen keamanan informasi berdasarkan hasil analisis klausa dan kontrol ISO 27001:2013 pada lembaga pemerintahan XYZ?
2. Bagaimana rekomendasi solusi manajemen keamanan sistem informasi yang belum terpenuhi berdasarkan klausa dan kontrol ISO 27001:2013 yang ada pada lembaga pemerintahan XYZ?

I.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menganalisis sistem manajemen keamanan informasi pada lembaga pemerintahan XYZ berdasarkan ISO 27001:2013.
2. Memberikan rekomendasi solusi berdasarkan hasil kondisi *eksisting* klausa dan kontrol ISO 27001:2013 pada Lembaga XYZ.

I.4 Batasan Penelitian

Terdapat batasan-batasan dalam melaksanakan penelitian tugas akhir ini, yaitu:

1. Nama dan identitas perusahaan serta informasi spesifik lainnya akan dirahasiakan dalam seluruh laporan dan publikasi penelitian untuk menjaga anonimitas perusahaan, dokumen yang digunakan dalam penelitian ini hanya akan digunakan untuk keperluan analisis dan tidak akan dipublikasikan.
2. Penelitian ini menggunakan metode *Design Science Research* dengan pengumpulan data melalui wawancara dan dokumen.

I.5 Manfaat Penelitian

Manfaat yang bisa didapat dari penelitian ini, yaitu:

1. Bagi lembaga pemerintahan XYZ dapat mengambil manfaat dari hasilnya guna meningkatkan sistem manajemen keamanan sistem informasi sesuai dengan standar ISO 27001.
2. Meningkatkan tingkat keberhasilan pembaharuan sertifikasi dari ISO 27001:2013 ke ISO 27001:2022.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan permasalahan yang diteliti dan dibahas pula hasil-hasil penelitian terdahulu. Minimal terdapat lebih dari satu metodologi/metode/kerangka kerja yang disertakan pada bab ini untuk menyelesaikan permasalahan atau meminimalisir gap antara kondisi eksisting dengan target. Pada akhir bab, analisis

pemilihan metodologi/metode/kerangka kerja harus dijelaskan untuk menentukan metodologi/metode/kerangka kerja yang akan digunakan di penelitian ini.

Bab III Metodologi Penelitian

Metodologi penelitian merupakan strategi dan langkah-langkah (*plan of attack*) yang akan dilakukan di penelitian dalam rangka menjawab rumusan masalah yang disusun sebelumnya. Penyusunan metodologi penelitian harus dilakukan secara kritis apakah metode atau teknik yang dipilih memang tepat sesuai tujuan penelitian. Pada bab ini dijelaskan langkah-langkah penelitian secara rinci meliputi: tahap merumuskan masalah penelitian, merumuskan hipotesis, mengembangkan model penelitian, mengidentifikasi dan melakukan operasionalisasi variabel penelitian, menyusun kuesioner penelitian, merancang pengumpulan dan pengolahan data, melakukan uji instrumen, merancang analisis pengolahan data.

Bab IV Kajian Klausa dan Annex A ISO 27001:2013

Pada bab ini disajikan kajian terkait *framework* yang digunakan, yaitu ISO 27001:2013. Dimana bab ini berisikan penjelasan terkait deskripsi klausa dan kontrol yang ada pada ISO 27001:2013.

Bab V Hasil Analisis dan Rekomendasi

Pada bab ini, disajikan hasil rancangan, temuan, analisis, pengolahan data dan rekomendasi yang diberikan. Selain itu bab ini juga berisi tentang validasi atau verifikasi hasil dari penelitian, sehingga hasil tersebut apakah telah benar-benar menyelesaikan masalah. Secara keseluruhan bab ini membahas secara mendetail mengenai hasil dari penelitian dan refleksinya terhadap tujuan penelitian.

Bab VI Kesimpulan dan Saran

Pada bab ini dijelaskan kesimpulan dari penelitian yang dilakukan serta jawaban dari pertanyaan penelitian yang disajikan di

pendahuluan. Saran penelitian dikemukakan pada bab ini untuk penelitian selanjutnya.