BAB I

PENDAHULUAN

1.1 Latar Belakang

Data merupakan salah satu aset penting dan berharga baik bagi individu, organisasi/kelompok, bahkan instansi pemerintahan. Untuk memenuhi proses bisnis dan mencapai tujuan bisnis yang diharapkan, perlu dilakukan penyesuaian agar aset tersebut tetap terjaga. Penerapan TI merupakan salah satu penyesuaian yang dapat dilakukan untuk mendukung pencapaian rencana strategis guna mencapai visi, misi dan tujuan dari organisasi (Handoyo, 2020).

Penerapan TIK di lingkungan pemerintahan kerap dikaitkan dengan istilah *e-Government*. Dengan adanya *e-Government* diharapkan kualitas kinerja pemerintah dalam pelayanan masyarakat dapat lebih meningkat. Oleh karena itu Dinas Komunikasi dan Informatika Provinsi Jawa Timur sebagai salah satu instansi pemerintah sekaligus penyelenggara *e-Government* berupaya meningkatkan kualitas layanan publik melalui Sistem Pemerintahan Berbasi Elektronik (SPBE) yang didukung oleh *One Data to Big Data* melalui integrasi data dengan Perangkat Daerah dan Instansi Vertikal di lingkungan Pemerintah Provinsi Jawa timur (Diskominfo, 2019). Hal ini sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk menyediakan layanan kepada pengguna SPBE. Dengan adanya integrasi data berupa SPBE tersebut diperlukan pengelolaan TI yang baik dan benar sehingga dapat bekerja secara optimal dan

mendukung efektifitas kinerja TI untuk mencapai tujuan instansi. Sesuai dengan pasal 3 Perpres No. 95 Tahun 2018 ruang lingkup SPBE terbagi menjadi enam bagian, yaitu 1) Tata Kelola SPBE, 2) Manajemen SPBE, 3) Audit Teknologi Informasi dan Komunikasi, 4) Penyelenggara SPBE, 5) Percepatan SPBE, dan 6) Pemantauan dan Evaluasi SPBE.

Tujuan utama dari enam ruang lingkup SPBE tersebut adalah agar seluruh sistem yang masih berdiri sendiri di masing-masing badan pemerintahan baik di tingkat kabupaten/kota maupun provinsi dapat terhimpun menjadi satu sistem yang terpusat di tingkat nasional. Sehingga diharapkan proses bisnis pemerintahan dapat berjalan dengan lebih baik, lebih efektif dan lebih efisien. Dengan demikian SPBE melibatkan seluruh instansi pemerintahan baik pusat maupun daerah dalam penerapannya.

Dalam penyelenggaraan SPBE, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan mengingat SPBE menerapkan sistem integrasi data dari berbagai badan pemerintahan. Kinerja SPBE dapat terganggu apabila data dan informasi sebagai salah satu objek utama kesuksesan SPBE mengalami masalah baik berupa hambatan, gangguan dan ancaman yang melibatkan aspek kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaan *(availability)* (Effendy et al., 2020). Mengingat keamanan informasi saat ini merupakan isu strategis yang perlu diperhatikan sebagai upaya penanganan serangan siber yang semakin masif.

Keamanan informasi dapat dilakukan dengan menerapkan tata kelola TI yang sesuai termasuk struktur organisasi, kebijakan, proses, prosedur dan implementasi fungsi perangkat keras dan perangkat lunak (Handoyo, 2020).

Beberapa aspek tata kelola tersebut perlu ditetapkan, diterapkan, diawasi, dievaluasi, dan ditingkatkan untuk memastikan tercapainya tujuan bisnis dan keamanan informasi. Keamanan sistem informasi yang baik harus memenuhi standar *deming cycle of quality* (Handoyo, 2020), yaitu:

1. *Plan* (Merencanakan): merencanakan keamanan yang reaktif beralih menjadi proaktif.
2. *Develop* (Mengembangkan): keamanan merupakan serangkaian proses yang perlu dikembangkan mengikuti patokan keamanan.
3. *Check* (Periksa): keamanan dikontrol melalui audit dan tes penetrasi, dan metode yang paling umum.
4. *Act* (Tindakan): temuan malfungsi pada fase "periksa" perlu dilakukan Tindakan korektif, pencegahan dan perbaikan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur (Diskominfo Jatim) sebagai penyelenggara SPBE perlu memastikan penerapan TI dalam SPBE dapat berjalan dengan baik. Oleh karena itu sesuai dengan Permenkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi menyebutkan bahwa "Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya". Untuk memenuhi ketentuan tersebut Diskominfo Jatim saat ini telah berupaya untuk menerapkan standar SNI ISO/IEC 27001 dalam manajemen keamanan informasi.

Penelitian ini bertujuan untuk melakukan evaluasi berupa pengukuran terhadap Sistem Manajemen Keamanan Informasi untuk mengetahui seberapa jauh

tingkat kesiapan Diskominfo Jawa Timur untuk menjaga dan memastikan manajemen keamanan informasi yang dilakukan telah optimal dan dapat mencapai tujuan melalui pengukuran tingkat kapabilitas (*capability level*) yang menggunakan kerangka kerja COBIT 5. Saat ini Diskominfo Jawa Timur telah menerapkan Indeks Keamanan Informasi sebagai pedoman evaluasi SMKI. Sedangkan dalam penelitian ini digunakan kerangka kerja COBIT 5 yang bertujuan untuk memberikan *insight* baru dan sekaligus memberikan hasil evaluasi dari kerangka kerja yang berbeda, sehingga dapat dijadikan perbandingan dalam melakukan evaluasi manajemen keamanan informasi.

Evaluasi dilakukan dengan melakukan pengukuran tingkat kapabilitas terhadap Sistem Manajemen Keamanan Informasi (SMKI) yang telah direncanakan dan disusun oleh Bidang APTIKA Diskominfo Jatim dengan tujuan untuk mengetahui bagaimana kinerja keamanan SPBE dan mengimplementasikan manajemen risiko untuk meminimalisir potensi risiko yang dapat terjadi sehingga membantu memastikan tercapainya tujuan penyelenggaraan TI pada organisasi. SMKI merupakan rincian rencana manajemen untuk melindungi aset informasi dari seluruh gangguan keamanan dan melakukan kontrol keamanan sesuai dengan kebutuhan organisasi (Riadi et al., 2018). Target yang akan dicapai adalah untuk pengembangan Sistem Manajemen Keamanan Informasi lebih lanjut dan dapat mengidentifikasi pencapaian Sistem Manajemen Keamanan Informasi sehingga dapat dijadikan acuan dan arahan dalam pengambilan kebijakan untuk perbaikan selanjutnya.

Dalam pengukuran tingkat kapabilitas perlu adanya standar *base practice* sebagai acuan untuk membantu melakukan analisis manajemen TI serta menjadi

panduan aktivitas TI. Terdapat beberapa kerangka kerja tata kelola TI yang dapat dijadikan sebagai standar *base practice* antara lain COBIT, ITIL dan ISO 27001. Dalam pengukuran tingkat kapabilitas pada studi kasus ini digunakan kerangka kerja tata kelola TI yaitu COBIT 5.

COBIT atau *Control Objectives for Information and Related Technology* merupakan kerangka kerja yang memuat panduan tata kelola TI dan perangkat pendukung yang dapat digunakan untuk menemukan dan menjembatani *gap* antara kebutuhan dan bagaimana proses pemenuhan kebutuhan tersebut dalam organisasi (ITGID, 2016). COBIT mampu memberikan panduan lengkap untuk mengendalikan semua kegiatan dalam organisasi sehingga mampu membantu proses pengambilan keputusan di tingkat manajemen teratas dalam organisasi. COBIT 5 merupakan salah satu produk ISACA yang dirilis pada tahun 2012 untuk tata kelola TI. Seiring berjalannya waktu, kerangka kerja dan standar lainnya telah berkembang dan memunculkan tren teknologi dan bisnis baru dalam penggunaan TI seperti transformasi digital dan DevOps yang membuat COBIT melakukan penyelarasan lagi sehingga muncul COBIT 2019 dengan pembaruan yang berkelanjutan (ITGID, 2019a).

Penelitian terdahulu menunjukkan bahwa implementasi COBIT 2019 lebih sulit karena memiliki detail domain yang lebih banyak dan bersifat lebih *flexible* jika dibandingkan dengan COBIT 5 (Syuhada, 2021). Referensi studi terdahulu terkait COBIT 2019 dalam pengukuran tata kelola TI juga masih sangat terbatas. Oleh karena itu diputuskan untuk menggunakan COBIT 5 yang lebih banyak digunakan dalam pengukuran sebelumnya. COBIT 5 menyajikan kerangka kerja yang komprehensif dalam membantu instansi mencapai tujuan organisasi yang

berkaitan dengan pengelolaan keamanan informasi dan aset teknologi (Effendi et al., 2020). COBIT 5 memiliki sifat generik dan dapat digunakan untuk semua instansi, baik komersial maupun sektor publik. Bahkan COBIT 5 memiliki sebuah produk yang khusus berfokus pada keamanan informasi yaitu *COBIT 5 for Information Security* (ISACA, 2012b).

Jika dibandingkan dengan kerangka kerja lain seperti *Information Technology Infrastructure Library* (ITIL) yang berfokus pada manajemen pelayanan pelanggan, dan *International Standards Organizations* (ISO) yang memiliki produk terkait keamanan informasi yaitu ISO/IEC 27001. COBIT 5 memiliki lima (5) prinsip yang tidak dimiliki oleh kerangka kerja lain yaitu *meeting stakeholder needs, covering enterprise end-to-end, applying a single integrated framework, enabling a holistic approach* dan *separating governance from management* (ISACA, 2012a).

Penelitian terdahulu juga menunjukkan kelebihan COBIT 5 dalam hal keamanan informasi, karena pada praktiknya keamanan informasi tidak hanya berkaitan dengan aspek teknis tetapi juga aspek non teknis. COBIT menyediakan kerangka kerja yang mampu mencakup aspek teknis dan non teknis sehingga mendukung adanya metrik, tolok ukur dan melakukan audit (Sahibudin et al., 2008)(Gehrmann, 2012). Sedangkan ISO/IEC 27001 dan 27002 memiliki kelebihan dalam hal keamanan informasi tetapi hanya bersifat teknis (Sahibudin et al., 2008). Berikut tabel 1.1 merupakan perbandingan kelebihan dari setiap kerangka kerja yaitu ITIL, COBIT dan ISO/IEC 27001.

Tabel 1.1 Perbandingan ITIL, COBIT dan ISO/IEC 27001 (Ciptaningrum et al., 2015)(John Wallhoff, 2004)

ITIL	COBIT	ISO/IEC 27001 & 27002
Concept/Process	*Critical Success Factors*	*Information Security*
Activities	*Metrics (Critical Success Factors and Key Performance Indicator)*	
Cost/Benefits	*Benchmarking (CMM)*	
Planning for Implementation	*Control*	
	Audit	

COBIT 5 memiliki lima domain yang berfungsi untuk menentukan keselarasan antara tujuan bisnis, nilai antar *stakeholder* yang berbeda, dan nilai TI yang digunakan. COBIT 5 berisikan panduan untuk integrasi dengan tata kelola TI di organisasi yang bertujuan untuk menciptakan nilai dengan menentukan peran, kegiatan dan hubungan serta menunjukkan bahwa COBIT 5 berperan sebagai *framework* panduan (Turang & Turang, 2020).

Berdasarkan uraian tersebut, penelitian ini mengacu pada *Internal Stakeholder Needs* ke dua belas (12) yaitu "*Is the information I am processing wells secured?*" dimana COBIT 5 ditujukan untuk menilai tingkat keamanan pemrosesan informasi. Sehingga judul penelitian yang diajukan adalah "**Pengukuran Tingkat Kapabilitas Manajemen Keamanan Informasi Pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur Menggunakan COBIT 5**".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, maka rumusan masalah yang menjadi fokus utama adalah bagaimana tingkat kesiapan manajemen keamanan informasi SPBE Diskominfo Jatim dan apa saja rekomendasi perbaikan yang

mungkin dilakukan berdasarkan pengukuran tingkat kapabilitas menggunakan kerangka kerja COBIT 5.

1.3 Batasan Masalah

Batasan masalah yang perlu diperhatikan dalam penyusunan proposal laporan skripsi ini adalah:

1. Pengukuran tingkat kapabilitas dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
2. Pengukuran tingkat kapabilitas Sistem Manajemen Keamanan Informasi mengacu pada kerangka kerja COBIT 5.
3. Pengukuran tingkat kapabilitas fokus proses pada APO13 dan DSS05.
4. Langkah – langkah yang digunakan dalam penelitian ini sesuai dengan *Assessment Process Activities.*

1.4 Tujuan

Sesuai dengan permasalahan yang telah dijelaskan, maka tujuan yang ingin dicapai dari penelitian skripsi ini adalah mendapatkan hasil pengukuran tingkat kapabilitas yang dapat dijadikan sebagai acuan tingkat kesiapan manajemen keamanan informasi dan mendapatkan rekomendasi perbaikan yang mungkin dilakukan oleh Diskominfo Jatim untuk meningkatkan kinerja dan pengelolaan keamanan informasi.

1.5 Manfaat

Adapun manfaat yang dapat diambil dari hasil penelitian ini adalah:

1. Bagi dunia akademis, hasil dari penelitian ini diharapkan dapat digunakan sebagai referensi penelitian dalam mengukur tingkat kapabilitas sesuai dengan COBIT 5 dan menjadi referensi untuk penelitian selanjutnya terkait manajemen keamanan informasi.
2. Bagi Dinas Komunikasi dan Informatika Provinsi Jawa Timur, penelitian ini diharapkan dapat digunakan sebagai gambaran tingkat kapabilitas dari manajemen keamanan informasi saat ini sehingga menjadi referensi evaluasi bagi instansi. Kemudian mengetahui *gap* antara kondisi yang diharapkan dengan kondisi saat ini. Serta mendapatkan rekomendasi perbaikan yang dapat digunakan sebagai pertimbangan dalam pengambilan keputusan.

1.6 Relevansi Audit Sistem Informasi dengan Sistem Informasi

Audit menurut Al-rasyid et al. (2015), adalah kegiatan mengumpulkan informasi faktual dan signifikan yang berorientasi pada azas nilai manfaat melalui interaksi berupa pemeriksaan, pengukuran, penilaian dan penarikan kesimpulan secara sistematis, objektif dan terdokumentasikan. Secara keseluruhan, audit mencakup penilaian terhadap aspek efektifitas, efisiensi, *availability system, reliability, confidentiality,* dan *integrity*.

Sedangkan definisi Sistem Informasi secara umum dapat diartikan sebagai serangkaian sistem yang terdiri dari *hardware, software, brainware,* dan *procedure* yang diorganisasikan secara integral untuk mengolah data menjadi informasi yang

lebih bermanfaat dan dapat membantu memecahkan masalah dan pengambilan keputusan (Sarno, 2009). Audit Sistem Informasi sendiri menurut Ron Webber (1999), merupakan proses pengumpulan dan penilaian bahan bukti untuk menentukan apakah sistem komputer dapat melindungi aset, memelihara integritas data, mampu mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

Relevansi audit sistem informasi dengan sistem informasi telah dijelaskan dalam Kurikulum Sistem Informasi yang telah disepakati pada Forum Pimpinan Prodi Sistem Informasi se-Indonesia yang menyatakan 15 item deskripsi disiplin ilmu Sistem Informasi beserta ruang lingkup dan karakteristiknya (AISINDO, 2018). Disiplin ilmu terkait audit sistem informasi tercantum pada poin ke tujuh yaitu "Disiplin ilmu Sistem Informasi mempelajari berbagai aspek mencakup Perencanaan Sistem Informasi, Perancangan Sistem Informasi, Pembangunan Sistem Informasi, Operasional Sistem Informasi, Evaluasi/Audit Sistem Informasi, faktor-faktor yang menyebabkan sebuah SI/TI dapat diterima penggunaannya (*Asoption/Diffusion*), bagaimana sebuah SI/TI digunakan target penggunaannya (*Domestication*), dan bagaimana pengaruh/dampak penggunaan sebuah SI/TI (*Impacts* atau *Post Adoption Stage*)". Dengan demikian, audit sistem informasi merupakan irisan dari serangkaian disiplin ilmu Sistem Informasi.

Di sisi lain juga seringkali dikenal dengan istilah audit keamanan sistem informasi. Adapun yang dimaksud dengan audit keamanan menurut Ahmad (2012) yang dikutip oleh Gunawan & Tjahjadi (2018) adalah suatu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan keadaan dari semua perlindungan yang ada, dan untuk memverifikasi apakah

perlindungan yang ada berjalan dengan baik. Tujuan utama dari audit keamanan adalah memberikan dan menjaga perlindungan agar sesuai dengan kebijakan dan standar keamanan yang ada serta memverifikasi apakah perlindungan sudah cukup dan berjalan dengan baik. Adapun empat tujuan audit sistem informasi adalah: 1) Melindungi aset organisasi, 2) Menjaga integritas data, 3) Menjaga efektivitas sistem, dan 4) Mencapai efisiensi sumberdaya (Sarno, 2009).

1.7 Sistematika Penulisan

Sistematika penulisan bertujuan untuk mengarahkan sekaligus menjadi acuan dalam penyusunan laporan skripsi agar sesuai dengan tujuan penulisan laporan skripsi yang diharapkan. Laporan skripsi terbagi menjadi 5 bab yaitu:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan yang digunakan dalam penyusunan laporan skripsi ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang profil singkat dari tempat studi kasus yaitu Dinas Komunikasi dan Informatika Provinsi Jawa Timur, serta berisi penjelasan tentang teori-teori dasar yang digunakan dalam penyusunan laporan skripsi ini yang diperoleh dari berbagai sumber pustaka dan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang urutan langkah-langkah yang dilakukan dan metode penelitian yang dibuat secara terstruktur sebagai pedoman agar dapat mencapai tujuan dari penelitian dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang rincian hasil yang didapat dan pembahasan dari setiap proses yang dilakukan mulai dari *initiation, planning the assessment, briefing, data collection, data validation, process attribute level, dan reporting the result*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Bab ini berisi daftar rujukan berupa literatur yang digunakan dalam penyusunan skripsi ini. Literatur didapat dari berbagai sumber mulai dari jurnal, buku dan internet.

LAMPIRAN

Lampiran berisi dokumentasi tentang dokumen atau informasi terkait yang diperlukan untuk mendukung penyusunan laporan skripsi ini.