Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Skripsi
untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Teknik Informatika

DiajukanOleh

Riawan Arbi Kusuma
10650016

Kepada

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UIN SUNAN KALIJAGA
YOGYAKARTA
2014

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Skripsi
untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Teknik Informatika

DiajukanOleh
RiawanArbiKusuma
10650016

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UIN SUNAN KALIJAGA
YOGYAKARTA
2014

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/ 385 /2014

Skripsi/Tugas Akhir dengan judul : Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Yang dipersiapkan dan disusun oleh :
Nama : Riawan Arbi Kusuma
NIM : 10650016
Telah dimunaqasyahkan pada : Senin, 27 Januari 2014
Nilai Munaqasyah : A
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

M. Mustakim, M.T
NIP. 19790331 200501 1 004

Penguji I

Sumarsono, M.Kom
NIP. 19770103 200501 1 003

Penguji II

Bambang Sugiantoro, M.T
NIP. 19751024 200912 1 002

Yogyakarta, 6 Februari 2014
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI UIN SUNAN KALIJAGA YOGYAKARTA

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama	: Riawan Arbi Kusuma
NIM	: 10650016
Program Studi	: Teknik Informatika
Fakultas	: SainsdanTeknologi

Menyatakan bahwa skripsi dengan judul "AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR STANDAR SNI ISO 27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS ISLAM NEGERI UIN SUNAN KALIJAGA YOGYAKARTA" tidak terdapat karya yang pernah diajukan untuk memper oleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 16 Januari 2014
Yang Menyatakan

Riawan Arbi Kusuma
NIM :10650016

KATA PENGANTAR

Alhamdulillah, segala pujibagi Allah *Subhanahuwata'ala* atas limpahan rahmat, hidayah, serta bimbingan-Nya. Shalawat serta salam semoga tercurah kepada Nabi Muhammad *Shallallohu 'alaihiwasallam*. Akhirnya penulis dapat menyelesaikan penelitian Tugas Akhir yang berjudul Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta**.**Oleh Karena itu, dengan segala kerendahan hati pada kesempatan ini penulis mengucapkan banyak terimakasih kepada:

1. Prof. Drs. H. Akh. Minhaji, M.A., Ph.D selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
2. Bapak Agus Mulyanto, S.Si, M.Kom. selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
3. Bapak M. Mustakim, ST., M.T., selaku pembimbing yang selalu sabar membimbing, mengarahkan, memberikan nasehat dan saran selama penyusunan skripsi.
4. Agung Fatwanto, S.Si.,M.Kom, Ph.D, selakuKepalaUPT PTIPD UIN Sunan Kalijaga yang telah memberikan izin penelitian.
5. Seluruh staf TI PKSI UIN Sunan Kalijaga yang telah bersedia meluangkan waktunya menjadi responden untuk pengambilan data penelitian.

6. Ibunda HJ. Suwarti Sumono dan Ayahanda Sumono, S.H. (alm) yang selalu setia memberikan dukungan pada penulis serta doa yang menjadi sumber motivasi dan inspirasi.
7. MbakOsy, MbakRia, MbakNeni yang selalu memberikan dukungan dan inspirasi.
8. Hanan, Rasyid, Ami, Pak Aulia dan seluruh teman-teman keluarga besar Program Studi Teknik Informatika, khususnya angkatan 2010 yang telah banyak sekali memberikan masukan, saran dan diskusi yang begitu berharga yang telah banyak membantu proses penelitian penulis.
9. Serta semua rekan-rekan penulis di berbagai kegiatan maupun organisasi yang juga telah memberikan banyak sekali masukan dan kontribusi yang sangat berarti bagi penulis

Penulis merasa masih banyak sekali kekurangan dan kelemahan dalam penelitian ini, oleh karena itu segala kritik dan saran senantiasa penulis harapkan dari para pembaca. Akhir kata,semoga penelitian ini dapat menjadi panduan serta referensi yang sangat berguna bagi pembaca dan dapat dimanfaatkan sebaik-baiknya.

Yogyakarta, 18 Januari 2014

Penulis

HALAMAN PERSEMBAHAN

Laahawlawalaaquwwataillabillah, tidak ada daya dan kekuatan kecuali Allah yang Maha Tinggi dan Maha Agung. Puji syukur kehadirat Allah yang Maha Pengasih dan Penyayang.Sholawat semoga tercurah pada junjungan Nabi Muhammad SAW.Alhamdulillah dengan kasih sayang dan petunjuk-Nya, saya dapat menyelesaikan penelitian ini.Terselesaikannya penelitian ini, tidak lepas dari doa dan dukungan banyak pihak. Maka, melalui kesempatan ini, saya mengucapkan terimakasih setulus hati kepada:

1. IbundakuHJ. Suwarti Sumono terimakasih untuk semua kasihsayang dan pengorbananmu. Tidak ada kata yang bisa mewakili betapa besar rasa terimakasihku. Semoga Allah senantiasa melimpahkan kasih sayang, rahmat dan barokah serta kemuliaan hidup dunia dan akhirat. *Love you mom, you always be my hero.*
2. Mbak Osy, Mbak Ria, Mbak Neni dan semua keponakan, keluarga besar Amad Djoyosetiko terimakasih untuk semua bantuan dan dukungan, *Thankyou for all* .
3. Keluarga Bambang Istiadi, *May be I though him as a second parents for me. Thankyou for giving me boarding house, home stay actually for 3 years i stayed in beloved Yogyakarta. Always give me different point a view about the world, nice person he is. Thankyou for all.*
4. Jalan Bali *crew* Reza, Priyo, Doni, Husna, kalian luarbiasa! Salah satu penghibur dikala hati galau. *Keep on this brotherhood fellas!*.

5. Keluarga UPT PTIPD UIN Sunan Kalijaga Yogyakarta terimakasih atas semua bantuan dan kerjasama-nya.
6. Kakak-kakak TIF UIN Sunan Kalijaga terimakasih untuksemua sharing ilmu yang kita lakukan.

HALAMAN MOTTO

Man never to sit down and do nothing
(Sitka, Brother Bear)

Merumuskan Visi dan Misi adalah salah satu bentuk dalam mengambil keputusan, bahkan pengambilan keputusan yang cukup fundamental. Visi dan Misi Anda akan menjiwai segala gerak dan tindakan di masa datang.

Man Jadda Wajada

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

RiawanArbiKusuma
NIM: 10650016

Tata kelola TI(IT Governance) adalah strukturyang saling berhubungan dan proses yang mengarahkan dan mengendalikan perusahaan dalam mencapai tujuan perusahaan melalui nilai yang ditambahkan danmenyeimbangkan antararisiko dan manfaat teknologi informasi dan proses itu. Pelaksanaan pemerintahan ini harus direncanakan dengan baik agar dapat dilaksanakan sesuai dengan kondisi dan kemampuan perusahaan.

Salah satu kerangka tata kelola TI adalah SNI - ISO 27001. Kerangka ini secara resmi digunakan oleh pemerintah Indonesia untuk memastikan sistem manajemen keamanan informasi ke dalam praktek yang baik. Kerangka kerja ini adalah adopsi otentik dari kerangka ISO 27001. Untuk mengukur kinerja sistem manajemen keamanan informasi menggunakan SNI-ISO 27001, Maturity Model digunakan dengan tujuan untuk melihat representasi dari kondisi saat ini

Dari penelitian ini, dapat disimpulkan bahwa tingkat keamanan dari SIA UIN Sunan Kalijaga Yogyakarta tentang keamanan informasi pada skala kematangan adalah model skala 2 (Repeatable but Intuitive). Ini berarti bahwa keamanan yang terkandung dalam SIA UIN Sunan Kalijaga telah dibakukan tetapi tidak didokumentasikan . Semua keamanan informasi di SIA UIN Sunan Kalijaga Yogyakarata dilengkapi dengan prosedur yang harus diikuti oleh individu yang memiliki tugas bersama. UPT PTIPD yang mengelola SIA UIN Sunan Kalijaga Yogyakarta belum mengadakan program pelatihan formal, yang bertujuan untuk mengkomunikasikan prosedur dan tanggung jawab dari masing-masing individu.

Kata kunci: SNI-ISO 27001, informasi keamanan, tingkat kematangan

Information Security Management System Audit using SNI – ISO 2700 Framework for Academic Information System State Islamic University of SunanKalijaga Yogyakarta

RiawanArbiKusuma
NIM: 10650016

ABSTRACT

IT governance (IT Governance) is an interconnected structure and processes which direct and control the company in achieving corporate goals through value added and balancing between risks and benefits of information technology and it processes. Implementation of this governance should be well planned in order to be implemented according to the conditions and company capabilities.

One of the IT governance framework is SNI – ISO 27001. This framework is officialy used by Indonesian government to make sure information security management system into good practices. This frame work is authentic adoption of ISO 27001 framework. To measure the performance of information security management system using SNI-ISO 27001, Maturity Model Level is used with the aim to see a representation of thecurrent condition of the company.

From this research, it can be concluded that secure level of SIA UIN Sunan Kalijaga Yogyakarta about information security at maturity scale is a scale model of 2 (Repeatable butIntuitive). It means that the security contained in SIA UIN Sunan Kalijaga had been standardized but not documented yet. All of the information security in SIA UIN Sunan Kalijaga Yogyakarata equipped with procedures to be followed by individuals whohave a common task. UPT PTIPD whose manage SIA UIN Sunan Kalijaga Yogyakarta has not held a formal training program, which aims tocommunicate the procedures and responsibilities of each individual.

Keywords : SNI-ISO 27001, information Security , maturity level

BAB I

PENDAHULUAN

1.1 Latar Belakang

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Untuk meningkatkan kesadaran akan pentingnya keamanan informasi, sejak tahun 2008 Kementerian Kominfo telah menyelenggarakan sosialisasi dan bimbingan teknis (bimtek) kepada instansi penyelenggara pelayanan publik, baik di lingkungan pemerintah pusat maupun daerah. Jika sosialisasi berisi tentang definisi, pengertian, kontrol-kontrol, persyaratan dokumentasi keamanan informasi dan contoh-contoh tindakan untuk mengamankan informasi, maka bimtek menjelaskan metode atau cara melakukan penilaian mandiri (*self assessment*) terhadap status keamanan informasi suatu instansi penyelenggara pelayanan publik dengan menggunakan alat bantu indeks KAMI yang telah disusun Direktorat Keamanan Informasi - Kementerian Kominfo.

Salah satu lembaga yang menerapkan teknologi informasi adalah Perguruan tinggi. Perguruan Tinggi di Indonesia akan berusaha memberikan pelayanan yang terbaik dengan memanfaatkan teknologi untuk mendukung suatu prosessehingga memberikan informasi yang cepat dan tepat, khususnya untuk memajukan institusi. Proses tersebut harus didukung oleh beberapa aktifitas penunjang untuk keberhasilan proses yang ada di perguruan tinggi.

Salah satu penunjang vital pada perguruan tinggi adalah layanan sistem informasi akademik yang mempunyai mekanisme prosedur keamanan data yang baik sehingga perlu adanya standar keamanan sistem informasi yang baik untuk mendukung tercapainya pelayanan akademik yang baik.Salah satu perguruan tinggi yang menggunakan Teknologi Informasi di Yogyakarta adalah Universitas Islam Negeri Sunan Kalijaga Yogyakarta.UIN menggunakan teknologi informasi sebagai sarana untuk memberikan informasi akademik kepada seluruh civitas akademika dan membantu terlaksananya kegiatan unit kerja yang ada.

Sistem Informasi Akademik (SIA) adalah layanan akademik yang berisi laporan nilai hasil kuliah mahasiswa, jadwal matakuliah mahasiswa, media input kartu rencana studi mahasiswa, dan sebagai pemberi informasi jadwal ujian dan absensi mahasiswa.

Mengingat pentingnya informasi yang terdapat dalam SIA , maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengendalian dokumen, prosedur pengendalian rekaman, prosedur tindakan perbaikan dan pencegahan, prosedur penanganan informasi, prosedur

penanganan insiden, dan prosedur pemantauan penggunaan fasilitas teknologi informasi (Direktorat Keamanan Informasi 2011:14).

Diperlukan audit keamanan sistem informasi pada Universitas Islam Negeri Sunan Kalijaga Yogyakarta untuk memastikan keamanan informasi diterapkan sesuai prosedur. Standar yang digunakan yaitu SNI ISO 27001. Beberapa hal yang menjadi pertimbangan dalam penggunaan standar ini adalah standar ini fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan dan juga SNI ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi SMKI yang diakui secara nasional dan internasional yang disebut Information Security Management System ISMS (Direktorat Keamanan Informasi 2011:09).

Audit IT / Sistem Informasi (SI) untuk keamanan Sistem Informasi akademik UIN Sunan Kalijaga Yogyakarta belum dilakukan. Maka penulis ingin melaksanakan audit keamanan sistem informasi SIA di Universitas Islam Negeri Sunan Kalijaga Yogyakarta untuk menerapkan audit dengan standar SNI ISO 27001. Standar SNI ISO 27001 merupakan standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil audit keamanan sistem informasi SIA di Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dengan adanya penelitian tentang audit yang dilakukan penulis diharapkan referensi audit sistem informasi bisa bertambah.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas , masalah yang akan diselesaikan dalam penelitian ini adalah :

- Bagaimana merencanakan audit keamanan Sistem Infomasi Akademik UIN SUNAN KALIJAGA YOGYAKARTA dengan menggunakan standar SNI ISO 27001.
- Bagaimana melaksanakan audit keamanan Sistem Informasi Akademik UIN SUNAN KALIJAGA YOGYAKARTA dengan menggunakan standar SNI ISO 27001 terhadap faktor keamanan informasi CIA (*Confidentiality, Integrity, Availability).*
- Bagaimana memformulasikan hasil audit keamanan Sistem Informasi Akademik UIN SUNAN KALIJAGA YOGYAKARTA dengan menggunakan standar SNI ISO 27001

1.3 Tujuan dan Manfaat Penelitian

1.3.1. Tujuan Penelitian

- Membuat perencanaan audit keamanan Sistem Informasi akademik di UIN SUNAN KALIJAGA YOGYAKARTA
- Melaksanakan audit keamanan Sistem Informasi Akademik di UIN SUNAN KALIJAGA YOGYAKARTA sesuai dengan standar SNI ISO 27001
- Memformulasikan hasil audit keamanan Sistem Informasi Akademik dengan melakukan evaluasi terhadap kendali dan bukti yang ada, mendokumentasikan temuan audit dan menyusun laporan audit.

1.3.2. Manfaat Penelitian

- Memperoleh kondisi aktual tentang Sistem Manajemen Keamanan Informasi (SMKI) di Sistem Informasi Akademik UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.
- Optimalisasi pelayanan akademik sebagai upaya mengidentifikasi kegiatan apa yang perlu dilakukan untuk meningkatkan kinerja dari Sistem Informasi Akademik di UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.
- Menghasilkan dokumen temuan dan rekomendasi dari hasil audit keamanan sistem informasi akademik di UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA yang dapat digunakan sebagai dokumentasi pengembangan sistem yang ada.

1.4 Batasan Penelitian

Batasan penelitian yang dilakukan adalah :

- Audit ini dilakukan dengan standar SNI ISO 27001
- Audit ini dilakukan dengan memfokuskan pada penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar SNI ISO 27001 dalam hal pengelolaan SIA UIN Sunan Kalijaga Yogyakarta.
- Ruang lingkup dari penelitian ini adalah *IT Operation, Application Control, Information security* dan *ISO Mandatory Requirements.*
- Dalam penelitian ini *penetration test* tidak dilakukan.
- Data acuan yang digunakan adalah hasil data wawancara yang dilakukan.

- Audit ini dilakukan dengan menggunakan checklist yang ada dalam panduan standar SNI ISO 27001.
- Tidak membahas manajemen jaringan seperti konfigurasi server, dan manajemen IP baik privat ataupun public.
- Output yang dihasilkan berupa temuan dan rekomendasi hasil audit keamanan sistem informasi SIA UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.

1.5 Keaslian Penelitian

Penelitian tentang audit sistem informasisudah banyak dilakukan sebelumnya. Beberapa penelitian yang sudah dilakukan misalnya oleh Melwin Syafrizal (2010) tentang Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005. Penelitian yang lain telah dilakukan oleh Marliana Halim, Haryanto Tanuwijaya, Ignatius Adrian Mastan tentang Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 (Studi Kasus: PT. Aneka Jaya Baut Sejahtera)

Terdapat pula penelitian yang dilakukan oleh Fine Ermana tentang Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM.Margo Utomo, Ahmad Holil Noor Ali, Irsal Affandi (2012) tentang Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I.

Peneliti berkeyakinan bahwa penelitian tentang audit keamanan sistem informasi dengan standar SNI ISO 27001 pada sistem informasi akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta belum pernah dilakukan.

Perbedaan penelitian ini dengan yang sudah ada adalah pada penelitian sebelumnya , klausul – klausul yang digunakan dalam penelitian belum mencakup seluruh elemen pengendalian. Sehingga masih banyak aspek dari klausul checklist ISO 27001 yang belum digunakan sebagai acuan pengendalian dalam audit yang dilakukan. Sedangkan audit yang akan dilakukan oleh peneliti akan mencakup seluruh aspek dan klausul yang ada dalam checklist SNI ISO 27001.

Selain itu, pada penelitian yang telah dilakukan sebelumnya belum mengikuti petunjuk dari Direktorat Keamanan Informasi Republik Indonesia tentang Tata Kelola Keamanan Informasi Bagi penyelenggara Pelayanan Publik. Sedangkan penelitian yang akan dilakukan penulis akan mengacu pada pedoman dari Direktorat Keamanan informasi dan Badan Standarisasi Nasional sebagai lembaga standarisasi nasional di Indonesia.

BAB VI

KESIMPULAN DAN SARAN

6.1. Kesimpulan

1. Perencanaan audit untuk kegiatan penelitian audit keamanan sistem informasi dengan standar SNI – ISO 27001 pada Sistem Informasi Akademik yang dikelola UPT PTIPD UIN Sunan Kalijaga telah berhasil dilaksanakan.
2. Berdasarkan dari hasil analisis data evaluasi sistem manajemen keamanan informasi untuk Sistem Informasi Akademik (SIA) UIN Sunan Kalijaga Yogyakarta dengan maturity level, SIA UIN Sunan Kalijaga Yogyakarta saat ini berada pada angka 1,85 dan kemudian dibulatkan menjadi 2 yaitu *Repeatable but Intuitive*, artinya pada pengamanan informasi pada Sistem Informasi Akademik (SIA) UIN Sunan Kalijaga Yogyakarta yang dikelola di UPT PTIPD UIN Sunan Kalijaga telah distandarkan tetapi belum didokumentasikan. Semua proses pengamanan informasi untuk SIA baru sebatas mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi .
3. Rekomendasi diberikan auditor di setiap faktor keamanan informasi untuk memperbaiki sistem manajemen keamanan informasi pada Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta.

4. Berdasarkan analisis dan hasil pengukuran nilai *maturity level* domain *information security*, tingkat kematangan Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta dalam faktor *confidentialy* adalah 1,58. Artinya proses dan usaha pengamanan informasi untuk menjaga kerahasiaan informasi hanya mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi.
5. Berdasarkan analisis dan pengukuran nilai *maturity level* untuk domain *IT Operations* dan *Application Controls*, maka didapatkan *maturity level* Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta dalam faktor *integrity* adalah 2,32. Artinya proses dan usaha pengamanan informasi untuk menjaga integritas sistem informasi hanya mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan dan user lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi.
6. Berdasarkan analisis dan hasil pengukuran nilai *maturity level* domain *ISO Mandatory* , tingkat kematangan Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta dalam faktor *availability* adalah 1,64. Artinya proses dan usaha pengamanan informasi untuk menjaga dan memastikan ketersediaan data dan informasi (*availability*) pada sistem informasi hanya mengikuti pola yang

teratur dimana prosedur serupa diikuti pegawai/karyawan dan user lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi.

6.2. Saran

Dari percobaan yang telah dilakukan dalam penelitian ini, masih terdapat kekurangan-kekurangan. Oleh karena itu, untuk penelitian lebih lanjut peneliti perlu memberikan saran sebagai berikut:

1. Perlu ditingkatkannya kesadaran dari pimpinan perusahaan, manajer serta para stakeholder mengenai pentingnya keamanan sistem informasi dalam mendukung proses kerja guna mencapai visi, misi dan tujuan perusahaan. Langkah-langkah implementasi teknologi informasi berdasarkan standar SNI-ISO 27001 dilaksanakan secara bertahap dengan harapan UPT PTIPD sebagai pengelola SIA dapat menghadapi perubahan tersebut, yang nantinya harus dilakukan audit serta perbaikan yang berkesinambungan.
2. Penelitian yang lebih lanjut atas penelitian ini diharapkan dapat mendefinisikan ukuran-ukuran performa yang lebih mendetil dari sistem manajemen keamanan informasi untuk SIA UIN Sunan Kalijaga Yogyakarta menurut standar SNI – ISO 27001 sehingga manajemen UPT PTIPD Sunan Kali jaga akan dapat menilai apakah pengelolaan keamanan informasi SIA sudah mencapai performa yang diharapkan atau belum.

DAFTAR PUSTAKA

Margo, Utomo, Ahmad Holil Noor Ali, and Irsal Affandi. "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I." *Tata Kelola Keamanan Informasi*, 2012.

Nurdiani, Fariza Ayu. *AUDIT SIAMIK (SISTEM INFORMASI AKADEMIK) DALAM HAL PENGELOLAAN SDM (SUMBER DAYA MANUSIA) UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR MENGGUNAKAN COBIT 4.1*. Skripsi, Surabaya: Universitas Pembangunan Nasional veteran jawa timur, 2011.

Syafrizal, Melwin. "Information Security Management System." *Sistem manajemen keamanan informasi*, 2010.

wikipedia. *Wikipedia*. April 7, 2013. http://id.wikipedia.org/wiki/Audit (accessed April 15, 2013).

Badan Standarisasi Nasional. "Standar Nasional Indonesia." *Standar Keamanan Sistem Informasi*, 2009: 8.

Ermana, Fine. "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM." Penelitian, Surabaya, 2009.

Tim Direktorat Keamanan Informasi. "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Pelayanan Publik." *Sistem Keamanan Sistem Informasi* (Depkominfo), 2011.

Kadir, Abdul, and Wahyuni Terra Ch. *Pengenalan Teknologi Informasi.* Yogyakarta: Penerbit Andi, 2005.

Sarno, R, and iffano. *Sistem Manajemen Keamanan Informasi.* Surabaya: ITS Press, 2009.

Azanti Suryaningsih, Yenny. *AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN COBIT FRAMEWORK PADA PKSI UIN SUNAN KALIJAGA YOGYAKARTA.* Skripsi, Yogyakarta: UIN Sunan Kalijaga Yogyakarta, 2013.

LAMPIRAN A *Project Definition*

Audit Charter

Project ID : SNI-ISO 27001-Audit-01

Project Name : Information System Management Audit

Auditor : RiawanArbiKusuma

Project Description :

Penelitian yang berkaitandengankeamananinformasiinimenggunakan parameterSNI-ISO27001.Berkenaandenganmaksudpenelitian, dikembangkanwawancaradari SNI-ISO27001, yang dibatasipada domain *IT Operations*, *Application Control*, dan*Information Security*, dan*ISO Mandatory requirements* yangmenitikberatkankepada proses penerapan SMKI (SistemManajemenKeamananInformasi) dengantujuaninstansisecaraumum.

Project Schedule : November – February

Stake Holder List :

Respondent	Actual Respondent	Audit Clause
Chief Information Officer (CIO)	AgungFatwanto, S.Si., M.Kom., Ph.D	
Head Operations (HO)	AgungFatwanto, S.Si., M.Kom., Ph.D	SNI-ISO 27001 *Mandatory Documents*, SNI – ISO 27001 A.11.1, SNI – ISO 27001 A.11.2, SNI – ISO 27001 A.11.4
Chief Architect (CA)	AgungFatwanto, S.Si., M.Kom., Ph.D	
Head Development (HD)	AgungFatwanto, S.Si., M.Kom., Ph.D	
Compliance, Audit, Risk and Security (CARS)	HendraHidayat, S.Kom	SNI-ISO27001 A.10.6.1, SNI-ISO27001 A.10.6.2,

		SNI-ISO27001 A.11.5.1, SNI-ISO27001 A.11.5.2, SNI-ISO27001 A.11.5.3, SNI-ISO27001 A.11.5.5
Information System Division	SalimAthari, S.Kom	SNI-ISO27001 A.12.1.1, SNI-ISO27001 A.12.4.1, SNI-ISO27001 A.12.4.3, SNI-ISO27001 A.13.1.1, SNI-ISO27001 A.13.1.2, SNI-ISO27001 A.13.2.1, SNI-ISO27001 A.13.2.2, SNI-ISO27001 A.13.2.3
Information and Technology Division	RamadhanGatra, S.T.	SNI-ISO27001 A.10.6.1, SNI-ISO27001 A.10.6.2, SNI-ISO27001 A.11.5.1, SNI-ISO27001 A.11.5.2, SNI-ISO27001 A.11.5.3, SNI-ISO27001 A.11.5.5

Yogyakarta, 1 November 2013

Mengetahui
Kepala PTIPD UIN SunanKalijaga

Auditor

AgungFatwanto, S.Si.,M.Kom., Ph.D
NIP : 19770103 200501 1 003

RiawanArbiKusuma
NIM : 10650016

LAMPIRAN B Surat Ijin Penelitian

LAMPIRAN C.a. *Process Definition IT Operations*

Lembar Kertas Kerja Audit

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001

Pada Sistem Informasi Akademik Universitas Islam Negeri SunanKalijaga Yogyakarta

Document ID	: ITOP-INTV
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
Auditor	: Riawan Arbi Kusuma
Auditee	: Hendra Hidayat ,S.Kom (Head of CARS Departments)
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penilitan tugas akhir mahasiswa Program Studi Teknik Informatika, Univensitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi *IT Operation* pada pengelolaan Sistem Informasi Akademik UIN Sunan Kalijaga yang terkait dengan unsur CIA.
Date	:

Approved by | Auditor

Hendra Hidayat, S.Kom. | Riawan Arbi Kusuma

LAMPIRAN C.b. *Process Definition* Information Security

Lembar Kertas Kerja Audit

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001

Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: INSEC-INTV
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
Auditor	: Riawan Arbi Kusuma
Auditee	: Salim Athari, S.Kom
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penilitan tugas akhir mahasiswa Program Studi Teknik Informatika, Univensitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi *Information Security* pada pengelolaan Sistem Informasi Akademik UIN SunanKalijaga yang terkait dengan unsur CIA.
Date	:

Approved by Auditor

SalimAthari, S.Kom. RiawanArbiKusuma

LAMPIRAN C.c. *Process Definition Application Control*

Lembar Kertas Kerja Audit

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001

Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: APPCTR-INTV
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
Auditor	: Riawan Arbi Kusuma
Auditee	: Agung Fatwanto, S.Si.,M.Kom., Ph.D
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penilitan tugas akhir mahasiswa Program Studi Teknik Informatika, Univensitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi *Application Control* pada pengelolaan Sistem Informasi Akademik UIN Sunan Kalijaga yang terkait dengan unsur CIA.
Date	:

Approved by | Auditor

AgungFatwanto,S.Si,M.Kom,Ph.d. | RiawanArbiKusuma

LAMPIRAN C.d. *SNI – ISO*

Lembar Kertas Kerja Audit

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001

Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: ISO-INTV
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
Auditor	: Riawan Arbi Kusuma
Auditee	: Agung Fatwanto, S.Si., M.Kom., Ph.D
Description	: Lembar kertas kerja audit ini merupakan bagian dari penilitan tugas akhir mahasiswa Program StudiTeknikInformatika, Univensitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi *ISO Mandatory Requirements* pada pengelolaan Sistem Informasi Akademik UIN Sunan Kalijaga yang terkait dengan unsur CIA.
Date	:

Approved by | Auditor

Agung Fatwanto,S.Si,M.Kom,Ph.d. | Riawan Arbi Kusuma

LAMPIRAN D *Maturity Model*

Skala	Explanation
0 (Non- Existent)	Proses manajemen tidak diterapkan samasekali. Semua proses tidak dapat diidentifikasi dan dikenali. Status kesiapan keamanan informasi tidak diketahui.
1 (initial/ad hoc)	Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan, Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik, pihak yang terlibat tidak menyadari tanggung jawab mereka.
2 (Repeatable but Intuitive)	Proses mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi
3 (Defined)	Proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan dan dikomunikasikan melalui pelatihan. Proses berada pada keadaan diamanatkan namun, kecil kemungkinan penyimpangan dapat terdeteksi. Prosedur yang ada hanya formalisasi praktek yang ada
4 (Managed and measurable)	Monitor dari manajemen dan mengukur kepatuhan prosedur dan mengambil tindakan apabila diperlukan. Selalu ada proses pembaharuan yang konstan dan berkala dan memberikan pelaksanaan yang baik. Otomasi dan alat – alat yang digunakan diakases secara terbatas dan sudah terfragmentasi
5 (Optimized)	Praktek yang baik diikuti dan secara otomatis. proses telah disempurnakan ke tingkat pelaksanaan yang baik, berdasarkan hasil dari peningkatan berkelanjutan dan maturity pemodelan dengan informasi lainnya tentang perusahaan. TI digunakan secara terpadu untuk mengotomatisasi alur kerja, menyediakan alat untuk meningkatkan kualitas dan efektivitas, membuat badan cepat beradaptasi.

LAMPIRAN E *Control List*

No	Code	Control
1	SNI - ISO27001 - A.10.6.1	Kebijakan pengamanan jaringan
2	SNI - ISO27001 - A.10.6.1	Dokumentasi kebijakan pengamanan jaringan
3	SNI - ISO27001 - A.10.6.2	Mekanisme pengamanan jaringan sebagai upaya pencegahanserangan
4	SNI - ISO27001 - A.10.6.2	Pembaharuan yang dilakukan terhadap strategi pencegahan serangan pada jaringan
5	SNI - ISO27001 - A.10.6.2	Manajemen mengidentifikasi titik jaringan yang rawan terhadap serangan
6	SNI - ISO27001 - A.10.6.2	Tim/petugas yang khusus menangani keamanan jaringan
7	SNI - ISO27001 - A.10.6.2	Mekanisme recovery jaringan yang diterapkan
8	SNI - ISO27001 - A.10.6.2	Menerapkan SNMP dalam upaya menjaga sekuritas jaringan
9	SNI - ISO27001 - A.11.5.1	*Log on* procedure
10	SNI - ISO27001 - A.11.5.2	USER ID untuk penggunaan personal masing-masing user
11	SNI - ISO27001 - A.11.5.2	Teknik validasi dalam setiap user id yang terdaftar
12	SNI - ISO27001 - A.11.5.3	System manajemen password
13	SNI - ISO27001 - A.11.5.3	Sistem manajemen password yang interaktif
14	SNI - ISO27001 - A.11.5.5	Mekanisme *session time out*

No	Code	Kontrol
	SNI - ISO27001 - A.11.1.1	Kebijakan yang mengaturakses control aplikasi
	SNI - ISO27001 - A.11.1.1	Dokumentasi kebijakan yang mengaturakses control aplikasi
	SNI - ISO27001 - A.11.2.1	Prosedurregistrasiakunuser ? (dalam hal ini mahasiswa dankaryawan)
	SNI - ISO27001 - A.11.2.1	Prosedur penonaktifan akun user
	SNI - ISO27001 - A.11.2.2	Kebijakan pemberian hak akses kepada user
	SNI - ISO27001 - A.11.2.2	Sistem / program / aplikasi yang digunakan untuk mengelola hak akses user
	SNI - ISO27001 - A.11.2.2	Divisi yang ditunjuk dalam hal pengelolaan hak akses user
	SNI - ISO27001 - A.11.2.3	Mekanisme user mendapatkan password akun / pin akun
	SNI - ISO27001 - A.11.2.4	Review atau pemindaian untuk setiap akun yang ada
	SNI - ISO27001 - A.11.4.1	Kebijakan pemberian servis jaringan untuk user
	SNI - ISO27001 - A.11.4.1	Servis jaringan yang didapatkan user sesuai dengan kebijakan yang ditetapkan management
	SNI - ISO27001 - A.11.4.2	Mekanisme *logon procedure* untuk user sebelum menggunakan atau mendapatkan servis jaringan
	SNI - ISO27001 - A.11.4.4	Petugas khusus yang menangani port jaringan
	SNI - ISO27001 - A.11.3.1	Petunjuk untuk membuat kombinasi password yang baik
	SNI - ISO27001 - A.11.3.1	Mengubah pin standar anda kekombinasi password yang baik
	SNI - ISO27001 - A.11.3.1	Sosialisasi dari manajemen pengelola untuk pengelolaan password

	SNI - ISO27001 - A.11.3.3	Kombinasi password disembunyikan

No	Code	Kontrol
1	SNI – ISO - A.12.1.1	Keamanan system informasi yang dibangun termasuk dalam *business statements*
2	SNI – ISO - A.12.1.1	Keamanan system informasi yang dibangun termasuk dalam perancangan
3	SNI – ISO - A.12.1.1	Implementasi rancangan keamanan sistemtersebut
4	SNI – ISO - A.12.1.1	Pembagian tugas dari manajemen dalam penanganan serangan sistem
5	SNI – ISO - A.12.1.1	Mekanisme keamanan dalam Sistem informasi yang ada
6	SNI – ISO - A.12.1.1	Mekanisme pengamanan tersebut terdokumentasi
7	SNI – ISO - A.12.1.1	Monitoring manajemen kepada petugas terkait mekanisme pengamanan sistem
8	SNI – ISO - A.12.1.1	Petugas selalu mengidentifikasi titik-titik lemah pada system informasi yang ada
9	SNI – ISO - A.12.1.1	Petugas selalu melakukan pengujian terhadap titik lemah yang teridentifikasi
10	SNI – ISO - A.12.4.1	SOP dalam hal operational system informasi yang ada
11	SNI – ISO - A.12.4.3	Petugas yang ditunjuk khusus untuk mengontrol program *source code*
12	SNI – ISO - A.13.1.1	Laporan keamanan system selalu dilaporkan dengan cepat
13	SNI – ISO - A.13.1.2	Petugas melakukan identifikasi titik lemah sistem
14	SNI – ISO - A.13.1.2	Petugas selalu melaporkan temuan kelemahan system kepada manajemen secara berkala
15	SNI – ISO - A.13.2.1	Manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi
16	SNI – ISO - A.13.2.1	Solusi yang diberikan manajemen terhadap insiden efektif
17	SNI – ISO - A.13.2.2	Petugas dan manajemen selalu memonitor dalam penanganan insiden
18	SNI – ISO - A.13.2.2	Pembaharuan mekanisme sistem keamanan

19	SNI – ISO - A.13.2.3	Petugasselalumendokumentasikanserangantersebut
20	SNI – ISO - A.13.2.3	Petugasselalumerincidampak yang dialamidariinsidentersebut

Klausul SNI ISO 27001	Mandatory Requirements untuk Sistem Manajemen Keamanan Informasi
4	**Sistem Manajemen Keamanan Informasi**
4,1	**General Requirements**
	Organisasi harus membangun, mengimplementasi, mengoperasikan, memonitor , mengkaji, merawat dan memperbarui SMKI yang terdokumentasi
4,2	**Membangun dan Menjalankan SMKI**
4.2.1	**Membangun SMKI**
a	Mendefinisikan batasan dan ruang lingkup dari SMKI
b	Mendefinisikan SMKI *Policy*
c	Mendefinisikan *risk assessment approach*
d	Mengidentifikasi Resiko
e	Menganalisis dan mengevaluasi resiko
f	Mengidentifikasi Resiko dan mengevaluasi pilihan penanganan resiko
g	Memilih objek kontrol dan kontrol terhadap penanganan resiko
h	Persetujuan manajemen terhadap usulan *residual risk*
i	Persetujuan manajemen untuk mengimplementasi dan mengoperasikan SMKI
4.2.2	**Mengimplementasikan SMKI**
a	Memformulasikan *risk treatment plan*
b	mengimplementasikan *risk treatment plan* untuk mencapai *control objectives*
c	Mengimplementasikan control yang telah dipilih di (4.2.1 g) agar sesuai dengan
	control objective
d	Mendefinisikan bagaimana mengukur efektifitas dari kontrol yang dipilih atau
	dari kumpulan kontrol dan menyepesifikasi bagaimana hasil pengukuran ini digunakan
	untuk menilai efektifitas control agar menghasilkan hasil yang comparable dan reproducible

e	Mengadakan pelatihan dan *awareness program* (see 5.2.2)
f	Mengelola operasional SMKI
g	Mengelola sumberdaya SMKI (see 5.2)
h	Mengimplementasikan prosedur dan kontrol lainya yang menghandle
	prompt detection of security dan respon untuk *security incident*
4.2.3	**Monitor dan Kajian SMKI**
a	Menjalankan monitoring dan pengkajian prosedur dan kontrol yang ada
	dalam setiap bidang
b	Membuat kajian secara berkala dan rutin terhadap efektifitas dari SMKI
c	Mengukur efektifitas dari kontrol - kontrol yang ada agar sesuai dengan
	security requirements
d	Mengkaji *Risk Assesment* pada waktu yang telah direncanakan, mengkaji
	efek yang ditimbulkan dan mengkaji tingkat resiko yang dapat diterima
e	Mengadakan audit internal terhadap SMKI dalam interval tertentu
f	Melakukan *mangement review* terhadap SMKI secara berkala dan rutin
g	Memperbaharui sistem keamanan berdasarkan temuan dari kegiatan monitoring
	dan kajian
h	Merekam kegiatan yang berdampak langsung terhadap efektifitas dan *perfomance*
	dari SMKI
4.2.4	**Merawat dan Meningkatkan kinerja SMKI**
a	Mengimplementasi dan mengidentifikasi *improvements* dari SMKI
b	Melakukan tindakan korektif dan pencegahan yang sesuai dengan 8.2 dan 8.3
c	Mengkomunikasikan tindakan dan *improvements* yang dilakukan pada semua pihak
	terkait
d	Memastikan bahwa *improvements* telah sesuai dengan tujuan *improvements*

4,3	***Documentation requirements***
4.3.1	**Dokumentasi umum SMKI**
a	Dokumentasi pernyataan *ISMS Policy (see 4.2.1b)* dan objektif
b	Ruang lingkup dari SMKI (*see* 4.2.1a)
c	*Procedures and controls in suport of the isms*
d	Deskripsi dari *risk assessment methodology (see 4.2.1c)*
e	Laporan *risk assessment (see 4.2.1c - 4.2.1g)*
f	*Risk treatment plan (see 4.2.2b)*
g	Prosedur organisasi untuk memastikan efektifitas *planning* , operasional, dan kontrol dari
	psoses pengamanan informasi dan mendiskripsikan bagaimana mengukur efektifitas dari
	semua kontrol (see 4.2.3c)
h	Arsip yang dibutuhkan dalam mengimplementasikan standar ISO 27001
i	Mendefinisikan SoA
4.3.2	**Kontrol dokumentasi**
4.3.2	Dokumen yang dibutuhkan oleh SMKI harus dilindungi dan di kontrol, Dokumentasi prosedur
	harus di dibangun dan dilaksanakan untuk mendefinisikan tindakan yang perlu dilakukan
	manajemen yaitu:
a	Menyetujui dokumen yang akan diterbitkan
b	Mengkaji dan *mengupdate* sesuai kebutuhan kemudian menyetujui kembali
c	Memastikan bahwa status perubahan dan revisi telah diidentifikasi
d	Memastikan ketersedian *applicable documents* sesuai dengan versi yang relevan.
e	Memastikan penggunaan kosa kata dokumen dapat dipahami dengan mudah (Jelas)
f	Memastikan ketersedian dokumen bagi yang membutuhkan , dan disimpan dengan prosedur
	yang jelas dan diklasifikasikan
g	Memastikan dokumen yang berasal dari luar manajemen telah diidentifikasi

h	Memastikan bahwa distribusi dokumen telah diawasi dan dikontrol
i	Mencegah penggunaan dokumen yang tidak berlaku
j	Memberikan identifikasi dokumen yang sesuai untuk memudahkan perawatan
4.3.3	**Kontrol arsip**
a	Membangun sebuah mekanisme kearsipan dokumen
b	Arsip harus diawasi dan dilindungi
c	Arsip harus mudah dijangkau dan mudah diidentifikasi
d	Kontrol kearsipan harus di dokumentasi
5	**Tanggung Jawab Manajemen**
5,1	**Manajemen harus menyediakan bukti komitmenya terhadap penetapan, penerapan,**
	pengoperasian, pemantauan, pengkajian, pemeliharaan dan peningkatan SMKI dengan:
a	Menetapkan kebijakan SMKI
b	Memastikan sasaran dan rencana SMKI telah ditetapkan
c	Menetapkan peran dan tanggung jawab untuk keamanan informasi
d	Mengkomunikasikan kepada organisasi tentang pentingnya memenuhi sasaran keamanan
	informasi dan kesesuain terhadap kebijakan keamanan informasi, tanggung jawabnya berdasarkan hukum dan kebutuhan untuk peningkatan berkelanjutan
e	Menyediakan sumberdaya yang cukup untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI (*see 5.2.1)*
f	Memutuskan kriteria resiko yang dapat diterima dan tingkat keberterimaan resiko.
g	Memastikan bahwa audit internal SMKI dilaksanakan (*see* 6)
h	Melaksanakan kajian SMKI (*see 7)*
5,2	**Manajemen Sumberdaya**
5.2.1	**Ketentuan Sumberdaya**
	Organisasi harus menetapkan dan menyediakan sumberdaya yang dibutuhkan untuk:

a	Menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI
b	Memastikan bahwa prosedur keamanan informasi mendukung persyaratan bisnis
c	Mengidentifikasi dan memenuhi persyaratan hukum dan perundang - undangan serta kewajiban keamanan kontrak
d	Memelihara keamanan secara memadai dengan penerapan yang tepat dari semua pengendalian yang diterapkan
e	Melaksanakan kajian jika diperlukan , dan menindaklanjuti hasil kajian secara tepat
f	Apabila dipersyaratkan , meningkatkan keefektifan SMKI
5.2.2	**Pelatihan, kepedulian dan kompetensi**
	Organisasi harus memastikan bahwa semua personel yang diberikan tanggung jawab yang ditetapkan dalam SMKI kompeten untuk melaksanakan tugas dengan kriteria:
a	Menetapkan kompetensi yang perlu untuk personel yang melaksanakan pekerjaan yang mempengaruhi SMKI
b	Menyediakan pelatihan atau mengambil tindakan lainya (misalnya memperkerjakan personel yang kompeten) untuk memenuhi kebutuhan tersebut
c	Mengevaluasi tindakan yang diambil
d	Memelihara rekaman pendidikan, pelatihan, ketrampilan, pengalaman dan kualifikasi (*see 4.3.3)*
6	**Audit internal SMKI**
	Organisasi harus melaksanakan audit internal SMKI pada interval yang terencana untuk menetapkan sasaran pengendalian, dan kontrol, dengan proses dan
	prosedur sebagai berikut:
a	Sesuai dengan persyaratan Standar ini dan persyaratan hukum atau peraturan perundang-undangan yang berlaku.
b	Sesuai dengan persyaratan keamanan informasi yang diidentifikasi
c	Dilaksanakan dan dipelihara secara efektif
d	Dilaksanakan sesuai yang diharapkan
7	**Kajian manajemen SMKI**

7,1	**Umum**
	Manajemen harus mengkaji SMKI organisasi pada interval yang terencana (minimal setahun sekali) untuk memastikan kesesuaian,
	kecukupan dan kefektifanya secara berkesinambungan
7,2	**Masukan kajian**
	Masukan untuk kajian manajemen harus mencakup
a	Hasil audit dan kajian SMKI
b	Umpan balik dari pihak yang berkempentingan
c	Teknik, produk atau prosedur, yang dapat digunakan dalam organisasi untuk meningkatkan kinerja dan kefektifan SMKI
d	Status tindakan korektif dan tindakan pencegahan
e	Kelemahan atau ancaman yang tidak ditangani secara memadai dalam asasesmen risiko sebelumnya
f	Hasil dari pengukuran keefektifan
g	Tindak lanjut dari kajian manajemen sebelumnya
h	Setiap perubahan yang dapat mempengaruhi SMKI
i	Rekomendasi untuk peningkatan
7,3	**Keluaran kajian**
	Keluaran kajian manajemen harus mencakup setiap keputusan dan tindakan yang terkait hal-hal berikut:
a	Peningkatan keefektifan SMKI
b	Pemutakhiran asesmen resiko dan rencana perlakuan resiko
c	Modifikasi prosedur dan pengendalian yang mempengaruhi keamanan informasi, jika perlu, untuk menanggapi kejadian internal dan eksternal yang dapat berdampak
	SMKI, termasuk perubahan terhadap:
C.1.	Persyaratan bisnis
C.2.	Persyaratan keamanan.
C.3.	Proses bisnis yang mempengaruhi persyaratan bisnis yang ada

C.4.	Persyaratan peraturan perundang-perundangan atau hukum
C.5.	Kewajiban kontrak
C.6.	Tingkat resiko dan/atau kriteria resiko yang dapat diterima
d	Kebutuhan sumberdaya
e	Peningkatan atas keefektifan pengukuran pengendalian.
8	**Peningkatan SMKI**
8,1	**Peningkatan berkelanjutan**
	Organisasi harus meningkatkan keefektifan SMKI secara berkelanjutan melalui kebijakan keamanan informasi, sasaran keamanan informasi, hasil audit, analisis
	kejadian yang dipantau, tindakan korektif dan pencegahan, dan kajian manajemen (see 7)
8,2	**Tindakan korektif**
	Organisasi harus mengambil tindakan untuk menghilangkan penyebab ketidaksesuaian dengan persyaratan SMKI untuk mencegah terulangnya kembali
	ketidaksesuaian tersebut. Prosedur terdokumentasi untuk tindakan korektif harus menetapkan persyaratan untuk:
a	Mengidentifikasi ketidaksesuaian
b	Menetapkan penyebab ketidaksesuaian
c	Mengevaluasi kebutuhan tindakan untuk memastikan bahwa ketidaksesuaian tidak terulang
d	Menetapkan dan menerapkan tindakan korektif yang diperlukan
e	Merekam hasil tindakan yang diambil (*see 4.3.3)*
f	Mengkaji tindakan korektif yang diambil
8,3	**Tindakan Pencegahan**
	Organisasi harus menetapkan tindakan untuk menghilangkan ketidaksesuaian yang mungkin terjadi. Prosedur tindakan pencegahan harus menetapkan
	persyaratan untuk:
a	Mengidentifikasi ketidaksesuaian potensial dan penyebabnya

b	Mengevaluasi kebutuhan tindakan untuk mencegah terulangnya ketidaksesuaian
c	Menetapkan dan menerapkan tindakan pencegahan yang diperlukan
d	Merekam hasil tindakan yang diambil (see 4.3.3)
e	Mengkaji tindakan pencegahan yang diambil

LAMPIRAN F *QuestionList*

CODE	Question	Responsible By				
		CARS	Information System Division	Head Operations	Information and TechnologyDivision	User
Untuk memastikan dan menjamin keamanan informasi pada jaringan dan pengamanan pada infrastructure pendukung jaringan.	**Network Security**					
SNI - ISO27001 - A.10.6.1	Sudah adakah kebijakan pengamananjaringan ?	√			√	
	Apakahsudahterdokumentasi ?	√			√	
SNI - ISO27001 - A.10.6.2	Apakahsudahterdapatmekanismepengamananjaringansebagaiupayapencegahanserangan?	√			√	
SNI - ISO27001 - A.10.6.2	Adakahpembaharuan yang dilakukanterhadapstrategipencegahanseranganpadajaringan?	√			√	
SNI - ISO27001 - A.10.6.2	Apakahmanajemensudahmengidentifikasititikjaringan yang rawanterhadapserangan?	√			√	
SNI - ISO27001 - A.10.6.2	Apakahsudahadatim/petugas yang khususmenanganikeamananjaringan?	√			√	
SNI - ISO27001 - A.10.6.2	Apabilaserangantelahterjadi, adakahmekanisme recovery jaringan yang diterapkan?	√			√	
SNI - ISO27001 - A.10.6.2	Apakahmanajemensudahmenerapkan SNMP dalamupayamenjagasekuritasjaringan?	√			√	

Untukmencegah*Unauthorized access*padasistemoperasi	**Operating System Access Control**					
SNI - ISO27001 - A.11.5.1	Apakahsudahada*log on* procedure ?	√			√	
SNI - ISO27001 - A.11.5.2	Apakahsetiap user sudahmempunyai USER ID untukpenggunaan personal masing-masing user?	√			√	
SNI - ISO27001 - A.11.5.2	Apakahsudahadateknikvalidasidalamsetiap user id yang terdaftar ?	√			√	
SNI - ISO27001 - A.11.5.3	Apakahsudahada system manajemen password?	√			√	
SNI - ISO27001 - A.11.5.3	Apakahsistemmanajemen password yang adasudahinteraktif ?	√			√	
SNI - ISO27001 - A.11.5.5	Apakahsudahadamekanisme*session time out* ?	√			√	
Kehandalansisteminformasi, pengembangandanperawatan						
Untukmemastikanbahwakeamananadalahbagianpentingdarisisteminformasi	**Persyaratankeamanandarisisteminformasi**					
SNI – ISO - A.12.1.1	Padatahapperancangansistem, apakahkeamanansisteminformasi yang dibangunsudahtermasukdalam*business statements*?		√			
SNI – ISO - A.12.1.1	Padatahapperancangansistem, apakahkeamanansisteminformasi yang dibangunsudahtermasukdalamperancangan?		√			
SNI – ISO - A.12.1.1	Padasaatsisteminformasisudahterbangun, apakahrancangankeamanansistemtersebutsudahterimplementasi?		√			
SNI – ISO - A.12.1.1	Adakahpembagiantugasdarimanajemendalampenangananserangansistem?		√			
SNI – ISO - A.12.1.1	Apabilaterjadiseranganpadasistem,SudahadakahmekanismekeamanandalamSisteminformasi yang ada?		√			
SNI – ISO - A.12.1.1	Apakahmekanismepengamanantersebutsudahterdokumentasi?		√			
SNI – ISO - A.12.1.1	Apakahada monitoring manajemenkepadapetugasterkaitmekanismepengamanansistem?		√			
SNI – ISO - A.12.1.1	Apakahpetugasselalumengidentifikasititik-titiklemahpadasisteminformasi yang ada?		√			
SNI – ISO - A.12.1.1	Apakahpetugasselalumelakukanpengujianterhadaptitiklemah yang teridentifikasi?		√			
Keamanan*system file*						

SNI – ISO - A.12.4.1	Apakahsudahada SOP dalamhal operational sisteminformasi yang ada?		√			
SNI – ISO - A.12.4.3	Sudahadakahpetugas yang ditunjukkhususuntukmengontrol program *source code?*		√			
ManajemenPenangananinsidenpadasisteminformasi						
Untukmemastikansemuahal yang berhubungandengankeamanansisteminformasidankelemahansisteminformasidikomunikasikandenganbenar, cepat, danakuratkepadamanajemen	**Laporansemuahal yang berhubungandengankeamanansisteminformasidankelemahansisteminformasi**					
SNI – ISO - A.13.1.1	Apakahlaporankeamanansistemselaludilaporkandengancepat?		√			
SNI – ISO - A.13.1.2	Apakahpetugassudahmelakukanidentifikasititiklemahsistem?		√			
SNI – ISO - A.13.1.2	Apakahpetugasselalumelaporkantemuankelemahansistemkepadamanajemensecarab erkala?		√			
Untukmemastikantindakanyanefektifdantepatdalamhalpenangananinsidenkeamanansisteminformasi	**Manajemenkeamanansisteminformasidanpembaharuan**					
SNI – ISO - A.13.2.1	Apakahmanajemensudahmemberikanrespon yang cepatterhadaplaporankeamanansisteminformasi?		√			
SNI – ISO - A.13.2.1	Apakahsolusi yang diberikanmanajementerhadapinsidensudahefektif?		√			
SNI – ISO - A.13.2.2	Apakahpetugasdanmanajemenselalumemonitordalampenangananinsiden?		√			
SNI – ISO - A.13.2.2	Apakahadapembaharuanmekanismesistemkeamanan?		√			
SNI – ISO - A.13.2.3	Apabilaterjadiinsiden, apakahpetugasselalumendokumentasikanserangantersebut?		√			
SNI – ISO - A.13.2.3	Apabilaterjadiinsiden, apakahpetugasselalumerincidampak yang dialamidariinsidentersebut?		√			

Application Access Control						
Untukmengontrolaksesinformasi	**Persyaratanbisnisuntuk control akses**					
SNI - ISO27001 - A.11.1.1	Apakahsudahadakebijakan yang mengaturakses control aplikasi ?			√		
SNI - ISO27001 - A.11.1.1	Apakahsudahterdokumentasi ?			√		
Untukmemastikan user yang mengaksesaplikasiadalah user yang mempunyai*previlages*danmenghindariakses illegal terhadapsisteminformasi	**Manajemenaksesuntuk user**					
SNI - ISO27001 - A.11.2.1	Apakahsudahadaprosedurregistrasiakunuser ? (dalamhalinimahasiswadankaryawan)			√		
SNI - ISO27001 - A.11.2.1	Apakahsudahadaprosedurpenonaktifanakunuser ?			√		
SNI - ISO27001 - A.11.2.2	Sudahadakahkebijakanpemberianhakakseskepadauser ?			√		
SNI - ISO27001 - A.11.2.2	Sudahadakahsistem / program / aplikasi yang digunakanuntukmengelolahakaksesuser ?			√		
SNI - ISO27001 - A.11.2.2	Sudahadakahdivisi yang ditunjukdalamhalpengelolaanhakaksesuser ?			√		
SNI - ISO27001 - A.11.2.3	Bagaimanamekanisme user mendapatkan password akun / pin akun?			√		
SNI - ISO27001 - A.11.2.4	Apakahmanajemenselalumelakukan review ataupemindaianuntuksetiapakun yang ada ?			√		
Untukmencegahakses illegal terhadaplayananjaringan	**Kontrolaksesjaringan**					
SNI - ISO27001 - A.11.4.1	Adakahkebijakanpemberianservisjaringanuntukuser ?			√		
SNI - ISO27001 - A.11.4.1	Apakahservisjaringan yang didapatkan user sudahsesuaidengankebijakan yang ditetapkanmanagement ?			√		
SNI - ISO27001 - A.11.4.2	Apakahadamekanisme*logon procedure* untuk user sebelummenggunakanataumendapatkanservisjaringan?			√		
SNI - ISO27001 - A.11.4.4	Adakahpetugaskhusus yang menangani port jaringan?			√		

Untuk mencegahakses akun illegal, dan pengamanan informasi	**User Responsibilities**					
SNI - ISO27001 - A.11.3.1	Apakahadapetunjukuntukmembuatkombinasi password yang baik?					√
SNI - ISO27001 - A.11.3.1	Apakahandamengubah pin standarandakekombinasi password yang baik?					√
SNI - ISO27001 - A.11.3.1	Adakahsosialisasidarimanajemenpengelolauntukpengelolaan password?					√
SNI - ISO27001 - A.11.3.3	Ketikamengisikan password, apakahkombinasi password sudahdisembunyikan ?					√

LAMPIRAN G *Review Assesment*

Klausul SNI ISO 27001	Mandatory Requirements untuk Sistem Manajemen Keamanan Informasi	
4	**Sistem Manajemen Keamanan Informasi**	
4,1	**General Requirements**	
	Organisasi harus membangun, mengimplementasi, mengoperasikan, memonitor , mengkaji, merawat dan memperbarui SMKI yang terdokumentasi	D
4,2	**Membangun dan Menjalankan SMKI**	
4.2.1	**Membangun SMKI**	
a	Mendefinisikan batasan dan ruang lingkup dari SMKI	MD
b	Mendefinisikan SMKI *Policy*	D
c	Mendefinisikan *risk assessment approach*	RD
d	Mengidentifikasi Resiko	D
e	Menganalisis dan mengevaluasi resiko	RD
f	Mengidentifikasi Resiko dan mengevaluasi pilihan penanganan resiko	RD
g	Memilih objek kontrol dan kontrol terhadap penanganan resiko	RD
h	Persetujuan manajemen terhadap usulan *residual risk*	D
i	Persetujuan manajemen untuk mengimplementasi dan mengoperasikan SMKI	D
4.2.2	**Mengimplementasikan SMKI**	
a	Memformulasikan *risk treatment plan*	RD
b	mengimplementasikan *risk treatment plan* untuk mencapai *control objectives*	RD
c	Mengimplementasikan control yang telah dipilih di (4.2.1 g) agar sesuai dengan	RD
	control objective	
d	Mendefinisikan bagaimana mengukur efektifitas dari kontrol yang dipilih atau	PNP
	dari kumpulan kontrol dan menyepesifikasi bagaimana hasil pengukuran ini digunakan	

	untuk menilai efektifitas control agar menghasilkan hasil yang comparable dan reproducible	
e	Mengadakan pelatihan dan *awareness program* (see 5.2.2)	RD
f	Mengelola operasional SMKI	D
g	Mengelola sumberdaya SMKI (see 5.2)	D
h	Mengimplementasikan prosedur dan kontrol lainya yang menghandle	D
	prompt detection of security dan respon untuk *security incident*	
4.2.3	**Monitor dan Kajian SMKI**	
a	Menjalankan monitoring dan pengkajian prosedur dan kontrol yang ada	D
	dalam setiap bidang	
b	Membuat kajian secara berkala dan rutin terhadap efektifitas dari SMKI	PNP
c	Mengukur efektifitas dari kontrol - kontrol yang ada agar sesuai dengan	PNP
	security requirements	
d	Mengkaji *Risk Assesment* pada waktu yang telah direncanakan, mengkaji	RD
	efek yang ditimbulkan dan mengkaji tingkat resiko yang dapat diterima	
e	Mengadakan audit internal terhadap SMKI dalam interval tertentu	NA (Not Applicable)
f	Melakukan *mangement review* terhadap SMKI secara berkala dan rutin	PNP
g	Memperbaharui sistem keamanan berdasarkan temuan dari kegiatan monitoring	RD
	dan kajian	
h	Merekam kegiatan yang berdampak langsung terhadap efektifitas dan *perfomance*	PNP
	dari SMKI	
4.2.4	**Merawat dan Meningkatkan kinerja SMKI**	
a	Mengimplementasi dan mengidentifikasi *improvements* dari SMKI	D
b	Melakukan tindakan korektif dan pencegahan yang sesuai dengan 8.2 dan 8.3	D

c	Mengkomunikasikan tindakan dan *improvements* yang dilakukan pada semua pihak	D
	terkait	
d	Memastikan bahwa *improvements* telah sesuai dengan tujuan *improvements*	D
4,3	***Documentation requirements***	
4.3.1	**Dokumentasi umum SMKI**	
a	Dokumentasi pernyataan *ISMS Policy (see 4.2.1b)* dan objektif	MD
b	Ruang lingkup dari SMKI (*see* 4.2.1a)	RD
c	*Procedures and controls in suport of the isms*	MD
d	Deskripsi dari *risk assessment methodology (see 4.2.1c)*	D
e	Laporan *risk assessment (see 4.2.1c - 4.2.1g)*	RD
f	*Risk treatment plan (see 4.2.2b)*	RD
g	Prosedur organisasi untuk memastikan efektifitas *planning* , operasional, dan kontrol dari	PNP
	psoses pengamanan informasi dan mendiskripsikan bagaimana mengukur efektifitas dari	
	semua kontrol (see 4.2.3c)	
h	Arsip yang dibutuhkan dalam mengimplementasikan standar ISO 27001	NA (Not Applicable)
i	Mendefinisikan SoA	NA (Not Applicable)
4.3.2	**Kontrol dokumentasi**	
4.3.2	Dokumen yang dibutuhkan oleh SMKI harus dilindungi dan di kontrol, Dokumentasi prosedur	
	harus di dibangun dan dilaksanakan untuk mendefinisikan tindakan yang perlu dilakukan	
	manajemen yaitu:	
a	Menyetujui dokumen yang akan diterbitkan	D
b	Mengkaji dan *mengupdate* sesuai kebutuhan kemudian menyetujui kembali	RD
c	Memastikan bahwa status perubahan dan revisi telah diidentifikasi	D

d	Memastikan ketersedian *applicable documents* sesuai dengan versi yang relevan.	D
e	Memastikan penggunaan kosa kata dokumen dapat dipahami dengan mudah (Jelas)	D
f	Memastikan ketersedian dokumen bagi yang membutuhkan , dan disimpan dengan prosedur	RD
	yang jelas dan diklasifikasikan	
g	Memastikan dokumen yang berasal dari luar manajemen telah diidentifikasi	RD
h	Memastikan bahwa distribusi dokumen telah diawasi dan dikontrol	D
i	Mencegah penggunaan dokumen yang tidak berlaku	MD
j	Memberikan identifikasi dokumen yang sesuai untuk memudahkan perawatan	MD
4.3.3	**Kontrol arsip**	
a	Membangun sebuah mekanisme kearsipan dokumen	D
b	Arsip harus diawasi dan dilindungi	D
c	Arsip harus mudah dijangkau dan mudah diidentifikasi	D
d	Kontrol kearsipan harus di dokumentasi	MD
5	**Tanggung Jawab Manajemen**	
5,1	**Manajemen harus menyediakan bukti komitmenya terhadap penetapan, penerapan,**	
	pengoperasian, pemantauan, pengkajian, pemeliharaan dan peningkatan SMKI dengan:	
a	Menetapkan kebijakan SMKI	D
b	Memastikan sasaran dan rencana SMKI telah ditetapkan	D
c	Menetapkan peran dan tanggung jawab untuk keamanan informasi	RD
d	Mengkomunikasikan kepada organisasi tentang pentingnya memenuhi sasaran keamanan	PNP
	informasi dan kesesuain terhadap kebijakan keamanan informasi, tanggung jawabnya berdasarkan hukum dan kebutuhan untuk peningkatan berkelanjutan	
e	Menyediakan sumberdaya yang cukup untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI (*see 5.2.1)*	RD

f	Memutuskan kriteria resiko yang dapat diterima dan tingkat keberterimaan resiko.	RD
g	Memastikan bahwa audit internal SMKI dilaksanakan (*see* 6)	PNP
h	Melaksanakan kajian SMKI (*see 7)*	RD
5,2	**Manajemen Sumberdaya**	
5.2.1	**Ketentuan Sumberdaya**	
	Organisasi harus menetapkan dan menyediakan sumberdaya yang dibutuhkan untuk:	
a	Menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI	D
b	Memastikan bahwa prosedur keamanan informasi mendukung persyaratan bisnis	RD
c	Mengidentifikasi dan memenuhi persyaratan hukum dan perundang - undangan serta kewajiban keamanan kontrak	D
d	Memelihara keamanan secara memadai dengan penerapan yang tepat dari semua pengendalian yang diterapkan	RD
e	Melaksanakan kajian jika diperlukan , dan menindaklanjuti hasil kajian secara tepat	PNP
f	Apabila dipersyaratkan , meningkatkan keefektifan SMKI	PNP
5.2.2	**Pelatihan, kepedulian dan kompetensi**	
	Organisasi harus memastikan bahwa semua personel yang diberikan tanggung jawab yang ditetapkan dalam SMKI kompeten untuk melaksanakan tugas dengan kriteria:	
a	Menetapkan kompetensi yang perlu untuk personel yang melaksanakan pekerjaan yang mempengaruhi SMKI	D
b	Menyediakan pelatihan atau mengambil tindakan lainya (misalnya memperkerjakan personel yang kompeten) untuk memenuhi kebutuhan tersebut	D
c	Mengevaluasi tindakan yang diambil	PNP
d	Memelihara rekaman pendidikan, pelatihan, ketrampilan, pengalaman dan kualifikasi (*see 4.3.3)*	D
6	**Audit internal SMKI**	
	Organisasi harus melaksanakan audit internal SMKI pada interval yang terencana untuk menetapkan	

	sasaran pengendalian, dan kontrol, dengan proses dan	
	prosedur sebagai berikut:	
a	Sesuai dengan persyaratan Standar ini dan persyaratan hukum atau peraturan perundang-undangan yang berlaku.	PNP
b	Sesuai dengan persyaratan keamanan informasi yang diidentifikasi	PNP
c	Dilaksanakan dan dipelihara secara efektif	PNP
d	Dilaksanakan sesuai yang diharapkan	PNP
7	**Kajian manajemen SMKI**	
7,1	**Umum**	
	Manajemen harus mengkaji SMKI organisasi pada interval yang terencana (minimal setahun sekali) untuk memastikan kesesuaian,	RD
	kecukupan dan kefektifanya secara berkesinambungan	
7,2	**Masukan kajian**	
	Masukan untuk kajian manajemen harus mencakup	
a	Hasil audit dan kajian SMKI	RD
b	Umpan balik dari pihak yang berkempentingan	PNP
c	Teknik, produk atau prosedur, yang dapat digunakan dalam organisasi untuk meningkatkan kinerja dan kefektifan SMKI	D
d	Status tindakan korektif dan tindakan pencegahan	D
e	Kelemahan atau ancaman yang tidak ditangani secara memadai dalam asasesmen risiko sebelumnya	D
f	Hasil dari pengukuran keefektifan	PNP
g	Tindak lanjut dari kajian manajemen sebelumnya	D
h	Setiap perubahan yang dapat mempengaruhi SMKI	D
i	Rekomendasi untuk peningkatan	D
7,3	**Keluaran kajian**	

	Keluaran kajian manajemen harus mencakup setiap keputusan dan tindakan yang terkait hal-hal berikut:	
a	Peningkatan keefektifan SMKI	D
b	Pemutakhiran asesmen resiko dan rencana perlakuan resiko	D
c	Modifikasi prosedur dan pengendalian yang mempengaruhi keamanan informasi, jika perlu, untuk menanggapi kejadian internal dan eksternal yang dapat berdampak	
	SMKI, termasuk perubahan terhadap:	D
C.1.	Persyaratan bisnis	D
C.2.	Persyaratan keamanan.	D
C.3.	Proses bisnis yang mempengaruhi persyaratan bisnis yang ada	D
C.4.	Persyaratan peraturan perundang-perundangan atau hukum	NA (Not Applicable)
C.5.	Kewajiban kontrak	D
C.6.	Tingkat resiko dan/atau kriteria resiko yang dapat diterima	D
d	Kebutuhan sumberdaya	MD
e	Peningkatan atas keefektifan pengukuran pengendalian.	PNP
8	**Peningkatan SMKI**	
8,1	**Peningkatan berkelanjutan**	
	Organisasi harus meningkatkan keefektifan SMKI secara berkelanjutan melalui kebijakan keamanan informasi, sasaran keamanan informasi, hasil audit, analisis	RD
	kejadian yang dipantau, tindakan korektif dan pencegahan, dan kajian manajemen (see 7)	
8,2	**Tindakan korektif**	
	Organisasi harus mengambil tindakan untuk menghilangkan penyebab ketidaksesuaian dengan persyaratan SMKI untuk mencegah terulangnya kembali	
	ketidaksesuaian tersebut. Prosedur terdokumentasi untuk tindakan korektif harus menetapkan persyaratan untuk:	

a	Mengidentifikasi ketidaksesuaian	D
b	Menetapkan penyebab ketidaksesuaian	D
c	Mengevaluasi kebutuhan tindakan untuk memastikan bahwa ketidaksesuaian tidak terulang	RD
d	Menetapkan dan menerapkan tindakan korektif yang diperlukan	D
e	Merekam hasil tindakan yang diambil (*see 4.3.3)*	MD
f	Mengkaji tindakan korektif yang diambil	RD
8,3	**Tindakan Pencegahan**	
	Organisasi harus menetapkan tindakan untuk menghilangkan ketidaksesuaian yang mungkin terjadi. Prosedur tindakan pencegahan harus menetapkan	
	persyaratan untuk:	
a	Mengidentifikasi ketidaksesuaian potensial dan penyebabnya	RD
b	Mengevaluasi kebutuhan tindakan untuk mencegah terulangnya ketidaksesuaian	RD
c	Menetapkan dan menerapkan tindakan pencegahan yang diperlukan	RD
d	Merekam hasil tindakan yang diambil (see 4.3.3)	PNP
e	Mengkaji tindakan pencegahan yang diambil	RD

Detail Control Objective	Responsible by	Description
Network Security	Compliance, Audit, Risk and Security (CARS)	Proses pengamanan jaringanuntukpengelolaan SIA sudahdilakukandenganberbagaiusahadiantaranya SNMP
	Information and Technology Division	Proses pengamananjaringanuntukpengelolaan SIA sudahdilakukan, pengamananinsidendilakukaninsidental
	Auditor	Belumada standard dandokumentasi yang jelasuntukdijadikanacuanpengamanan. Proses yang adahanyamengikutipola yang sudahada
	Maturity Score	2
Operating System Access Control	Compliance, Audit, Risk and Security (CARS)	Usaha untukmelindungikeamanan SIA sudahditunjangmelaluisistemoperasi yang digunakan. Semuaprosedursudahdidokumentasikan
	Information and Technology Division	Aplikasi yang menunjangpengelolaan SIA memiliki*active session* selama 60 menitjadi user harusmelakukan logon untuk 60 menitakses
	Auditor	Usaha untukmelindungiinformasidanaksesterhadapinformasisudahbagus, hanyasajatidakada monitoring danpelatihan yang berkaladilakukan
	Maturity Score	2

Detail Control Objective	Responsible by	Description
KehandalanSistemInformasi, Pengembangan, danPerawatan	Information System Division	Polakeamanandalamsisteminformasisudahtercantumdalam*business statements* hanyasajabelumterimplementasi, mekanismepengamanansisteminformasioleh petugastidakdilakukansecaraberkala, tidakada monitoring untukmengawasimekanismepengamanansisteminformasi, penangananinsidendilakukansecara incidental saja.
	Auditor	Polakeamanansudahterdokumentasi, hanyasajaimplementasidaripolakeamanantersebutbelumberjalan, belumadatindakan pro aktifseperti monitoring danidentifikasi*weakness spot* yang mungkinmenjadititikinsiden.
	Maturity Score	2
ManajemenPenangananinsidenpadaSistemInformasi	Information System Division	Tidakmengimplementasikan fast report walopunsolusiefektifdarimanajementetapdiberikan.
	Auditor	*Fast report* tidakdiimplementasikanpadahalsangatbergunasebagaibahanlaporandanevaluasi.Walapunbegitumanajemenselalumemberikansolusiuntuksetiapinsiden.
	Matuirity Score	2