

# **BAB I PENDAHULUAN**

## **1.1 Latar Belakang Masalah**

Informasi adalah sebuah aset bisnis yang sebagaimana bisnis lainnya memiliki nilai esensial dan karenanya harus dilindungi keamanannya. Seiring dengan perkembangan teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan terkait keamanan semakin meningkat. Untuk itu perusahaan harus menerapkan suatu kebijakan yang tepat dalam melindungi aset informasi yang dimiliki, dimana perusahaan mengambil suatu kebijakan untuk mengatasi gangguan keamanan sistem informasi yaitu dengan menerapkan SMKI.

ISO 27001:2005 (SMKI) adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. ISO 27001:2005 merupakan SMKI atau *Information Security Management System*, biasa disebut ISMS, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan berdasarkan "*best practise*" dalam pengamanan informasi.

PT.KAI merupakan perusahaan BUMN yang bergerak dalam bidang jasa transportasi darat yang sudah menerapkan sistem informasi dalam menjalankan usahanya. Dalam mendukung keamanan informasi PT.KAI diperlukannya suatu standarisasi yang dapat mengelola insiden keamanan informasi misalnya dengan untuk memastikan kejadian dan kelemahan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu, kemudian untuk memastikan bahwa keamanan merupakan bagian utuh dari sistem informasi dalam melindungi kerahasiaan, keaslian atau integritas informasi, serta pengelolaan yang benar dalam perangkat lunak sistem aplikasi dan informasi dan juga mengurangi

resiko terhadap kerawanan teknis yang dipublikasikan. PT.KAI juga harus dapat mengatasi gangguan kegiatan bisnis dan juga kesesuaian terhadap undang-undang peraturan dan kewajiban dalam memenuhi persyaratan keamanan.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah dijelaskan pada 1.1 maka masalah yang akan dikaji dalam Tugas Akhir ini adalah sebagai berikut:

1. Apakah unit IT telah melakukan akuisisi terhadap pengembangan dan pemeliharaan sistem informasi terkait keamanan dalam melindungi kerahasiaan, keaslian atau integritas informasi pada PT.KAI?
2. Apakah unit IT telah mengelola insiden yang dilakukan keamanan informasi untuk memastikan kejadian dan kelemahan informasi yang terkait dalam sistem informasi pada PT.KAI?
3. Apakah unit IT telah mengatasi setiap gangguan teknis terkait keamanan informasi agar tidak mengganggu keamanan bisnis yang dilakukan pada PT.KAI?
4. Apakah penggunaan sistem informasi sudah dijalankan sesuai dengan peraturan ataupun undang-undang yang ditetapkan PT.KAI?

## **1.3 Tujuan Pembahasan**

Adapun tujuan pembahasan dari Tugas kahir ini adalah sebagai berikut:

1. Untuk melindungi keaslian, kerahasiaan atau integritas informasi dari setiap resiko yang terjadi pada PT.KAI .
2. Untuk memastikan setiap kelemahan dan kejadian terkait keamanan sistem informasi dikomunikasikan dan diambil tindakan koreksi secara tepat waktu.
3. Untuk melindungi kegiatan bisnis yang diakibatkan dari gangguan dan kegagalan sistem informasi agar keberlanjutan bisnis dari PT.KAI dapat dipastikan secara tepat waktu.

4. Untuk mencegah terjadinya pelanggaran ataupun penyalahgunaan dari sistem informasi yang dipakai oleh PT.KAI.

## 1.4 Ruang Lingkup Kajian

Ruang Lingkup kajian penelitian adalah sebagai berikut:

1. Analisis dilakukan pada PT.KAI Bandung.
2. ISO 27001:2005 merupakan SMKI atau *Information Security Management System* memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan.
3. Menggunakan 4 kontrol yang terdapat di dalam ISO 27001:2005
  - a. Manajemen Insiden Keamanan Informasi  
Sasaran dalam proses ini adalah untuk memastikan kejadian dan kelemahan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu.
  - b. Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi  
Sasaran dalam proses ini adalah untuk memastikan bahwa keamanan merupakan bagian utuh dari sistem informasi dalam melindungi kerahasiaan, keaslian atau integritas informasi, serta pengelolaan yang benar dalam perangkat lunak sistem aplikasi dan informasi dan juga mengurangi resiko terhadap kerawanan teknis yang dipublikasikan.
  - c. Manajemen Keberlanjutan Bisnis  
Sasaran dalam proses ini adalah untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi dan untuk memastikan keberlanjutan secara tepat waktu.

d. Kesesuaian

Sasaran dalam proses ini adalah untuk mencegah pelanggaran terhadap undang-undang peraturan atau kewajiban dan persyaratan keamanan.

### 1.5 Sumber Data

Metode penelitian yang digunakan dalam penyelesaian Tugas Akhir ini adalah:

1. Observasi

Melakukan pengamatan langsung terhadap objek yang dituju mengenai mekanisme evaluasi dan perbaikan secara berkesinambungan pada organisasi.

2. Wawancara

Berkomunikasi langsung dengan orang/pegawai di organisasi yang diteliti untuk mendapatkan data dan informasi yang diperlukan dalam penelitian ini.

3. Kuesioner

Memberikan beberapa pertanyaan secara tertulis kepada responden untuk mendapatkan informasi informasi yang diperlukan dalam penelitian ini.

4. Studi *Literature*

Menggunakan referensi dan metode penelitian dari buku, *textbook*, dan *e-book*, artikel yang berkaitan dengan penelitian.

### 1.6 Sistematika Penyajian

Secara umum, sistematika penyajian diuraikan sebagai berikut:

#### **BAB I PENDAHULUAN**

Bab ini membahas mengenai latar belakang permasalahan, rumusan masalah, tujuan yang hendak dicapai, metode penelitian, dan sistematika penyajian.

## **BAB II KAJIAN TEORI**

Bab ini membahas mengenai dasar atau kajian teori yang digunakan dalam penyusunan Tugas Akhir.

## **BAB III ANALISIS DAN EVALUASI**

Bab ini membahas mengenai profil dari PT.KAI, *GAP* Analisis Manajemen Keamanan Informasi pada bagian Unit TI di PT.KAI menggunakan standar ISO 27001:2005

## **BAB IV SIMPULAN DAN SARAN**

Bab ini membahas mengenai kesimpulan dan saran pengembangan berdasarkan analisis dan evaluasi yang telah dibahas pada BAB III.