BAB I

PENDAHULUAN

1.1 Gambaran Objek Penelitian

Objek penelitian ini adalah perusahaan XYZ, sebuah instansi yang bergerak di bidang teknologi informasi dan berperan sebagai penyedia layanan sistem informasi untuk mendukung proses bisnis di sektor pendidikan, khususnya bagi civitas akademika. Perusahaan XYZ mengelola berbagai aset informasi krusial, antara lain *storage server, portal website, database*, komputer (PC), serta dokumen prosedural yang mendukung infrastruktur teknologi informasi. Mengingat sifat layanan dan informasi yang dikelola bersifat *confidential*, potensi kebocoran data menjadi ancaman serius yang dapat berdampak signifikan terhadap reputasi dan keberlangsungan layanan akademik.

Sebagai bentuk upaya menjaga kualitas pengendalian risiko, perusahaan XYZ secara rutin melakukan pengembangan dan optimalisasi sistem manajemen keamanan informasi, salah satunya dengan melaksanakan *pre-assessment* ISO 27001:2022 dan mengikuti proses sertifikasi Sistem Manajemen Keamanan Informasi (SMKI). Langkah ini menjadi indikator keseriusan perusahaan dalam menguji kesiapan sistem keamanan informasi yang dimiliki. Meskipun demikian, dalam proses peningkatan layanan teknologi informasi, perusahaan XYZ masih sering menghadapi gangguan yang berpotensi mengancam aset informasi. Oleh karena itu, penerapan mitigasi risiko keamanan informasi yang efektif menjadi hal yang sangat penting untuk memastikan keberlanjutan layanan serta menjaga kepercayaan civitas akademika.

1.2 Latar Belakang Penelitian

Di era digital, layanan teknologi informasi menjadi tulang punggung operasional berbagai institusi. Namun, seiring meningkatnya pemanfaatan teknologi, ancaman terhadap keamanan informasi juga kian kompleks dan beragam. Serangan siber tidak lagi hanya bersifat global, tetapi juga menyasar

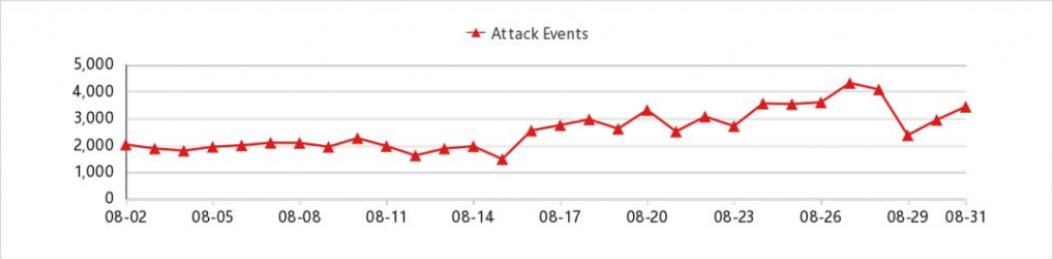
sistem internal organisasi, termasuk institusi pendidikan. Kementrian Komunikasi dan Informatika (JAKARTA (IndoTelko), 2020) melakukan survey terhadap penggunaan internet di indonesia, jumlah penguna internet di tahun 2017 lebih dari 50% penduduk Indonesia. Seiring dengan penggunaan internet meningkat terdapat juga ancaman terhadap keamanan informasi.

Dengan adanya keamanan informasi diharapkan seluruh lapisan masyarakat terlindungi dari ancaman Cyber, dimana saat ini banyak sekali kejadian dan ancaman *Cyber Security* berupa *Ransomware, Malware, Phising* yang terjadi di Indonesia. Tindak kejahatan berupa serangan siber juga terjadi sepanjang tahun 2018 dengan objek pantau situs web sebanyak 16.939 serangan. Situs web dengan domain.go.id mendapat serangan terbanyak dibanding *Country Code Top Level Domain* (ccTLD) .id lainnya. Bentuk insiden yang terjadi pada situs web adalah *web defacement* (Serangan Web et al., 2019).

Perusahaan XYZ, sebagai penyelenggara layanan teknologi informasi, pernah mengalami berbagai bentuk serangan siber. Berdasarkan hasil wawancara, terungkap insiden penyisipan iklan *slot gacor* pada beberapa web portal berbasis WordPress. Serangan ini tidak hanya merusak tampilan situs, tetapi juga berpotensi menyebar ke seluruh sistem karena adanya keterkaitan antarwebsite dalam satu domain institusi pendidikan. Selain itu, terdapat percobaan *SQL Injection* dan *Cross-Site Scripting* (XSS) yang menargetkan database server, serta serangan *Distributed Denial of Service* (DDoS) yang mengganggu infrastruktur jaringan.

Selain serangan teknis, perusahaan mengalami insiden kebocoran dokumen internal akibat file yang diunggah ke *website* tanpa perlindungan memadai, sehingga dapat diakses oleh pihak luar. Dari sisi operasional bisnis, terdapat pula risiko ketidaksesuaian sinkronisasi waktu antarperangkat dan jaringan (NTP & NPR) yang dapat memengaruhi keakuratan pencatatan log serta proses autentikasi. Kondisi ini menimbulkan risiko nyata terhadap keberlangsungan layanan, mulai dari gangguan operasional, potensi *downtime* akibat

ketergantungan pada pasokan listrik dan internet, penurunan reputasi institusi, hingga kemungkinan DNS provider bisa memblokir seluruh domain sektor pendidikan.



Gambar 1. 1 Serangan siber perusahaan XYZ

Sumber: Laporan Threat Intelligence, Agustus 2024

Laporan Threat Intelligence bulanan dari perusahaan XYZ juga mendukung temuan ini, di mana pada periode Juni - November 2024 teridentifikasi berbagai jenis ancaman yang berulang kali menyerang sistem perusahaan XYZ. Beberapa temuan dominan di antaranya adalah *web vulnerabilities, SQL injection, weak password, OS command injection*, dan *cross-site scripting* (XSS). Ancaman-ancaman tersebut selaras dengan 5 aset penelitian, pada komponen *website portal* dan *database* civitas akademik, yang memiliki kerentanan tinggi.

Serangkaian insiden serangan siber yang terjadi di perusahaan XYZ menunjukkan bahwa risiko keamanan informasi memerlukan upaya mitigasi yang relevan dan selaras dengan kebutuhan operasional serta proses bisnis perusahaan. Upaya mitigasi seperti security hardening, penerapan firewall, penggunaan antivirus pada server, pembatasan akses dokumen, dan penambahan watermark, telah dilakukan. Namun, perlindungan yang efektif memerlukan evaluasi risiko yang sistematis dan keterlibatan aktif seluruh karyawan dalam mengenali serta mencegah potensi celah keamanan.

Karyawan merupakan pihak yang memiliki interaksi langsung dengan dunia maya *cyberspace*, sehingga tingkat pengalaman dan kesadaran mereka dalam menggunakan teknologi informasi sangat berpengaruh terhadap kemampuan mengenali potensi celah dan kelemahan dalam sistem. Pengguna yang memiliki

pengalaman tinggi cenderung lebih peka terhadap risiko kerentanan yang bisa dimanfaatkan oleh pelaku *cybercrime*. Oleh karena itu, keterlibatan karyawan dalam menjaga kestabilan dan keamanan informasi menjadi faktor krusial dalam strategi mitigasi risiko. *(A. Alamsyah et al., 2022).*

Dalam konteks penelitian ini, dipilih ISO/IEC 27005:2022 dan NIST SP 800-30 Revision 1. ISO 27005 memberikan panduan menyeluruh untuk proses risk assessment dan *risk treatment* yang selaras dengan ISMS pada ISO 27001, sementara NIST SP 800-30 memberikan pendekatan detail dan terperinci dalam analisis risiko termasuk penentuan *likelihood* dan *impact* berbasis skenario risiko. Penelitian ini akan membahas bagaimana strategi mitigasi risiko keamanan informasi melalui optimalisasi NIST 800-30 revisi 1 sebagai pelengkap panduan *Risk Assessment* dan ISO 27005 sebagai *framework* manajemen risiko yang akan diimplementasikan oleh penulis. Tujuan utamanya adalah melakukan *risk identification, risk analysis, risk evaluation*, dan *risk mitigation* berupa rekomendasi strategi mitigasi risiko serta kontrol keamanan informasi untuk meningkatkan layanan sistem informasi di perusahaan XYZ. Aset yang diidentifikasi berasal dari aset informasi dan juga teknologi informasi yang mendukung proses bisnis layanan teknologi informasi di perusahaan XYZ.

Dengan justifikasi ini, pemilihan ISO 27005 dan NIST SP 800-30 dinilai paling relevan dibandingkan *framework* lain karena mampu mendukung tujuan penelitian yang tidak hanya mengukur risiko teknis, tetapi juga memberikan dasar rekomendasi mitigasi risiko yang berdampak pada keberlangsungan proses bisnis perusahaan XYZ. Maka dari itu, penulis terinspirasi untuk membuat judul penelitian ” **MITIGASI RISIKO KEAMANAN INFORMASI MELALUI OPTIMALISASI RISK ASSESSMENT BERDASARKAN STANDAR ISO 27005:2022 & NIST SP 800-30 REVISI 1 DI PERUSAHAAN XYZ”.**

1.3 Pertanyaan Penelitian

Berdasarkan uraian rumusan masalah tersebut, maka perlu dilakukan penilaian tingkat risiko keamanan informasi berdasarkan ISO/IEC 27005:2022 yang didukung dengan NIST SP 800-30 Revisi 1 untuk menjawab rumusan masalah penelitian sebagai berikut:

1) Bagaimana hasil identifikasi risiko berdasarkan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 terhadap layanan TI di perusahaan XYZ?
2) Bagaimana hasil analisis & evaluasi risiko berdasarkan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 terhadap layanan TI di perusahaan XYZ?
3) Bagaimana hasil rekomendasi strategi mitigasi risiko melalui penerapan kontrol keamanan informasi berdasarkan ISO 27002:2022 terhadap layanan TI di perusahaan XYZ?

1.4 Perumusan Masalah

Di era yang semakin digital, perusahaan menghadapi tantangan yang signifikan terkait keamanan informasi. Meningkatnya ancaman pencurian data seperti *ransomware*, *malware*, dan *phishing* dapat berakibat pada terancamnya reputasi perusahaan. Oleh karena itu, penting untuk melakukan proses manajemen risiko terhadap ancaman keamanan informasi *risk assessment* di perusahaan. Penelitian ini berfokus pada bagaimana perusahaan XYZ dapat mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan informasi dengan menggunakan standar ISO 27005:2022 dan NIST SP 800-30 revisi 1.

1.5 Tujuan Penelitian

Mengacu pada pertanyaan penelitian yang telah diuraikan sebelumnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1) Mengidentifikasi risiko berdasarkan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 terkait layanan TI pada perusahaan XYZ.
2) Menganalisis dan mengevaluasi tingkat risiko berdasarkan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 terkait layanan TI pada perusahaan XYZ.
3) Menyusun rekomendasi strategi mitigasi risiko melalui penerapan kontrol keamanan informasi berdasarkan ISO 27002:2022 terhadap layanan TI di perusahaan XYZ?

1.6 Manfaat Penelitian

1.6.1 Aspek Teoritis

Penelitian ini diharapkan dapat dijadikan masukan untuk mengkaji bagaimana *risk assessment* tingkat risiko keamanan informasi pada aktivitas proses bisnis perusahaan yang menggunakan sistem informasi sebagai layanan teknologi informasi. Penelitian ini juga diharapkan dapat mengembangkan penilaian risiko keamanan informasi melalui kombinasi *framework* ISO 27005 dan NIST SP 800-30 Revisi 1. Menghasilkan rekomendasi strategi mitigasi risiko yang dapat diterapkan untuk meningkatkan keamanan sistem informasi di perusahaan XYZ.

1.6.2 Aspek Praktis

Penelitian ini digunakan sebagai tolak ukur informasi dalam hal penerapan keamanan informasi pada perusahaan XYZ dengan tujuan menjaga integritas, keamanan, ketersediaan dan pengelolaan aset informasi yang tersedia. Berdasarkan NIST SP 800-30 Revisi 1 yang memberikan panduan secara rinci mengenai penilaian risiko dan ISO 27005:2022 sebagai kerangka kerja manajemen risiko agar perusahaan XYZ melakukan pengukuran tingkat risiko

secara berkala terhadap kerentanan ancaman keamanan informasi sehingga reputasi perusahaan tetap terjaga dan mendukung pengambilan keputusan yang didukung oleh semua lapisan pemangku kepentingan. Penelitian ini memberikan gambaran sejauh mana penerapan manajemen risiko keamanan informasi berdasarkan ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 pada sistem informasi yang berupa layanan teknologi informasi di perusahaan XYZ dan evaluasi tingkat risiko keamanan informasi.

1.7 Sistematika Penulisan Tugas Akhir

Sistematika penulisan penelitian berguna untuk memberikan gambaran yang jelas mengenai penelitian yang dilakukan, sistematika penulisan penelitian ini adalah sebagai berikut:

BAB I: PENDAHULUAN

Bab ini berisikan cakupan gambaran umum objek penelitian, latar belakang penelitian, perumusan masalah, pertanyaan penelitian, manfaat penelitian, ruang lingkup penelitian dan sistematika penulisan tugas akhir.

BAB II: TINJAUAN PUSTAKA

Bab ini berisikan landasan teori mengenai hal-hal yang berkaitan dengan penelitian dan model penelitian. Bab ini juga memperlihatkan beberapa penelitian terdahulu yang digunakan sebagai perbandingan, kerangka pemikiran, dan ruang lingkup penelitian.

BAB III: METODE PENELITIAN Bab ini berisikan tentang uraian, pendekatan, metode dan teknik yang digunakan untuk mengumpulkan dan menganalisis data yang dapat menjawab rumusan masalah pada penelitian.

BAB IV: HASIL PENELITIAN DAN PEMBAHASAN Bab ini berisikan hasil pengolahan data yang didapat dan hasilnya akan dianalisis sesuai dengan data yang didapatkan.

BAB V: KESIMPULAN DAN SARAN Bab ini berisikan kesimpulan serta saran-saran dari hasil penelitian yang telah dilakukan.