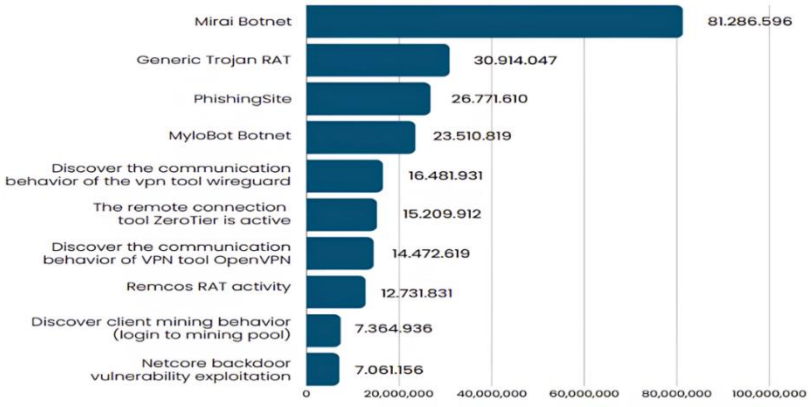
BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi (TI) dalam dekade terakhir telah secara signifikan mengubah paradigma bisnis dan operasional perusahaan, khususnya di sektor *financial technology* (fintech). PT XYZ, sebagai perusahaan penyedia layanan fintech berbasis aplikasi mobile, memiliki ketergantungan tinggi terhadap sistem digital dan data sebagai aset utama perusahaan. Dalam ekosistem digital yang sangat kompetitif, informasi telah menjadi sumber daya strategis yang harus dilindungi secara menyeluruh guna menjaga keandalan layanan, kepercayaan pengguna, serta memastikan kepatuhan terhadap regulasi yang berlaku.

Namun demikian, semakin canggih teknologi yang digunakan, semakin besar pula risiko keamanan informasi yang mengiringinya. Ancaman siber seperti *phishing*, *ransomware*, *trojan*, *exploit*, dan *botnet* menjadi isu serius yang dapat mengancam aspek kerahasiaan, integritas, dan ketersediaan sistem informasi. Laporan dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang tahun 2024 terjadi lonjakan signifikan serangan siber terhadap sektor keuangan digital. Serangan tersebut tidak hanya menargetkan infrastruktur teknis, tetapi juga mengeksploitasi kelemahan pengguna, seperti penggunaan kata sandi yang lemah dan rendahnya kesadaran terhadap keamanan informasi.



Gambar I. 1 Serangan *cyber* Di Indonesia Tahun 2024

Sumber: (BSSN, 2024)

Selain ancaman eksternal, PT XYZ juga menghadapi tantangan internal dalam pengelolaan keamanan informasi. Salah satu permasalahan utama adalah belum optimalnya proses identifikasi, klasifikasi, dan pencatatan aset informasi secara sistematis dan konsisten. Tanpa klasifikasi yang tepat, organisasi akan kesulitan menentukan tingkat kepentingan aset serta menetapkan prioritas perlindungan yang sesuai, sehingga pengelolaan risiko menjadi tidak efektif.

Penelitian yang dilakukan oleh (K. Andersson, 2023) mencatat bahwa sekitar 54% data dalam organisasi tidak memiliki label klasifikasi yang jelas, yang berdampak pada hambatan dalam pengelolaan risiko keamanan informasi. Sementara itu, (J. Bergstrom et al., 2021) menyatakan bahwa ketidaktepatan dalam skema klasifikasi dan lemahnya batasan interpretasi dapat menyebabkan ketidakkonsistenan dalam pengelolaan aset, sehingga mengurangi efektivitas manajemen risiko internal. Penelitian lain oleh (S. Zhang, 2021) dalam konteks sistem fintech juga menunjukkan bahwa organisasi sering kali gagal menyelaraskan proses klasifikasi aset dengan strategi proteksi aktual, mengakibatkan aset kritikal tidak memperoleh kontrol keamanan yang memadai. (A. Adesemowo, 2020) menambahkan bahwa lemahnya pemahaman dalam mendefinisikan dan mencatat aset informasi berdampak pada efektivitas kontrol internal serta kepatuhan terhadap regulasi.

Untuk merespons tantangan tersebut, pemerintah Indonesia telah menerbitkan berbagai kebijakan guna memperkuat ketahanan siber nasional, di antaranya:

- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE);
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE);
- Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital;
- Peraturan Bank Indonesia No. 23/6/PBI/2021 tentang Penyelenggara Jasa Pembayaran;
- SEOJK No. 6/SEOJK.07/2024 tentang Inovasi Teknologi Sektor Keuangan.

Melihat kompleksitas permasalahan dan meningkatnya tekanan regulasi, penerapan ISO/IEC 27001:2022 dipandang sebagai strategi penting dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur, adaptif, dan berkelanjutan. Standar ini mengedepankan pendekatan berbasis risiko, dokumentasi kebijakan keamanan, penerapan kontrol yang terukur, serta penyusunan *Statement of Applicability* (SoA) sebagai indikator efektivitas dan kepatuhan terhadap kontrol keamanan (ISO/IEC, 2022).

Implementasi ISO/IEC 27001:2022 di PT XYZ diharapkan dapat mengatasi sejumlah permasalahan utama, seperti belum tersedianya dokumentasi aset informasi yang memadai, lemahnya pengelolaan risiko terhadap aset kritikal, serta ketidaksesuaian kontrol keamanan dengan praktik dan regulasi terkini. Sebagai entitas teknologi informasi di sektor fintech, PT XYZ memiliki tanggung jawab besar dalam menjaga kerahasiaan, integritas, dan ketersediaan data nasabah dan informasi operasional.

Agar implementasi berlangsung efektif dan berkelanjutan, pendekatan Plan–Do–Check–Act (PDCA) direkomendasikan sebagai metode siklus manajemen dalam kerangka ISO. Tahapan ini mencakup: (1) Plan: merencanakan sistem manajemen keamanan informasi, termasuk identifikasi aset, analisis risiko, serta penyusunan kebijakan dan kontrol yang sesuai; (2) Do: menerapkan kontrol keamanan seperti enkripsi, manajemen akses, pelatihan keamanan, dan prosedur penanganan insiden; (3) Check: mengevaluasi dan mengaudit efektivitas kontrol serta kesesuaian dengan kebijakan; (4) Act: melakukan perbaikan berkelanjutan dan menyesuaikan strategi keamanan dengan dinamika ancaman serta perubahan regulasi.

Penelitian ini dilakukan untuk menganalisis secara komprehensif proses identifikasi, klasifikasi, dan pencatatan aset informasi di PT XYZ dalam mendukung implementasi sistem manajemen keamanan informasi berbasis ISO 27001:2022. Selain itu, penelitian mengevaluasi risiko keamanan terhadap aset kritikal dan strategi mitigasi yang diterapkan, serta menilai kesiapan implementasi melalui analisis kondisi saat ini dan penyusunan SoA. Hasil penelitian diharapkan dapat memberikan kontribusi strategis dan teknis untuk memperkuat sistem keamanan informasi PT XYZ secara menyeluruh.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana proses identifikasi, klasifikasi, dan pencatatan aset informasi dilakukan oleh PT XYZ dalam mendukung implementasi Sistem Manajemen Keamanan Informasi berbasis ISO/IEC 27001:2022?
2. Apa saja risiko keamanan informasi yang dihadapi PT XYZ terhadap aset informasi, dan bagaimana strategi mitigasi yang diterapkan dalam konteks penerapan ISO/IEC 27001:2022?
3. Bagaimana hasil penilaian kondisi saat ini (*current state assessment*) dan *Statement of Applicability* (SoA) yang mencerminkan kesiapan PT XYZ dalam memenuhi kontrol keamanan ISO/IEC 27001:2022?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengidentifikasi dan menganalisis proses pencatatan serta klasifikasi aset informasi yang relevan dengan lingkup implementasi ISO/IEC 27001:2022 di PT XYZ.
2. Mengevaluasi tingkat risiko keamanan informasi terhadap aset digital yang dikelola PT XYZ, serta menilai kesesuaian langkah mitigasi berdasarkan prinsip-prinsip manajemen risiko dalam ISO/IEC 27001:2022.
3. Menilai kesiapan implementasi ISO/IEC 27001:2022 di PT XYZ melalui analisis kondisi saat ini dan penyusunan *Statement of Applicability* (SoA) berdasarkan kontrol yang diterapkan.

I.4 Batasan Penelitian

Batasan penelitian ini adalah:

1. Penelitian ini hanya mencakup implementasi ISO 27001:2022 di PT XYZ, yang terfokus pada Divisi *IT Security & Operation, IT & Network,* serta *IT Planning & Development*
2. Lingkup penerapan Sistem Manajemen Keamanan Informasi ini mencakup semua aset fisik dan perangkat lunak yang digunakan untuk

mesupport produk aplikasi mobile dan *scope* Sistem Manajemen Keamanan Informasi ini tidak mencakup kantor/fasilitas lain dan entitas grup PT. XYZ.

3. Aspek-aspek teknis implementasi ISO 27001:2022 tidak akan dibahas dalam konteks keamanan informasi dan kepatuhan regulasi di PT XYZ.
4. Penelitian ini tidak mencakup perbandingan antara PT XYZ dan perusahaan lain dalam penerapan ISO 27001:2022, maupun evaluasi standar keamanan informasi lainnya, seperti ISO 27002 atau standar keamanan informasi internasional lainnya.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Bagi PT XYZ: Memberikan rekomendasi strategis untuk mengimplementasikan ISO 27001:2022 secara efektif, sehingga dapat meningkatkan sistem manajemen keamanan informasi dan memastikan kepatuhan terhadap regulasi.
2. Bagi Peneliti Lain: Memberikan kontribusi terhadap literatur akademik terkait implementasi ISO 27001:2022 di perusahaan teknologi, serta dapat menjadi referensi bagi penelitian lebih lanjut dalam bidang pengelolaan keamanan informasi dan kepatuhan regulasi.