BAB 1
PENDAHULUAN

1.1 Latar Belakang

Politeknik Pos Indonesia adalah institusi pendidikan tinggi yang didirikan oleh Yayasan Pendidikan Bhakti Pos Indonesia (YPBPI), pada tanggal 5 Juli 2001, berdasarkan SK Mendiknas No. 56/D/O/2001. Dengan visi, menjadi perguruan tinggi vokasi yang unggul secara nasional dalam bidang logistik dan manajemen rantai pasok pada tahun 2020.

Informasi dihasilkan dari keterkaitan beberapa elemen, misalnya berupa data, *software, hardware,* dan SDM. Informasi yang dihasilkan digunakan sebagai data untuk menghasilkan informasi baru oleh pihak-pihak yang berkepentingan. Pengelolaan berbagai informasi yang ada di Politeknik Pos Indonesia, tidak lagi menggunakan sistem manual, melainkan sudah terkomputerisasi. Hal tersebut merupakan tanggung jawab divisi TIK Politeknik Pos Indonesia.

Pengelolaan dan penggunaan informasi yang ada di Politeknik Pos Indonesia masih belum dianggap aman. Hal tersebut disebabkan karena belum terpenuhinya kriteria CIA (*Confidentally, Integrity, Availability*) yang menjadi fungsi pada pengelolaan keamanan informasi. Hal tersebut juga disebabkan karena ketidaktersediaan kebijakan yang dapat digunakan untuk mencegah dan mengantisipasi adanya berbagai insiden yang tidak diharapkan.

Dalam penelitian ini, ISO 27001:2013 digunakan untuk sistem manajemen keamanan informasi yang berfokus pada kontrol kebijakan keamanan, pengaturan keamanan informasi, keamanan sumber daya manusia, pengelolaan aset, dan pengendalian akses. Hal-hal tersebut akan berguna untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi yang sesuai dengan kebutuhan bisnis, peraturan, dan hukum yang berlaku.

1.2 Rumusan Masalah

Rumusan masalah berdasarkan latar belakang tersebut, adalah:

1. Apakah kebijakan keamanan informasi pada divisi TIK Politeknik Pos Indonesia sudah sesuai dengan kebutuhan organisasi, sesuai dengan standar ISO 27001:2013 serta dapat diukur tingkat kematangannya?
2. Apakah pengaturan keamanan informasi yang dikelola oleh divisi TIK Politeknik Pos Indonesia sudah sesuai dengan standar ISO 27001:2013 dan menghasilkan sesuatu yang dapat diukur dan dinilai efektif?
3. Apakah keamanan sumber daya manusia pada divisi TIK Politeknik Pos Indonesia sudah sesuai dengan ISO 27001:2013 dan menghasilkan sesuatu yang dapat diukur dan dinilai efektif?
4. Apakah pengelolaan manajemen aset pada divisi TIK Politeknik Pos Indonesia sudah diterapkan sesuai dengan ISO 27001:2013 dan menghasilkan sesuatu yang dapat diukur dan dinilai efektif??
5. Apakah pengendalian akses pada divisi TIK Politeknik Pos Indonesia sudah diterapkan sesuai dengan ISO 27001:2013 dan menghasilkan sesuatu yang dapat diukur dan dinilai efektif?

1.3 Tujuan Pembahasan

Tujuan dilakukannya penelitian adalah:

1. Membuat analisa dan pengukuran tingkat kematangan klausul *information security policies* (kebijakan keamanan informasi) pada divisi TIK Politeknik Pos Indonesia berdasarkan ISO 27001:2013.
2. Membuat analisa dan pengukuran tingkat kematangan klausul *organization of information security* (pengaturan keamanan informasi) pada divisi TIK Politeknik Pos Indonesia berdasarkan ISO 27001:2013.
3. Membuat analisa dan pengukuran tingkat kematangan klausul *human resources security* (keamanan sumber daya manusia) pada divisi TIK Politeknik Pos Indonesia berdasarkan ISO 27001:2013.
4. Membuat analisa dan pengukuran tingkat kematangan klausul *asset management* (manajemen aset) pada divisi TIK Politeknik Pos Indonesia berdasarkan ISO 27001:2013.

5. Membuat analisa dan pengukuran tingkat kematangan klausul *access control* (pengendalian akses) pada divisi TIK Politeknik Pos Indonesia berdasarkan ISO 27001:2013.

1.4 Ruang Lingkup

Ruang lingkup dalam penelitian tugas akhir ini, adalah:

1. Penelitian ini dilakukan pada divisi TIK Politeknik Pos Indonesia.
2. Penelitian ini tidak membahas tentang *risk analysis* dan *risk management.*
3. Pembahasan mengacu pada penggunaan ISO 27001:2013.
4. Penelitian ini menggunakan 5 kontrol subjek klausul pada ISO 27001:2013, yaitu:
   a. *Annex 5 – Information Security Policies*
      i) *A.5.1 Management direction for information security*
         (1) A.5.1.1 Policies for information security
         (2) A.5.1.2 Review of the policies for information security
   b. *Annex 6 – Organization of Information Security*
      i) *A.6.1 Internal Organization*
         (1) A.6.1.1 Information security roles and responsibilities
         (2) A.6.1.2 Segregation of duties
         (3) A.6.1.3 Contact with authorities
         (4) A.6.1.4 Contact with special interests groups
         (5) A.6.1.5 Information security in project management
      ii) *A.6.2 Mobiles devices and teleworking*
         (1) A.6.2.1 Mobile device policy
         (2) A.6.2.2 Teleworking
   c. *Annex 7 – Human Resources Security*
      i) *A.7.1 Prior to employment*
         (1) A.7.1.1 Screening
         (2) A.7.1.2 Terms and conditions of employment
      ii) *A.7.2 During employment*
         (1) A.7.2.1 Management responsibilities
         (2) A.7.2.2 Information security awareness, education and training

(3) *A.7.2.3 Disciplinary process*

iii) *A.7.3 Termination and change of employment*

(1) *A.7.3.1 Termination or change of employment responsibilities*

d. *Annex 8 – Asset Management.*

i) *A.8.1 Responsibility for assets*

(1) *A.8.1.1 Inventory of assets*

(2) *A.8.1.2 Ownership of assets*

(3) *A.8.1.3 Acceptable of use assets*

(4) *A.8.1.4 Return of assets*

ii) *A.8.2 Information Classification*

(1) *A.8.2.1 Classification of information*

(2) *A.8.2.2 Labelling of information*

(3) *A.8.2.3 Handling of assets*

iii) *A.8.3 Media Handling*

(1) *A.8.3.1 Management of removable media*

(2) *A.8.3.2 Disposal of media*

(3) *A.8.3.3 Physical media transfer*

e. *Annex 9 – Access Control*

i) *A.9.1 Business requirements of access control*

(1) *A.9.1.1 Access control policy*

(2) *A.9.1.2 Access to networks and network services*

ii) *A.9.2 User access management*

(1) *A.9.2.1 User registration and de-registration*

(2) *A.9.2.2 User access provisioning*

(3) *A.9.2.3 Management of privileged access rights*

(4) *A.9.2.4 Management of secret authentication information of users*

(5) *A.9.2.5 Review of user access rights*

(6) *A.9.2.6 Removal or adjustment of access rights*

iii) *A.9.3 User responsibilities*

(1) *A.9.3.1 Use of secret authentication information*

iv) *A.9.4 System And Application Access Control*

(1) *A.9.4.1 Information access restriction*

(2) A.9.4.2 Secure log-on procedures

(3) A.9.4.3 Password management system

(4) A.9.4.4 Use of privileged utility programs

(5) A.9.4.5 Access control to program source code

1.5 Sumber Data

Penelitian ini menggunakan data primer dan data sekunder. Data-data tersebut dihasilkan dengan menggunakan metode triangulasi, yaitu:

1. Wawancara terstruktur

   Adalah teknik untuk mendalami sebuah informasi melalui informan. Selama proses wawancara berlangsung, alat perekam suara digunakan sebagai media untuk melakukan dokumentasi. Narasumber wawancara adalah pegawai yang bertanggung jawab pada bidangnya masing-masing.

2. Observasi

   Dilakukan dengan melakukan pengecekan langsung ke lapangan, mengklarifikasi antara pengakuan narasumber dengan kondisi di lapangan secara langsung.

3. Dokumentasi

   Teknik pengumpulan data ini dilakukan dengan maksud untuk mengumpulkan *evidence* yang menguatkan hasil penilaian. Proses dokumentasi dilakukan dengan bantuan alat perekam suara, kamera, serta dokumen instansi.

1.6 Sistematika Penyajian

Sistematika penyajian tugas akhir ini diuraikan sebagai berikut:

BAB I PENDAHULUAN, bab ini menjelaskan gambaran singkat mengenai latar belakang, rumusan masalah, tujuan pembahasan, ruang lingkup kajian, sumber data yang digunakan, serta sistematika penyajian.

BAB II KAJIAN TEORI, bab ini menjelaskan pembahasan mengenai dasar atau kajian teori yang digunakan dalam penyusunan tugas akhir.

BAB III ANALISIS DAN HASIL PENELITIAN, bab ini menjelaskan tentang analisis manajemen keamanan informasi yang dilakukan pada divisi TIK Politeknik Pos Indonesia dengan batasan-batasan yang telah ditentukan.

BAB IV SIMPULAN DAN SARAN, bab ini merupakan bagian penutup pada laporan yang berisi penjelasan mengenai simpulan dan saran berupa rekomendasi yang berguna untuk organisasi sesuai dengan ruang lingkup penelitian tugas akhir yang dikerjakan.