

BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan TI (Teknologi Informasi) mengalami kemajuan yang sangat cepat di era globalisasi. Saat ini, teknologi informasi telah menjadi suatu kebutuhan mendasar bagi masyarakat maupun organisasi. Fungsinya tidak hanya sebagai alat komunikasi, namun juga sebagai sarana utama untuk mencari informasi dan menjalankan operasional organisasi guna meningkatkan efektivitas kinerja (Purba et al., 2018).

Pemanfaatan teknologi informasi sekarang menjadi bagian penting bagi banyak organisasi, termasuk lembaga pemerintah. Penerapan teknologi informasi di pemerintahan atau yang biasa disebut *e-government*, diharapkan bisa meningkatkan efisiensi, efektivitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan. Tujuan dari *e-government* di Indonesia dijelaskan dalam Inpres No. 3 Tahun 2003 yang bertujuan untuk memperbaiki penyelenggaraan pemerintahan dengan memanfaatkan teknologi informasi (Inpres, 2003). Hal tersebut dilakukan untuk meningkatkan efektivitas dan efisiensi layanan publik dengan merancang ulang sistem manajemen dan proses kerja di instansi pemerintah melalui pengembangan *e-government*. Instruksi Presiden ini menjadi landasan bagi implementasi kebijakan *e-government* di berbagai lembaga pemerintahan untuk mencapai tujuan tersebut (Setiawan & Mustofa, 2013).

Instruksi Presiden tersebut menjadi dasar bagi implementasi kebijakan *e-government* di berbagai lembaga pemerintahan. Lembaga XYZ merupakan salah satu yang turut berperan dalam implementasi ini, sebuah lembaga pemerintah non kementerian yang secara langsung bertanggung jawab kepada Presiden. Lembaga XYZ diharapkan dapat mengimplementasikan *e-government* dalam proses kerja di instansi pemerintah, sehingga layanan publik dapat ditingkatkan secara signifikan sesuai dengan arahan Inpres tersebut.

Dalam pemanfaatan teknologi informasi, keamanan informasi harus sangat diperhatikan. Keamanan informasi tidak hanya berperan dalam melindungi aset teknologi, tetapi juga informasi yang menjadi fondasi operasi setiap organisasi. Fokus utama dari keamanan informasi adalah menjaga integritas, kerahasiaan, dan ketersediaan data, dengan tujuan mengurangi risiko dalam aktivitas bisnis, memaksimalkan pengembalian investasi, memanfaatkan peluang bisnis, serta menjamin kelangsungan operasional perusahaan (Nisri, 2023). Manajemen keamanan informasi pada dasarnya bertujuan untuk melindungi data secara aman dan memastikan bahwa organisasi mematuhi peraturan, undang-undang, dan standar yang berlaku. Karakteristik khusus manajemen keamanan informasi dikenal sebagai 6P yaitu: *planning, policy, programs, protection, people, dan project management* (Whitman & Mattord, 2011).

Keamanan informasi merupakan aspek yang perlu didukung untuk memastikan bahwa informasi yang dimiliki aman, rahasia, akurat, dan tersedia. Adanya tata kelola organisasi bertujuan untuk mengurangi dan menghindari ancaman terhadap keamanan informasi. Keamanan informasi adalah bagian penting dari tata kelola organisasi. Jika keamanan informasi mengalami masalah, kinerja TI akan terganggu. Masalah ini berkaitan dengan kerahasiaan, integritas, dan ketersediaan (Utomo et al., 2012).

Sebagai lembaga pemerintahan dalam mengelola keamanan informasi harus juga memperhatikan peraturan yang ada. Seperti yang tercantum pada peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (BSSN, 2021). Oleh karena itu, organisasi perlu melakukan evaluasi terhadap implementasi teknologi informasi yang terkait dengan infrastruktur TI. Tujuan evaluasi ini adalah untuk menilai sejauh mana manajemen infrastruktur TI telah dilaksanakan secara efektif, sehingga keamanan informasi dapat dipertahankan dengan optimal (Saleh et al., 2021).

Keselarasan antara tujuan organisasi dan penerapan teknologi informasi menentukan keberhasilan tata kelola TI. Dalam strategi pengembangan dan

peningkatan kinerja organisasi, teknologi informasi sangat penting. Untuk menghadapi perkembangan teknologi yang cepat, perlu membuat keputusan tentang teknologi informasi dengan cepat dan tepat (Setiawan & Mustofa, 2013).

Salah satu hal terpenting dari penerapan manajemen perusahaan yang baik adalah tata kelola TI. Tata kelola TI memastikan pengukuran efisiensi dan efektivitas peningkatan proses bisnis perusahaan dengan menggunakan struktur terkait teknologi informasi untuk mencapai tujuan strategis perusahaan (Gondodiyoto, 2007). Tata kelola TI yang efektif tentunya diperlukan agar pemanfaatan TI berjalan dengan baik. Kesesuaian antara penerapan TI dan tujuan organisasi sangat menentukan keberhasilan tata kelola TI. Teknologi Informasi telah menjadi komponen penting dalam strategi pengembangan dan peningkatan kinerja perusahaan. Keputusan TI harus dibuat dengan cepat mengingat perkembangan teknologi yang cepat. Evolusi lingkungan TI saat ini adalah proses adaptasi alami terhadap lingkungan bisnisnya (Setiawan & Mustofa, 2013).

COBIT 2019 adalah kerangka kerja untuk tata kelola dan pengelolaan teknologi informasi yang mendefinisikan komponen yang diperlukan untuk membangun dan menjalankan sistem tata kelola teknologi informasi, yang mencakup proses, struktur organisasi, kebijakan dan prosedur, arus informasi, budaya dan perilaku, keterampilan, dan infrastruktur. Prinsip-prinsip utama kerangka kerja COBIT 2019 adalah prinsip-prinsip yang menggambarkan persyaratan utama untuk sistem tata kelola teknologi informasi, serta bertujuan untuk menyempurnakan efektivitas, efisiensi, keamanan, dan ketaatan dalam pengelolaan teknologi informasi dalam suatu organisasi (Saleh et al., 2021). COBIT 2019 merupakan referensi terbaik untuk praktik pengelolaan teknologi informasi, khususnya dalam hal keamanan informasi. Ini karena memiliki bagian khusus yang membahas masalah tertentu selama pengimplementasiannya. Fokus area keamanan informasi adalah salah satu contohnya (Panjaitan & Abdurrahman, 2021).

Dalam implementasi *e-government* di Lembaga XYZ, terdapat kompleksitas terkait keamanan informasi. Tantangan utama mencakup bagaimana mengintegrasikan sistem yang ada dengan teknologi baru sambil memastikan bahwa kerahasiaan, integritas, dan ketersediaan data tetap terjaga. Selain itu, tidak

adanya pedoman kebijakan keamanan informasi yang komprehensif dan menyeluruh menjadi masalah tersendiri. Kompleksitas ini semakin meningkat dengan adanya ancaman siber yang semakin canggih dan regulasi yang ketat. Lembaga XYZ harus mengatasi berbagai ancaman keamanan, termasuk serangan siber, kebocoran data, dan ketidakpatuhan terhadap peraturan.

Kompleksitas yang ada pada Lembaga XYZ dapat ditangani dengan menerapkan kerangka kerja COBIT 2019, terutama pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*). APO13 berfokus pada pengelolaan keamanan secara menyeluruh dengan menetapkan kebijakan keamanan, memastikan kepatuhan, dan mengelola risiko keamanan. DSS05, di sisi lain, berfokus pada layanan keamanan yang dikelola, termasuk pemantauan dan deteksi ancaman, serta respons terhadap insiden keamanan. Dengan menggunakan COBIT 2019, Lembaga XYZ dapat mengidentifikasi dan mengevaluasi risiko keamanan, mengembangkan kebijakan yang sesuai, dan memastikan bahwa langkah-langkah keamanan yang diperlukan diterapkan secara efektif.

Implementasi COBIT 2019 dalam aspek keamanan informasi memungkinkan Lembaga XYZ untuk meningkatkan tata kelola TI dan memastikan bahwa keamanan informasi dikelola dengan baik. Ini akan membantu Lembaga XYZ dalam menghadapi tantangan kompleksitas keamanan informasi dan mencapai resolusi yang efektif, sehingga mendukung tujuan *e-government* yang diamanatkan oleh Inpres No. 3 Tahun 2003. Dengan demikian, Lembaga XYZ dapat meningkatkan efisiensi, efektivitas, dan keandalan layanan publik yang diberikan, sekaligus memastikan bahwa data dan informasi yang dikelola tetap aman dan terlindungi.

I.2 Perumusan masalah

Rumusan masalah yang mendasari penelitian ini adalah:

1. Bagaimana hasil analisis kapabilitas tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*)?

2. Bagaimana kondisi tata kelola TI saat ini di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*)?
3. Bagaimana rekomendasi untuk meningkatkan tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*)?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan penelitian ini adalah sebagai berikut:

1. Mengetahui hasil analisis kapabilitas tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*).
2. Mengetahui kondisi tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*).
3. Mengetahui hasil rekomendasi untuk meningkatkan tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*).

I.4 Batasan Penelitian

Berikut merupakan batasan masalah dari penelitian ini:

1. Penelitian ini berfokus pada penilaian kapabilitas dan kesenjangan dari tata kelola TI di Lembaga XYZ berdasarkan *framework* COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*) untuk menilai kemampuan manajemen keamanan informasi di Lembaga XYZ.
2. Penelitian yang dilakukan hanya sampai fase keempat yaitu *Build Improvement*. Tahap penyusunan rekomendasi solusi.

I.5 Manfaat Penelitian

Berdasarkan tujuan yang ingin penulis capai, penelitian ini diharapkan memiliki manfaat sebagai berikut:

1. Bagi Lembaga XYZ, penelitian ini diharapkan dapat memberikan gambaran mengenai tata kelola TI yang baik dan mendapatkan rekomendasi solusi untuk membantu meningkatkan agar menjadi lebih baik.
2. Bagi peneliti, memberikan pengembangan pengetahuan terkait tata kelola TI yang baik dan pemahaman dari hasil analisis yang sudah dilakukan.
3. Menjadikan referensi kedepan untuk penelitian yang mengambil bidang tata kelola teknologi informasi menggunakan *framework* COBIT 2019.

I.6 Sistematika Penulisan

Penelitian ini dijabarkan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini menguraikan latar belakang yang mendasari dilakukannya penelitian ini. Di dalamnya juga dipaparkan perumusan masalah, tujuan penelitian, serta manfaat yang diharapkan dari penelitian ini. Selain itu, bab ini juga menjelaskan batasan masalah penelitian dan sistematika pembahasan yang akan digunakan dalam laporan.

Bab II Tinjauan Pustaka

Bab ini menyajikan literatur yang relevan dengan permasalahan yang menjadi fokus penelitian. Berbagai teori dan konsep yang berkaitan dengan topik penelitian dibahas secara mendalam untuk memberikan landasan teoritis yang kuat. Hasil-hasil penelitian terdahulu juga diulas untuk memberikan konteks dan pemahaman yang lebih komprehensif terhadap topik yang diteliti.

Bab III Metodologi Penelitian

Dalam bab ini, metode dan langkah-langkah yang digunakan dalam penelitian dijelaskan secara rinci. Pendekatan penelitian, teknik pengumpulan data, dan metode analisis yang digunakan diuraikan dengan jelas. Bab ini juga menjelaskan alasan pemilihan metode tersebut dan bagaimana metode tersebut akan diterapkan dalam konteks penelitian ini.

Bab IV Analisis Data

Bab ini menyajikan hasil analisis data yang diperoleh dari penelitian yang telah dilakukan. Proses pengolahan data dan interpretasi temuan diuraikan secara

sistematis dan mendalam. Pembahasan temuan dikaitkan dengan permasalahan yang diteliti, memberikan wawasan baru dan menjawab pertanyaan penelitian yang telah dirumuskan.

Bab V Rekomendasi dan Perancangan

Berdasarkan hasil analisis data, bab ini menyajikan rekomendasi yang diberikan untuk mengatasi permasalahan yang diteliti. Perancangan solusi yang diusulkan dijelaskan secara rinci, termasuk langkah-langkah implementasi dan potensi dampaknya. Bab ini juga membahas bagaimana rekomendasi dan perancangan tersebut dapat berkontribusi pada perbaikan situasi yang diteliti.

Bab VI Kesimpulan dan Saran

Bab ini merangkum hasil penelitian dan menyajikan kesimpulan yang ditarik dari keseluruhan proses penelitian. Saran-saran untuk penelitian selanjutnya diuraikan untuk memberikan arah bagi pengembangan topik ini di masa depan. Bab ini juga memberikan rekomendasi praktis untuk perbaikan dalam implementasi hasil penelitian, menekankan pentingnya penelitian ini dalam konteks yang lebih luas.