

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Berdasarkan survei yang dilaksanakan oleh Lembaga Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia telah mencapai 78,19% dari jumlah populasi Indonesia, jumlah tersebut meningkat 1,17% sejak tahun 2022 [1]. Perkembangan ini merupakan perubahan masif yang menggerakkan industri-industri untuk mendigitalisasi proses-proses bisnisnya, termasuk dalam industri keuangan. Peningkatan pada angka pengguna internet pun terlihat dari peningkatan pengguna layanan internet banking dari 28% di tahun 2014 hingga 30% pada tahun 2018 [2]. Pergerakan digitalisasi ini tidak hanya menggeser proses bisnis penyedia jasa keuangan konvensional menjadi digital, namun juga memunculkan disrupti baru berupa layanan keuangan berbasis teknologi atau *financial technology (fintech)*. Salah satu perusahaan yang menjadi bagian industri ini adalah PT ABC, sebagai perusahaan pembiayaan berbasis teknologi.

Dengan adanya inovasi baru ini, para penyedia jasa dan penyusun regulasi pun didesak untuk menjamin keamanan, kenyamanan, dan ketersediaan layanan. Salah satu poin penting dalam pelaksanaan proses bisnis adalah penjaminan keamanan informasi, mengingat industri finansial non-bank pun mengelola *data personally identifiable information (PII)* dan dokumen sensitif lainnya. Urgensi untuk menjaga keamanan informasi ini dapat dilihat pada keterangan pers OJK yang membahas webinar berjudul '*Digital Governance: Akselerasi Digitalisasi untuk Perlindungan Konsumen di Ruang Digital*'. Pada acara tersebut, Sophia Wattimena, selaku Ketua Dewan Audit OJK menyatakan bahwa keamanan teknologi lembaga layanan keuangan harus diperbarui dengan standar terkini dan selalu dipantau, selain itu perusahaan pun harus memitigasi risiko siber [3]. Selain itu, pemerintah telah menyusun undang-undang untuk melindungi *personally identifiable information (PII)* dengan nama Undang-

Undang 27 tahun 2022 Perlindungan Data Pribadi (PDP) [4] dan POJK no 4 tahun 2021, pasal 21 ayat 2, huruf h, angka 5 yang berbunyi,

"Informasi termasuk sistem dan perangkat yang digunakan untuk memproses, menyimpan, dan mengirimkan informasi, merupakan aset yang harus dijamin keamanannya oleh pihak penyedia jasa. Teknologi Informasi dengan cara dilindungi dari musuh dan ancaman bahaya yang dapat mengganggu prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) [5]."

Usaha untuk menjaga keamanan pun dapat dilakukan dari pembangunan tata kelola teknologi yang baik, terutama pada keamanan informasi. Hal ini dapat dilansir dari pernyataan Sophia Wattimena pada webinar *Digital Governance* yang menyatakan, "Dalam POJK dan SEOJK tersebut, diatur penerapan manajemen risiko dan tata kelola teknologi informasi, upaya untuk menjaga ketahanan dan keamanan siber, pelaporan berkala kepada OJK, hingga kewajiban melakukan perlindungan data pribadi," [6]. Tata kelola yang baik merupakan bagian penting dalam cakupan manajemen, struktur organisasi, dan proses-proses bidang teknologi informasi yang mampu menunjang dan diselaraskan dengan strategi dan objektif organisasi [7]. Usaha PT ABC dalam penerapan *framework* ISO 27001:2013 sebagai salah satu cara untuk menerapkan keamanan informasi perlu dilengkapi dengan adanya tata kelola yang baik.

Penerapan Tata Kelola Keamanan TI dapat dilakukan melalui berbagai cara, beberapa penerapan dilakukan melalui pembuatan peraturan dan prosedur sebagai kerangka pada proses yang terjadi di perusahaan. Untuk memastikan peraturan dan prosedur tersebut diterima dan dilaksanakan dengan baik, maka perusahaan perlu mengadakan pelatihan dan pemeriksaan (audit) secara berkala. Perusahaan dapat melakukan perbaikan yang berkesinambungan dengan menggunakan temuan-temuan pada laporan audit, insiden-insiden, serta evaluasi berdasarkan *framework* dan *best practice* yang digunakan. Menurut ISACA, audit merupakan inspeksi formal dan verifikasi untuk memastikan sebuah standar atau *guideline* telah diimplementasikan, *records* yang disimpan bersifat akurat, atau efektivitas dan efisiensi target perusahaan sudah dicapai [8].

## 1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah penelitian ini adalah sejauh ini tidak ada pengukuran tingkat kapabilitas PT ABC untuk mengevaluasi dan memastikan tata kelola teknologi informasi, terutama pada bagian keamanan informasi dan agar memenuhi UU Perlindungan Data Pribadi, POJK no 4 tahun 2021, dan sasaran perusahaan untuk melaksanakan audit internal terkait keamanan informasi minimal satu kali setahun.

## 1.3. Pertanyaan Penelitian

Berikut merupakan beberapa pertanyaan penelitian yang selaras dengan perumusan masalah yang telah diuraikan:

1. Bagaimana cara mengevaluasi tata kelola keamanan teknologi informasi di PT ABC berdasarkan *framework* COBIT 5?
2. Bagaimana hasil evaluasi dan rekomendasi untuk meningkatkan kesesuaian tata kelola keamanan teknologi informasi yang digunakan PT ABC, dengan menggunakan *framework* COBIT 5?

## 1.4. Tujuan Penelitian

Adapun tujuan penelitian yang dilaksanakan pada PT ABC adalah:

1. Penelitian ini bertujuan untuk menilai tingkat kemampuan (*capability level*) untuk tata kelola keamanan teknologi informasi yang digunakan pada PT ABC.
2. Penelitian ini bertujuan untuk memberikan rekomendasi untuk perbaikan dan pembaruan tata kelola keamanan teknologi informasi dalam PT ABC.

## 1.5. Batasan Masalah

Untuk membatasi ruang lingkup atau *scope* penelitian, maka penelitian ini dibatasi pada aspek berikut:

1. Penelitian akan dilangsungkan dalam PT ABC.
2. Analisis tata kelola keamanan teknologi informasi pada PT ABC akan dilaksanakan dengan pelaksanaan audit.
3. Ruang lingkup analisis penelitian ini ada pada Tata Kelola Keamanan Informasi.

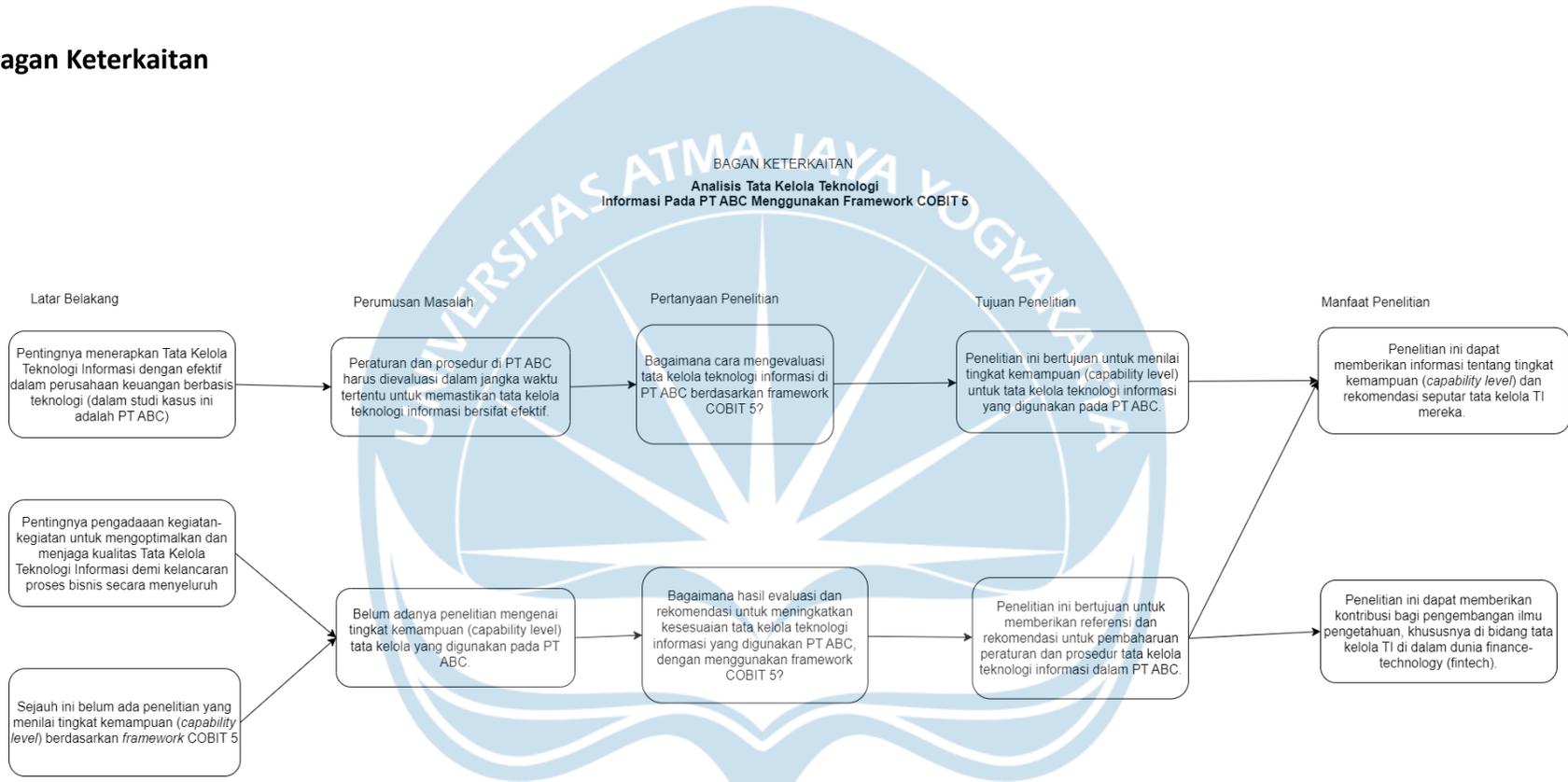
4. Pada COBIT, ada 4 proses yang terkait dengan keamanan informasi. Penelitian ini meneliti 3 proses (EDM03, APO13, MEA03) dengan kesepakatan *auditor* dan *auditee* pada proses pemetaan.

#### **1.6. Manfaat Penelitian**

Penelitian ini diharapkan dapat memberikan manfaat kepada PT ABC untuk memberikan informasi tentang tingkat kemampuan (*capability level*) dan rekomendasi seputar tata kelola Tata nformasi PT. ABC.



## 1.7. Bagan Keterkaitan



Gambar 1.1 Bagan Keterkaitan