BAB I
PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi informasi (TI) dalam operasional organisasi menjadikan informasi sebagai aset strategis yang perlu dikelola dan dilindungi secara sistematis. Keamanan informasi mencakup tiga aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) yang berperan penting dalam menjaga keberlangsungan layanan organisasi [1]. Seiring meningkatnya ketergantungan terhadap sistem digital, organisasi menghadapi ancaman keamanan informasi yang semakin kompleks, seperti penyalahgunaan hak akses, gangguan layanan sistem, dan kebocoran data. Risiko tersebut dapat menimbulkan kerugian finansial, menurunkan kepercayaan publik, serta mengganggu keberlangsungan layanan apabila tidak dikelola secara tepat. Oleh karena itu, proses digitalisasi perlu diikuti dengan pengelolaan keamanan informasi yang terstruktur dan berbasis risiko [2].

Dalam konteks sektor publik, instansi pemerintah memiliki tanggung jawab besar dalam menjaga keamanan informasi karena data yang dikelola tidak hanya berkaitan dengan kebutuhan internal organisasi, tetapi juga menyangkut kepentingan masyarakat. Dinas Komunikasi dan Informatika Provinsi Jawa Timur (Diskominfo Jatim), berdasarkan Peraturan Gubernur Provinsi Jawa Timur Nomor 72 Tahun 2023 [3], memiliki mandat dalam penyelenggaraan sistem dan teknologi informasi serta mendukung penerapan pemerintahan berbasis elektronik (*e-Government*) yang transparan dan efisien. Sebagai instansi yang mengelola data strategis dan sensitif, Diskominfo Jatim perlu memastikan bahwa informasi dapat diakses secara efektif tanpa mengabaikan aspek keamanan. Pengelolaan keamanan informasi juga perlu dilakukan secara berkelanjutan untuk menjaga mutu layanan publik [4]. Hal ini sejalan dengan Rencana Strategis (Renstra) Diskominfo Jatim [5] yang menegaskan bahwa ancaman keamanan informasi di era digital mencakup potensi risiko dan bahaya yang dapat memengaruhi keamanan data serta sistem komputer.

Berdasarkan observasi awal dan hasil wawancara, penilaian risiko keamanan informasi di lingkungan Diskominfo Jatim masih cenderung bersifat

kualitatif dan deskriptif. Kondisi tersebut menimbulkan kendala dalam pengambilan keputusan karena hasil penilaian risiko sulit digunakan untuk menentukan prioritas mitigasi secara objektif [6]. Akibatnya, organisasi berpotensi mengalami ketidaksesuaian antara tingkat risiko dan kontrol keamanan yang diterapkan, baik berupa penerapan kontrol berlebihan pada risiko rendah maupun kurangnya pengamanan pada risiko kritis. Ketidaktepatan ini dapat memengaruhi efektivitas alokasi sumber daya, terutama pada layanan publik yang melibatkan data sensitif.

Diskominfo Jatim memiliki beberapa layanan utama, seperti pengelolaan informasi publik (PPID), pengembangan infrastruktur digital (*e-Government*), keamanan informasi atau siber, penyediaan data statistik sektoral, serta diseminasi informasi pemerintahan. Salah satu layanan yang memiliki tingkat sensitivitas tinggi adalah layanan sertifikasi elektronik. Layanan ini dilaksanakan di bawah Bidang Persandian dan Keamanan Informasi dengan dukungan tim verifikator serta jabatan fungsional terkait. Proses layanan mencakup pengajuan permohonan, verifikasi dokumen, validasi data, hingga penerbitan sertifikasi elektronik yang digunakan dalam dokumen digital.

Hasil penggalian awal menunjukkan bahwa layanan sertifikasi elektronik memiliki kompleksitas proses bisnis yang cukup tinggi. Kompleksitas tersebut terlihat dari keterlibatan berbagai aktor, seperti pemohon, tim verifikator, admin, dan pejabat fungsional, serta adanya ketergantungan pada validasi data dan dokumen pendukung pengguna. Layanan ini tidak hanya bersifat administratif, tetapi juga melibatkan pengelolaan data pribadi dan kedinasan yang sensitif, termasuk penggunaan *passphrase* sebagai instrumen pengamanan akses [7]. Selain itu, ditemukan beberapa kondisi operasional yang dapat meningkatkan risiko, seperti perbedaan tingkat literasi digital pengguna, penggunaan kanal komunikasi nonformal dalam koordinasi tertentu, ketergantungan pada satu PIC, kesalahan *input* data, serta potensi dokumen identitas palsu atau hasil manipulasi digital. Kondisi tersebut menunjukkan bahwa risiko keamanan informasi pada layanan sertifikasi elektronik tidak hanya berasal dari aspek teknis, tetapi juga dari proses bisnis dan interaksi manusia.

Bukti nyata dari kerentanan ini teridentifikasi dalam daftar risiko yang disusun pada Lampiran 12. Rincian Risiko. Beberapa temuan kunci menunjukkan adanya kelemahan pada aspek administratif dan validasi, seperti munculnya surat permohonan yang tidak sesuai format serta penggunaan kanal komunikasi tidak resmi (*WhatsApp*/*Email* pribadi) yang menyebabkan informasi tidak tercatat dan sulit dilacak. Dari sisi sumber daya manusia, ditemukan risiko ketergantungan pada satu PIC (*single point of person*) serta koordinasi yang buruk antar aktor (verifikator-admin-pemohon) yang berpotensi menghentikan seluruh proses layanan jika terjadi kendala pada salah satu pihak. Selain itu, terdapat celah pada akurasi data dan validasi identitas, mulai dari kesalahan *input* (*typo*) hingga risiko lolosnya dokumen identitas palsu atau hasil manipulasi digital dalam proses verifikasi. Oleh karena itu, diperlukan analisis risiko keamanan informasi yang terstruktur dan berbasis prioritas pada seluruh tahapan layanan sertifikasi elektronik.

Pengelolaan keamanan informasi di Diskominfo Jatim dilaksanakan melalui penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar internasional ISO/IEC 27001:2022. Standar ini menyediakan kerangka kerja pengelolaan keamanan informasi berbasis risiko yang menekankan keterpaduan antara kebijakan, proses, dan teknologi [8]. ISO/IEC 27001:2022 juga mewajibkan organisasi melakukan penilaian risiko secara sistematis sebagai dasar dalam menentukan kontrol keamanan informasi yang sesuai [1]. Penerapan SMKI di lingkungan Diskominfo Jatim turut didukung oleh Peraturan Menteri Dalam Negeri Nomor 57 Tahun 2021 [9] yang mengatur kewajiban perangkat daerah dalam menerapkan pengelolaan keamanan informasi secara terstruktur dan berkelanjutan. Namun, ISO/IEC 27001:2022 tidak menetapkan metode kuantitatif tertentu dalam proses penilaian risiko, sehingga organisasi memiliki keleluasaan untuk memilih metode analisis risiko yang sesuai dengan kebutuhan dan karakteristik layanannya [10].

Meskipun ISO/IEC 27005 menyediakan panduan khusus mengenai manajemen risiko keamanan informasi, standar tersebut lebih berperan sebagai panduan konseptual yang mendukung implementasi keamanan informasi sebagaimana ditetapkan dalam ISO/IEC 27001 [11]. Oleh karena itu, ISO/IEC

27001:2022 dipilih sebagai kerangka utama dalam skripsi ini karena memiliki keterkaitan langsung antara penilaian risiko, penerapan SMKI, dan rekomendasi kontrol keamanan melalui Annex A. Kerangka ini selaras dengan fokus skripsi yang menganalisis risiko dan menyusun rekomendasi pengendalian keamanan informasi pada layanan sertifikasi elektronik.

Berbagai pendekatan penilaian risiko keamanan informasi telah digunakan dalam praktik, seperti NIST *Cybersecurity Framework* (CSF), *Control Objectives for Information and Related Technologies* (COBIT), ITIL, dan Indeks KAMI [12]. Dalam skripsi ini, metode *Failure Mode and Effect Analysis* (FMEA) dipilih karena mampu memberikan penilaian risiko yang lebih terstruktur dan terukur melalui perhitungan *Risk Priority Number* (RPN). Nilai RPN diperoleh dari tiga parameter utama, yaitu tingkat keparahan (*Severity*), kemungkinan kejadian (*Occurrence*), dan kemampuan deteksi (*Detection*). Melalui pendekatan tersebut, FMEA membantu menghasilkan penilaian risiko yang lebih terstruktur, terukur, dan dapat diprioritaskan melalui perhitungan RPN [13]. FMEA juga memiliki keunggulan dalam mengidentifikasi kegagalan yang paling kritis serta memetakan risiko berdasarkan tingkat prioritasnya [14], [15].

Berdasarkan literatur yang telah dikaji, penelitian terdahulu telah membahas analisis risiko keamanan informasi menggunakan metode FMEA berbasis ISO/IEC 27001. Namun, sebagian besar penelitian tersebut masih berfokus pada organisasi secara umum dan belum secara spesifik mengkaji layanan pemerintahan digital yang bersifat kritis, seperti layanan sertifikasi elektronik. Selain itu, beberapa penelitian masih menggunakan ISO/IEC 27001 versi 2013 dan belum mengaitkan hasil analisis risiko secara eksplisit dengan siklus *Plan, Do, Check, Act* (PDCA). Penelitian sebelumnya juga menunjukkan bahwa instansi pemerintah masih menghadapi tantangan dalam mengintegrasikan standar internasional ISO/IEC 27001 dengan regulasi lokal, seperti Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [16] serta dalam menerapkan pengawasan berkelanjutan melalui siklus PDCA [17], [18]. Dari sisi metode, FMEA tradisional juga memiliki keterbatasan berupa potensi subjektivitas dalam penentuan risiko prioritas tinggi [19].

Berdasarkan uraian tersebut, skripsi ini berupaya mengisi celah penelitian dengan melakukan analisis risiko keamanan informasi pada layanan sertifikasi elektronik Diskominfo Jatim menggunakan metode FMEA berbasis ISO/IEC 27001:2022. Fokus skripsi ini adalah mengidentifikasi risiko, menilai tingkat risiko, menentukan prioritas risiko melalui nilai RPN, serta menyusun rekomendasi kontrol keamanan informasi berdasarkan hasil analisis. Dengan demikian, skripsi ini diharapkan dapat memberikan dasar yang lebih objektif bagi Diskominfo Jatim dalam menentukan prioritas mitigasi risiko dan meningkatkan pengelolaan keamanan informasi pada layanan sertifikasi elektronik. Atas dasar pertimbangan tersebut, skripsi ini mengangkat judul: **"ANALISIS RISIKO KEAMANAN INFORMASI LAYANAN SERTIFIKASI ELEKTRONIK MENGGUNAKAN METODE FMEA BERBASIS ISO/IEC 27001:2022 (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah yang diangkat adalah bagaimana hasil analisis terkait risiko keamanan informasi pada layanan sertifikasi elektronik menggunakan metode FMEA berdasarkan ISO/IEC 27001:2022 di Diskominfo Jatim?

1.3 Batasan Masalah

Untuk menjaga fokus penelitian agar tetap terarah dan sesuai dengan tujuan yang telah ditetapkan, maka batasan masalah dalam penelitian ini dirumuskan sebagai berikut :

1. Objek penelitian difokuskan pada Layanan Sertifikasi Elektronik Individu di Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
2. Analisis risiko dibatasi pada proses bisnis layanan sertifikasi elektronik individu, mulai dari pengajuan permohonan, pemeriksaan dan verifikasi dokumen, validasi identitas, pembuatan dan aktivasi akun, distribusi kredensial, penggunaan akun dan *passphrase*, *reset passphrase*, *Review* hak akses, hingga penonaktifan akun pengguna.
3. Metode yang digunakan dalam analisis risiko keamanan informasi adalah *Failure Mode and Effect Analysis* (FMEA) dengan parameter penilaian

Severity, *Occurrence*, dan *Detection*, serta perhitungan *Risk Priority Number* (RPN).

4. Standar yang digunakan sebagai acuan dalam penyusunan rekomendasi pengendalian adalah ISO/IEC 27001:2022, khususnya kontrol keamanan informasi yang terdapat dalam Annex A.
5. Penerapan siklus *Plan*, *Do*, *Check*, dan *Act* (PDCA) dalam penelitian ini dibatasi sampai tahap *Check*. Setelah tahap *Check*, penelitian dilanjutkan dengan tahap *Output Check* untuk menyusun rekomendasi pengendalian dan rancangan dokumentasi tata kelola keamanan informasi. Penelitian tidak mencakup tahap *Act* berupa implementasi maupun pengujian efektivitas pengendalian.
6. Sumber data penelitian dibatasi pada responden yang memiliki keterlibatan langsung terhadap layanan sertifikasi elektronik individu di lingkungan Diskominfo Provinsi Jawa Timur.

1.4 Tujuan

Skripsi ini bertujuan untuk mengetahui hasil analisis risiko keamanan informasi pada layanan sertifikasi elektronik menggunakan metode FMEA berdasarkan ISO/IEC 27001:2022 di Diskominfo Jatim.

1.5 Manfaat

Skripsi ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Manfaat Teoretis

   Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang Sistem Informasi, khususnya dalam kajian manajemen risiko keamanan informasi. Selain itu, penelitian ini juga memberikan kontribusi metodologis melalui penerapan metode *Failure Mode and Effect Analysis* (FMEA) yang diintegrasikan dengan standar ISO/IEC 27001:2022 dalam konteks layanan pemerintahan digital.
2. Manfaat Praktis

   Bagi Dinas Komunikasi dan Informatika Provinsi Jawa Timur, hasil penelitian ini diharapkan dapat menjadi dasar dalam memahami profil risiko keamanan informasi pada layanan sertifikasi elektronik individu secara lebih sistematis dan terukur. Selain itu, hasil penelitian ini dapat digunakan

sebagai acuan dalam menentukan prioritas mitigasi risiko, meningkatkan efektivitas pengelolaan keamanan informasi, serta mendukung pengambilan keputusan berbasis risiko dalam pengelolaan layanan digital.

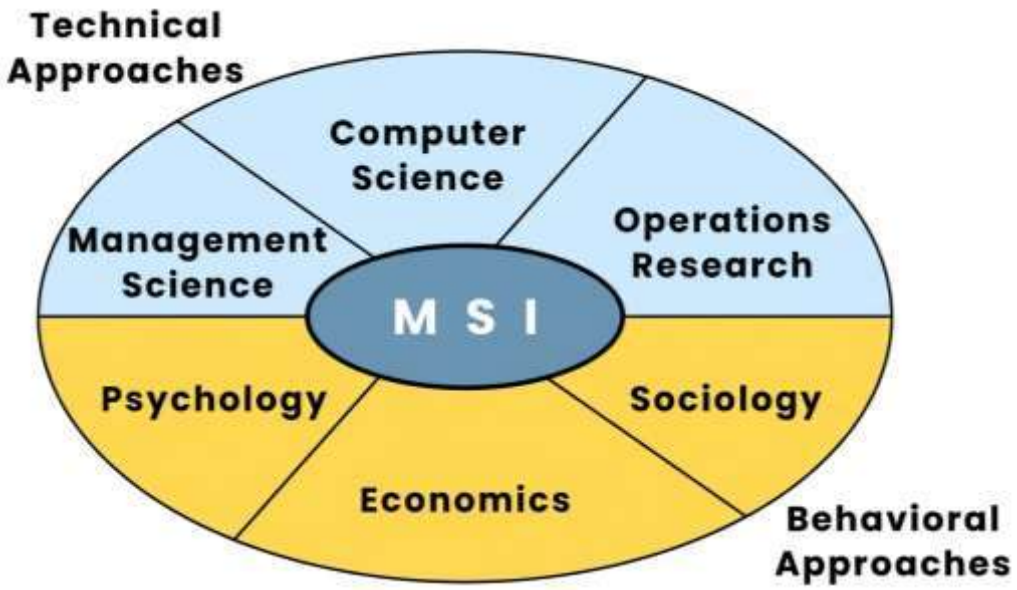
3. Manfaat Kebijakan dan Tata Kelola

   Penelitian ini diharapkan dapat mendukung upaya penyelarasan antara praktik pengelolaan keamanan informasi di instansi pemerintah dengan standar internasional ISO/IEC 27001:2022. Hasil penelitian ini juga dapat menjadi referensi dalam penyusunan kebijakan, prosedur, serta penguatan tata kelola keamanan informasi pada layanan publik berbasis digital.

4. Manfaat Bagi Penelitian Selanjutnya

   Penelitian ini diharapkan dapat menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan analisis risiko keamanan informasi, khususnya yang menggunakan metode FMEA dalam konteks layanan digital pemerintahan atau organisasi sektor publik.

1.6 Relevansi Sistem Informasi



Gambar 1.1 Pendekatan atas Sistem Informasi [20]

Berdasarkan kerangka *Management Information Systems* (MIS), sistem informasi dipandang sebagai bidang interdisipliner yang dipengaruhi oleh pendekatan teknis dan pendekatan perilaku. Skripsi ini cenderung berada pada ranah pendekatan teknis (*technical approaches*), terutama pada irisan *Management Science* dan *Computer Science*. Hal ini terlihat dari fokus skripsi yang

menitikberatkan pada proses pengukuran, analisis, dan pemeringkatan risiko keamanan informasi melalui metode FMEA dengan parameter *Severity, Occurrence , dan Detection* serta perhitungan RPN.

Selain itu, hasil analisis risiko dalam skripsi ini dipetakan ke rekomendasi pengendalian yang mengacu pada kontrol ISO/IEC 27001:2022 Annex A. Dengan demikian, skripsi ini menekankan aspek evaluasi pengendalian, prosedur operasional, tata kelola keamanan informasi, serta pengambilan keputusan berbasis risiko. Unsur pendekatan perilaku (*behavioral approaches*) tetap dipertimbangkan, terutama dalam pembahasan mengenai *human error*, *security awareness*, kepatuhan terhadap SOP, dan pemisahan tugas. Namun, unsur tersebut ditempatkan sebagai faktor penyebab atau kontributor risiko, bukan sebagai landasan utama dalam pemilihan metode skripsi [20].

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun secara sistematis untuk menyajikan pembahasan yang runtut dan mudah dipahami. Adapun susunan laporan skripsi ini terdiri atas sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat, relevansi Sistem Informasi terhadap penelitian yang dilakukan, serta sistematika penulisan skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini membahas landasan teori yang menjadi dasar skripsi, meliputi konsep keamanan informasi, manajemen risiko, sertifikasi elektronik, Penyelenggara Sertifikasi Elektronik (PSrE), layanan Tanda Tangan Elektronik (TTE), metode FMEA, kuesioner, responden, dan instrumen pertanyaan. Selain itu, bab ini juga membahas standar ISO/IEC 27001:2022 sebagai acuan pengendalian keamanan informasi serta penelitian terdahulu yang relevan. Pada bagian akhir, disajikan gambaran umum objek skripsi, yaitu

Diskominfo Jatim, yang dijelaskan berdasarkan peraturan perundang-undangan yang berlaku.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan penelitian yang dilakukan, termasuk metode pengumpulan data dan proses analisis risiko keamanan informasi menggunakan metode FMEA yang dikaitkan dengan siklus PDCA.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil skripsi berupa identifikasi risiko, perhitungan nilai RPN, evaluasi tingkat risiko, serta pembahasan hasil analisis yang dihasilkan. Selain itu, pada bab ini juga disampaikan rekomendasi kontrol keamanan informasi berdasarkan hasil analisis risiko.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diperoleh dari hasil skripsi serta saran atau rekomendasi yang ditujukan untuk pengembangan dan peningkatan implementasi keamanan informasi di masa mendatang, serta sebagai bahan pertimbangan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Bagian ini memuat daftar referensi atau literatur yang digunakan sebagai dasar pendukung dalam penyusunan skripsi, baik berupa buku, jurnal, maupun sumber daring yang relevan.

LAMPIRAN

Bagian ini menyajikan dokumen pendukung, data tambahan, serta bukti-bukti yang digunakan dalam pelaksanaan skripsi.

Halaman ini sengaja dikosongkan