

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

PT PJB Unit Pembangkit Gresik merupakan perusahaan pembangkit tenaga listrik Indonesia. Teknologi informasi memiliki fungsi sebagai alat bantu utama dalam berkembangnya kemajuan perusahaan dan memberikan kontribusi yang sangat penting dalam terciptanya visi, misi, dan tujuan strategis dalam perusahaan.

PT. PJB Unit Pembangkit Gresik menyusun sebuah kerangka kerja yang terstruktur serta langkah-langkah untuk mencapai kualitas keamanan sistem informasi yang sesuai dengan standar dari teknologi keamanan informasi. Sub direktorat (subdit) teknologi informasi pada sub indikator Sumber Daya Manusia (SDM) mempunyai tiga bagian utama yaitu *Human Capital Readiness (HCR)*, *Organization Capital Readiness (OCR)*, dan *Information Capital Readiness (ICR)*. Bagian *Information Capital Readiness (ICR)* merupakan indikator penilaian kinerja yang dilakukan oleh tim *assessor* dan terdiri dari tiga proses utama yang menilai tentang *infrastructure*, dan *Application*. Teknologi informasi pada PT PJB Unit Pembangkit Gresik diatur dalam bagian ICR yang dilakukan oleh divisi manajemen teknologi informasi yaitu SINFO. SINFO mempunyai tugas dan fungsi dalam penyedia layanan teknologi sistem informasi kepada *user* (unit) yang ada dalam lingkungan PT PJB Unit Pembangkit Gresik. PT PJB menetapkan *Assesment Kontrak Kinerja* untuk mendukung kelangsungan proses bisnis dalam kualitas teknologi informasi khususnya untuk keamanan informasi. *Assesment Kontrak Kinerja* pada ICR berfungsi sebagai landasan penilaian setiap

unit yang diperoleh dari dokumen kriteria ICR dan *Opportunity For Improvement* (OFI). OFI merupakan rekomendasi yang dibuat untuk kelangsungan kualitas dari teknologi informasi yang diberikan kepada *user*, sedangkan kriteria ICR terdiri dari kriteria-kriteria dalam ICR yang harus dipenuhi dalam mencapai target kinerja.

Untuk mencapai target kinerja yang sudah ditetapkan pada *Assesment Kontrak Kinerja* memerlukan kriteria-kriteria yang harus dipenuhi oleh ICR dalam menghasilkan nilai standar tertentu pada unit. Di dalam dokumen kriteria ICR menjelaskan poin-poin target yang perlu dicapai dan dipenuhi dalam hal keamanan sistem informasi. SINFO mengalami kesulitan dalam memenuhi kriteria tersebut karena tidak terdapat pengolahan keamanan informasi yang sesuai standar agar kriteria tersebut dapat terpenuhi. Apabila kriteria pada ICR tidak dipenuhi, maka SINFO tidak dapat melakukan *improvement* terhadap sistem keamanan informasi PT PJB Unit Pembangkit Gresik. Dampak yang ditimbulkan apabila tidak terdapat pengolahan mengenai keamanan sistem informasi dapat membuat ICR mengalami hambatan pada layanan keamanan informasi dan kondisi kualitas dari teknologi informasi khususnya keamanan informasi pada PT PJB Unit Pembangkit Gresik. Pemenuhan kriteria ICR dan OFI sangat diperlukan dalam menentukan nilai target unit sebagai dasar dari *Assesment Kontrak Kinerja*.

Untuk memecahkan masalah keamanan informasi ICR pada PT PJB Unit Pembangkit Gresik, SINFO membutuhkan sebuah perencanaan sistem manajemen keamanan informasi pada ICR untuk mengelola keamanan informasi yang sesuai standar. Proses ini memiliki tujuan untuk memberikan pedoman pengolahan untuk mengantisipasi keamanan informasi pada ICR. Luaran dari perencanaan sistem

manajemen keamanan informasi adalah dibuatnya dokumen perencanaan SMKI. Dokumen tersebut berfungsi untuk mengelola teknologi keamanan informasi dalam proses perlindungan terhadap aspek keamanan informasi yang nantinya dapat memenuhi kriteria ICR sehingga ICR dapat menentukan nilai untuk target unit pada *Assesment Kontrak Kinerja*. Dalam dokumen kriteria ICR, menjelaskan kriteria yang harus di dukung dari kesiapaan pengamanan sistem informasi. Kesiapan pengamanan sistem informasi tersebut terdiri atas beberapa area yang harus dipenuhi. Dalam ISO 27001:2005 menjelaskan tentang dasar kebutuhan untuk keamanan informasi termasuk dalam hal kesiapan pengamanan sistem informasi serta tahapan dalam penerapan sistem manajemen keamanan informasi (ISMS). Dalam pembuatan perencanaan sistem manajemen keamanan informasi ini akan menggunakan *standard* ISO/IEC 27001:2005 *Information Security Management System Requirments* dan ISO/IEC 27002:2005 *Code Of Practice For ISMS*. Pemilihan kedua *standard* ini dipilih karena pada ISO/IEC 27001:2005 menjelaskan persyaratan yang harus dipenuhi dalam membangun ISMS, sedangkan ISO/IEC 27002:2005 berfungsi untuk menentukan kontrol objektif dan kontrol yang dibutuhkan dalam perencanaan dan persyaratan SMKI yang ada dalam ISO/IEC 27001:2005 dalam menyediakan serta mengelola pengamanan sistem informasi ICR di PT PJB Unit Pembangkit Gresik.

Penelitian perencanaan sistem manajemen keamanan informasi ini akan menghasilkan dokumen-dokumen pada perencanaan SMKI meliputi laporan asesmen resiko (*risk assessment*), prosedur, instruksi kerja, dan dokumen lain terkait pada tahap perencanaan sistem manajemen keamanan informasi pada PT PJB Unit Pembangkit Gresik yang menggunakan *standard* ISO/IEC 27001:2005

dan ISO/IEC 27002:2005. Perencanaan sistem manajemen keamanan informasi yang akan dihasilkan diharapkan dapat membantu dalam mengelola keamanan informasi dalam memenuhi kriteria ICR untuk *improvement* kualitas keamanan sistem informasi

## 1.2 Rumusan Masalah

Dengan melihat latar belakang yang telah dibahas, maka dapat dirumuskan permasalahan PT PJB Unit Pembangkit Gresik yang akan diselesaikan pada penelitian ini adalah bagaimana merencanakan sistem manajemen keamanan informasi pada *Information Capital Readiness* PT PJB Unit Pembangkit Gresik.

## 1.3 Batasan Masalah

Dalam penelitian di PT PJB Unit Pembangkit Gresik, lingkup pembahasan dibatasi pada :

1. Perencanaan sistem manajemen keamanan sistem informasi dilakukan pada kinerja proses untuk sub bagian Sumber Daya Manusia khususnya bagian *Information Capital Readiness (ICR)*.
2. Perencanaan sistem manajemen keamanan sistem informasi pada ICR didasarkan pada *standard* ISO/IEC 27001:2005 *Information Security Management System Requirments* dan ISO/IEC 27002:2005 tentang *Code Of Practice for ISMS*

#### 1.4 Tujuan

Tujuan dalam penelitian ini adalah merencanakan sistem manajemen keamanan informasi pada *Information Capital Readiness* PT PJB Unit Pembangkit Gresik yang menghasilkan dokumen perencanaan sistem manajemen keamanan informasi meliputi laporan asesmen risiko, kebijakan, prosedur, instruksi kerja, dan rekam kerja.

#### 1.5 Manfaat

Adapun manfaat dari penelitian yang akan dibangun nantinya adalah :

1. Membantu SINFO dalam mengelola keamanan informasi yang akan dibangun dan mengacu ke dalam standar internasional ISO 27001:2005 tentang *ISMS Requirements* dan ISO/IEC 27002:2005 tentang *Code Of Practice For ISMS*.
2. Membantu memberikan pedoman dalam memenuhi kriteria keamanan sistem informasi ICR pada SINFO di PT. PJB Unit Gresik.
3. Membantu PT PJB UP Gresik dalam melakukan *improvement* keamanan informasi untuk bersaing dalam dunia global.

#### 1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan laporan tugas akhir ini dibagi menjadi bab-bab dengan rincian sebagai berikut :

##### BAB I PENDAHULUAN

Dalam bab ini dijelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan, manfaat, dan sistematika penulisan.

##### BAB II KAJIAN PUSTAKA

Dalam bab ini dijelaskan landasan-landasan teori yang digunakan untuk membantu menyelesaikan masalah yang meliputi antara lain Sistem Manajemen Keamanan Informasi (SMKI), ISO 27001:2005, ISO 27002:2005, SOP, Instruksi Kerja, *Risk Assessment*, *Assessment Kontrak Kinerja*, dan *Information Capital Readiness*.

### BAB III METODE PENELITIAN

Dalam bab ini dijelaskan tahap-tahap yang dikerjakan dalam penyelesaian tugas akhir mulai dari tahap awal, tahap pengembangan, dan tahap akhir.

### BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini dijelaskan tentang hasil yang telah diperoleh dari analisa data untuk dokumen dalam perencanaan sistem manajemen keamanan informasi.

### BAB V PENUTUP

Dalam bab ini dijelaskan tentang kesimpulan dari pembahasan permasalahan yang telah dilakukan dan saran dalam perencanaan sistem manajemen keamanan informasi.