BAB 4. SIMPULAN DAN SARAN

4.1 Simpulan

Simpulan yang dapat diambil dari hasil analisis SNI ISO/IEC 27001:2009 menggunakan proses Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset dan Keamanan Sumber Daya Manusia adalah sebagai berikut :

1. Pada klausul 5.1 terkait dengan kebijakan keamanan informasi merupakan klausul yang paling utama, karena pada klausul 5.1 merupakan isi dari keseluruhan klausul mulai dari klausul 5 sampai dengan klausul 15. Untuk saat ini pihak manajemen ITENAS sebenarnya sudah mengetahui serta memahami terkait dengan keamanan informasi, hanya saja belum terdapat suatu kebijakan khusus terkait dengan keamanan informasi. Pihak manajemen yaitu pihak rektorat masih belum terlalu memfokuskan pada pentingnya subuah keamanan informasi, tetapi lebih banyak di fokuskan pada kegiatan akademik. Meskipun ITENAS belum menerapkan kebijakan keamanan informasi, tetapi sudah terdapat dokumen kebijakan pengelolaan sistem informasi ITENAS yang secara tidak langsung telah menunjang dalam penerapan keamanan informasi. Kemudian untuk kaji ulang keamanan informasi masih belum terdapat dikarenakan belum ada prosedur khusus terkait dengan kebijakan keamanan informasi.
2. Pihak manajemen ITENAS yaitu rektorat ITENAS sudah mengetahui serta memahami pengelolaan keamanan informasi di dalam maupun diluar organisasi, tetapi masih belum sepenuhnya dilakukan dengan baik terutama pada eksternal organisasi. Pihak rektorat telah menunjuk UPT-TIK sebagai pengelola teknologi informasi dan komunikasi ITENAS. Rektorat juga telah melakukan koordinasi terkait dengan keamanan informasi sesuai dengan hak akses dan kewenangan masing-masing. Pembagian tanggung jawab terhadap keamanan informasi juga sudah ditetapkan oleh Rektorat, tetapi kurangnya koordinasi dan keterbatasan waktu untuk melakukan sosialisasi masih menjadi kendala UPT-TIK

sehingga masih terdapat saling lempar tanggung jawab jika terjadi masalah yang menyangkut keamanan informasi. Untuk perjanjian kerahasiaan dan pedoman pelaksanaan teknis keamanan informasi yang mengatur tentang sangsi jika terjadi pelanggaran juga belum ada. Untuk Tim khusus Telah dibentuk tim yang menangani pengembangan dan pengelolaan sistem informasi, tetapi kurangnya sosialisasi menjadi kendala dalam melakukan kontak dengan tim tersebut. Kaji ulang mengenai keamanan informasi juga belum terdapat. Untuk keamanan informasi oleh pihak eksternal masih kurang baik dikarenakan Belum terdapat identifikasi resiko kontrol terkait dengan pihak ke tiga, Penekanan keamanan ketika berhubungan dengan pelanggan dan Penekanan keamanan perjanjian. Akan tetapi sebagian yang berkaitan dengan keamanan informasi organisasi sudah dituangkan di dalam dokumen kebijakan pengelolaan sistem informasi.

3. ITENAS sudah memahami pentingnya pemeliharaan aset serta perlindungan terhadap aset dengan dibuatnya SIMAS (Sistem Informasi Manajemen Aset). Aset juga sudah ditentukan kepemilikannya dan siapa yang bertanggung jawab atas aset tersebut. Akan tetapi aset yang dilindungi masih mencakupi aset fisik, layanan dan aset piranti lunak, Untuk aset informasi belum. Untuk pedoman klasifikasi informasi sudah ada tetapi klasifikasi informasi hanya lebih ditekankan kepada hak akses, tidak ada klasifikasi khusus terkait dengan aset informasi. Kemudian untuk Pelabelan dan penanganan keamanan informasi masih belum ada sehingga terkadang pihak pengguna berinisiatif sendiri untuk memperbaikinya, dan terkadang melibatkan pihak luar tanpa seijin pihak pimpinan. Sehingga dapat berpotensi terjadinya kebocoran informasi penting dan rahasia yang dapat merugikan pihak ITENAS.
4. ITENAS sudah memahami cara pengelolaan sumberdaya manusia sebelum dipekerjakan, selama bekerja, yang sudah diberhentikan atau jika terjadi perubahan pekerjaan. Tetapi belum semua dilakukan dan diterapkan. Aturan dan tanggung jawab sudah diberikan kepada

pegawai,proses seleksi karyawan juga sudah dilakukan, untuk syarat dan aturan kepegawaian juga sudah diberikan tetapi dalam hal keamanan informasi masih belum dijelaskan secara detail. Pihak manajemen juga telah mencoba merumuskan suatu aturan dalam bentuk dokumen kebijakan pengelolaan sistem informasi, namun isi dokumen masih menitik beratkan pada petunjuk pelaksana teknis, belum pada keamanan informasi. Pelatihan dan pendidikan terkait dengan keamanan informasi masih dalam tahap perencanaan. Untuk proses dan sangsi terkait kedisiplinan masih belum diterapkan. Tanggung jawab untuk melaksanakan pengakhiran pekerjaan atau perubahan pekerjaan sudah berjalan dengan baik. Pengembalian aset dan penghapusan hak akses juga sudah dilakukan.

4.2 Saran

Saran dari Tugas Akhir ini dibagi menjadi dua yaitu :

1. Untuk pihak ITENAS :
   a. ITENAS untuk saat ini harus lebih meningkatkan keamanan informasi dan yang paling utama yaitu membuat suatu kebijakan keamanan informasi terkait dengan klausul 5, mengingat pentingnya suatu Informasi dengan cara menerapkan tata kelola standarisasi sesuai dengan Sistem Manajemen Keamanan Informasi yaitu SNI ISO 27001:2009.
   b. Menyesuaikan sasaran pengendalian dan pengendaliannya, antara lain Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset dan Keamanan Sumber Daya Manusia.
      i. Kebijakan keamanan
         Sasaran dalam proses ini adalah untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi menurut persyaratan bisnis dan hukum serta regulasi yang relevan.
      ii. Organisasi keamanan informasi

Sasaran dalam proses ini adalah untuk mengelola keamanan informasi didalam maupun diluar organisasi.

iii. Pengelolaan aset.

Sasaran dalam proses ini adalah untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi serta memastikan bahwa informasi menerima tingkat perlindungan yang tepat.

iv. Keamanan sumber daya manusia

Sasaran dalam proses ini adalah untuk memastikan bahwa pegawai serta pengguna sistem beserta pihak-pihak lain yang berkepentingan di dalam pengelolaan atau perbaikan sistem memahami tanggung jawab sesuai dengan perannya yang bertujuan untuk mengurangi resiko pencurian, kecurangan atau penyalahgunaan fasilitas, serta kepedulian terhadap ancaman dan masalah di dalam keamanan informasi.

c. Referensi penerapan dokumen SNI ISO 27001:2009 pada ITENAS disesuaikan dengan dokumen tamplate pada ISO 27002 Meliputi kebijakan, prosedur, instruksi kerja, dan penjadwalan. Dokumen tamplate disertakan pada Lampiran K,L,M dan N.

2. Untuk peneliti ke depan :

a. Untuk penyusunan selanjutnya bagi yang berminat melanjutkan Tugas Akhir Audit keamanan informasi menggunakan SNI ISO 27001:2009 studi kasus pada ITENAS dapat melanjutkan klausul selanjutnya yaitu klausul 9 keamanan fisik dan lingkungan, klausul 10 manajemen komunikasi dan operasi, klausul 11 kontrol akses, klausul 12 akuisisi sistem informasi, pembangunan dan pemeliharaan, klausul 13 manajemen kejadian keamanan informasi, klausul 14 manajemen kelangsungan bisnis, dan klausul 15 kepatuhan.