BAB I
PENDAHULUAN

Dalam bab ini memberikan gambaran umum yang melatarbelakangi penelitian sehingga membantu pembaca memahami konteks dan topik pembahasan sesuai dengan judul penelitian. Masalah, tujuan, batasan dan manfaat yang akan diteliti akan menjadi fokus dalam kajian penelitian ini.

1.1. Latar Belakang

Peran Teknologi Informasi (TI) dalam memudahkan manusia untuk menyebarkan informasi dan mengolah data telah memasuki di segala bidang, dari kesehatan, pendidikan, ekonomi dan lain sebagainya (Agyztia Premana et al., 2020). Organisasi atau perusahaan akan menghasilkan teknologi informasi yang optimal jika mereka memaksimalkan pengelolaan dan pemanfaatan teknologi informasi dengan baik (Richardo & Sitokdana, 2021). Namun, semakin maju organisasi dalam mengadopsi teknologi informasi, semakin besar risiko teknologi informasi yang dapat mengancam pada sistem organisasi tersebut, sehingga perlu manajemen risiko yang tepat bagi sebuah perusahaan (Nikmat, 2024). Risiko merupakan keadaan yang mengakibatkan timbulnya bahaya dalam optimalisasi proses bisnis perusahaan. Sebagai bentuk pengendalian keadaan risiko yang ada, perlu adanya manajemen risiko teknologi informasi untuk meminimalisir kemungkinan dan dampak yang akan timbul (Andika & Wijaya, 2022).

Mengelola potensi risiko teknologi informasi (TI) di organisasi maupun instansi membuat aset TI lebih bermanfaat bagi suatu instansi sehingga instansi tersebut dapat meningkatkan proses operasionalnya (Kurniati et al., 2020). Manajemen risiko tidak terpaku paku satu sektor tertentu, tetapi juga diperlukan oleh organisasi yang beroperasi di berbagai bidang (Muhammad Asir et al., 2023), termasuk di sektor keamanan. Melalui penerapan manajemen risiko TI organisasi dapat memastikan bahwa semua proses dan sistem yang bergantung pada suatu teknologi informasi berjalan dengan aman dan tepat (Zagoto N. Sitokdana, 2021).

Sebagai bagian dari pemanfaatan teknologi informasi, Organisasi XYZ merupakan organisasi keamanan wilayah daerah Jawa Timur yang didalamnya terdapat unsur

badan pelaksana yaitu Departemen Informasi & Pengolahan Data sebagai kantor yang berperan dalam pengelolaan informasi dan data, hal ini dapat dibuktikan dengan adanya layanan yang bernama Smart Integrated Comand Center (SICC). layanan tersebut dirancang dalam pengumpulan, analisis serta informasi berbentuk dashboard sehingga dapat mempermudah aktivitas sumber daya manusia yang bertugas di instansi tersebut. Dalam penggunaanya, layanan SICC telah berjalan dari tahun 2019 akhir dan masih tergolong versi pertama dari layanan diluncurkan hingga saat ini. Pengembangan sistem tersebut ditujukan kepada personel lapangan di-wilayah Operasional Jawa Timur. Personel lapangan merupakan anggota yang berkaitan erat dengan suatu pembangunan diwilayah desa (Sembiring & Sembiring, 2024).

Layanan SICC dirancang untuk memfasilitasi pelaporan situasi dan kejadian di wilayah binaan personel lapangan, seperti bencana alam, stunting, personel lapangan sekolah, dapur bina desa dan lain sebagainya. Dalam implementasinya, proses bisnis layanan SICC dimulai dari personel lapangan sebagai pengguna yang melakukan input data secara langsung ke dalam layanan SICC. Data yang dilaporkan mencakup berbagai kondisi wilayah binaan. Setelah data dikirimkan, layanan SICC akan mengolah informasi tersebut dan menyajikannya dalam bentuk dashboard yang dapat diakses kembali oleh personel lapangan untuk memantau perkembangan di wilayahnya secara real-time. Data yang telah diinputkan oleh personel lapangan dipantau oleh Departemen Informasi & Pengolahan Data Organisasi XYZ selaku pengelola sistem untuk melakukan analisis informasi berbasis data dan pelaporan internal guna mendukung pengambilan keputusan di tingkat pimpinan pusat.

Departemen Informasi & Pengolahan Data Organisasi XYZ telah mengadopsi teknologi informasi dalam proses bisnis operasionalnya, namun implementasi tersebut tidak selalu berjalan lancar dan menghadirkan berbagai risiko operasional. Berdasarkan pemetaan risiko selama lima tahun terakhir, ditemukan sejumlah kendala yang menunjukkan bahwa penerapan teknologi informasi juga membawa potensi ancaman yang perlu dikelola secara sistematis. Hal tersebut selaras dengan peneltiian sebelumnya, yaitu penelitian yang mengangkat topik manajemen risiko

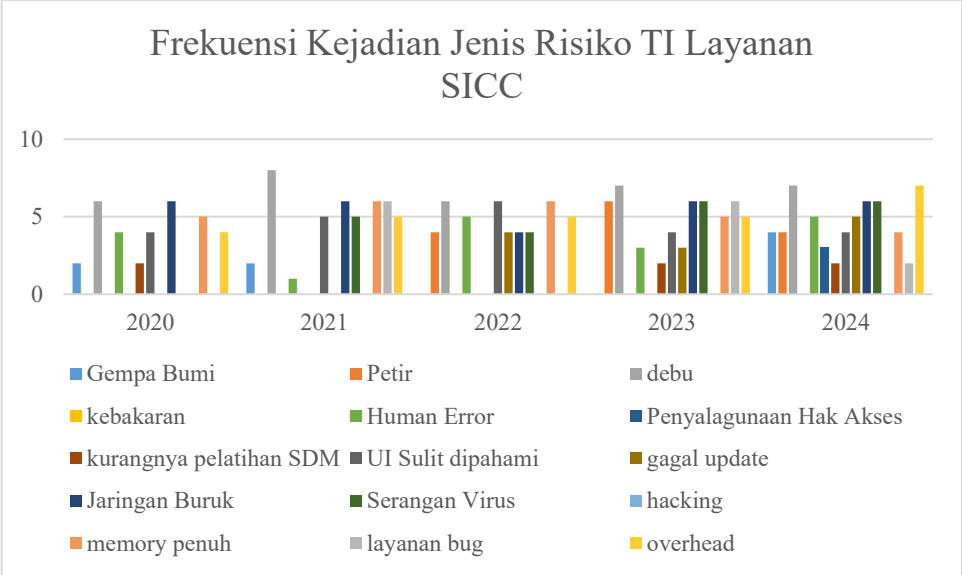
TI dengan judul “Analisis Manajemen Risiko TI pada Layanan E-SIM di Satlantas Polres XXX Menggunakan ISO 31000:2018” penelitian tersebut berfokus pada layanan E-SIM di Satlantas Polres XXX. Hasil dari penelitian tersebut ditemukan penilaian risiko berupa 2 risiko tingkat tinggi, 7 risiko tingkat sedang dan 14 risiko tingkat rendah. Sehingga hasil ISO 31000:2018 diharapkan membantu Polres XXX dalam mempertimbangkan standar tersebut sebagai identifikasi dan menilai risiko dalam membantu meningkatkan kualitas pelayanan pada Layanan E-SIM (M. W. Mubarok & Amelia, 2024). Namun, jarang ada penelitian serupa yang secara spesifik mengkaji penerapan manajemen risiko TI pada bidang keamanan, terutama di lingkungan Organisasi XYZ.

Penelitian ini melakukan pengelompokkan berdasarkan jenis risiko IT yang dihasilkan dari preliminary study melalui wawancara pada penerima dampak risiko yaitu personel lapangan menghasilkan beberapa jenis risiko TI yang muncul selama penggunaan layanan SICC yang dapat dilihat pada Tabel I. 1 dan grafik frekuensi yang menyertainya.

Tabel I. 1 Hasil *Preliminary Study* Frekuensi Kejadian Risiko TI Layanan SICC

Frekuensi Kejadian Risiko TI Layanan SICC <5 Tahun Terakhir					
Jenis Risiko	**Frekuensi Kejadian**				
	2020	**2021**	**2022**	**2023**	**2024**
Gempa Bumi	2	2	0	0	4
Petir	0	0	4	6	4
debu	6	8	6	7	7
kebakaran	0	0	0	0	0
Human Error	4	1	5	3	5
Penyalagunaan Hak Akses	0	0	0	0	3
kurangnya pelatihan SDM	2	0	0	2	2
UI Sulit dipahami	4	5	6	4	4
gagal update	0	0	4	3	5
Jaringan Buruk	6	6	4	6	6
Serangan Virus	0	5	4	6	6

Jenis Risiko	Frekuensi Kejadian				
	2020	2021	2022	2023	2024
hacking	0	0	0	0	0
memory penuh	5	6	6	5	4
layanan bug	0	6	0	6	2
overhead	4	5	5	5	7

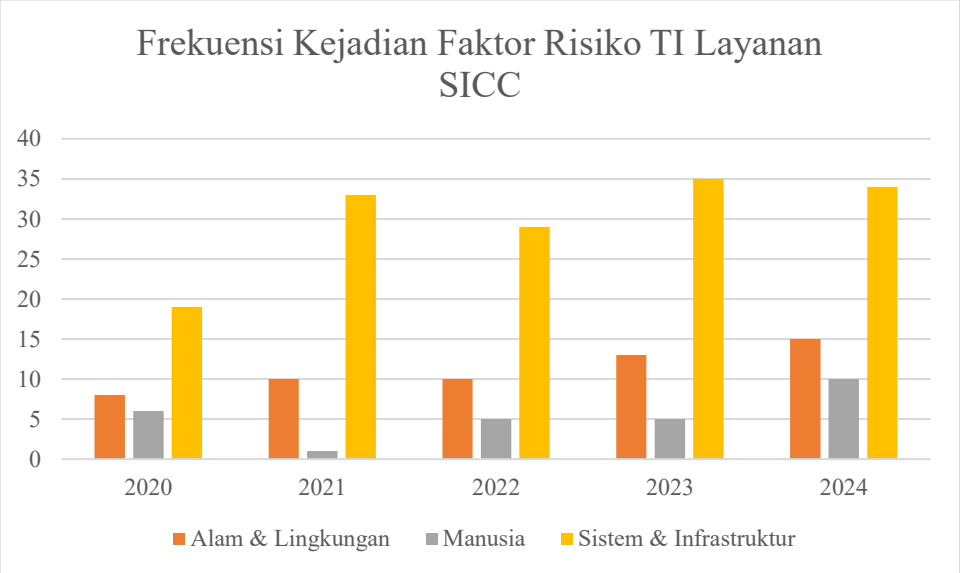


Gambar I. 1 Grafik Kejadian Risiko TI Layanan SICC

Berdasarkan tabel dan grafik frekuensi kejadian potensi risiko TI yang dihasilkan dari hasil observasi dan wawancara *preliminary study* ditemukan beberapa permasalahan yang kerap berdampak pada layanan SICC seperti debu, *human error*, terputusnya koneksi jaringan dan UI sulit dipahami oleh *user* serta jenis risiko TI lainnya. Untuk memberikan pemahaman yang lebih sistematis, seluruh jenis risiko TI kemudian dikelompokkan kedalam tiga kategori utama berdasarkan faktor risiko, yaitu alam dan lingkungan, risiko manusia, dan risiko sistem dan infrastruktur TI. Hasil pengelompokkan ini ditampilkan pada Tabel I. 2 dan grafik frekuensi yang menyertainya.

Tabel I. 2 Kejadian Risiko TI Berdasarkan Faktor Risiko

Frekuensi Kejadian Risiko TI Layanan SICC					
Faktor Risiko	**Jumlah Kejadian**				
	2020	**2021**	**2022**	**2023**	**2024**
Alam & Lingkungan	8	10	10	13	15
Manusia	6	1	5	5	10
Sistem & Infrastruktur	19	33	29	35	34



Gambar I. 2 Grafik Kejadian Risiko TI Berdasarkan Faktor Risiko

Hasil dari pengelompokkan ini bertujuan untuk melakukan pengerucutan terhadap jenis risiko TI. Dari hasil tersebut ditemukan bahwa jenis-jenis risiko TI yang terjadi dan memberikan dampak pada penggunaan layanan SICC memiliki kesesuaian dengan pendekatan ISO 31000:2018 dalam mengidentifikasi risiko berdasarkan konteks organisasi. Risiko-risiko tersebut tidak hanya bersifat teknis, tetapi melibatkan aspek manusia, lingkungan serta infrastruktur TI pendukung sistem. Serta hasil dari *preliminary study* yang dilakukan hanya menggunakan dua informan. Oleh karena itu, perlu adanya memperbarui dan mengukur ulang informasi dengan melibatkan beberapa informan tambahan melalui metode pengumpulan data berupa kuesioner. Sehingga, peneliti dapat memperoleh data yang lebih komprehensif dan mendukung validitas pengukuran risiko secara

keseluruhan di layanan SICC. Pendekatan ini akan memastikan bahwa analisis risiko lebih akurat dan mencerminkan berbagai perspektif yang ada.

Risiko pada masalah yang timbul di organisasi akan mempengaruhi juga pada kualitas dan kuantitas operasional suatu organisasi (Antoni & Prasetyo, 2023), sedangkan Organisasi XYZ sendiri belum ada tim khusus yang bertanggung jawab untuk mengelola risiko pada struktur organisasinya. Berdasarkan penelitian terdahulu bahwa risiko dapat menimbulkan peluang buruk terhadap munculnya risiko yang tidak terduga dan tidak diinginkan mengakibatkan ketidakpastian yang akan menimbulkan kerugian (Hastin Nuraini, 2022). Menurut Peraturan Pemerintah RI Nomor 60 tahun 2008 tentang sistem pengendalian intern pemerintah pasal 13 yaitu instansi pemerintah wajib melakukan penilaian risiko (BPK RI, 2008). Selain itu, Peraturan Menteri Keamanan Republik Indonesia Nomor 17 Tahun 2021 tentang penerapan manajemen risiko Kementerian Keamanan dan Tentara Nasional Indonesia (Kemhan RI, 2021). Dari kedua dasar hukum tersebut bahwa Departemen Informasi & Pengolahan Data Organisasi XYZ sudah semestinya untuk melakukan penilaian manajemen risiko khususnya dengan pendekatan analisis manajemen risiko TI, guna melindungi operasionalnya dari potensi risiko yang dapat menggangu pencapaian tujuan organisasi. Namun demikian, hingga saat ini belum dilakukan evaluasi risiko, padahal telah muncul dampak yang dirasakan oleh para pengguna layanan SICC.

Proses mengelola risiko dilakukan berbagai tahapan mulai dari identifikasi, analisis, evaluasi hingga perlakuan risiko (Hastin Nuraini, 2022) serta pelaksanaan tindakan manajemen risiko. Analisa ini menggunakan ISO (*International Organization for Standardization*) 31000:2018 sebagai acuan pedoman dalam melaksanakan analisis manajemen risiko. ISO 31000:2018 terdiri atas tiga elemen meliputi prinsip (*principle*), kerangka kerja (*framework*) dan proses (*process*) yang merupakan dasar praktik manajemen risiko (Mahardika et al., 2019). Secara umum, ISO 31000:2018 adalah penyederhaan dari edisi 2009 terlihat dari nama yang berubah "*principles and guidelines*" menjadi hanya "*guidelines*" dengan jumlah halaman sebelumnya yaitu 24 menjadi 16 halaman, pada edisi 2009 mengambarkan prinsip, kerangka kerja dan proses sebagai elemen yang berurutan, tetapi versi 2018

menggambarkan ketiga bagian ini sebagai sistem terbuka yang saling berkaitan (Utamajaya et al., 2021).

Penerapan ISO 31000:2018 membantu organisasi dalam mengidentifikasi dan mengelola risiko dengan baik, sehingga menimalisir dampak Negatif terhadap operasionalnya (Buaty et al., 2023). Risiko dari penggunaan TI yang muncul dari berbagai sumber ancaman internal maupun ekternal secara signifikan, organisasi perlu menerapkan strategi manajemen risiko yang efektif untuk melindungi sistem mereka (Saputri et al., 2024). Selain itu, penelitian ini menunjukkan penerapan manajemen risiko TI juga berperan dalam meningkatkan reputasi suatu instansi dan menjaga kepercayaan publik (Bella F, 2023).

Dalam konteks layanan SICC Organisasi XYZ, penerapan manajemen risiko TI dilakukan untuk memastikan bahwa layanan yang diberikan pada pengguna akhir tersebut aman dan andal. Dengan menggunakan pendekatan berbasis ISO 31000:2018, analisis risiko dapat dilakukan secara sistematis untuk mengidentifikasi potensi ancaman dan merumuskan strategi penanganan (Fadiyah, 2025), sehingga sejalan dengan kebutuhan untuk menciptakan lingkungan yang mendukung inovasi dan produktivitas dalam suatu layanan (Natalie & Manuputty, 2022).

Berdasarkan latar belakang diatas penelitian ini melakukan analisis manajemen risiko yang terjadi pada Layanan SICC Organisasi XYZ dengan menggunakan ISO 31000:2018 sebagai standar acuan untuk melaksanakan analisis manajemen risiko. Hasil dari *preliminary study* terhadap potensi risiko yang muncul memberikan fakta bahwa penerapan ISO 31000:2018 dalam melakukan penilaian risiko pada penelitian ini adalah relevan dan tepat, mengingat potensi risiko yang teridentifikasi dari aspek alam, infrastruktur dan manusia. Setelah melakukan proses analisis, sebagai bagian dari upaya penanganan risiko, kontrol tambahan yang merujuk pada COBIT 2019 dan NIST SP 800-53 Rev. 5. Penggunaan kontrol tersebut didasari pada kesesuaian kontrol terhadap peristiwa risiko yang dihadapi dan mempertimbangkan kematangan proses organisasi di konteks instansi keamanan. Penelitian ini menghasilkan dokumen *risk register* sebagai luaran utama karena dokumen ini berfungsi sebagai alat yang terstruktur dan mendokumentasikan

seluruh proses manajemen risiko secara menyeluruh. Selain itu, Institute of Risk Management (IRM) menyatakan bahwa *risk register* adalah dokumen kunci dalam proses manajemen risiko karena memberikan visibilitas terhadap risiko yang dihadapi organisasi serta kontrol yang diterapkan (IRM, 2017). Harapannya dengan adanya penelitian ini dapat memberikan panduan strategis dan praktis bagi manajemen Departemen Informasi & Pengolahan Data Organisasi XYZ untuk mengelola risiko secara sistematis, sehingga dapat mendukung keberlanjutan operasional teknologi informasi terhadap potensi ancaman risiko yang ada.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah peneliti tulis, permasalahan yang mendasari penelitian ini adalah:

1. Bagaimana hasil *risk assessment* teknologi informasi pada layanan SICC Organisasi XYZ berdasarkan ISO 31000:2018?
2. Bagaimana penyusunan dokumen *risk register* berdasarkan risiko teknologi informasi ISO 31000:2018 yang muncul dari layanan SICC sesuai dengan kebutuhan di Organisasi XYZ?

1.3. Tujuan Penelitian

Adapun tujuan pada penelitian ini yaitu:

1. Untuk mengetahui hasil dari *risk assessment* teknologi informasi pada layanan SICC Organisasi XYZ berdasarkan ISO 31000:2018.
2. Untuk menghasilkan *risk register* sebagai pengelolaan risiko teknologi informasi ISO 31000:2018 pada layanan SICC sesuai dengan kebutuhan Organisasi XYZ.

1.4. Batasan Penelitian

Berdasarkan rumusan masalah dan tujuan diatas, adapun batasan masalah penelitian ini sebagai berikut:

1. Hasil dari penelitian ini dikaji dengan menggunakan ISO 31000:2018 melalui proses penilaian risiko pada tahap identifikasi risiko, analisis risiko, evaluasi risiko, perlakuan risiko dan usulan penanganan risiko.

2. Teknologi Informasi yang dianalisis mengenai manajemen risiko dan upaya penanganan risiko yaitu layanan *Smart Integrated Comand Center* (SICC)
3. Pengambilan data hanya dilakukan pada personel lapangan di wilayah Surabaya karena mempertimbangkan beberapa aspek selain keterbatasan waktu dan sumber daya penelitian yaitu karena surabaya sering menjadi pusat kegiatan operasional di wilayah Jawa Timur, sehingga memiliki bobot strategis untuk memahami penerapan TI dan peluang yang lebih kompleks terhadap beban kerja

1.5. Manfaat Penelitian

Terdapat juga manfaat pada penelitian yaitu sebagai berikut:

1. Bagi Instansi, melalui penyusunan dokumen *risk register* diharapkan dapat membantu Organisasi XYZ meningkatkan kesadaran terhadap potensi ancaman risiko yang ada sekaligus menyediakan solusi yang tepat untuk mengatasinya. Dengan demikian, organisasi dapat mengelola risiko secara lebih efisien, mengurangi dampak negatif terhadap operasional, dan meningkatkan keandalan layanan yang diberikan.
2. Bagi peneliti, penelitian ini memberikan kesempatan peneliti untuk mengasah keterampilan dalam proses analisis, identifikasi dan menyusun rekomendasi dari penerapan manajemen risiko TI berdasarkan ISO 31000:2018 pada intitusi keamanan.

1.6. Sistematika Penulisan

Berikut adalah susunan atau struktur yang digunakan dalam penyusunan penelitian tugas akhir yaitu sebagai berikut:

Bab I Pendahuluan

Bab I menjelaskan latar belakang masalah yang menjadi dasar dilakukannya penelitian ini. Selain itu, terdapat tahap *preliminary study* didalam latar belakang, serta terdapat uraian tentang tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan tugas akhir.

Bab II Landasan Teori

Pada bab II memuat teori yang relevan dengan topik penelitian. Bab ini juga terdapat 10 penelitian terdahulu yang menjadikan acuan, gambaran umum perusahaan dan dasar teori. Pada penelitian terdahulu memuat judul, penulis, predikat, tahun, dan hasil dari setiap penelitian. Gambaran umum perusahaan berisikan struktur organisasi dengan tugas pokok dan fungsi, serta layanan yang dijadikan fokus penelitian. Pada dasar teori memuat teori dari manajemen risiko, proses ISO 31000:2018 dan teori lainnya.

Bab III Metodologi Penelitian

Bab III dijelaskan langkah-langkah dan metode yang digunakan dalam penelitian. Di dalamnya dijelaskan berdasarkan pendekatan yang dipilih mencakup, teknik pengumpulan data, instrumen penelitian, dan metode analisis yang dipilih.

Bab IV Pengumpulan dan Pengolahan Data

Pada bab ini, dijelaskan mengenai teknik bagaimana data yang telah dikumpulkan pada penelitian akan diolah. Bab ini memuat analisis deskriptif pada tiap variabel penelitian dari hasil data yang diperoleh data penyebaran kuisioner.

Bab V Analisis dan Pembahasan

Bab V memuat hasil pembahasan dari proses penilaian risiko yang mencakup identifikasi risiko, analisis risiko dan evaluasi risiko. Kemudian, dilakukan rekomendasi perbaikan pada hasil penilaian risiko yang telah dilakukan sebelumnya.

Bab VI Kesimpulan dan Saran

Pada bab ini berisiko kesimpulan dari hasil keseluruhan proses penelitian. Kesimpulan tersebut menjawab rumusan masalah, urgensi serta manfaat pada penelitian tugas akhir. Selain itu, disampaian saran terhadap penelitian yang telah dilakukan dan juga saran untuk rencana penelitian selanjutnya.