BAB I
PENDAHULUAN

Bab ini merupakan bagian awal dari laporan yang memberikan gambaran umum mengenai penelitian yang dilakukan. Bab ini terdiri dari beberapa sub bab, yaitu latar belakang yang menjelaskan konteks dan alasan penelitian, rumusan masalah yang merinci pertanyaan utama yang ingin dijawab, tujuan penelitian yang menjabarkan sasaran yang ingin dicapai, serta sistematika penulisan yang menggambarkan struktur keseluruhan laporan. Penjelasan mengenai setiap sub bab dalam bab pendahuluan akan diuraikan secara rinci pada bagian berikut ini.

I.1 Latar Belakang

Teknologi digital di Indonesia berkembang pesat pada beberapa tahun terakhir. Teknologi digital berpengaruh sebesar 89% pada kinerja sebuah negara dalam memenuhi target *Sustainable Development Goals* (SDGs) (Mahardhika & Aris, 2019). Perusahaan yang sedang menjalankan aktivitas bisnis, memerlukan suatu sistem yang dapat mendukung pada setiap komponen dan kinerja perusahaan (Margaretha & Nababan, 2020). Teknologi informasi merupakan sebuah inovasi yang berupa artefak, teknik, dan pengetahuan yang dapat memecahkan masalah manusia (Ivander & Papilaya, 2023). Penerapan teknologi informasi di suatu perusahaan, terutama Badan Usaha Milik Negara (BUMN), adalah aspek yang krusial dan merupakan bagian integral dari proses bisnis (Miftakhatun, 2020).

Di Indonesia, perhatian terhadap masalah *cybercrime* telah meningkat dengan baik oleh masyarakat maupun pemerintah (Nyoman & Nuarta, 2023). Dalam kurung waktu 2 tahun terakhir, Indonesia telah mengalami beberapa kasus kejahatan *cyber* yang mengguncang masyarakat, dimulai pada tahun 2020 dengan kasus Tokopedia yang mengalami pencurian data secara masif, dengan kurang lebih 91 juta data pribadi dijual oleh penjahat *cyber* di situs pasar gelap (Anantaka et al., 2023). Menurut Khasanah & Sutabri (2023), berbagai macam kejahatan *cybercrime* diantaranya adalah penjiplakan situs, *cyber espionage*, *cyber terrorism*, kejahatan konten *illegal*, data *forgery*, OTP *Fraud*, kejahatan *skimming*, peretasan *email* serta situs, SIM *swap*, penipuan online, serangan *ransomware*, kejahatan *carding*, dan kejahatan *phising*. Serangan *ransomware* yang menimpa Pusat Data Nasional Sementara (PDNS) pada 20 Juni 2024, yang menyebabkan gangguan pada berbagai

layanan publik, termasuk layanan imigrasi. Badan Siber dan Sandi Negara (BSSN) mengidentifikasi serangan ini sebagai *ransomware Brain Cipher*, versi terbaru dari *Lockbit 3.0*, yang memanfaatkan kelemahan dalam sistem keamanan. Insiden ini menunjukkan pentingnya langkah mitigasi dan manajemen risiko dalam menjaga keamanan infrastruktur kritis seperti PDNS (Kominfo, 2024).

PT XYZ telah membuat aplikasi berbasis *website* pada tahun 2018 dan mulai penggunaannya dalam proses Manajemen Risiko sejak tahun 2019. Penggunaan teknologi dalam pengelolaan risiko ini sejalan dengan Peraturan Menteri Badan Usaha Milik Negara Nomor Republik Indonesia Nomor PER-2/MBU/03/2023 Tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara. (Pura, 2018).

Dalam upaya peningkatan yang lebih baik dalam aset teknologi informasi, sangat penting untuk diingat bahwa selalu ada potensi risiko yang dapat menghadirkan ancaman dan menghambat pencapaian tujuan perusahaan (Hutabarat & Manuputty, 2020). Dari kejadian sebelumnya diharapkan dapat mengidentifikasi risiko-risiko lainnya yang dapat terjadi dimasa mendatang. Penanganan masalah *cybercrime* dilakukan melalui undang-undang yang terkait dengan kemungkinan risiko *cybercrime* pada penelitian ini.

PT XYZ merupakan perusahaan jasa yang beroperasi dalam pengelolaan manajemen pada bidang transportasi yang tersebar di berbagai wilayah Indonesia, seperti pada daerah Surabaya. Dalam menjalankan proses bisnisnya, PT XYZ telah menerapkan teknologi informasi berupa *website*. Menurut Hendrawati et al., (2021), *website* merupakan suatu sistem internet yang memberikan peluang kepada siapa pun untuk menyediakan informasi yang dapat diakses kapan saja selama 24 jam dan dikelola oleh mesin.

Pada penelitian ini mengambil objek amatan *website*. *Website risk management* sebagai platform utama dalam manajemen risiko perusahaan, memfasilitasi pengumpulan, pemantauan, dan analisis data risiko dari setiap divisi serta digunakan oleh berbagai pemangku kepentingan seperti, Manajer dan General Manajer. Mengingat pentingnya peran *website* dalam memfasilitasi pengumpulan, pemantauan, dan analisis data risiko, penelitian ini menganalisis risiko dari hasil penetrasi untuk melindungi dari celah serangan *cyber* terutama yang ada pada

website. Dampak adanya celah ancaman ini dapat menghambat proses bisnis dengan mengganggu mitigasi risiko seperti kendali internal yang telah berjalan.

Permasalahan penelitian sebelumnya menunjukkan bahwa risiko dalam Teknologi Informasi dapat muncul pada berbagai tahapan, mulai dari perencanaan, pelaksanaan, hingga evaluasi Teknologi Informasi dalam proses bisnis. Berdasarkan temuan lapangan di PT XYZ, perusahaan ini belum memiliki manajemen risiko yang memadai dalam menghadapi tantangan tersebut (Pratama et al., 2019). Selain itu, terdapat kekurangan dalam kebijakan autentikasi dan otorisasi yang berkaitan dengan keamanan informasi. Hal ini menjadi kendala bagi pengguna yang memiliki hak akses terhadap informasi penting terkait penentuan kualitas, perencanaan, pengendalian, dan evaluasi proses bisnis utama. Akibatnya, ketika terjadi kehilangan atau kesalahan informasi, proses bisnis dapat terganggu, dan manajemen kesulitan menelusuri sumber kesalahan yang terjadi (Nizar et al., 2021).

PT XYZ telah menerapkan *framework* ISO 31000:2018 untuk mengidentifikasi risiko yang terdapat pada proses bisnis dan perencanaan perusahaan. Penelitian ini bertujuan untuk memahami pentingnya menjaga keamanan dan kinerja *website risk management* PT XYZ.

Tabel I. 1 Hasil Tingkat Kematangan Risiko Tahun 2017-2022 (Pura, 2018)

No.	Tahun	Nilai Maturitas	Predikat
1	2017	3,12	*Progresif*
2	2019	3,37	*Progresif*
3	2020	3,58	*Progresif*
4	2021	3,60	*Progresif*
5	2022	3,31	*Managed*

Untuk meningkatkan nilai maturitas seperti Tabel I.1 diharapkan tidak terjadi risiko yang fatal pada *website risk management* PT XYZ demi keberlangsungan proses bisnis perusahaan. Maturitas sendiri berarti kematangan atau tingkat kematangan. Semakin tinggi nilai maturitas, maka semakin baik kualitas pengelolaan sistem manajemen risiko. Sebaliknya, semakin rendah nilai maturitas, maka proses manajemen risiko belum berkembang secara optimal dan memerlukan perbaikan serta peningkatan yang lebih lanjut. Untuk menaikan nilai

maturitas diperlukannya kelancaran dalam pengunaan *website risk management* PT XYZ sebagai pengumpulan data risiko pada setiap divisi.

Dalam melakukan analisis teknologi informasi dibutuhkan *framework* yang tepat agar dapat menjadi perbaikan atau pencegahan pada langkah mitigasi risiko yang lebih baik. Pada penelitian ini *framework* yang akan digunakan untuk menganalisis risiko adalah ISO (*International Organization for Standardization*) khususnya menggunakan ISO 31000:2018 untuk manajemen risiko. *Framework* ISO 31000:2018 digunakan untuk mengelola risiko dari tahap identifikasi, tahap analisis, tahap evaluasi, dan tahap perlakuan risiko. ISO 31000:2018 memungkinkan penerapan manajemen risiko untuk mencegah kemunculan risiko dan penanganannya secara efektif ketika risiko tersebut terjadi (Alfian et al., 2020).

Tujuan penelitian dapat mengidentifikasi dan menganalisis risiko pada *website risk management* PT XYZ menggunakan *framework* ISO 31000:2018. Adapun tujuan khusus yaitu dapat mengidentifikasi dampak risiko dan memberi rekomendasi atau langkah mitigasi risiko pada PT XYZ. Berdasarkan dari permasalahan yang telah dijelaskan maka sangat menarik untuk mengangkat penelitian dengan judul "Analisis Manajemen Risiko dengan *Framework* ISO 31000:2018 pada *Website Risk Management* PT XYZ".

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah "Bagaimana hasil analisis manajemen risiko pada *website risk management* PT XYZ dengan menggunakan *framework* ISO 31000:2018?"

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengidentifikasi dan menganalisis risiko pada *website risk management* PT XYZ menggunakan *framework* ISO 31000:2018. Adapun tujuan khusus yaitu dapat mengidentifikasi dampak risiko dan memberi rekomendasi atau langkah mitigasi risiko pada PT XYZ.

I.4 Kontribusi

Kontribusi yang diperoleh dari penelitian ini dalam hal analisis manajemen risiko pada *website risk management* adalah sebagai berikut :

1. Bagi Perusahaan (PT XYZ):

a. Hasil penelitian memberikan wawasan yang mendalam bagi perusahaan mengenai risiko-risiko yang dihadapi dan bagaimana menerapkan langkah-langkah mitigasi yang efektif. Ini akan membantu perusahaan meningkatkan keamanan *website* mereka dan melindungi data serta informasi penting.

2. Bagi Perguruan Tinggi:
   a. Penelitian ini menambah pengetahuan di bidang manajemen risiko dan penetrasi celah keamanan *website*, yang dapat dijadikan referensi bagi mahasiswa dalam studi terkait.
   b. Hasil penelitian dapat digunakan sebagai studi kasus dalam kurikulum, memberikan mahasiswa pemahaman praktis tentang penerapan teori manajemen risiko dalam dunia industri nyata.

I.5 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab I berisikan mengenai konteks permasalahan, latar belakang tugas akhir, perumusan masalah, tujuan tugas akhir, manfaat tugas akhir, serta sistematika penulisan.

Bab II Tinjauan Pustaka

Bab II berisi literatur yang relevan dengan permasalahan yang diteliti dan pembahasan hasil-hasil penelitian terdahulu. Pada bab ini menjelaskan kerangka kerja yang diperlukan pada penelitian ini. Pada akhir bab, analisis pemilihan kerangka kerja menjelaskan untuk menentukan permasalahan yang akan digunakan di penelitian ini.

Bab III Metodologi Penelitian

Metodologi penelitian merupakan strategi dan langkah-langkah yang dilakukan dalam penelitian untuk menjawab rumusan masalah yang telah ditentukan. Penyusunan metodologi penelitian harus dilakukan secara kritis untuk memastikan bahwa metode dan teknik yang dipilih tepat dan sesuai dengan tujuan penelitian. Pada bab ini, dijelaskan langkah-langkah

penelitian secara rinci, yang meliputi: tahap merumuskan masalah penelitian, menentukan metode penelitian yang sesuai, mengidentifikasi dan mendefinisikan variabel penelitian, menyusun desain penelitian, merancang instrumen pengumpulan data, melakukan pengumpulan data, melakukan analisis data, serta menguji validitas dan reliabilitas instrumen yang digunakan.

Bab IV Pengumpulan dan Pengolahan Data

Pada bab ini, disajikan hasil rancangan, temuan, analisis dan pengolahan data. Analisis sensitivitas juga dapat digunakan di bab ini untuk lebih mengetahui hasil penelitian dapat diterapkan baik secara khusus di konteks penelitian maupun secara umum di konteks serupa. Selain itu metode-metode evaluasi yang lain dapat diterapkan untuk memvalidasi hasil TA sesuai dengan kebutuhan.

Bab V Analisis dan Pembahasan

Pada bab ini, disajikan hasil dari analisis dan pembahasan yang meliputi temuan penelitian, pengolahan data, serta interpretasi hasil berdasarkan data yang telah diperoleh. Selain itu, bab ini juga membahas validasi atau verifikasi hasil penelitian, dengan tujuan untuk mengevaluasi apakah solusi yang diusulkan benar-benar mampu menyelesaikan masalah yang diidentifikasi atau setidaknya mengurangi kesenjangan antara kondisi eksisting dan target yang ingin dicapai.

Bab VI Kesimpulan dan Saran

Pada bab VI menjelaskan kesimpulan dari penelitian yang dilakukan serta jawaban dari pertanyaan penelitian yang disajikan di pendahuluan. Saran penelitian dikemukakan pada bab ini untuk penelitian selanjutnya.