

## **BAB I**

### **PENDAHULUAN**

#### **1.1 Latar Belakang**

Tata kelola keamanan teknologi sebagai sarana sistem informasi, saat ini dapat dikatakan menjadi tuntutan dan kebutuhan di setiap instansi dan organisasi, baik itu didalam pemerintahan, industri, perusahaan, seluruh level pendidikan, seluruh aspek kesehatan, dan lainnya. Teknologi informasi bisa meningkatkan efisiensi juga tingkat efektifitas organisasi untuk menciptakan sebuah layanan yang berkualitas berdasarkan proses bisnisnya yang dimiliki. Hambatan dan gangguan yang dapat terjadi untuk sebuah kegiatan aktivitas yang terkait pada aset organisasi adalah risiko apabila terjadi gangguan pada keamanan informasi. Informasi yang selama ini dimiliki oleh pihak instansi dan organisasi bisa saja dicuri dan disalah gunakan untuk kepentingan pribadi maupun golongan. Kekuatan keamanan informasi dikontrol dengan sistem manajemen keamanan informasi agar dapat sesuai prosedur. Organisasi dapat menunjukkan bahwa mereka memiliki kontrol internal yang baik proses keuangan, dan yang lebih penting bahwa mereka dapat membantu mengurangi risiko keamanan informasi dengan beroperasi di bawah satu sistem. Standar ISO 27001 adalah standar yang diharapkan dapat digunakan untuk membantu terutama pihak manajemen merencanakan dan menerapkan keamanan informasi sesuai aturan (ISO/IEC 27001)

Salah satu instansi di bidang pendidikan yang mengikuti perkembangan teknologi informasi adalah Universitas Pembangunan Nasional “Veteran” Jakarta. Unit Pelaksana Teknis (UPT) terkait Teknologi Informasi dan Komunikasi (TIK) Pusat Komunikasi (PUSKOM) memiliki Sistem informasi akademik yang merupakan unsur penunjang sistem informasi terdiri dari aset utama dan aset pendukung informasi. Keamanan dapat berasal dari gangguan yang bersifat fisik dan non fisik. Berdasarkan wawancara, Kepala

**Darma Yanto Putra, 2020**

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS**

**PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Sistem Informasi

[[www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id)]

dan Pegawai UPT TIK memerlukan panduan rekomendasi sesuai standar dalam arahan manajemen untuk kebijakan keamanan informasi, prosedur yang dapat diberlakukan dan kebijakan dalam dukungan keamanan pada aset informasi dan *maintenance* aset pendukung informasi secara rutin, juga prosedur dan akses oleh pihak eksternal, Terjadinya kerusakan di beberapa aset penting untuk mendukung jalannya kegiatan sistem informasi, belum pernah dilakukan analisis/audit sistem manajemen keamanan informasi di UPT TIK UPN “Veteran” Jakarta, selain itu ditemukan kondisi kurangnya perangkat untuk mendukung jalannya kegiatan sistem informasi pada ruangan kantor. Penulis memiliki pengalaman bekerja dengan auditor dan membantu kegiatan audit perusahaan, tertarik untuk membantu UPT TIK untuk memberikan rekomendasi dan melakukan audit untuk memberikan hasil yang menggambarkan seberapa besar penilaian yang didapat oleh organisasi, kemudian akan memberikan rekomendasi yang tentu saja di analisis terlebih dahulu dari berbagai sumber. Audit atau pemeriksaan adalah kegiatan evaluasi sebuah organisasi, produk, sistem, atau proses. Audit dilaksanakan dan dilakukan oleh pihak yang berkompeten, tidak memihak, dan objektif. Tujuan mengadakan audit yaitu untuk menjalankan verifikasi pada objek dari audit telah dilakukan dan berjalan sesuai dengan standar, sesuai regulasi, dan praktik yang telah disetujui dan tentu saja diterima. Sistem manajemen keamanan informasi (SMKI) telah diakui baik dalam negeri maupun mancanegara. ISO/IEC 27001 menetapkan poin kontrol keamanan informasi yang akan dibahas dalam penelitian ini. ISO/IEC

27001:2013 menyajikan standar yang diperbarui dan memberi panduan untuk evaluasi kinerja.

ISO/IEC 27001 menyediakan bentuk kerangka kerja untuk menjaga normalnya kegiatan menggunakan teknologi, sistem manajemen yang dapat memungkinkan perusahaan atau sebuah organisasi memastikan pengukuran keefektifan keamanan informasi, menyimpan

**Darma Yanto Putra, 2020**

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS**

**PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Sistem Informasi

[[www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id)]

keamanan informasi yang rahasia, melindungi perusahaan dan organisasi, melindungi aset, Pertukaran informasi yang aman, mengelola dan meminimalisir eksposur terhadap resiko.

Keamanan informasi ISO/IEC 27001 adalah kewajiban instansi yang merupakan kebutuhan organisasi untuk menjaga keamanan informasi. Maka dari itu peneliti akan melakukan audit dan memberikan rekomendasi mengenai keamanan sistem informasi akademik UPN

“Veteran’

Jakarta. Peneliti mengajukan judul skripsi “Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional

“Veteran Jakarta” yang diharapkan mampu memberikan rekomendasi kebijakan untuk meningkatkan keamanan informasi pada sistem informasi akademik UPN “Veteran” Jakarta yang kemudian dapat membantu UPT TIK untuk melakukan audit secara resmi.

## **1.2 Rumusan Masalah**

Rumusan masalah yang dapat diambil dari penulisan skripsi ini yaitu:

1. Apakah kebijakan dan prosedur yang sekarang dilaksanakan sudah memenuhi aspek keamanan informasi berdasarkan ISO/IEC 27001:2013?.
2. Apakah kepatuhan/ketaatan sebuah organisasi kepada tindakan dan pencapaian yang harusnya diterapkan sudah memenuhi sebuah keamanan informasi?.
3. Apakah sebuah saran dan rekomendasi terhadap kebijakan juga prosedur yang peneliti buat dapat membuat peningkatan keamanan informasi?.
4. Bagaimana melakukan analisis/audit sistem manajemen keamanan informasi dengan menggunakan ISO/IEC 27001 pada UPT TIK UPN “Veteran” Jakarta?.

### 1.3 Ruang Lingkup

Adapun ruang lingkup dari penulisan skripsi ini adalah:

1. Analisis sistem manajemen keamanan informasi dilakukan pada kantor UPT TIK UPN “Veteran” Jakarta
2. Penelitian ini fokus pada analisis keamanan Sistem Informasi (SI) Akademik yang terdiri dari aset utama dan aset pendukung juga tata kelola manajemen keamanan informasi di kantor UPT TIK UPN “Veteran” Jakarta
3. Penggunaan ISO/IEC 27001: 2013 Sebagai standar audit keamanan informasi
4. Penggunaan *checklist* untuk kegiatan audit yang berasal dari panduan ISO/IEC 27001
5. Kegiatan Identifikasi aset dari hasil wawancara dan analisis dokumen dengan staff TI dan kepala UPT TIK
6. Data yang digunakan adalah hasil wawancara, kuesioner, dan analisis dokumen pada bagian IT Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi
7. Metodologi Plan, Do, Check, Act (PDCA) pada ISO/IEC 27001 digunakan di penelitian ini
8. Tools kuesioner skala pengukuran tingkat kematangan pada ISO 27001 menggunakan *risk assessment and treatment* dengan pendekatan metode kualitatif
9. Tools yang digunakan untuk mengukur efektivitas menggunakan metode SSE CMM

(System Security Engineering Capability Maturity Model) pendekatan ISO/IEC 27001

Darma Yanto Putra, 2020

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS**

**PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Sistem Informasi

[[www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id)]

10. Output yang dihasilkan dari penelitian ini adalah, temuan dan rekomendasi terkait keamanan sistem informasi UPT TIK UPN “Veteran” Jakarta

#### **1.4 Tujuan Penelitian**

Tujuan umum penelitian di UPT TIK adalah melakukan analisis/audit mengenai SMKI dengan menggunakan ISO/IEC 27001 pada UPT TIK dan mengetahui apakah sebuah kebijakan dengan prosedur yang sekarang dilaksanakan sudah memenuhi aspek keamanan informasi?, Juga mengetahui, apakah organisasi patuh terhadap capaian dan tindakan yang diterapkan? apakah sudah memenuhi sebuah aspek keamanan informasi agar menghasilkan temuan dan rekomendasi dalam peningkatan sistem manajemen keamanan informasi SIAKAD dan UPT TIK.

#### **1.5 Manfaat Penelitian**

1. Manfaat Teoritis.

1.1. Memberi hasil dokumentasi audit keamanan sistem informasi Sistem Informasi

Akademik UPN “Veteran” Jakarta

1.2. Menghasilkan rekomendasi lebih lengkap mengenai kebijakan dan prosedur terhadap aspek – aspek keamanan Sistem Informasi

1.3. Meningkatkan kreatifitas berfikir dan menganalisa suatu masalah di proses bisnis

1.4. Informasi yang didapat dari hasil analisis sistem menjadi bahan untuk mengambil keputusan untuk membangun kebijakan sistem informasi

1.5. Memberikan gambaran untuk meningkatkan keamanan sistem dan teknologi informasi

**Darma Yanto Putra, 2020**

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS**

**PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Sistem Informasi

[[www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id)]

## UPT TIK

### 2. Manfaat Praktis

- 2.1. Membantu perusahaan mengetahui kondisi sistem manajemen keamanan informasi saat ini
- 2.2. Membina kerjasama yang baik antara lingkungan akademis dan lingkungan kerja di lingkup UPN “Veteran” Jakarta
- 2.3. Membantu misi UPN “Veteran” Jakarta poin d, yaitu mewujudkan budaya organisasi dan budaya mutu dengan menerapkan sistem audit dan manajemen risiko yang kredibel

### 1.6 Batasan Masalah

Berikut batasan masalah dalam skripsi ini, yaitu:

1. Kegiatan penilaian tingkat keamanan informasi dilakukan dengan menggunakan Standar SNI/IEC/ISO 27001 yang terdiri dari area Sistem Informasi Akademik juga faktor pendukungnya, dan prosedur tata kelola manajemen keamanan informasi.
2. Identifikasi aset UPT TIK UPN “Veteran” Jakarta dan menilai berdasarkan aspek keamanan informasi *Confidentiality, Integrity, dan Availability*

### 1.7 Metodologi Penelitian

Penelitian ini menggunakan beberapa metode untuk mendapatkan informasi, berikut adalah metode pada penelitian ini

#### 1. Desain Penelitian

Pada desain penelitian, penulis menggunakan metode kualitatif, untuk mendapatkan data deskriptif baik lisan maupun tulisan pada UPT TIK

## 2. Metode Pengumpulan Data

### A. Data primer

Yaitu didapat langsung yang berasal dari UPT TIK yaitu:

- a. Observasi, dimana penulis secara langsung mendapat data dan informasi disaat melihat dan mengamati secara langsung.
- b. Wawancara, penulis secara langsung berkomunikasi untuk mendapatkan informasi yang lebih khusus ke permasalahan.
- c. Kuesioner, penulis melakukan pengumpulan data dengan memberi pertanyaan kepada pihak UPT TIK UPN “Veteran” Jakarta

### B. Data sekunder

Yaitu berasal dari *study literature* dimana penulis akan mempelajari penelitian yang sejenis juga membaca dan memahami dokumen serta buku.

## 3. Metode Analisis

Penelitian ini menggunakan analisis data deskriptif dan kualitatif.

## 4. Metode Analisis Sistem Manajemen Keamanan Informasi

Terdapat beberapa tahapan penerapan SMKI berdasarkan ISO/IEC 27001 yaitu: *a.*

### *Plan*

Penulis akan melakukan perencanaan dan perancangan manajemen keamanan informasi

### *b. Do*

Penulis akan melakukan identifikasi risiko, ancaman dan kelemahan serta analisis risiko

*c. Check*

Penulis akan melihat penerapan keamanan informasi pada klausul ISO 27001, penentuan kemampuan serta tingkat kematangan (maturity level). *d. Act* Penulis akan menentukan gap (*gap analysis*) dan memberikan rekomendasi berdasar kepada ISO 27001.

## **1.8 Luaran Yang Diharapkan**

Dengan adanya audit ini diharapkan dapat menghasilkan luaran yang bermanfaat, yaitu:

1. Sistem Informasi Akademik memiliki mutu di masa depan yang lebih baik
2. Para pegawai PUSKOM menerima rekomendasi dan mendapatkan manfaat dari kegiatan audit ini.

## **1.9 Sistematika Penulisan**

Sistematika penulisan skripsi ini dibagi dalam 5 bab, masing masing bab diuraikan sebagai berikut:

### **BAB 1 PENDAHULUAN**

Bab ini terdapat penjelasan mengenai latar belakang, rumusan masalah, Ruang Lingkup, tujuan penelitian, manfaat penelitian, batasan masalah, metodologi penelitian, luaran yang diharapkan dan sistematika penulisan

### **BAB 2 TINJAUAN PUSTAKA**

Bab ini berisi uraian teori – teori dasar penelitian secara detail, dapat berupa metode, teknik, konsep, prosedur atau definisi yang bersangkutan dengan topik penelitian.

### **BAB 3 METODE PENELITIAN**

Bab ini terdapat penjelasan mengenai tahapan penelitian dengan menggunakan PDCA, deskripsi, untuk mencapai tujuan penelitian.

### **BAB 4 HASIL DAN PEMBAHASAN**



Bab ini berisi laporan dan pembahasan hasil penelitian.

## **BAB 5 PENUTUP**

Bab ini berisi kesimpulan dan saran

## **DAFTAR PUSTAKA**

Berisi sumber – sumber yang penulis gunakan untuk menulis penelitian, baik literature dari internet, buku panduan, jurnal, atau media lainnya.

**Darma Yanto Putra, 2020**

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS**

**PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Sistem Informasi

[[www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id)]