BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini penggunaan teknologi informasi merupakan kebutuhan primer yang tidak hanya selalu ada, melainkan hal yang harus diperhatikan dalam suatu organisasi. Penerimaan teknologi informasi dalam suatu organisasi dapat menjadi sarana yang akan membantu dalam menyaring sebuah informasi sebagai alat bantu untuk menjalankan proses bisnis organisasi. Informasi yang dihasilkan sebaiknya dapat dipercaya dan sesuai dengan keadaan yang sebenarnya. Karena informasi tersebut bisa dimanfaatkan sebagai kepentingan pribadi, bisnis, lingkup pemerintahan, sekaligus dapat digunakan sebagai bahan untuk mengambil keputusan (Riadi et al., 2018). Penyelesaian masalah dengan menggunakan teknologi informasi tersebut tidak menutup kemungkinan akan memunculkan berbagai risiko yang akan dijumpai. Dengan risiko yang muncul tersebut akan membuat kurang optimalnya proses kerja, penurunan kualitas hingga minimnya pencapaian tujuan organisasi (Setyaningrum et al., 2018). Untuk meminimalisir adanya potensi kerugian adalah dengan cara melihat dan mengelola ancaman risiko yang bisa terjadi kapan saja (Wibawa et al., 2020). Dengan perkembangan teknologi informasi, pemanfaatannya pun berkembang di instansi pemerintahan dengan guna untuk memaksimalkan pelayanan publik. Dinas Komunikasi dan Informatika Kabupaten Sumenep merupakan salah satu Satuan Kerja (SatKer) di lingkungan pemerintahan Kabupaten Sumenep yang memiliki tanggung jawab dalam pelaksanaan urusan pemerintahan di bidang informasi dan komunikasi publik, teknologi informatika serta statistik dan

persandian. Setiap proses bisnis yang dilakukan pada setiap bidang di Diskominfo Kabupaten Sumenep membutuhkan keamanan informasi, sehingga membutuhkan satu bidang yang memegang tanggungjawab dalam penyelenggaraan kebijakan atas keamanan informasi instansi dan pemerintah daerah yaitu oleh seksi persandian pada bidang statistik dan persandian. Bidang statistik dan persandian memiliki tugas yang terpisah dalam Diskominfo Kabupaten Sumenep. Hal ini sesuai dengan Peraturan Bupati Sumenep No. 98 Tahun 2021 tentang kedudukan, susunan organisasi, tugas & fungsi serta tata kerja Dinas Komunikasi dan Informatika Kabupaten Sumenep dan di undangkan dalam berita daerah Kabupaten Sumenep pada tanggal 17 Desember 2021 dimana sebelumnya berdiri dengan 2 bidang yang berbeda, yaitu untuk persandian menjadi satu di bidang teknologi dan persandian sedangkan untuk statistik berdiri di bidang statistika dan pemberdayaan TIK. Seksi persandian mempunyai tugas dalam melaksanakan pengelolaan proses pengamanan informasi pemerintah daerah, pengumpulan bahan dan menyusun peraturan teknis pengamanan komunikasi sandi, hingga mengelola informasi berklasifikasi melalui pengklasifikasian milik pemerintah daerah. Ini menyesuaikan dengan yang telah dijabarkan dalam peraturan tupoksi surat No. 98 tahun 2021.

Dalam pelaksanaan tugasnya seksi persandian melakukan proses bisnis untuk memberi perlindungan informasi melalui Penyediaan Perangkat Teknologi Keamanan Informasi dan Jaring Komunikasi Sandi (JKS) serta melaksanakan pengiriman, menyimpan, hingga menghancurkan informasi yang bersifat umum dan rahasia. Informasi yang diterima berupa surat masuk yang berasal dari pusat (Presiden, Kementerian, Kedutaan besar luar negeri, dan dinas terkait di Provinsi

Jawa Timur maupun luar provinsi yang kemudian akan di distribusikan menyesuaikan tembusan surat didalamnya (Bupati/wakil, Sekretaris Daerah, dinas dan kecamatan terkait di lingkungan Pemerintah Kabupaten Sumenep,dsb. Dari pelaksanaan tersebut selanjutnya akan disusun kebijakan teknis terkait keamanan informasi, terutama di lingkungan pemerintah daerah Kabupaten Sumenep. Dari rincian tersebut dapat dibuktikan jika seksi persandian membutuhkan kebutuhan informasi untuk memenuhi proses bisnisnya. Dengan tugas dan fungsi kerja yang dilaksanakan oleh seksi persandian tidak dapat dipungkiri jika terdapat berbagai risiko keamanan yang mungkin akan terjadi. Saat ini, Diskominfo Kabupaten Sumenep sudah menerapkan sistem keamanan informasi terkait pertukaran dokumen dan informasinya yaitu dengan melakukan pencadangan data yang akan diterima atau dikirim. Surat atau berita yang diterima oleh seksi persandian untuk pertukaran informasi atas dinas dilakukan melalui alamat *email* kab_sumenep@sarapati.net, pada *email* ini dokumen pengiriman data akan di enkripsi sebelum didistribusikan kepada dinas terkait. Jika informasi yang akan dikirimkan bersifat rahasia akan secara langsung dikirimkan kepada pihak terkait melalui aplikasi *Whatsapp* dengan catatan telah dilakukan proses enkripsi data didalamnya.

Berdasarkan hasil penemuan melalui wawancara dan *observasi*, terdapat beberapa dokumen yang belum dilengkapi guna mendukung pelaksanaan manajemen risiko, hal ini membuktikan jika dalam rangka memenuhi kebutuhan untuk memaksimalkan manajemen risiko keamanan informasi seksi persandian didapatkan suatu kendala. Sehingga perlu dilakukan pengukuran untuk meminimalisir potensi risiko terkait pengiriman dan pertukaran informasi

khususnya yang bersifat rahasia. Evaluasi terkait Diskominfo Kabupaten Sumenep juga dilaksanakan agar diketahui sejauh mana instansi menerapkan manajemen risiko keamanan informasinya (Riadi et al., 2019). Proses disampaikannya dokumen dan informasi dapat dijamin keamanannya hingga sampai kepada pihak terkait guna melakukan tindakan preventif terhadap kebocoran aset informasi sensitif yang diterima. Evaluasi terkait keseluruhan keamanan informasi Diskominfo Kabupaten Sumenep dilakukan dengan penilaian Indeks KAMI secara internal, tetapi belum pernah dilaksanakan secara resmi atau bersertifikasi dikarenakan terdapat kendala pada anggarannya dan penilaian Indeks KAMI yang dilaksanakan pada tahun 2022 berada pada kondisi baik. Dalam peningkatan sumber daya manusia sandi yang belum sesuai dengan kompetensinya, dilakukan pelatihan dan bimbingan teknis yang dilakukan oleh pemerintah pusat untuk mengembangkan kinerja dalam penerapan SDM persandian dan keamanan informasi.

Pengukuran khusus untuk seksi persandian terkait keamanan informasinya belum diterapkan dan tidak adanya *Computer Security Incident Team* (CSIRT) yang bertugas mencegah terjadinya kerentanan mitigasi ancaman dan risiko serangan *cyber* sehingga jika terdapat ancaman yang datang akan langsung dipantau oleh CSIRT pusat, namun dari pemerintah kabupaten memberikan pengarahan untuk dilakukannya pendataan manajemen risiko untuk setiap bidang dan seksi di instansi. Dalam pelaksanaan tugas kerjanya, seksi persandian yang memiliki fungsi untuk menyusun peraturan teknis operasional pengamanan komunikasi sandi yang dimana belum dilakukan evaluasi dan diberikan standar terkait keamanan informasinya sehingga dapat menimbulkan beberapa risiko

keamanan yang dapat terjadi seperti masalah terkait kehilangan atau kerusakan dalam penyimpanan data *online* yang masuk ke dalam sistem informasi pendataan internalnya yang disebabkan oleh peretasan pihak yang tidak dikenal maupun terjadinya hal yang menyebabkan aset informasi yang bersifat rahasia dapat tersebar ke lingkungan luar persandian. Dari uraian tersebut, dibutuhkan sebuah standar *base practice* yang perlu dilakukan dalam penerapan sebagai pedoman untuk melakukan pengukuran kapabilitas, hal ini bertujuan untuk memberikan analisis optimalisasi terkait manajemen risiko keamanan informasi serta dapat meminimalisasi potensi risiko dalam pengiriman dan pertukaran aset dan dokumen, terutama untuk penyampaian informasi yang bersifat rahasia atau sensitif sehingga dapat dilakukan pencegahan agar tidak terjadinya penyebaran informasi yang dapat menghambat proses bisnis kinerja seksi persandian Diskominfo Kabupaten Sumenep. Terdapat beberapa standarisasi yang dapat dilakukan dalam pengelolaan TI seperti COBIT, ITIL, ISO/IEC 270001 dan setiap standar tersebut dapat digunakan dan dikelola dalam berbagai kondisi tertentu (Mukaromah, et al., 2022). Dalam pengukuran tingkat kapabilitas yang diangkat pada studi kasus skripsi ini adalah dengan menggunakan COBIT 5 sebagai panduan kerangka kerjanya,

Information Technology Infrastructure Library (ITIL) merupakan alat tata kelola TI yang berstandarisasi internasional yang penerapannya dilakukan untuk mengelola pengukuran terhadap kebijakan terkait keamanan teknologi informasi (Herlinudinkhaji, 2019). ITIL berfokus pada pengevaluasian terhadap kebijakan dan manajemen yang berkaitan dengan layanan teknologi informasi. ISO/IEC 270001 menyediakan pedoman kerja yang berisi beberapa standar dalam fokus

area organisasi dalam mengakses data secara berkala, kerahasiaan dokumen, dan integritas informasi yang dimiliki (Putra et al., 2016). *Control Objective for Information and Related* Technology (COBIT) merupakan kerangka kerja yang dapat digunakan sebagai alat dalam dalam pengimplementasian tata kelola TI. COBIT berfokus pada pengukuran kematangan organisasi dalam hal penerapan TI (Mukaromah et al., 2015). Dari data yang telah diolah dari mesin pencarian di internet, didapatkan hasil penemuan jika penggunaan kerangka kerja TI terbanyak pada domain Indonesia dan Luar Negeri pada selang waktu tahun 2014-2018 pada artikel yang terpublikasi adalah COBIT (Rochmania et al., 2020). Sedangkan kerangka kerja ISO 270001 dan ITIL mendapatkan jumlah penemuan artikel paling sedikit. Dalam hal manajemen risiko, ISO 270001 memiliki keterbatasan dengan pelaksanaan kontrol dan pengurangan risiko dalam hal biaya IT dimana pembahasan masalahnya tidak dilakukan secara komprehensif dibandingkan dengan ITIL dan COBIT yang mengarahkan tentang penentuan biaya manajemen risiko dan sudut pandang keuangan IT (Wibowo et al., 2016). Kerangka kerja ITIL terfokus pada pelayanan pelanggan. Pengimplementasian COBIT merupakan yang paling terbaru dan di dalam kerangka kerjanya memberikan pemodelan penelitian alternatif (Hilmawan et al., 2015).

Berdasarkan uraian perbandingan penggunaan *framework* COBIT 5, ITIL, dan ISO 270001 diatas, dapat disimpulkan jika COBIT 5 merupakan kerangka kerja yang paling sesuai dengan studi kasus yang membahas terkait manajemen risiko keamanan informasi. COBIT 5 merupakan penggabungan beberapa pengetahuan sebelumnya yang menyebar di berbagai *framework* berbeda. Pada

kerangka kerja, COBIT 5 mengumpulkan beberapa pada aturan ISACA yakni COBIT 4.1,Val IT 2.0, Risk IT, dan BMIS dan menyelaraskan dengan *base practice* yang ada yaitu ITIL V3, TOGAF, dan ISO (ISACA 2012). Pada COBIT 5 berisi 5 domain dengan 37 proses, dimana diberikan batasan antara tata kelola TI dan manajemen IT (ISACA,2012), domain yang akan digunakan pada studi kasus ini yaitu *Evaluate, Direct and Monitor* (EDM) pada domain proses EDM03 (*Ensure Risk Optimisation*) dan *Align, Plan and Organize* (APO) pada domain proses APO12 (*Manage Risk*). Domain dan sub domain tersebut digunakan karena keduanya yang nantinya akan menganalisis mengenai manajemen risiko TI. Beberapa penelitian sebelumnya dengan permasalahan yang sama tentang manajemen risiko keamanan informasi, banyak yang menerapkan COBIT 5 sebagai acuan kerangka kerjanya. Berdasarkan penelitian pada tahun 2018, pengevaluasian terkait manajemen risiko teknologi informasi dilakukan oleh Riyan Abdul Aziz, dkk untuk mengukur dan mengetahui cara meminimalisir berbagai risiko dan mencegah adanya kesalahan pada PT Taspen. Fokus penelitian menggunakan domain proses EDM03 dan APO12 dari hasil penghitungan di dapatkan nilai kapabilitas berada pada level 1 yang dimana PT Taspen telah melakukan pengimplementasian terkait manajemen risiko namun belum dioptimalisasi. Pada tahun yang sama, Arief melakukan pengukuran terkait kapabilitas pada Perum Jasa Tirta I Malang dengan menggunakan domain proses EDM03 dan APO12. Dimana keduanya memperoleh nilai kapabilitas pada level 2, yaitu jika pengimplementasian telah dikelola dengan baik dan hasil pekerjaan tetap terpantau dan terkelola dengan tepat. Hasil gap yang telah dibentuk untuk masing-masing domain proses adalah sebesar 1. Penelitian ini merujuk pada salah

satu *Stakeholder Needs* dalam COBIT 5 *Goals Cascade* yakni *Risk Optimation* dan salah satu fokus area tata kelola TI yaitu *manage risk,* terfokus pada manajemen risiko keamanan informasi yang terarah pada pengiriman dan pertukaran informasi kepada pihak tertuju dalam lingkup Pemerintahan Kabupaten Sumenep. Judul skripsi yang diajukan adalah **"Pengukuran Tingkat Kapabilitas Manajemen Risiko Keamanan Informasi pada Seksi Persandian Menggunakan COBIT 5"**.

1.2 Rumusan Masalah

Berdasarkan uraian yang telah dipaparkan pada latar belakang, rumusan masalah yang menjadi inti utama dalam skripsi ini adalah bagaimana melakukan pengukuran tingkat kapabilitas manajemen risiko keamanan informasi pada seksi persandian Diskominfo Kabupaten Sumenep berdasarkan kerangka kerja COBIT 5.

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang perlu diperhatikan dalam penyusunan proposal skripsi ini, adalah:

1. Pengukuran tingkat kapabilitas terfokus pada domain proses EDM03 dan APO12.
2. Pengukuran tingkat kapabilitas tertuju pada Dinas Komunikasi dan Informatika Kabupaten Sumenep.
3. Pengukuran tingkat kapabilitas manajemen risiko merujuk pada kerangka kerja COBIT 5.

4. Pemberian rekomendasi perbaikan berdasarkan temuan proses dan aktivitas yang ditemukan.
5. Pengukuran gap digunakan untuk mengetahui kesenjangan antara level harapan dan level saat ini telah dicapai.

1.4 Tujuan

Berdasarkan uraian yang telah dipaparkan pada permasalahan, tujuan yang ingin dicapai dalam skripsi ini adalah dengan mengetahui hasil pengukuran tingkat kapabilitas seksi persandian Diskominfo Kabupaten Sumenep berdasarkan kerangka kerja COBIT 5.

1.5 Manfaat

Adapun beberapa manfaat yang diharapkan dari penelitian ini adalah:

1. Bagi Dinas Komunikasi dan informatika Kabupaten Sumenep diharapkan dapat digunakan untuk membantu mengetahui tingkat kapabilitas dari manajemen risiko keamanan informasi pada seksi persandian hingga kemudian dapat mengetahui gap yang diinginkan dan kondisi saat ini. Serta memberikan rekomendasi perbaikan yang dapat menjadi parameter sebagai peningkatan dan pengelolaan kinerjanya.

2. Bagi akademis diharapkan dapat dijadikan sebagai referensi selanjutnya terkait pengukuran menggunakan COBIT 5 sekaligus dapat digunakan sebagai tambahan ilmu pengetahuan khususnya pada Program Studi Sistem Informasi UPN “Veteran” Jawa Timur.

1.6 Relevansi Audit Sistem Informasi dengan Sistem Informasi

Tata kelola teknologi informasi merupakan bagian penting yang tidak dapat dipisahkan bagi sebuah organisasi. Dengan memanfaatkan TI dapat mencapai tujuan suatu organisasi. Tata kelola TI memiliki peran dalam pengintegrasian serta optimalisasi metode untuk merencanakan, mengorganisasikan, melaksanakan akuisisi dan implementasi, *delivery* dan *support*, serta pengawasan dan evaluasi kinerja TI.

Untuk menjamin tata kelola TI yang baik perlu dilakukan audit atau evaluasi yang berfungsi untuk menganalisis kematangan dan kemampuan dari suatu teknologi informasi yang telah diterapkan oleh organisasi. Selain itu, relevansi audit sistem informasi dengan sistem informasi telah disepakati pada Forum Pimpinan Prodi Sistem Informasi se-Indonesia pada tahun 2018 yang menyatakan jika salah satu aspek disiplin ilmu Sistem Informasi adalah evaluasi/audit sistem informasi. Dimana audit sistem informasi menurut Ron Weber (1999) merupakan tahapan dalam pengumpulan dan penilaian beberapa bukti untuk menentukan apakah sistem dalam komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong capaian tujuan organisasi secara efektif, dan sumber daya digunakan secara efisien. Dengan demikian, audit sistem informasi merupakan suatu irisan dari disiplin ilmu Sistem Informasi.

Sedangkan COBIT 5 (*Control Objective for Informtion and Related Technology*) yang telah dibuat oleh ISACA merupakan suatu pedoman tata kelola TI atau dapat disebut sebagai alat pendukung yang dapat digunakan untuk menjembatani kesenjangan antara kebutuhan dalam suatu organisasi. Secara keseluruhan, COBIT 5 menyediakan kerangka kerja yang terstruktur dan

komprehensif dalam pengelolaan dan mengatur sistem informasi. Keterkaitan antara COBIT 5 dan sistem informasi terletak pada kemampuan untuk membantu organisasi dalam menyelaraskan TI dengan tujuan bisnis, membangun kontrol dan proses yang efektif, mengelola risiko, mengukur kinerja, dan mengintegrasikan standar lain yang relevan. Dengan mengadopsi COBIT 5, organisasi dapat meningkatkan nilai, keandalan, dan keamanan sistem informasi (ISACA,2012a).

1.7 Sistematika Penulisan

Penyusunan penelitian dalam proposal skripsi ini terbagi menjadi tiga bab dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan berisi latar belakang, rumusan masalah,batasan masalah,tujuan, manfaat,dan sistematika penulisan yang digunakan dan menjadi dasar dalam penelitian skripsi di Dinas Komunikasi dan Informatika Kabupaten Sumenep.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka akan menjelaskan profil singkat terkait Dinas Komunikasi dan Informatika Kabupaten Sumenep dan serta beberapa teori dasar yang diambil dan akan menjadi pedoman dalam pengerjaan skripsi. Dalam tinjauan pustaka dicantumkan pula terkait beberapa penelitian terdahulu sebagai alasan dalam pemilihan topik dan permasalahan yang akan diangkat dalam skripsi.

BAB III METODOLOGI PENELITIAN

Metodologi penelitian akan menjelaskan bagaimana langkah-langkah pengerjaan yang dibuat secara terstruktur serta metode yang akan digunakan untuk menyelesaikan masalah yang diangkat.

BAB IV HASIL DAN PEMBAHASAN

Hasil dan pembahasan akan menjelaskan secara rinci terkait hasil dari setiap langkah pada metodologi penelitian dan membahas secara sistematis pengukuran tingkat kapabilitas manajemen risiko keamanan informasi Seksi Persandian berdasarkan COBIT 5.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran berisi simpulan akhir dari hasil skripsi yang telah dilakukan dan saran untuk topik ke depan.

DAFTAR PUSTAKA

Bagian ini berisi daftar dari beberapa sumber literatur seperti jurnal, buku, dan situs web yang digunakan dalam pengerjaan skripsi.

LAMPIRAN

Dokumen atau gambar guna melengkapi isi skripsi.