BAB I
PENDAHULUAN

1.1 Latar Belakang

Tata kelola adalah hal yang sangat dibutuhkan dalam setiap organisasi baik untuk bidang industri maupun pemerintahan. Pemanfaatan teknologi seringkali memiliki permasalahan dalam pengelolaannya. Saat ini, teknologi informasi sudah banyak digunakan oleh pemerintahan untuk membantu tercapainya rencana strategis agar visi, misi, dan tujuan organisasi dapat diwujudkan. Penerapan tata kelola teknologi informasi yang tidak baik pada suatu instansi dapat mengakibatkan timbulnya permasalahan dan kendala yang dapat mempengaruhi kegiatan operasional (Effendi et al., 2020).

Penerapan teknologi informasi yang telah dilakukan juga harus diperhatikan dalam segi keamanan. Keamanan informasi merupakan hal yang penting karena data yang tersimpan dapat bersifat rahasia dan hanya dapat diakses oleh pemilik hak tertentu (Imany et al., 2019). Ancaman dan gangguan terhadap keamanan informasi merupakan tanggung jawab bersama yang harus dicegah dengan membuat kebijakan dan budaya kesadaran keamanan informasi mulai dari tingkatan manajemen tertinggi hingga pegawai teknis (Effendi et al., 2020).

Dinas Komunikasi dan Informatika Kabupaten Sidoarjo merupakan salah satu instansi pemerintah yang ditujukan untuk melayani masyarakat dibidang informatika dan komunikasi. Dalam menjalankan tugasnya, DISKOMINFO Kabupaten Sidoarjo sudah menggunakan *e-government* guna untuk pemanfaatan teknologi informasi dalam mencapai pelayanan publik yang berkualitas. Adanya *e-*

government dapat membantu DISKOMINFO dalam menjalankan pelayanan yang optimal secara bersih, efektif, responsif, efisiensi, responsif, transparan, dan akuntabel (DISKOMINFO, 2021).

Pelaksanaan *e-government* pada DISKOMINFO Kabupaten Sidoarjo dilakukan dengan menggunakan Sistem Pemerintahan Berbasis Elektronik (SPBE). Adanya SPBE diharapkan mampu memberikan manfaat bagi masyarakat antara lain dengan memperoleh dan memanfaatkan informasi dan pelayanan yang optimal, selain itu SPBE juga dapat membantu pemerintahan dalam implementasi *e-government*. Agar dapat menjalankan pelayanan masyarakat dengan baik maka DISKOMINFO Kabupaten Sidoarjo dituntut untuk ahli dalam SPBE (DISKOMINFO, 2021).

Sistem Pemerintahan Berbasis Elektronik (SPBE) dituliskan dalam Peraturan Presiden No. 95 tahun 2018 yang menjelaskan bahwa SPBE merupakan bentuk pemanfaatan teknologi informasi dan komunikasi dalam proses penyelenggaraan pemerintah. Terdapat enam ruang lingkup yang disebutkan meliputi 1) Tata Kelola SPBE, 2) Manajemen SPBE, 3) Audit Teknologi Informasi dan Komunikasi, 4) Penyelenggara SPBE, 5) Percepatan SPBE, 6) Pemantauan dan Evaluasi SPBE. Untuk mewujudkan agar penggunaan SPBE dapat digunakan aman, maka SPBE dibuat dan telah dilakukan standarisasi menggunakan ISO 27001. Terdapat beberapa cara untuk melakukan pengukuran kapabilitas keamanan teknologi informasi pada suatu instansi baik menggunakan COBIT 5, CMMI, *ITIL for information security*, dan Indeks KAMI (Effendi et al., 2020).

Berdasarkan hasil observasi lapangan, Dinas Komunikasi dan Informatika Kabupaten Sidoarjo melakukan evaluasi secara berkala tiap tahun pada Sistem

Manajemen Keamanan Informasi (SMKI) yang telah menerapkan ISO/IEC 27001:2013. Dinas Komunikasi dan Informatika Kabupaten Sidoarjo melakukan evaluasi dengan menggunakan kerangka kerja Indeks Keamanan Informasi (Indeks KAMI), namun terdapat permasalahan pada penerapan manajemen keamanan informasi masih belum optimal dan belum pernah dilakukan evaluasi dengan menggunakan kerangka kerja lainnya, adapun pertanyaan-pertanyaan yang diajukan terdapat pada lampiran 1. Indeks KAMI hanya digunakan untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi dan tidak dapat digunakan untuk melakukan analisis kelayakan atau efektivitas terhadap pengamanan yang ada (Wijatmoko, 2020). Untuk mewujudkan keamanan informasi yang optimal dan mendukung tujuan organisasi, evaluasi dengan menggunaan *framework* COBIT 5 dapat digunakan sebagai usulan rekomendasi perbaikan dan mengetahui kondisi manajemen keamanan informasi maupun penerapan SMKI dari sudut pandang yang berbeda. COBIT 5 menyediakan *base practices* yang mampu mendukung organisasi dalam meningkatkan penggunaan teknologi pada proses bisnis organisasi, menyediakan panduan manajemen untuk pengendalian tata kelola TI dalam mencapai tujuan organisasi (Mutia & Nur'ainy, 2020).

Control Objectives for Information and Related Technology (COBIT) adalah panduan yang digunakan untuk kerangka kerja bagaimana cara tata kelola teknologi informasi dengan cara menemukan dan bagaimana untuk menengahi gap antara kebutuhan dan proses pemenuhan kebutuhan dalam suatu organisasi (ITGID, 2016a). COBIT mampu menemukan isu-isu teknik dan kebutuhan kontrol, *framework* ini dirancang agar dapat menjadi alat dalam pemecahan suatu

permasalahan pada tata kelola teknologi informasi dengan memahami dan mengelola resiko maupun keuntungan terkait sumber daya informasi (Darwis et al., 2021). Pada umumnya COBIT 4.1 digunakan untuk melakukan pengukuran tingkat kematangan yang ditujukan untuk memetakan bagaimana dan sejauh apa kondisi pengendalian terhadap proses TI saat ini terhadap standar internasional yang ingin dicapai (Mukaromah, 2016). Pada COBIT 5 metode perhitungan telah berubah menjadi *Capability Level* atau tingkat kapabilitas (Syuhada, 2021). Pengukuran tingkat kapabilitas ditujukan untuk menyediakan informasi tentang kemampuan proses TI pada organisasi sebagai acuan untuk perbaikan berdasarkan kebutuhan organisasi (Mutia & Nur'ainy, 2020).

COBIT 5 memiliki kelebihan karena sudah banyak perusahaan maupun instansi yang menggunakannya, selain itu domain pada COBIT 5 lebih ringkas dibandingkan dengan COBIT 2019 yang memiliki domain proses lebih banyak yang akan mempersulit untuk diimplementasikan (Syuhada, 2021). Pada penelitian terhadulu yang membahas tentang evaluasi infrastruktur teknologi informasi dengan menggunakan COBIT 5 dan ITIL V3 (*Information Technology Infrastructure Library*) yang menjelaskan bahwa COBIT memberikan pedoman kepada manajer teknologi informasi dalam pengelolaan organisasi baik dari *executive summary, framework, control objectives, audit guidelines, implementation tool set*, dan *management guidelines*. COBIT dapat menyediakan proses apa saja yang perlu untuk dilakukan, sedangkan ITIL memberikan bagaimana panduan secara rinci bagaimana cara melakukannya. Oleh karena itu Penerapan COBIT juga dapat dapat dilakukan melalui pemanfaatan ITIL (Fryonanda et al., 2019). Adapun penelitian terdahulu yang membahas pembuatan

dokumen prosedur keamanan informasi berdasarkan COBIT 5 dan 27001 yang menjelaskan bahwa COBIT 5 mampu memberikan *control objective* yang menginterpretasikan rencana strategis dari teknologi informasi, informasi arsitektur, serta memenuhi kebutuhan teknologi informasi pada *hardware* maupun *software* dalam mengoperasikan proses dan layanan teknologi informasi yang berhubungan dengan kinerjanya. Sedangkan ISO 27001:2013 membahas tentang bagaimana pengadaan Sistem Manajemen Keamanan Informasi (SMKI). Pengendalian dan kontrol pada ISO 27001:2013 ditujukan untuk memenuhi syarat-syarat yang diketahui berdasarkan risiko yang ada (Regina Woda & Bisma, 2020).

COBIT 5 dirancang dengan mempertimbangkan *framework* lain dan mampu mengintegrasikan *framework,* standar, dan praktik sebagai satu kesatuan (ISACA, 2012a). COBIT 5 adalah alasan yang tepat dan sesuai digunakan pada DISKOMINFO untuk melakukan pengukuran kapabilitas pada manajemen keamanan informasi yang saat ini sudah menerapkan standar ISO 27001. COBIT 5 memiliki 5 domain yang berfungsi untuk menentukan keselarasan antara tujuan bisnis, nilai stakeholder yang berbeda, dan nilai teknologi informasi yang digunakan (Turang & Turang, 2020). Untuk mencapai tujuan TI terkait tentang *security of information, processing infrastructure and application*, terdapat beberapa proses yang dibutuhkan antara lain adalah EDM03 *Ensure Risk Optimisation*, APO12 *Manage Risk,* APO13 *Manage Security*, BAI06 *Manage Changes,* dan DSS05 *Manage Security Services* (ISACA, 2012a).

Adapun domain dan proses yang digunakan dalam pengukuran ini antara lain adalah APO13 dan DSS05. APO13 merupakan salah satu proses pada domain *Align, Plan, and Organize* pada COBIT 5 yang menjelaskan tentang definisi proses,

pengoperasian, dan pengendalian terhadap sistem yang diterapkan pada organisasi untuk mengelola keamanan (Megasyah & Arifnur, 2020). Sedangkan proses DSS05 dalam domain *Deliver, Service and Support* menyediakan pedoman manajemen keamanan informasi untuk melakukan analisis terhadap layanan keamanan yang ada (Isnaini & Suhartono, 2022). Kedua proses tersebut adalah proses utama dalam COBIT 5 yang memiliki fokus dalam penerapan manajemen keamanan informasi (Imany et al., 2019)(ISACA, 2013c). Adapun alasan proses EDM03 dan APO12 tidak digunakan karena kedua proses tersebut memiliki fokus utama dalam manajemen risiko yang mengacu pada COBIT 5 *for Risk* (ISACA, 2017)(Zakkadiaksa et al., 2020). Pendefinisikan ruang lingkup dan tujuan dalam melakukan audit dapat dilakukan dengan menentukan proses TI dengan risiko tertinggi (Sarno, 2009).

Dari penjelasan latar belakang yang telah diuraikan, penelitian ini dilakukan dengan menggunakan judul ”**Pengukuran Tingkat Kapabilitas Manajemen Kemanan Informasi Menggunakan COBIT 5 pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo**”. Untuk mencapai tujuan tersebut, acuan yang digunakan pada COBIT 5 adalah dengan menggunakan *Stakeholder Needs* bagian ke dua belas (12) yaitu “*Is the information I am processing well secured*?” yang merujuk tentang manajemen keamanan informasi.

1.2 Rumusan Masalah

Dari latar belakang yang telah dijabarkan, rumusan masalah dalam penyusunan skripsi adalah bagaimana tingkat kapabilitas Sistem Manajemen Keamanan Informasi (SMKI) Dinas Komunikasi dan Informatika Kabupaten Sidoarjo?

1.3 Batasan Masalah

Beberapa batasan masalah yang perlu diperhatikan dalam penelitian ini meliputi:

1. Pengukuran tingkat kapabilitas tata kelola keamanan informasi dilakukan pada *Data Center* Dinas Komunikasi dan Informatika Kabupaten Sidoarjo
2. Pengukuran tingkat kapabilitas dilakukan dengan menggunakan COBIT 5 pada Sistem Manajemen Keamanan Informasi (SMKI)
3. Pengukuran tingkat kapabilitas berfokus pada proses DSS05 Manage Security Service dan APO13 Manage Security pada COBIT 5
4. Pengukuran tingkat kapabilitas dilakukan dengan menggunakan prosedur *Assessment Process Activities* termasuk melakukan analisis kesenjangan dan penyusunan rekomendasi untuk saran perbaikan.

1.4 Tujuan

Tujuan yang ingin dicapai pada penelitian ini adalah memperoleh hasil pengukuran tingkat kapabilitas manajemen keamanan informasi pada Diskominfo Kab. Sidoarjo.

1.5 Manfaat

Sangat besar harapan untuk memberikan manfaat dengan dilakukannya penelitian ini. Berikut merupakan manfaat dari penelitian ini antara lain:

1. Dalam bidang pendidikan, penelitian ini diharapkan mampu memberikan pemahaman tentang bagaimana proses dalam melakukan pengukuran tingkat kapabilitas dengan menggunakan COBIT 5 yang terkait dengan permasalahan keamanan informasi serta menjadi referensi yang dapat digunakan untuk penelitian-penelitian selanjutnya.

2. Dinas Komunikasi dan Informatika Kabupaten Sidoarjo mampu memahami bagaimana gambaran kondisi tingkat kapabilitas keamanan informasi saat ini beserta perbandingan gap dengan kondisi yang ingin diraih. Hasil temuan usulan dan rekomendasi juga dapat digunakan sebagai referensi dalam melakukan evaluasi bagi instansi maupun pengembangan Sistem Manajemen Keamanan Informasi (SMKI).

1.6 Relevansi Audit SI / TI dengan Sistem Informasi

Audit teknologi dan sistem informasi adalah proses pengumpulan data serta evaluasi terhadap bukti temuan dengan tujuan untuk memastikan suatu sistem aplikasi komputerasi telah diterapkan dan telah melakukan sistem pengendalian baik meliputi efektivitas dan efisiensi penyelenggaraan informasi berbasis komputer, pengendalian internal, perlindungan terhadap aktivitas dan integritas data dan informasi (Turang et al., 2018). Pengukuran tingkat kapabilitas merupakan kegiatan yang dilakukan untuk melakukan evaluasi terhadap penerapan tata kelola dan manajemen teknologi informasi, tujuannya adalah untuk menyediakan informasi tentang bagaimana kondisi kemampuan proses teknologi informasi untuk memetakan pengembangan dan perbaikan berdasarkan kebutuhan organisasi (Mutia & Nur'ainy, 2020).

Sistem informasi merupakan gabungan dari perangkat keras, perangkat lunak, pengguna, dan prosedur yang dikelola secara integral sehingga data dapat diolah hingga menjadi informasi untuk memecahkan masalah dan pengambilan keputusan. Tujuan dilakukannya audit teknologi dan sistem informasi adalah mengamankan aset, menjaga integritas data, menjaga efektivitas sistem, dan mencapai efisiensi sumberdaya (Sarno, 2009). Adapun ruang lingkup disiplin ilmu

sistem informasi yang merupakan hasil pembahasan pertemuan Forum Pimpinan Prodi Sistem Informasi se-Indonesia pada 2 Juli 2018 yang didukung oleh AISINDO dan APTIKOM menjelaskan bahwa disiplin ilmu sistem informasi mempelajari tentang banyak macam aspek yang termasuk dalam perencanaan, perancangan, pembangunan, dan operasional sistem informasi, evaluasi atau audit sistem informasi, faktor-faktor yang mempengaruhi penerimaan SI atau TI oleh pengguna (*adoption/diffusion*), bagaimana SI atau TI digunakan oleh target pengguna (*domestication*), dan bagaimana pengaruh/dampak penggunaan suatu SI atau TI (*impacts/post adoption stage*) (AISINDO, 2018). Terkait evaluasi atau audit sistem informasi, COBIT 5 menyediakan kerangka komprehensif untuk membantu organisasi mencapai tujuannya, salah satunya dengan cara menyediakan pedoman dalam pengelolaan dari segi *framework*, *control objectives*, *audit guidelines*, *implementation tool set*, hingga *executive summary* (Fryonanda et al., 2019). Dari hal tersebut dapat disimpulkan bahwa audit teknologi dan sistem informasi menggunakan COBIT 5 dapat dikatakan relevan atau memiliki kaitan dengan ruang lingkup disiplin ilmu sistem informasi.

1.7 Sistematika Penulisan

Sistematika penyusunan laporan skripsi dibagi menjadi 5 (lima) bab meliputi:

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang bagaimana penulisan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan dalam penyusunan skripsi.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang profil instansi Dinas Komunikasi dan Informatika Kabupaten Sidoarjo, gagasan umum dan teori dasar yang digunakan dalam penyusunan skripsi ini serta penelitian-penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan tentang bagaimana urutan dan langkah-langkah dalam menjalankan penelitian ini yang sesuai dengan langkah *Assessment Process Activities* pada COBIT 5. Langkah ini akan digunakan sebagai pedoman untuk memperoleh hasil akhir penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan tentang bagaimana penjelasan tentang hasil dari tahapan-tahapan dilakukannya audit keamanan sistem informasi yang dimulai dari tahap *initiation, planning the assessment, briefing, data collection, data validation*, *process attribute level,* dan *reporting the result*. Bab ini juga menyediakan interpretasi hasil dari proses audit dan juga rekomendasi yang dapat diberikan kepada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo.

BAB V KESIMPULAN DAN SARAN

Pada bab ini menjelaskan tentang kesimpulan dari penjelasan pada bab-bab sebelumnya serta saran untuk peneliti selanjutnya dan saran yang dapat digunakan sebagai rekomendasi untuk pihak Dinas Komunikasi dan Informatika Kabupaten Sidoarjo untuk pengembangan yang lebih lanjut.

DAFTAR PUSTAKA

Pada bab ini berisi tentang rujukan yang digunakan dalam penyusunan skripsi ini. Literatur yang digunakan meliputi jurnal, buku, hingga situs pada internet.

LAMPIRAN

Pada bab ini menyajikan hasil dokumentasi yang berisi tentang dokumen ataupun informasi yang dapat mendukung penyusunan skripsi.