

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi di Indonesia berkembang dengan cepat dan terus meningkat, menjadikannya salah satu fokus utama masyarakat, terutama di era industri 4.0. Inovasi teknologi ini semakin maju dan bergerak ke arah digital, yang bertujuan untuk mempermudah berbagai aktivitas agar lebih efektif dan efisien [1]. Penggunaan teknologi informasi tidak hanya terbatas pada sektor swasta, melainkan juga telah merasuki berbagai aspek pemerintahan [2]. Dengan kehadiran teknologi informasi saat ini, dapat membantu banyak organisasi termasuk instansi pemerintahan dalam menjalankan proses bisnis mereka. Maka dari itu, pengelolaan teknologi informasi yang baik dapat memberikan efektivitas, efisiensi, pengambilan keputusan dan mengelola pekerjaan dengan baik [1].

Dengan adanya manajemen risiko, suatu instansi atau dapat mengurangi risiko yang berpotensi merugikan besar. Di sebuah instansi pemerintahan, banyak dokumen kritis yang harus disimpan dalam sistem dan diambil kembali secara rutin untuk memastikan keamanannya dan mencegah kerusakan atau kehilangan data [4]. Instansi harus menghadapi sejumlah ancaman yang semakin meningkat, seperti serangan siber, penyalahgunaan hak akses, kesalahan oleh para pegawai dan kesalahan yang di akibatkan oleh bencana yang dapat memengaruhi efisiensi dan kelangsungan hidup organisasi. Hal ini mengharuskan suatu instansi memberikan perhatian yang lebih terhadap masalah manajemen risiko operasional, khususnya dalam konteks teknologi informasi. Manajemen risiko dalam organisasi teknologi informasi terus mengalami perkembangan seiring dengan berjalannya waktu [5]. Penggunaan teknologi informasi oleh Diskominfo Kota XYZ tidak terlepas dari risiko-risiko tertentu yang perlu dikelola secara cermat. Risiko-risiko tersebut dapat timbul dari berbagai faktor, mulai dari kesalahan manusia hingga potensi serangan siber atau kegagalan sistem [3]. Oleh karena itu,

manajemen risiko teknologi informasi menjadi esensial bagi Diskominfo Kota XYZ. Proses manajemen risiko teknologi informasi diartikan sebagai suatu pendekatan sistematis untuk mengidentifikasi, menilai, dan mengelola risiko-risiko teknologi informasi yang dapat mempengaruhi pencapaian tujuan organisasi [5].

ISO 31000:2018 hadir sebagai standar internasional yang memberikan kerangka kerja untuk manajemen risiko. Sebelum menetapkan ISO 31000:2018 sebagai kerangka kerja, dilakukan evaluasi terhadap berbagai standar dan metode yang tersedia, serta mengulas kelebihan dan kelemahan masing-masing. Penelitian ini difokuskan pada Diskominfo Kota XYZ Bidang Infrastruktur Teknologi Informasi dan Komunikasi. Dalam melaksanakan tugasnya, Bidang Infrastruktur Teknologi Informasi dan Komunikasi didukung oleh aset teknologi informasi yang memiliki peran penting untuk segala kelancaran pekerjaan pada bidang ini. Dari hasil wawancara yang dilakukan dengan salah satu staf Diskominfo Kota XYZ, pernah terjadi ancaman dan insiden yaitu serangan *Web Defacement* oleh situs judi online, tidak hanya itu serangan umum yang sering terjadi pada instansi seperti kesalahan manusia, gangguan operasional, hilangnya data perusahaan ataupun ancaman-ancaman lain yang dapat mengganggu keberlangsungan pada keamanan suatu instansi. Diskominfo Kota XYZ belum pernah melakukan *IT risk assessment* yang sistematis dan struktural dalam manajemen risiko menggunakan ISO 31000:2018 akibatnya, ancaman risiko yang sudah terjadi atau yang mungkin terjadi tidak dapat diidentifikasi dan diantisipasi secara efektif berdasarkan ISO 31000:2018.

Oleh karena itu, dengan melakukan penelitian ini mampu menganalisis manajemen risiko teknologi informasi yang diimplementasikan oleh Diskominfo Kota XYZ Bidang Infrastruktur Teknologi Informasi dan Komunikasi menggunakan kerangka kerja ISO 31000:2018. Dengan harapan mampu memberikan gambaran tentang efektivitasnya, mengantisipasi ancaman risiko yang mungkin terjadi, memberikan solusi terukur dan efektif dalam mengelola risiko-risiko teknologi informasi yang dihadapi oleh

Diskominfo Kota XYZ Bidang Infrastruktur Teknologi Informasi dan Komunikasi, serta dapat meningkatkan kesadaran dan kemampuan staff dalam menghadapi risiko yang terkait dengan teknologi informasi.

1.2 Rumusan Masalah

1. Bagaimana proses kerangka kerja manajemen risiko TI yang dilakukan oleh Diskominfo Kota XYZ pada Bidang Infrastruktur Teknologi Informasi dan Komunikasi?
2. Bagaimana hasil rekomendasi yang dapat diberikan kepada Diskominfo Kota XYZ Bidang Infrastruktur Teknologi Informasi dan Komunikasi untuk meningkatkan efektivitas manajemen risiko TI?

1.3 Tujuan

1. Mengidentifikasi, menganalisis dan mengevaluasi secara komprehensif proses manajemen risiko TI yang tengah diimplementasikan oleh Diskominfo Kota XYZ pada Bidang Infrastruktur Teknologi Informasi dan Komunikasi.
2. Memberikan masukan dan rekomendasi konkret kepada Diskominfo Kota XYZ Bidang Infrastruktur Teknologi Informasi dan Komunikasi sebagai langkah-langkah perbaikan dan peningkatan efektivitas manajemen risiko TI, berdasarkan hasil evaluasi menggunakan kerangka kerja ISO 31000:2018 dan ISO 27002:2022.

1.4 Batasan Masalah

1. Berfokus pada Bidang Infrastruktur Teknologi Informasi dan Komunikasi Diskominfo Kota XYZ.
2. Analisis risiko dilakukan pada aset teknologi informasi seperti infrastruktur, dan aplikasi yang digunakan oleh di Bidang Infrastruktur Teknologi Informasi dan Komunikasi Diskominfo Kota XYZ.
3. Penelitian ini menggunakan kerangka kerja ISO 31000:2018 dan ISO 27002:2022.