AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI - ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

Darma Yanto Putra [1], Theresia Wati[2], I Wayan Widi P[3]
Jurusan Sistem Informasi S1, Fakultas Ilmu Komputer Universitas Pembangunan Nasional 'Veteran Jakarta
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia
E-mail: darmaputra728@gmail.com[1], theresiawati@upnvj.ac.id[2], wayan.widi@upnvj.ac.id[3].

Abstract -- The occurrence of damage to information system assets, do not have information system security policy that must be applied in security also supervision of information academic service assets, the possibility of threat and risk against information system support. This research have a purpose to plan Information Security Management System (ISMS) with its use as guidelines of information system policy in UPT TIK UPN "Veteran" Jakarta. The main discussion in this research is Information Security Management System (ISMS) analysis using ISO/IEC 27001 to UPT TIK UPN "Veteran" Jakarta Information Academic System. This research using Plan, Do, Check, and Act methods in collecting, analyze, and processing data. The result of this research is maturity level of ISO 27001 with average located in level two, be expected this research would be helpfull to provide a recomendation to control information security as guidance and procedure for implementation of information security policy.

Keywords: ISO 27001, Information Security Management System (ISMS), Plan, Do, Check, Act

Abstrak -- Terjadinya kerusakan pada aset sistem informasi, tidak memiliki kebijakan tentang keamanan informasi yang memiliki keharusan diterapkan didalam keamanan juga pengawasan aset pelayanan informasi akademik, juga kemungkinan ancaman dan risiko terhadap dukungan sistem informasi. Penelitian ini memiliki tujuan untuk perencanaan Sistem Manajemen Keamanan Informasi (SMKI) dimana penggunaannya sebagai pedoman terhadap kebijakan keamanan informasi di UPT TIK UPN "Veteran" Jakarta. Bahasan dalam penelitian ini adalah analisis Sistem Manajemen Keamanan Informasi (SMKI) dengan ISO/IEC 27001 pada sistem informasi akademik UPT TIK UPN "Veteran" Jakarta. Penelitian ini menggunakan metode Plan, Do, Check, dan Act dalam kegiatan mengumpulkan, menganalisis, dan mengolah data. Hasil penelitian ini adalah tingkat kematangan ISO 27001 dengan rata – rata berada di level dua, diharapkan penelitian ini sangat membantu memberikan rekomendasi terhadap kontrol keamanan informasi sebagai pedoman dan prosedur untuk menerapkan kebijakan keamanan informasi.

Kata kunci: ISO 27001, Sistem Manajemen Keamanan Informasi (SMKI), Plan, Do, Check, Act
.

I. PENDAHULUAN

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. [1]

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 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 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.

Penelitian yang dilakukan oleh penulis bertujuan untuk mendukung adanya pengamanan SMKI di masa yang akan datang, berikut aspek pendukung SMKI: perencanaan (Planning), keamanan (Security Policy), program (prosedur dan proses), penilaian risiko (risk assessment), Sumber Daya Manusia /SDM (People) dan tanggung jawab (responsibility) [2], sebuah keamanan sistem informasi harus menjaga informasi dari bermacam – macam aspek untuk menjamin kelangsungan perusahaan dan organiasasi serta meminimalisir kerusakan akibat ancaman. [3].

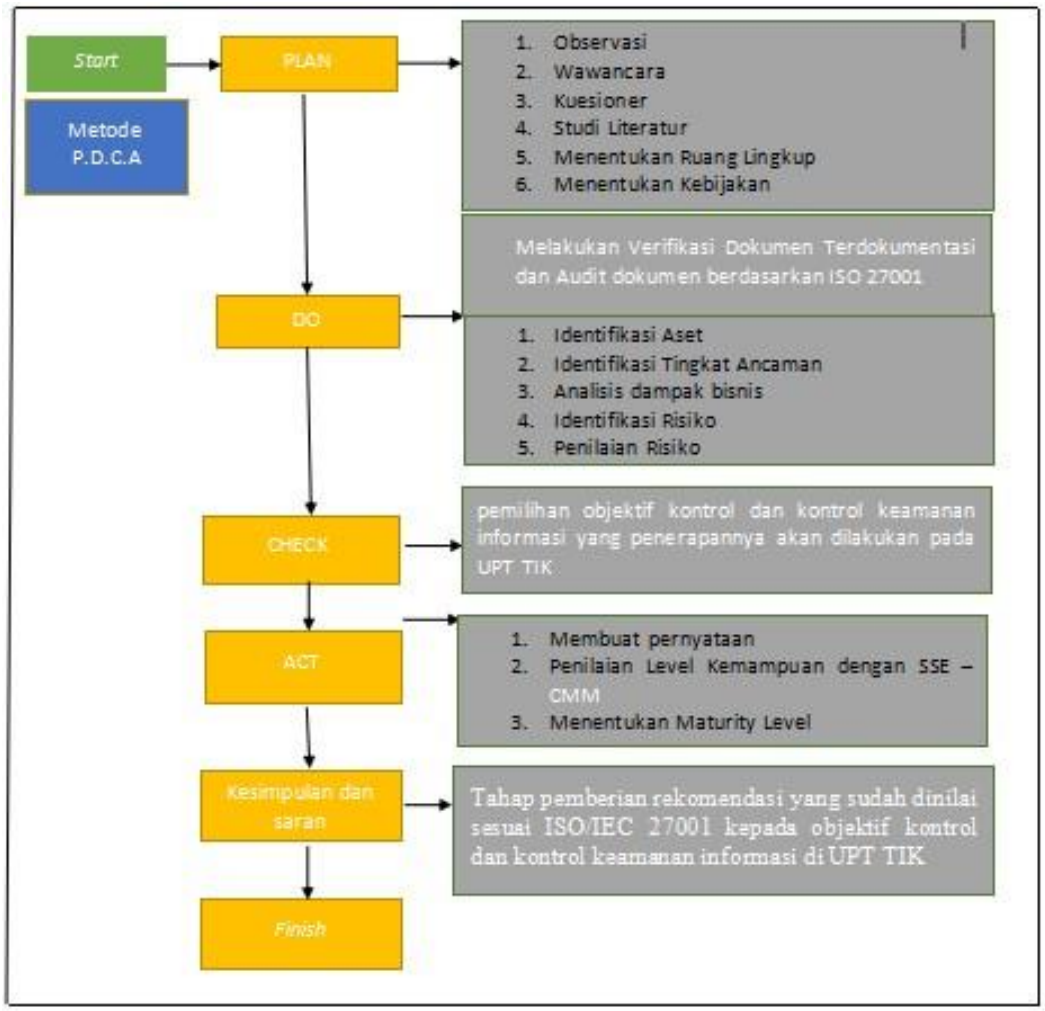
Penelitian yang dilakukan oleh Mukhlis Amin pada tahun 2014 yang berjudul “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MDCA)” dengan permasalahan yang diangkat ialah tingkat kesadaran keamanan informasi bagi masyarakat yang dikhususkan kepada Pegawai Negeri Sipil. Penelitian tersebut menggunakan variabel seperti selalu taat pada aturan perusahaan, Menjaga kerahasiaan password dan PIN, Menggunakan e-mail dan internet dengan bijaksana, berhati-hati menggunakan perangkat seluler, melaporkan insiden keamanan informasi, menyadari konsekuensi setiap tindakan, selalu

melakukan backup data. Hasil dari penelitian tersebut menunjukkan bahwa tingkat kesadaran keamanan informasi di Pemkot Makassar secara keseluruhan berada pada level "sedang" sehingga perlu dimonitor untuk kemungkinan dilakukan pembenahan. Hasil penelitian juga menunjukkan bahwa tingkat kesadaran setiap dimensi pengetahuan, sikap dan perilaku berada pada level yang memuaskan. Namun demikian, hasil pengukuran juga menunjukkan bahwa ada beberapa area kesadaran keamanan informasi yang tidak memuaskan sehingga perlu dilakukan tindakan seperti menjaga kerahasiaan password, pelaporan insiden keamanan, kebijaksanaan menggunakan e-mail dan internet.

Penelitian lain yang dilakukan oleh Endi Lastyono dkk pada tahun 2014 dengan judul "Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. dengan Menggunakan Indeks Keamanan Informasi (KAMI). Permasalahan yang diangkat dalam penelitian ini ialah kondisi keamanan informasi di Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Hasil penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi di Pemkot Makassar secara keseluruhan berada pada level "sedang" sehingga perlu dimonitor untuk kemungkinan dilakukan pembenahan. Hasil penelitian juga menunjukkan bahwa tingkat kesadaran setiap dimensi pengetahuan, sikap dan perilaku berada pada level yang memuaskan. Namun demikian, hasil pengukuran juga menunjukkan bahwa ada beberapa area kesadaran keamanan informasi yang tidak memuaskan sehingga perlu dilakukan tindakan, seperti menjaga kerahasiaan password, pelaporan insiden keamanan, dan bijaksana menggunakan e-mail dan internet

II.METODOLOGI PENELITIAN

Dalam metodologi penelitian ini, tahapan penelitian yang digunakan adalah menggunakan metode *Plan, Do, Check*, dan *Act*. Dimana akan terlihat seperti gambar 1



Gambar 1. Tahapan Penelitian

Pelaksanaan kegiatan audit dibagi menjadi empat tahap kegiatan yaitu *Plan*, *Do*, *Check*, *Act*. Tahap Plan bertujuan sebagai persiapan sebelum melakukan audit dan analisis pada sistem informasi akademik seperti misalnya mengetahui sistem informasi akademik dan gambaran instansi dan organisasi sehingga dapat diketahui siapa dan permasalahan apa yang perlu diaudit. Tahap Do bertujuan untuk mengetahui indikator/kontrol klausul untuk mengukur keamanan informasi dan dokumen yang akan di audit. Tahap check bertujuan untuk mengetahui tingkat kematangan dari masing – masing responden berdasarkan klausul yang dipilih sehingga menghasilkan nilai analisis dengan menggunakan metode SSE – CMM. Tahap Act bertujuan memberikan rekomendasi dari masing masing tahap do dan check juga analisis dengan metode CIA pada aset yang telah dilakukan sebelumnya.

Kegiatan audit menggunakan standar ISO merupakan standar industri dan komersial yang berlaku di dunia. Standar internasional ISO/IEC 27001 digunakan untuk menentukan, menerapkan, mengoperasikan, mengawasi, meninjau, memelihara, dan meningkatkan kebijakan dan dokumen Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan kebutuhan organisasi [4] ISO 27001 dibuat untuk menyediakan persyaratan penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap sistem manajemen keamanan informasi [5]

Penentuan SMKI organisasi membutuhkan penilaian risiko sesuai kebutuhan pada ISO/IEC 27001. Setelah penilaian, sistem kontrol lalu dipilih dari Annex A/Klausal A [6].

A. Studi Literatur

Penulis melakukan pencarian informasi terkait dengan topik permasalahan, penulis mencari jurnal, buku standar ISO 27001 dari BSN, buku terkait, skripsi terdahulu dan media internet.

Tabel 1. Contoh Pernyataan Kontrol Manajemen Aset

A.8	**Manajemen Aset**		
A.8.1	**Tanggung Jawab Terhadap Aset**		
A.8.1.1	**InventarisAset**		
No	**Pernyataan**	**Bobot**	**Nilai**
1	Pihak manajemen telah membuat inventaris aset informasi dan fasilitas pengolahan informasi secara lengkap, akurat, dan terpelihara?		
A.8.1.2	**Kepemilikan,Aset**		
No	**Pernyataan**	**Bobot**	**Nilai**
1	Pihak Manajemen telah melakukan identifikasi dan pencatatan kepemilikan aset		
2	Pihak manajemen memiliki personel yang bertanggung jawab untuk menjaga aset		

Pembobotan dilakukan pada tiap pernyataan dan ditentukan dari panduan implementasi dan tingkat kepentingan dari pernyataan yang ada.

Tabel 2. Bobot Tingkat Kematangan

Tingkat kemampuan	Deskripsi
1	*Performed Informally* (Dilakukan Informal)
2	*Planned and Tracked* (Direncanakan dan Dilacak)
3	*Well Defined* (Didefinisikan dengan baik)
4	Quantitatively Controlled (Dikendalikan secara kuantitatif
5	*Continously Improving* (Ditingkatkan terus menerus)

Kuesioner disebarkan dan dihitung untuk pengukuran tingkat kematangan dengan cara berikut:

1. Rekapitulasi skor tiap pernyataan
2. Menghitung rata – rata dari skor tiap klausul

1.Auditee

Tabel 3. Auditee dokumen

Nama	Jabatan
Sigit Pradana ST,MT	Kepala UPT TIK

2.Penerima Kuesioner SSE – CMM

Tabel 4. Penerima Kuesioer SSE – CMM

Nama	Jabatan
Sigit Pradana ST,MT	Kepala UPT TIK
Farhan Abiyanto	Staff Jaringan dan Perangkat Keras
Asep Saiful Ridwan	Staff Informasi dan Website

III. HASIL DAN PEMBAHASAN

A. Plan

1. **Audit**
   Bertujuan untuk mengumpulkan dan menilai bukti – bukti dengan tujuan menentukan apakah sebuah sistem dapat mengamankan aset, menjaga integritas data dan mendorong capaian tujuan organisasi dengan efektif dan efisien dalam sumber daya. Audit sistem informasi memiliki tujuan untuk mengetahui sejauh mana sistem mempertahankan informasi dan integritas data, sejauh manakah sistem efektif membantu pencapaian organisasi dan sejauh mana optimalisasi penggunaan sumber data optimal. [7]

2. **Analisis CIA**
   Analisis CIA bertujuan untuk mengetahui tingkat risiko kemungkinan kerusakan aset dan bertujuan untuk menghasilkan rekomendasi pada aset pendukung sistem informasi

3. **Analisis SSE – CMM**
   Analisis SSE CMM bertujuan mengetahui tingkat kematangan dari masing – masing pegawai untuk mengetahui kematangan kapabilitas dari masing – masing pegawai di bidang yang berbeda dari penerima angket dengan syarat persetujuan dari kepala upt tik, angket yang diberikan berdasarkan ISO 27001 dan merepresentasikan pekerjaan/jobdesk dari masing – masing pegawai.

B. Do

1. **Pelaksanaan Audit Dokumen**
   Kegiatan audit sistem informasi berdasarkan kontrol yang dipilih pada annex A oleh auditor dan hanya berdasarkan kebijakan dan SOP yang dibuat diatas dilain itu akan ditetapkan dengan keterangan kebijakan belum dibuat. Tabel 5 dan tabel 6 akan memberikan informasi mengenai prosedur dan SOP yang dimiliki oleh Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi.

Tabel 5. Prosedur Operasional Baku UPT TIK

Nomor Kebijakan	Judul
UPNVJ/POB/PUSTIK/001/17-00	POB REKAM DATA
UPNVJ/POB/PUSTIK/002/17-00	POB PEMUTAKHIRAN DATA UNIVERSITAS
UPNVJ/POB/PUSTIK/003/17-00	POB TRANSFORMASI DAN DISTRIBUSI DATA
UPNVJ/POB/PUSTIK/004/17-00	POB PEMELIHARAAN HARDWARE
UPNVJ/POB/PUSTIK/005/17-00	POB PEMBANGUNAN APLIKASI SISTEM

UPNVJ/POB/PUSTIK/006/17-00	POB PENGELOLAAN CONTENT WEBSITE
UPNVJ/POB/PUSTIK/007/17-00	POB DOKUMENTASI SISTEM
UPNVJ/POB/PUSTIK/008/17-00	POB PENGENDALIAN PEMBELIANHARDWARE DAN SOFTWARE
UPNVJ/POB/PUSTIK/009/17-00	POB PEMELIHARAAN SERVER
UPNVJ/POB/PUSTIK/0010/17-00	POB PERBAIKAN SOFTWARE

Tabel 6. Daftar SOP

Nama SOP
SOP Pemasangan Jaringan
SOP Pembuatan dan Pengubahan DNS
SOP Penanganan Gangguan Koneksi Internet Jaringan Lokal
SOP Penanganan Gangguan Koneksi Internet Jaringan Utama
SOP Penanganan Gangguan Server Web
SOP Daftar Email Hosting
SOP Daftar Login Internet
SOP Penitipan Server

Pada tahap *do* akan diberikan hasil audit terhadap dokumen yang dimiliki oleh UPT TIK yang dapat dilihat di tabel 5 dan 6,berikut pada tabel 7 dan 8 akan menjelaskan audit dokumen pada annex A mengenai manajemen aset. Kenali aset organisasi dan penetapan tanggung jawab dalam perlindungan.

Dokumen terkait: UPNVJ/POB/PUSTIK/008/17-00

Tabel 7. Manajemen Aset

A.8.1.1 Inventaris Aset	**Implementasi**	**Justifikasi**
Aset sistem informasi diidentifikasi lalu dicatat dan dipelihara	YA	Aset UPT TIK di inventarisasi dan dicatat Bukti: UPNVJ/POB/PUSTIK/008/17-00
A.8.1.2 Kepemilikan Aset		
Aset yang dipelihara terdapat personel yang bertanggung jawab	YA	Aset yang dipelihara memiliki personel yang bertanggung jawabdalam pemeliharaan Bukti: UPNVJ/POB/PUSTIK/004/17-00 UPNVJ/POB/PUSTIK/009/17-00
A.8.1.3 Penggunaan Yang Dapat Diterima Atas Aset		
Aturan dalam penggunaan aset informasi dan fasilitas pengelolaan informasi	YA	Aset memiliki ketentuan tata cara penggunaan dan dokumentasi penggunaan Bukti: UPNVJ/POB/PUSTIK/009/17-00 UPNVJ/POB/PUSTIK/0010/17-00 UPNVJ/POB/PUSTIK/007/17-00 UPNVJ/POB/PUSTIK/004/17-00
A.8.1.4 Pengembalian Aset		
Pegawai dan pihak eksternal harus mengembalikan aset organisasi yang dikuasai	TIDAK	Rekomendasi:Pengembalian aset organisasi harus didokumentasikan secara formal ketika adanya pemberhentian

	pegawai kecuali milik pribadi atau golongan
Nilai Kepatuhan: Jumlah jawaban sesuai = 3 Jumlah pernyataan = 4 ¾ x 100 = 75%	

Untuk mencegah kerugian, kerusakan, pencurian tanpa hak atas aset dan gangguan operasi organisasi.

Tabel 8. Manajemen Aset

A.11.2.4 PemeliharaanPeralatan	**Implementasi**	**Justifikasi**
Peralatan dipelihara dalam menjamin ketersediaan berkelanjutan	YA	Terdapat kebijakan software dan hardware Bukti: UPNVJ/POB/PUSTIK/009/17-00 UPNVJ/POB/PUSTIK/004/17-00 UPNVJ/POB/PUSTIK/0010/17-00
Nilai Kepatuhan: Jumlah jawaban sesuai = 1 Jumlah pernyataan yang harus ada = 9 (Sesuai jumlah sub klausul ISO 27001) 1/9 x 100 = 11%		

Berikut pada tabel 9 akan menjelaskan audit dokumen pada annex A mengenai prosedur dan tanggung jawab operasional.Untuk menjamin operasi fasilitas pengolahan informasi benar dan aman.

Tabel 9. Prosedur dan Tanggung Jawab Operasional

A.12.1.1 Prosedur Operasional Yang Didokumentasikan	**Implementasi**	**Justifikasi**
Prosedur operasional harus didokumentasikan dan tersedia untuk semua yang membutuhkan	YA	SOP Pegawai mengikuti prosedur berlaku. Bukti: SOP
A.12.1.2 Manajemen Perubahan		
Perubahan proses bisnis dan fasilitas informasi harus dikendalikan	YA	Kebijakan apabila terjadi transformasi data Bukti: UPNVJ/POB/PUSTIK/002/17-00 UPNVJ/POB/PUSTIK/003/17-00
Nilai Kepatuhan: Jumlah jawaban sesuai = 2 Jumlah pernyataan yang harus ada = 4 (Sesuai jumlah sub klausul ISO 27001) 2/4 x 100 = 50%		

Berikut pada tabel 10 akan menjelaskan audit dokumen pada annex A mengenai kendali perangkat lunak operasional. Untuk memastikan integritas sistem operasional.

Tabel 10. Kendali Perangkat Lunak Operasional

A.12.5.1 Instalasi Perangkat Lunak Pada Sistem Operasional	**Implementasi**	**Justifikasi**
Prosedur instalasi perangkat lunak pada operasional	YA	Adanya prosedur pembangunan aplikasi dan pengelolaannya. Bukti: UPNVJ/POB/PUSTIK/005/17-00 UPNVJ/POB/PUSTIK/006/17-00
Nilai Kepatuhan: Jumlah jawaban sesuai = 1 Jumlah pernyataan yang harus ada = 1 (Sesuai jumlah sub klausul ISO 27001) 1/1 x 100 = 100%		

Berikut pada tabel 11 akan menjelaskan audit dokumen pada annex A mengenai peralatan.

Tabel 11. Peralatan

A.11.2.4 Pemeliharaan Peralatan	**Implementasi**	**Justifikasi**
Peralatan dipelihara dalam menjamin ketersediaan berkelanjutan	YA	Terdapat kebijakan software dan hardware Bukti: UPNVJ/POB/PUSTIK/009/17-00 UPNVJ/POB/PUSTIK/004/17-00 UPNVJ/POB/PUSTIK/0010/17-00
Nilai Kepatuhan: Jumlah jawaban sesuai = 1 Jumlah pernyataan yang harus ada = 9 (Sesuai jumlah sub klausul ISO 27001) 1/9 x 100 = 11%		

2. Analisis CIA Pada Aset

Kemudian dilakukan risk assessment terhadap aset dengan metode CIA pada aset. Dari hasil identifikasi kelemahan dan ancaman UPT TIK diperoleh temuan bahwa kelemahan yang sering terjadi yaitu adanya virus (pada aset laptop dan windows 10), permasalahan pada Air Conditioner (tidak dingin, bocor, mati karena timer) sedangkan pendingin utama server adalah Air Conditioner, gangguan jaringan internal, software bug/error (virtual server). Penemuan ancaman berasal dari dalam dan luar organisasi. Dari dalam yaitu: human error, gangguan listrik, dan gangguan hardware. Dari luar yaitu: hacker, cracker, pencuri, akses illegal, dan serangan virus. Analisis risiko pada UPT TIK mendapatkan hasil pada aset utama dan

pendukung. Aset berisiko tinggi sangat memerlukan penanganan keamanan tinggi dibandingkan aset lainnya, aset dengan risiko tinggi sering mendapatkan ancaman kejadian sering terjadi dengan risiko aset mendapatkan adanya gangguan. Berdasarkan ISO/IEC 27001 identifikasi risiko yang mungkin dapat terjadi pada UPT TIK adalah sebagai berikut:

1. Risiko bisnis yang dapat terjadi yaitu lamanya melakukan perbaikan aset dan mempengaruhi bisnis dapat dikategorikan Business Impact Analysis (BIA)
2. Masalah lingkungan tidak bisa diprediksi baik dari tindak kejahatan atau bencana alam
3. Risiko terjadinya kehilangan data yaitu pencurian data, hacker, dan cracker.

C. Check

Penentuan nilai tingkat kemampuan dalam melakukan pengukuran tingkat kedewasaan yang menggambarkan sejauh mana UPT TIK UPN "Veteran" Jakarta memenuhi standar pengelolaan keamanan informasi dengan baik, dimana penilaian tingkat kematangan (*Maturity Level*) dilakukan pada tiap kontrol sesuai audit yang dilakukan. Daftar pertanyaan yang dibuat berdasar pada kontrol keamanan objektif kontrol yang telah dipilih dan akan diterapkan pada UPT TIK UPN "Veteran" Jakarta, dimana daftar dari pertanyaan berdasarkan ISO/IEC 27001:2013 menggunakan pengukuran tingkat kematangan *System Security Engineering Maturity Level* (SSE – CMM). Berikut adalah penghitungan tingkat kematangan dan kemampuan dari kontrol keamanan:

Tabel 12. Kebijakan Keamanan Informasi

A.5.1.1	**Kebijakan Untuk Keamanan Informasi**							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pihak manajemen telah memiliki kebijakan keamanan informasi	**1**			**v**			**3**
2	Pihak manajemen telah membicarakan kebijakan keamanan informasi kepada pegawai	**1**		**v**				**2**
3	Pihak manajemen telah mengesahkan kebijakan secara formal kepada seluruh pihak manajemen dan karyawan juga pihak terkait	**1**		**v**				**2**
4	Apakah kebijakan mudah diakses oleh pihak yang membutuhkan	**1**			**v**			**3**
	Total Bobot	4	**Tingkat Kemampuan**					2,5
A.5.1.2	**Reviu Kebijakan Keamanan Informasi**							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pihak manajemen telah meriviu kebijakan keamanan informasi	**1**				**v**		**4**

2	Pihak manajemen meriviu secara berkala kebijakan tersebut	**1**	**v**		**2**
3	UPT TIK sudah menerapkan program sosialisasi dan meningkatkan pemahaman keamanan informasi bagi seluruh pihak terkait	**1**	**v**		**2**
	Total Bobot	3	**Tingkat Kemampuan**		2.6

Tabel 13. Tingkat Kematangan

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-Rata/ Objektif Kontrol**
A.5 Kebijakan Keamanan Informasi	A.5.1 Arahan Manajemen Untuk Keamanan Informasi	A.5.1.1 Kebijakan Untuk Keamanan Informasi	4	2,5
		A.5.1.2 Reviu Kebijakan Keamanan Informasi	3	2,6
		***Maturity Level* Klausul 5**		**2,55**

Tabel 14. Manajemen Aset

A.8.1.1	**Inventaris Aset**								
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pihak manajemen telah membuat inventaris aset informasi dan fasilitas pengolahan informasi secara lengkap, akurat, dan terpelihara?	**1**				**V**		**4**
Total Bobot		1	**Tingkat Kemampuan**					4
A.8.1.2	**Kepemilikan Aset**								
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pihak Manajemen telah melakukan identifikasi dan pencatatan kepemilikan asset	**1**				**V**		**4**
2	Pihak manajemen memiliki personel yang bertanggung jawab untuk menjaga asset	**1**				**V**		**4**
Total Bobot		2	**Tingkat Kemampuan**					4

A.8.1.3	Penggunaan Yang Dapat Diterima Atas Aset							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pihak manajemen telah mendokumentasikan aset secara formal	**1**				**V**		**4**
2	Pihak manajemen memiliki ketentuan tata cara penggunaan aset informasi dan fasilitas penyimpan informasi	**1**				**V**		**4**
3	Pihak manajemen memiliki dokumentasi pelaksanaan/implementasi penggunaan asset	**1**				**V**		**4**
Total Bobot		3	**Tingkat Kemampuan**					4

A.8.2.3	Penanganan Aset							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Apakah organisasi mempunyai ketentuan prosedur penanganan aset informasi	**1**				**V**		**4**
2	Apakah penanganan aset informasi didokumentasikan secara formal	**1**				**V**		**4**
3	Apakah instansi telah menetapkan batasan risiko yang dapat diterima	**1**			**V**			**3**
4	Ancaman dan kelemahan aset sudah diidentifikasi sebelumnya	**1**			**V**			**3**
Total Bobot		4	**Tingkat Kemampuan**					3,5

Tabel 15. Tingkat Kematangan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-Rata/ Objektif Kontrol
A.8. Manajemen Aset	A.8.1 Tanggung Jawab Terhadap Aset	A.8.1.1 Inventaris Aset	1	4
		A.8.1.2 Kepemilikan Aset	2	4
		A.8.1.3 Penggunaan Yang Dapat Diterima Atas Aset	3	4
	A.8.2 Klasifikasi Informasi	A.8.2.3 Penanganan Aset	4	3,5
		***Maturity Level* Klausul 8**		**3,87**

Tabel 16. Kriptografi

A.10.1.1	Kebijakan Terhadap Penggunaan Kendali Kr							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Apakah UPT TIK mempunyai standar penggunaan enkripsi	**1**			**v**			**3**

Total Bobot		1	**Tingkat Kemampuan**					3
A.10.1.2	**Manajemen Kunci**							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Apakah UPT TIK menerapkan enkripsi untuk melindungi aset informasi sesuai dengan kebijakan dalam pengelolaan	**1**		**v**				**2**
Total Bobot		1	**Tingkat Kemampuan**					2

Tabel 17. Tingkat Kematangan

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-Rata/ Objektif Kontrol**
A.10 Kriptografi	A.10.1 Kendali Kriptografi	A.10.1.1 Kebijakan Terhadap Penggunaan Kendali Kriptografi	1	3
		A.10.1.2 Manajemen Kunci	1	2
	***Maturity Level* Klausul 10**			**2,5**

Tabel 18. Keamanan Fisik dan Lingkungan

A.11.1.1	**Batas Fisik Keamanan**							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Apakah UPT TIK sudah mendefinisikan lingkup keamanan dan penempatan berdasar pada kebutuhan keamanan aset	**1**			**v**			**3**
2	Tersedianya area penerima tamu untuk pembatasan akses fisik yaitu pembatasan otorisasi dengan pegawai	**1**			**v**			**3**
	Total Bobot	2	**Tingkat Kemampuan**					3
A.11.1.2	**Kendali Masuk Fisik**							
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Pengunjug memiliki tanggal masuk dan kepergian yang terekam dan diawasi kecuali akses mereka sudah disetujui	**1**		**v**				**2**
2	UPT TIK telah menerapkan pengamanan fasilitas fisik sesuai kepentingan aset informasi secara berlapis dan dapat mencegah pihak tidak berwenang	**1**		**v**				**2**
3	UPT TIK memiliki proses mengamankan lokasi kerja dari pihak ketiga untuk mengamankan instansi	**1**		**v**				**2**
	Total Bobot	3	**Tingkat Kemampuan**					2
A.11.1.3	**Mengamankan Kantor Ruangan dan Fasilitas**							

No	Pernyataan	Bobot	1	2	3	4	5	Nilai
1	UPT TIK memiliki proses pengelolaan alokasi kunci masuk (Fisik dan Elektronik) ke fasilitas fisik	**1**				**v**		**4**
2	UPT TIK memiliki peraturan untuk mengamankan lokasi kerja penting contoh: server dari risiko perangkat yang membahayakan aset informasi dan pengolah informasi yang di berada di dalamnya	**1**			**v**			**3**
	Total Bobot	2			**Tingkat Kemampuan**			3,5

A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan

No	Pernyataan	Bobot	1	2	3	4	5	Nilai
1	Infrastruktur UPT TIK terlindungi dari dampak lingkungan dan dalam kondisi dengan suhu dan kelembaban yang sesuai dengan persyaratan	**1**		**v**				**2**
2	UPT TIK memiliki aset yang terlindung dari ancaman listrik atau petir	**1**				**v**		**4**
3	Konstruksi ruangan pengolah sistem informasi berupa perangkat penyimpanan menggunakan rancangan juga material yang bisa mengurangi risiko kebakaran dan dilengkapi fasilitas pendukungnya	**1**			**v**			**3**
	Total Bobot	3			**Tingkat Kemampuan**			3

A.11.1.5 Bekerja dalam daerah aman

No	Pernyataan	Bobot	1	2	3	4	5	Nilai
1	Pengambilan gambar, video, suara tidak diperkenankan, kecuali telah di otorisasi terlebih dahulu	**1**			**v**			**3**
2	Tersedia peraturan pengamanan perangkat komputasi milik instansi apabila digunakan di luar lokasi kerja	**1**			**v**			**3**
	Total Bobot	2			**Tingkat Kemampuan**			3

A.11.2.1 Penempatan dan Perlindungan Peralatan

No	Pernyataan	Bobot	1	2	3	4	5	Nilai
1	Kontrol ditetapkan untuk mengurangi ancaman risiko fisik dan lingkungan	**1**			**v**			**3**
2	Perlindungan peralatan pengolahan informasi untuk meminimalisir risiko kebocoran informasi	**1**			**v**			**3**
	Total Bobot	2			**Tingkat Kemampuan**			3

A.11.2.3 Keamanan Kabel

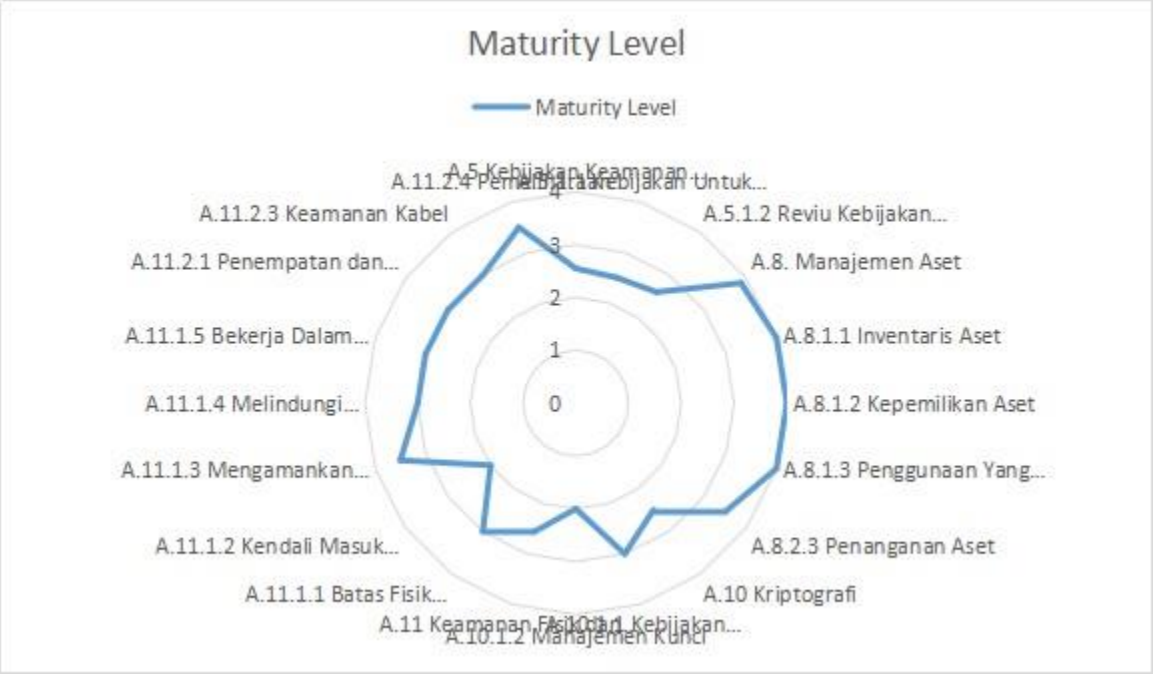
No	Pernyataan	Bobot	1	2	3	4	5	Nilai
1	Posisi saluran listrik dan telekomunikasi berada dibawah tanah atau adanya perlindungan alternative	**1**			**v**			**3**

2	Memisahkan antara kabel daya dan kabel komunikasi	**1**			**v**				**3**
3	Kabel terlindungi dari gangguan lingkungan	**1**			**v**				**3**
	Total Bobot	3			**Tingkat Kemampuan**				3
A.11.2.4	**Pemeliharaan Peralatan**								
No	**Pernyataan**	**Bobot**	**1**	**2**	**3**	**4**	**5**		**Nilai**
1	Adanya kebijakan juga proses inspeksi perawatan perangkat computer dan fasilitas pendukungnya	**1**			**v**				**3**
2	UPT TIK memiliki peraturan tata cara inspeksi sesuai prosedur dan SDM yang terlatih di bidangnya	**1**				**v**			**4**
	Total Bobot	2			**Tingkat Kemampuan**				3,5

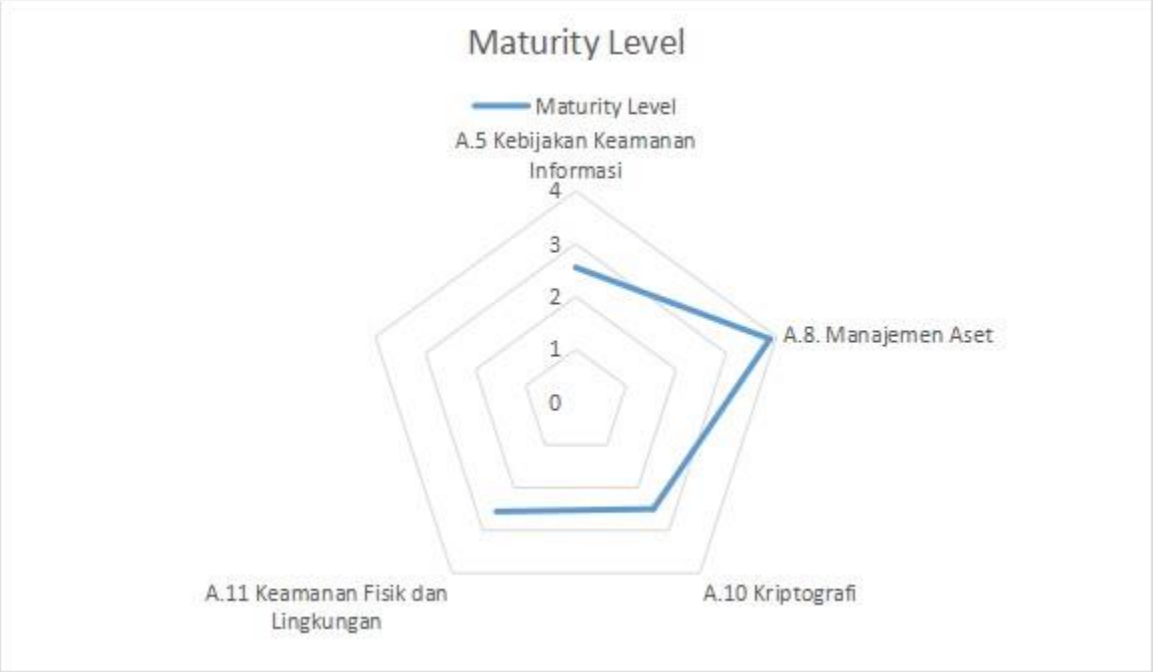
Tabel 19. Tingkat Kematangan

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-Rata/ Objektif Kontrol**
A.11 Keamanan Fisik dan Lingkungan	A.11.1 Daerah Aman	A.11.1.1 Batas Fisik Keamanan	2	3
		A.11.1.2 Kendali Masuk Fisik	3	2
		A.11.1.3 Mengamankan Kantor, Ruangan dan Fasilitas	2	3,5
		A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan	3	3
		A.11.1.5 Bekerja Dalam Daerah Aman	2	3
	A.11.2 Peralatan	A.11.2.1 Penempatan dan Perlindungan Peralatan	2	3
		A.11.2.3 Keamanan Kabel	3	3
		A.11.2.4 Pemeliharaan Peralatan	2	3,5
		***Maturity Level* Klausul 11**		**2,56**

Berikut adalah hasil dari tingkat kematangan berdasarkan hasil analisis menggunakan CIA, SSE, dan CMM, beberapa contoh penelitian sebelumnya banyak menggunakan *Spider Chart* menjadi acuan penulis untuk menggunakan diagram tersebut selain itu diagram dapat lebih mudah dipahami secara visual.



Gambar 2. Grafik SSE - CMM



Gambar 3. Grafik SSE – CMM per klausul

IV. KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah diulas di BAB sebelumnya, peneliti dapat menyimpulkan bahwa:

1. Kebijakan dan prosedur yang sekarang dilaksanakan belum memenuhi aspek standar keamanan informasi berdasarkan ISO/IEC 27001:2013.
2. Kepatuhan organisasi kepada capaian dan tindakan yang diterapkan belum memenuhi sebuah aspek keamanan informasi.
3. Saran dan rekomendasi terhadap kebijakan dan prosedur yang telah dibuat agar dapat meningkatkan keamanan informasi melalui media penelitian ini yaitu agar dapat diketahui terkait bagaimana menetapkan tujuan, kebijakan, dan arahan terhadap kontrol keamanan informasi dengan analisis pada nilai aset dan risiko untuk menentukan penggunaan klausul ISO/IEC 27001 yang menghasilkan rekomendasi dalam menetapkan kebijakan keamanan informasi di sistem informasi akademik.
4. Analisis sistem manajemen keamanan informasi menggunakan ISO/IEC 27001 pada UPT TIK UPN "Veteran" Jakarta dilakukan dengan metode PDCA *(Plan, Do, Check,* dan *Action/Act)*. Berikut rinciannya:

    a. *Plan*
    Pada tahap plan menghasilkan ruang lingkup penelitian pada UPT TIK UPN "Veteran" Jakarta yang khusus pada aset utama dan aset pendukung sistem informasi akademik yang kemudian masuk ke sub bagian pengolahan informasi masing – masing. Menentukan arah dan tujuan kebijakan dan peraturan keamanan informasi menurut ISO/IEC 27001 dimana seluruh pegawai harus mengikuti keseluruhan SMKI dalam membantu perlindungan dan keamanan aset baik itu aset utama maupun aset pendukung sistem informasi akademik dan pemeliharaan aset. Kepala UPT TIK bertanggung jawab dalam pengelolaan Sistem Manajemen Keamanan Informasi baik dalam perihal kebijakan dan peraturan inventaris atas aset, menilai risiko berkala, pemeliharaan aset dan tingkat keamanan pada fisik

    b. *Do*
    Audit dilakukan pada klausul yang bersangkutan dengan dokumen yang diberikan Klausul manajemen aset dengan tingkat kepatuhan sebesar 75%, Klausul peralatan dengan tingkat kepatuhan sebesar 11%, Klausul prosedur dan tanggung jawab operasional dengan tingkat kepatuhan sebesar 50%, dan Kendali perangkat lunak operasional dengan tingkat kepatuhan sebesar 100%. Pada tahap *do* menghasilkan analisis pada aset sistem informasi akademik berdasarkan identifikasi dan perhitungan nilai aset, nilai aset utama yaitu 10 medium dan nilai aset pendukung yaitu 8 – 11 di dalam kategori *medium,* dengan rata – rata hasil analisis pada aset utama dan pendukung berada pada level risiko *high risk.*

    c. *Check*
    Menghasilkan tingkat kematangan rata – rata berada di level 2 dan 3 yaitu "direncanakan dan dilacak" dan "didenfinisikan dengan baik" sehingga di beberapa objek kebijakan sudah dijalankan dan dikelola dengan cukup baik. Berdasarkan pemilihan klausul ISO/IEC 27001 peneliti merekomendasikan seluruh klausul untuk identifikasi masalah:
        - A.5 Kebijakan Keamanan Informasi dengan *maturity level* 2,55 (direncanakan dan dilacak)
        - A.8 Manajemen Aset dengan *maturity Level 3,87* (didefinisikan dengan baik)
        - A.10 Kriptografi dengan *maturity Level* 2,5 (direncanakan dan Dilacak)
        - A.11 Keamanan Fisik dan Lingkungan dengan *maturity level* 2,56 (direncanakan dan dilacak)

    d. *Act*
    Pada tahap ini UPT TIK perlu:
        - Menyediakan kebijakan keamanan informasi seperti *awareness* keamanan informasi di seluruh sub – bag pimpinan dan pegawai.

- Membuat peraturan dan kebijakan untuk meningkatkan kepatuhan dalam penggunaan fasilitas keamanan fisik.
- Menyediakan kebijakan perlindungan database
- Membuat kebijakan perawatan aset dan pemeriksaan aset secara teratur.

Berdasarkan penelitian yang telah dilakukan yaitu evaluasi dalam tata kelola teknologi informasi dengan fokus pada sistem manajemen keamanan informasi dengan framework ISO/IEC 27001 pada UPT TIK UPN "Veteran" Jakarta, maka peneliti memberikan saran penelitian selanjutnya sebagai berikut:

1. Peneliti selanjutnya dapat melakukan evaluasi dengan ISO/IEC 27001 dengan responden dan klaususul yang berbeda.
2. Menggunakan framework cobit 5 pada evaluasi keamanan.

V. DAFTAR PUSTAKA

[1] ISO/IEC 27001:2013. 2017. ISN..
[2] Sarno, R., & Iffano, I. (2009). *Surabaya: Sistem Manajemen Keamanan Informasi* (p. 382).ITS Press.
[3] Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.
[4] ISO/IEC 27001:2013. 2017. ISN..
[5] ISO/IEC 27001:2013. 2017. ISN..
[6] Humphreys, E. (2011). Information security management system standards. Datenschutz Und Datensicherheit-DuD, 35(1), 7–11.
[7] Swastika, A., Agus, P., & Putra, I. (2016). Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus. In Audit Sistem Informasi dan Tata Kelola
Teknologi Informasi: Implementasi dan Studi Kasus". Yogyakarta: Andi.