BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mempermudah suatu organisasi atau perusahaan dalam mengatur proses bisnisnya. Dalam konteks ini tidak menutup kemungkinan akan ada terjadinya kebocoran data dan informasi atau serangan siber pada suatu perusahaan. Data dan asset menjadi komponen penting bagi suatu perusahaan dan harus dijaga agar dapat memberikan jaminan keamanan informasi bagi penggunanya. PT XYZ merupakan perusahaan yang bergerak di bidang IT Services dan IT Consulting serta menyediakan jasa pembayaran berbasis server. Menurut POJK Nomor 4/POJK.05/2021, yang mengatur penerapan manajemen risiko dalam penggunaan teknologi informasi oleh lembaga jasa keuangan non-bank, suatu perusahaan harus menerapkan tata kelola.

Jika tidak ada tata kelola digital yang baik, industri jasa keuangan lebih rentan terhadap serangan siber, kebocoran data, penyalahgunaan informasi, pemalsuan transaksi, dan jenis kejahatan lainnya yang membahayakan konsumen. Untuk alasan ini, Sophia, Ketua Dewan Audit OJK, menekankan bahwa standar terbaru untuk keamanan teknologi informasi IJK harus dipantau dan diterapkan, seperti penerapan tujuh lapis keamanan ISO 27001, yang mencakup jaringan, koneksi data, transportasi, presentasi, pertemuan, dan aplikasi. Selain itu, perusahaan harus melindungi diri dari ancaman siber dengan memberikan update antivirus rutin, pengujian penetrasi pada aplikasi penting, dan meningkatkan kesadaran keamanan IT bagi karyawan.

Keamanan informasi sangat penting untuk menjaga keberlangsungan operasional, mengurangi risiko bisnis, dan meningkatkan nilai investasi dan peluang usaha (Bawono, Soetomo, & Apriatin, 2020). Penerapan kerangka standar internasional dapat memungkinkan perlindungan informasi karena urgensi untuk mencapai atau mempertahankan tingkat perlindungan yang sesuai untuk penggunaan aset (Disterer, 2013) (Clarissa & Wang, 2023). Kejahatan siber (*cybercrime*) kini semakin marak terjadi di Indonesia dan

menimbulkan dampak negatif bagi suatu organisasi maupun individu. Banyak bentuk kejahatan siber yang sering terjadi, namun bentuk kejahatan siber yang paling merugikan bagi suatu organisasi maupun individu yaitu kebocoran data. Teknologi finansial atau *fintech*, adalah salah satu industri yang rentan terhadap peretas, hal ini tentunya akan menghambat kegiatan operasionalnya serta menimbulkan reputasi buruk bagi suatu perusahaan.

Tokopedia, salah satu situs e-commerce dan fintech terbesar di Indonesia, terkena serangan siber pada tahun 2020 yang menyebabkan kebocoran data. Sekitar 91 juta akun pengguna terekspos, dengan 7 juta di antaranya berhasil diretas dan diambil datanya (Fathur, 2020). Dalam kasus ini, pertanyaan tentang tanggung jawab penyelenggara muncul karena data pengguna Tokopedia, termasuk nama lengkap, tempat lahir, nomor telepon, jenis kelamin, dan alamat email, dibocorkan. Pelaku bahkan meminta harga US$5.000, atau sekitar Rp74 juta, untuk data tersebut (Fathur, 2020).

Mengingat bahwa teknologi informasi merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing perusahaan, perusahaan harus menerapkan kebijakan pengelolaan teknologi informasi untuk meminimalisir risiko yang terkait dengan teknologi yang digunakan serta guna memaksimalkan penggunaannya. Dalam mempertahankan kepercayaan dan integritasnya sebagai perusahaan yang bergerak di bidang *financial* service, perlu dilakukannya audit ISO 27001:2022 untuk mengetahui apakah tata kelola teknologi informasi yang diterapkan oleh PT XYZ dapat mencegah risiko kebocoran data dan informasi. Audit ISO 27001:2022 atau audit *external* harus dilakukan minimal setahun sekali sebagai bentuk dari kepatuhan suatu organisasi terhadap peraturan maupun perundang-undangan yang berlaku. Dalam Peraturan OJK Nomor 73/POJK.05/2016 Tahun 2016 tentang Tata Kelola Perusahaan yang Baik Untuk Perusahaan Perasuransian, angka 25 Pasal 1 menjelaskan apa yang dimaksud dengan Good Corporate Governance untuk perusahaan perasuransian sebagai berikut:

"Tata Kelola Perusahaan Yang Baik Bagi Perusahaan Perasuransian adalah sistem dan prosedur yang digunakan dan diterapkan oleh organisasi

perusahaan perasuransian untuk mencapai tujuan hasil usaha dan meningkatkan nilai bagi seluruh pemangku kepentingan, termasuk tertanggung, pemegang polis, peserta, dan pihak yang berhak mendapatkan manfaat secara akuntabel dan berdasarkan peraturan." (Sumarto et al., 2024).

Audit ISO 27001:2022 merupakan suatu proses pengecekan serta evaluasi tata kelola teknologi informasi secara keseluruhan, yang mencakup kebijakan, prosedur, kontrol, dan infrastruktur teknologi informasi. Proses audit bertujuan untuk memastikan bahwa data dan aset informasi perusahaan maupun pelanggan dapat terjaga kerahasiaan (*Confidentiality*), integritas (*Integrity*) dan ketersediaan (*Availability*) dalam menjalankan keberlangsungan proses bisnisnya, serta memastikan bahwa sistem informasi memenuhi kebutuhan keamanan organisasi dan meminimalkan risiko yang terkait dengan keamanan informasi.

ISO 27001:2022 mengatur bagaimana pengaturan individu harus dibangun, diterapkan, dipantau, dan diperbaiki secara terus menerus. Pengaturan ini digunakan secara independen dalam bisnis di mana manajemen risiko diperlukan. Selain itu, pengaturan ini dirancang untuk menjamin bahwa pengaturan sistem keamanan yang digunakan dapat mencegah informasi dan aset dari bermacam potensi risiko dan memberikan kepercayaan sistem keamanan (Riana et al., 2022). Standar ISO 27001 adalah kerangka kerja yang digunakan untuk mengukur dan mengaudit tingkat keamanan informasi (*cybersecurity*). Standar ini membantu sebuah organisasi menjaga aset dan sistem manajemen keamanan informasinya aman.

Untuk mempermudah proses dilakukannya audit ISO 27001:2022 dalam mengevaluasi suatu tata kelola teknologi informasi serta meminimalisir terjadinya insiden keamanan informasi dibutuhkannya suatu metode yaitu dengan menggunakan siklus PDCA (*Plan*, *Do*, *Check*, *Act*). Pemimpin manajemen mutu Walter Shewhart pertama kali mengusulkan model PDCA, dan Edward Deming mengembangkannya lagi ketika dia bekerja di Jepang setelah perang dunia kedua. Dasar dari model PDCA ini adalah semua aspek terkait pada operasional bisa selalu untuk diperbaiki serta ditingkatkan

sehingga terus menuju lebih sempurna atau menuju pada kondisi yang lebih efisien dan efektif (Heizer et al., 2020) (Berkelanjutan, 2024). Salah satu prinsip yang digunakan dalam Sistem Manajemen Keamanan Informasi ISMS ISO 27001 adalah proses Plan-Do-Check-Act (PDCA). Siklus Plan-Do-Check-Act (PDCA) ISMS ISO 27001:2022 akan mendefinisikan pengertian tentang bagaimana tata kelola diterapkan serta apakah itu sesuai dengan objektif kegiatan operasional organisasi.

Dalam upaya melakukan monitoring hasil audit ISO 27001:2022, sebuah sistem dapat membantu perusahaan dalam mengetahui tingkat kesiapannya selama proses audit berlangsung. Sistem ini membantu memberikan rekomendasi atau *best practice* bagi departemen terkait jika hasil audit belum optimal. Algoritma *Decision Tree* atau ID3 pada sistem dapat membantu memberikan *best practice* bagi kegiatan operasional perusahaan. Decision Tree ID3 adalah pemodelan pohon yang memiliki kemampuan untuk mengimplementasikan beberapa Keputusan, memiliki setiap cabang pohon yang menunjukkan karakteristik yang telah diuji, dan setiap daun menunjukkan kelompok kelas tertentu (Setio dkk., 2020).

Menilai dari penjabaran yang telah dijelaskan diatas, penulisan ilmiah yang dibuat perlu dilakukannya audit tata kelola teknologi informasi pada PT XYZ sebagai upaya mitigasi risiko pencegahan pencurian data sesuai dengan standar SNI-ISO 27001. *Framework* yang ditetapkan yaitu ISMS ISO 27001:2022, mempunyai klausul, objektif kontrol, serta kontrol yang dapat ditetapkan sebagai pedomam dalam mengevaluasi manajemen tata kelola teknologi informasi yang terdapat pada lingkup organisasi ataupun perusahaan. Seluruh klausul dan Annex yang ditetapkan dalam proses audit ISO 27001:2022. Untuk perbaikan dari temuan audit pada penelitian ini menggunakan Algoritma *Decision Tree* atau ID3 guna mengoptimalkan proses bisnis PT XYZ.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam proposal ini adalah sebagai berikut:

1. Mengapa diperlukan audit ISO 27001:2022 bagi PT XYZ dalam mencegah adanya pencurian data dan asset perusahaan?
2. Bagaimana tingkat kesiapan PT XYZ dalam mencegah adanya pencurian data dan asset perusahaan?
3. Bagaimana decision tree dapat mengidentifikasi kontrol ISO 27001:2022 yang paling memengaruhi kesiapan dalam mencegah pencurian data pada PT XYZ?

1.3 Tujuan Masalah

Tujuan dari proposal ini adalah sebagai berikut:

1. Mengetahui pentingnya pelaksanaan audit ISO 27001:2022 dalam mencegah pencurian data dan asset pada PT XYZ.
2. Mengetahui tingkat kesiapan sebagai langkah preventif dalam mencegah adanya pencurian data dan asset perusahaan.
3. Mengetahui kontrol ISO 27001:2022 yang paling memengaruhi kesiapan dalam mencegah pencurian data pada PT XYZ

1.4 Batasan Masalah

Agar penelitian ini lebih berfokus dan terarah, terdapat beberapa batasan masalah yang perlu ditetapkan, antara lain:

1. Lingkup Audit ISO 27001

Studi ini hanya akan membahas implementasi dan evaluasi audit ISO 27001 pada sistem manajemen keamanan informasi (ISMS) PT XYZ. Fokus utama penelitian akan berada pada elemen keamanan informasi perusahaan, seperti kebijakan, prosedur, dan kontrol yang digunakan. Tidak ada standar ISO

atau sistem keamanan lain di luar ISO 27001 yang akan dibahas dalam penelitian ini.

2. Jenis Insiden Keamanan yang Dibahas

Dalam penelitian ini, penulis akan membahas masalah keamanan informasi yang sering terjadi di perusahaan teknologi finansial, seperti kebocoran data.

3. Waktu Penelitian

Untuk memastikan relevansi data dan informasi yang diambil, penelitian ini hanya akan melihat audit dan program pengetahuan IT yang digunakan selama periode tertentu, yaitu satu tahun terakhir. Ini tidak akan melihat implementasi yang dilakukan sebelumnya atau proyeksi masa depan yang belum terjadi. Rentan waktu yang ditentukan untuk penelitian ini yaitu mulai dari April 2025 – Agustus 2025.

Dengan adanya batasan masalah ini, diharapkan penelitian dapat berjalan lebih terarah dan mendalam sesuai dengan tujuan yang telah ditetapkan.

1.5 Kontribusi Penelitian

Penelitian ini memiliki kontribusi yang signifikan dalam pengembangan keamanan informasi di perusahaan teknologi finansial, khususnya pada aplikasi PT XYZ. Berikut adalah kontribusi utama dari penelitian ini:

1. **Penerapan Framework ISO 27001:2022 dalam Mitigasi Risiko Keamanan Data**

   Penelitian ini berfokus pada penerapan standar pengamanan informasi ISO 27001, khususnya dalam industri finansial digital, dan mengembangkan model audit yang dapat digunakan untuk mengidentifikasi dan mengurangi kemungkinan pencurian data dan aset digital pada PT XYZ. Framework ISO 27001:2022 ini telah terbukti berhasil di berbagai industri. Studi ini akan memberikan informasi lebih lanjut tentang cara menggunakan kontrol yang tepat untuk melindungi data pelanggan dan transaksi yang dilakukan di platform PT XYZ.

2. **Penerapan Kontrol-Kontrol dalam ANNEX A ISO 27001:2022**

   Menurut Annex A ISO 27001:2022, kontrol teknis, administratif, dan fisik akan dievaluasi secara menyeluruh dalam penelitian ini. Penelitian ini akan menentukan kontrol mana yang paling efektif dan relevan untuk mengurangi risiko pencurian data dan aset digital dalam sistem yang ada di PT XYZ. Kontribusi ini diharapkan dapat memberikan pedoman lebih lanjut bagi perusahaan dalam memilih dan menerapkan kontrol ISO tertentu untuk melindungi data dan aset penting mereka.

3. **Model Audit Berbasis ISO 27001 untuk PT XYZ**

   Pengembangan model audit berbasis ISO 27001:2022, yang dapat diterapkan pada lingkungan operasional PT XYZ, merupakan kontribusi utama penelitian ini. Model ini akan mencakup metode untuk menilai dan mengukur tingkat kepatuhan terhadap kontrol-kontrol yang ada dalam Annex A dan memberikan saran untuk perbaikan berkelanjutan. Selain itu, audit ini dapat digunakan sebagai alat untuk mencegah ancaman pencurian data dan aset secara lebih terorganisir dan efisien.

4. **Penguatan Keamanan Data dan Kepercayaan Pengguna**

   Dengan meninjau dan mengaudit sistem keamanan yang ada di PT XYZ, penelitian ini membantu menjaga data pengguna dan pelanggan lebih aman. Dalam industri fintech, kepercayaan pengguna sangat bergantung pada seberapa baik perusahaan menjaga kerahasiaan, integritas, dan ketersediaan data. Hasil penelitian ini dapat membantu PT XYZ mengurangi risiko dan meningkatkan kepercayaan pengguna.

5. **Model Pemantauan Berkelanjutan untuk Keamanan Informasi**

   Selain itu, penelitian ini membantu mengembangkan model pemantauan berkelanjutan yang dapat digunakan oleh PT XYZ untuk memastikan bahwa kontrol yang diterapkan tetap efektif dalam jangka panjang. Dengan menggunakan model audit yang mengacu pada ISO 27001:2022, perusahaan dapat memantau dan mengevaluasi kepatuhan

terhadap kebijakan keamanan informasi secara teratur dan mengubah strategi mitigasi mereka untuk menangani ancaman baru.

Dengan kontribusi-kontribusi tersebut, penelitian ini tidak hanya membantu PT XYZ dalam mengoptimalkan manajemen risiko dan pengamanan data, tetapi juga dapat menjadi referensi bagi perusahaan fintech lainnya dalam meningkatkan sistem keamanan informasi mereka.