BAB I PENDAHULUAN

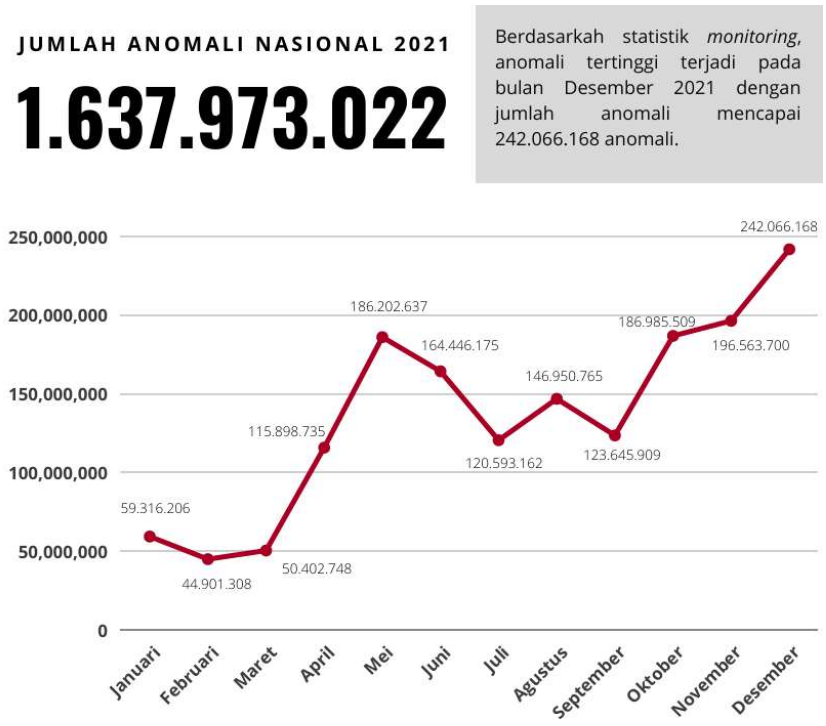
I.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa masyarakat ke era digital (Andre, 2024), di mana teknologi memainkan peran sentral dalam berbagai aspek kehidupan. Penerapan teknologi seperti kecerdasan buatan (AI), *internet of things* (*IoT*), dan *big data* kini banyak dimanfaatkan oleh perusahaan untuk meningkatkan efisiensi, produktivitas, dan ketepatan dalam pengambilan keputusan. Teknologi-teknologi ini membantu perusahaan untuk merespons kebutuhan pelanggan dengan lebih cepat, merancang strategi yang lebih terukur, serta mengoptimalkan operasional harian. Dengan adanya sistem yang saling terhubung dan pengolahan data yang semakin canggih, perusahaan mampu berinovasi dan menciptakan nilai tambah yang lebih besar, sekaligus mempertahankan daya saing di tengah persaingan pasar yang semakin ketat.

Namun, seiring dengan manfaat yang luar biasa ini, teknologi juga menghadirkan tantangan besar, terutama terkait dengan masalah keamanan dan kerahasiaan data. Penggunaan perangkat yang terhubung melalui jaringan internet memberi kesempatan bagi pihak yang tidak bertanggung jawab untuk melakukan serangan siber, pencurian data, atau bahkan sabotase sistem. Ancaman ini semakin nyata dengan berkembangnya perangkat IoT yang terpasang di berbagai titik operasional perusahaan, yang membuatnya rentan terhadap akses tidak sah.

Peningkatan risiko keamanan ini dapat mengakibatkan kerugian finansial yang signifikan, serta kerusakan reputasi perusahaan yang dapat mengurangi kepercayaan pelanggan. Oleh karena itu, penting bagi setiap perusahaan untuk

memiliki sistem manajemen risiko yang kuat, yang dapat melindungi aset digital dan data penting dari ancaman yang semakin berkembang di era digital ini.



Gambar I-1 Statisitik Jumlah Anomali Nasional Tahun 2021

Sumber : (Laporan Tahunan Monitoring Keamanan Siber Tahun 2021 BSSN)

Berdasarkan Gambar I.1 Grafik Jumlah Anomali Nasional Tahun 2021 yang di keluarkan oleh Badan Sandi dan Siber Negara (BSSN) (Rahman dkk., 2021), jumlah anomali yang terdeteksi di Indonesia mencapai 1.637.973.022 kasus. Anomali tertinggi tercatat pada Desember 2021, dengan total 242.066.168 anomali. Angka ini menunjukkan tingginya aktivitas siber yang mencurigakan di jaringan nasional dan menegaskan pentingnya manajemen risiko keamanan informasi yang lebih baik dan terintegrasi. Tanpa langkah mitigasi yang tepat, perusahaan berpotensi menghadapi risiko kerugian besar akibat gangguan yang terjadi secara tiba-tiba pada sistem yang mereka operasikan (Budiono dkk., 2021).

Manajemen risiko menjadi kunci penting bagi perusahaan untuk menghadapi berbagai ancaman yang terus berkembang. Dengan penerapan manajemen risiko yang baik, perusahaan dapat mendeteksi potensi bahaya sejak dini dan menyusun langkah-langkah mitigasi yang tepat. Manajemen risiko yang efektif juga membantu perusahaan dalam menjaga stabilitas operasional, mengurangi

kemungkinan gangguan besar, dan mencegah kerugian yang lebih besar. Selain itu, pengelolaan risiko yang terstruktur memberikan landasan yang kuat bagi perusahaan dalam mengembangkan rencana pemulihan yang efektif apabila terjadi insiden yang mengganggu sistem. Dalam jangka panjang, penerapan manajemen risiko yang baik tidak hanya melindungi aset dan data perusahaan, tetapi juga meningkatkan kepercayaan pelanggan dan mitra bisnis.

Diskominfo Provinsi Jawa Barat selaku instansi pemerintahan yang bergerak di bidang informasi dan data mempunyai tanggung jawab dalam melindungi data, baik data perusahaan, data konsumen, data pemerintah, dan data-data lainnya yang bersifat privasi. Berdasarkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020, setiap instansi pemerintahan diharuskan melakukan manajemen risiko dalam rangka mendukung Peraturan Presiden Nomor 95 Tahun 2018 mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE). Maka dari itu pentingnya melakukan analisis manajemen risiko untuk mencegah risiko-risiko yang dapat mengganggu tercapainya tujuan perusahaan.

Menurut penelitian terdahulu salah satu permasalahan yang dihadapi oleh Diskominfo Provinsi Jawa Barat adalah kurangnya Standar Operasional Prosedur (SOP) dalam Tata Kelola Teknologi Informasi (TI) (Thamrin, 2021). Hal ini dapat menyebabkan tidak jelasan peran dan tanggung jawab, serta tidak konsistenan dalam implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE).

Oleh karena itu, penerapan manajemen risiko yang lebih efektif dan terstruktur sangat diperlukan, dengan bantuan *framework* seperti COBIT 2019. COBIT 2019 memberikan panduan yang komprehensif untuk tata kelola dan manajemen risiko TI, yang dapat membantu organisasi dalam mengidentifikasi, menilai, dan mengelola risiko TI secara sistematis.

Meskipun Diskominfo Provinsi Jawa Barat sudah mengimplementasikan *framework* seperti COBIT 2019, ISO 31000, dan NIST, penerapannya masih belum maksimal, terutama dalam hal manajemen risiko keamanan informasi. Dengan meningkatnya kompleksitas TI, pengelolaan risiko di Diskominfo Provinsi Jawa Barat masih perlu diperbaiki untuk memastikan efektivitas dan

mengurangi potensi insiden yang dapat merugikan. Oleh karena itu, penelitian ini bertujuan untuk memberikan pedoman terkait bagaimana risiko TI dapat dikelola dengan lebih terstruktur dan sistematis, menggunakan COBIT 2019, serta meningkatkan efektivitas operasional dan pengelolaan manajemen risiko keamanan informasi di Diskominfo Provinsi Jawa Barat.

Dari hasil wawancara yang dilakukan dengan salah satu staf Diskominfo Provinsi Jawa Barat Divisi XYZ, pernah terjadi ancaman dan insiden yaitu serangan Web *Defacement* oleh situs judi *online* pada tahun 2024. 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 keamanan suatu instansi, juga menjadi tantangan besar. Hal ini menunjukkan bahwa meskipun beberapa upaya pengelolaan risiko telah dilakukan, penerapan yang ada masih belum cukup efektif dalam menangani ancaman yang berkembang. Kejadian-kejadian ini berpotensi menurunkan kepercayaan publik, merusak reputasi institusi, dan mempengaruhi kelangsungan operasional.

Dengan semakin kompleksnya ancaman yang dihadapi, pengelolaan risiko pada Diskominfo Kota XYZ membutuhkan pendekatan yang lebih terstruktur dan sistematis. Oleh karena itu, sangat penting untuk menerapkan *framework* seperti COBIT 2019 dan juga ISO 27005 guna membantu dalam mengidentifikasi, menilai, dan mengelola risiko IT secara lebih efektif, yang dapat meminimalisir dampak signifikan pada aspek operasional yang berpotensi merugikan instansi tersebut.

Oleh karena itu, hasil akhir dari penelitian ini akan memberikan pedoman dan penilaian terbaru terhadap sejauh mana risiko tersebut dapat diantisipasi dan dikelola dengan menggunakan *framework* COBIT 2019. Penelitian ini akan membantu Diskominfo Provinsi Jawa Barat, khususnya dalam meningkatkan efektivitas operasional dan pengelolaan manajemen risiko keamanan informasi yang sesuai dengan kebutuhan serta arah strategi digital pemerintah daerah. Diharapkan pula, rekomendasi dari penelitian ini dapat memberikan kontribusi positif terhadap keberlangsungan layanan publik, perlindungan data, dan

ketahanan sistem informasi di lingkungan Diskominfo Provinsi Jawa Barat di masa mendatang.

I.2 Perumusan Masalah

Diskominfo Provinsi Jawa Barat, yang bergantung pada teknologi informasi dalam menjalankan operasional bisnisnya, memerlukan sistem pengelolaan risiko yang efektif guna melindungi data dan infrastruktur kritis yang mereka miliki Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

a. Bagaimana kondisi *existing* pengelolaan risiko IT yang diterapkan oleh Diskominfo Divisi XYZ Provinsi Jawa Barat?
b. Bagaimana pengelolaan risiko menggunakan *framework* ISO/IEC 27005:2022?
c. Apa rekomendasi dan kontrol berdasarkan COBIT 2019 Domain APO12 untuk mengatasi risiko yang teridentifikasi?

I.3 Tujuan Penelitian

Berdasarkan dengan apa yang telah dirumuskan dalam rumusan masalah ini, penelitian ini bertujuan untuk:

a. Mengetahui kondisi *existing* pengelolaan risiko IT yang diterapkan oleh Divisi XYZ Diskominfo Provinsi Jawa Barat.
b. Melakukan pengelolaan risiko berdasarkan penerapan *framework* ISO 27005 untuk risiko yang mungkin muncul dalam Divisi XYZ Diskominfo Provinsi Jawa Barat.
c. Menyusun rekomendasi berdasarkan *framework* COBIT 2019 Domain APO12 yang dapat diimplementasikan untuk memperkuat sistem manajemen risiko keamanan informasi di Diskominfo Provinsi Jawa Barat.

I.4 Batasan Penelitian

Berdasarkan ruang lingkup yang telah dijelaskan, penelitian ini akan penulis batasi pada aspek-aspek berikut:

a. Penelitian ini di batasi hanya sampai penyusunan rekomendasi penanganan risiko.

b. Penelitian ini hanya berfokus dalam menganalisis ancaman pada aset IT.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Bagi Universitas Telkom, penelitian ini menambah referensi ilmiah di bidang manajemen risiko teknologi informasi, khususnya yang memadukan dua kerangka kerja ISO/IEC 27005 untuk analisis risiko dan COBIT 2019 domain APO12 untuk rekomendasi penguatan tata kelola. Penelitian ini dapat dijadikan sebagai referensi pembelajaran bagi mahasiswa dan dosen dalam memahami penerapan nyata *framework* manajemen risiko di lingkungan instansi pemerintahan.
2. Bagi Penulis, penelitian ini menjadi sarana untuk mengasah kemampuan analisis, berpikir kritis, dan menyusun rekomendasi strategis berbasis *framework* internasional. Pengalaman ini memperkaya pemahaman penulis dalam penerapan ISO/IEC 27005 sebagai metode analisis risiko serta COBIT 2019 dalam penyusunan kontrol dan kebijakan mitigasi yang selaras dengan tata kelola TI.
3. Bagi Diskominfo Provinsi Jawa Barat, hasil penelitian ini dapat memberikan gambaran kondisi aktual pengelolaan risiko TI yang sedang berjalan, serta membantu dalam mengenali potensi ancaman terhadap aset informasi. Rekomendasi yang disusun berdasarkan COBIT 2019 diharapkan mampu mendukung peningkatan efektivitas dan efisiensi dalam pengelolaan risiko keamanan informasi di Divisi XYZ, sejalan dengan standar dan praktik terbaik internasional.

I.6 Sistematika Penulisan

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Pada bab ini menyajikan tinjauan literatur yang berkaitan dengan permasalahan yang diteliti. Dalam bagian ini, akan dibahas berbagai teori, konsep, serta hasil penelitian terdahulu yang relevan dengan topik penelitian. Selain itu, bab ini juga menguraikan analisis terhadap metode yang digunakan dalam penelitian, termasuk analisis pemilihan metode yang sesuai dengan tujuan penelitian dan kerangka kerja yang berfungsi sebagai pedoman yang digunakan di penelitian ini.

Bab III Metodologi Penelitian

Pada bab ini menjelaskan strategi dan tahapan yang diterapkan dalam penelitian untuk menjawab rumusan masalah yang sebelumnya telah ditetapkan. Penyusunan metodologi dilakukan secara kritis guna memastikan bahwa metode yang dipilih sesuai dengan tujuan penelitian. Pada bab ini juga secara sistematis langkah-langkah penelitian yang mencakup, perumusan masalah dan hipotesis, pengembangan model penelitian, identifikasi serta operasionalisasi variabel, hingga perancangan pengumpulan dan pengolahan data.

Bab IV Penetapan Konteks dan Analisis Data

Pada bab ini, menjelaskan mengenai hasil rancangan, temuan, analisis dan pengolahan data dalam rangka menjawab rumusan masalah yang sebelumnya telah ditetapkan, berdasarkan metode dan proses yang digunakan pada penelitian ini. Bab ini juga bab ini juga akan menguraikan analisis risiko yang mencakup berbagai kategori pada perhitungan risiko, metode penilaian risiko, serta mengevaluasi risiko melalui penerapan matriks risiko yang ditentukan.

Bab V Rekomendasi dan Kontrol

Pada bab ini membahas mengenai strategi rekomendasi dan penetapan kontrol yang tepat untuk menangani analisis risiko yang sebelumnya telah diidentifikasi dalam penelitian ini, rekomendasi yang diberikan bertujuan untuk meminimalisir dampak yang signifikan melalui penentuan urgensi risiko. Bab ini juga mencakup

hasil dari penetapan kontrol yang dilakukan, dapat diimplementasikan secara efektif bagi perusahaan.

Bab VI Kesimpulan dan Saran

Pada bab ini menjelaskan mengenai hasil kesimpulan dari penelitian yang telah dilakukan, dengan menyampaikan rangkuman dari hasil analisis dari penelitian IT *Risk Management* pada Divisi XYZ Diskominfo Provinsi Jawa Barat yang telah dilakukan. Bab ini juga akan menjelaskan saran-saran yang dapat diberikan berdasarkan IT *Risk Management* serta strategi mitigasi yang dapat diterapkan secara lebih optimal, untuk dapat dikemukakan bagi penelitian selanjutnya.