AUDIT KEAMANAN INFORMASI BERDASARKAN STANDAR SNI-ISO 27001 PADA SISTEM ADMISI UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh:

Dwi Indah Permatasari

12651062

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2016

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/2529/2016

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

Yang dipersiapkan dan disusun oleh :
Nama : Dwi Indah Permatasari
NIM : 12651062
Telah dimunaqasyahkan pada : Senin, 18 Juli 2016
Nilai Munaqasyah : A / B
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.19710209 200501 1 003

Penguji II

Nurochman, M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 27 Juli 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Dwi Indah Permatasari
NIM : 12651062
Judul Skripsi : Audit Keamanan Informasi Berdasarkan Standar SNI - ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 24 Juni 2016
Pembimbing

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

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama	: Dwi Indah Permatasari
NIM	: 12651062
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul "**Audit Keamanan Informasi Berdasarkan Standar SNI – ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta"** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 24 Juni 2016

Yang Menyatakan,

Dwi Indah Permatasari

NIM. 12651062

KATA PENGANTAR

Segala puji syukur penulis panjatkan hanya bagi Allah Subhanahu wa Ta'ala Tuhan seluruh alam semesta. Shalawat dan salam kita curahkan kepada Nabi kita Nabi Muhammad Shallallahu 'Alaihi wa Sallam. Alhamdulillah, segala puji bagi Allah yang telah memberikan kekuatan kepada penulis dalam menyelesaikan skripsi yang berjudul "**Audit Keamanan Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta".**

Skripsi ini diselesaikan untuk memenuhi salah satu syarat guna mencapai gelar kesarjanaan pada program studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Selesainya tugas akhir ini tentunya tidak lepas dari dorongan dan uluran tangan berbagai pihak. Oleh karena itu, penulis mengucapkan rasa terima kasih dan penghargaan kepada :

1. Ayah – Ibu dan seluruh anggota keluarga yang tak henti-hentinya memberikan do'a, semangat, nasihat, motivasi dan dukungannya.
2. Bapak Prof. Drs. Yudian Wahyudi, M.A. Ph.D., selaku Rektor UIN Sunan Kalijaga Yogyakarta.
3. Bapak Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

4. Bapak Sumarsono, S.T., M.Kom., selaku Ketua Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
5. Bapak Nurochman, M.Kom., selaku Sekretaris Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
6. Bapak M. Mustakim , M.T selaku Dosen pembimbing yang dengan sabar memberikan masukan dan arahan selama penyusunan skripsi.
7. Bapak Agus Mulyanto, S.Si., M.Kom., selaku Dosen Pembimbing Akademik yang telah memberikan dukungan kepada penulis.
8. Bapak dan Ibu Dosen Teknik Informatika UIN SUNAN KALIJAGA yang telah memberikan banyak ilmu dan nasihat kepada penulis.
9. Agung Fatwanto, S.Si., M.Kom, Ph.D, selaku kepala UPT PTIPD UIN Sunan Kalijaga yang telah memberikan izin penelitian.
10. Seluruh staf UPT PTIPD UIN Sunan Kalijaga yang telah bersedia meluangkan waktunya menjadi responden untuk pengambilan data penelitian.
11. Teman – teman Program Studi Teknik Informatika angkatan 2012 atas segala bantuan dan dukungannya dalam pelaksanaan skripsi.
12. Semua pihak yang tidak mungkin penulis sebutkan satu-persatu dalam membantu pelaksanaan dan penyusunan skripsi.

Akhirnya penulis hanya dapat bersyukur kepada Allah semoga semua yang telah dilakukan selama ini menjadi amal dan bekal di akhirat nanti.

Penulis menyadari sepenuhnya masih banyak kesalahan dan kekurangan dalam skripsi ini, maka dari itu berbagai saran dan kritik sangat diharapkan demi perbaikan. Semoga skripsi ini dapat bermanfaat bagi penulis sendiri pada khususnya dan bagi para pembaca pada umumnya. Terima kasih.

Yogyakarta, 20 Juni 2016

Penulis,

Dwi Indah Permatasari

NIM.12651062

HALAMAN PERSEMBAHAN

Alhamdulillahirrabbil'alamin. Segala puji bagi Allah Tuhan Semesta Alam atas nikmat yang Engkau berikan sehingga penulis bisa menyelesaikan Penulisan Skripsi.

Kupersembahkan skripsi ini kepada :

- Orang tuaku tercinta, Bapak Bakrun, SP.d dan Ibu Umu Basiroh, mereka yang tak henti-hentinya memanjatkan do'a memberikan nasihat, motivasi, semangat dan dukungan baik moril maupun materiil kepada penulis. Semoga Allah memberkahi dan mengumpulkan kita di JannahNya.
- Kakakku Wawan Adi Setiawan SP.d yang sangat baik yang selalu mendidikku, memberi contoh serta memotivasiku.
- Keluarga Besar Trah Asmodyono dan Mbah H. Jamil yang telah memberikan segala dukungan dan pengarahan.
- Si Mery dan si Warior yang selalu menemaniku selama di Jogja.
- Bapak Mustakim selaku dosen pembimbing yang selalu memberikan solusi dalam menyelesaikan skripsi ini.
- Dosen-dosen TIF UIN SUKA, Pak Sumarsono, Pak Agus, Pak Mustakim, Pak Bambang, Pak Nurochman, Pak Didik, Pak Aulia, Pak Agung, Pak Taufik, Bu Uyun, Bu Ade, semoga ilmu yang disampaikan dapat bermanfaat dan menjadi amal jariyah.

- Pak Agung Fatwanto selaku kepala UPT PTIPD UIN Sunan Kalijaga yang telah memberikan izin penelitian.
- Keluarga UPT PTIPD UIN Sunan Kalijaga terimakasih atas semua bantuan dan kerjasama-nya.
- Teman – teman seperjuangan (KATAK) yang telah banyak membantu Zuni, Wiji, Ulfa, Erin, Kiki, Lusi, Ripa, Meta, KATAK cewek, Juhdan, Eri, mas Helmi, Rizky, Baini, Ikhsan, Kharisma dan semua teman Kelas K T.Informatika Mandiri 2012.
- Teman – teman Kos Muslimah Azizah , Sofia, Aisah, Akvi, Nona dkk yang telah memberikan dukungan dan semangat.
- Sahabatku tercinta dari kecil, terimakasih ELIA SOVINA MARDANI yang selalu memberikan nasihat, saran, dan dukungannya.
- Teman – teman KKN 86 kelompok 120 Putri, Sabil, Fatma, Fina, Kholidi, Irba', Chilmi, Mas Qodli, Mas Rokhim, yang selalu bisa membuat aku tertawa dan mejadi temen ngetrip, terimakasih atas dukungan selama ini.
- Kakak-kakak TIF UIN Sunan Kalijaga, Mas Arbi, Mas Heri, Mas Datofa, Mas Herman, Mas Aziz dll terimakasih untuk semua sharing ilmu yang kita lakukan.
- Mbah Kasinun, Budhe Kar, Pak Tarzan, Pak Tulus terimakasih atas do'a dan dukungannya.
- Kepada semua teman-teman dan pihak yang lainnya, yang sudah memberikan semangat dalam menyelesaikan skripsi ini.

HALAMAN MOTTO

Allah tidak membebani seseorang itu melainkan sesuai dengan kesanggupannya (Q.S. Al-Baqarah: 286)

Hai orang-orang beriman, jadikanlah sabar dan shalatmu sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar (Q.S. Al-Baqarah: 153)

Sesungguhnya bersama kesulitan itu ada kemudahan (Q.S. Al-Insyirah: 5-6)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

AUDIT KEAMANAN INFORMASI BERDASARKAN STANDAR SNI-ISO 27001 PADA SISTEM ADMISI UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

Dwi Indah Permatasari
NIM: 12651062

INTISARI

Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) merupakan salah satu Unit Pelaksana Teknis (UPT) yang mengelola seluruh aset teknologi informasi yang ada di UIN Sunan Kalijaga Yogyakarta. Salah satu pemanfaatan teknologi informasi yang dikelola PTIPD adalah sistem Admisi. Dengan adanya Sistem Admisi akan mempermudah pengelolaan pendaftaran dan penerimaan calon mahasiswa baru secara *online.* Namun dengan adanya sistem informasi yang diterapkan tentunya perlu dilakukan pengamanan terhadap semua data yang dimiliki oleh PTIPD.

Oleh karena itu, untuk mendapatkan keamanan sebuah layanan sistem informasi yang baik maka perlu adanya audit dari sistem Admisi dengan menggunakan standar SNI – ISO 27001. Standar ini secara resmi yang digunakan oleh pemerintah Indonesia dan adopsi otentik dari standar 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 hasil penelitian ini, dapat disimpulkan bahwa tingkat kematangan keamanan informasi sistem Admisi di UIN Sunan Kalijaga pada skala 2,08 *(Repeatable but Intuitive).* Jadi PTIPD telah mempunyai mekanisme perencanaan, prosedur yang berlaku dan *recovery* pasca serangan, tetapi tidak didokumentasikan. UPT PTIPD yang mengelola sistem Admisi belum mengadakan program pelatihan formal, yang bertujuan untuk mengkomunikasikan prosedur dan tanggung jawab masing- masing individu.

Kata kunci : Audit Sistem, keamanan informasi, SNI – ISO 27001, tingkat kematangan.

INFORMATION SECURITY AUDIT BASED ON SNI – ISO 27001 STANDARDS IN ADMISSION SYSTEM ISLAMIC STATE UNIVERSITY SUNAN KALIJAGA YOGYAKARTA

Dwi Indah Permatasari

NIM: 12651062

ABSTRACT

Center for Information Technology and Data Bases (PTIPD) is one of the Technical Implementation Unit (UPT) which manages the entire information technology assets in UIN Sunan Kalijaga Yogyakarta. One of the utilization of information technology managed by PTIPD is the Admission System With the Admission System will simplify the management of registration and admission of new students online. But with the applied information systems would need to be safeguards to all data owned by PTIPD

Therefore, to get the security of a good information system services it is necessary to audit of the system Admission using ISO standards - ISO 27001. This standard is officially used by the government of Indonesia and authentic adoption of the ISO 27001 standard for measuring the performance management system information security using SNI - ISO 27001, Maturity Model is used with the intention to see a representation of the current state

From this research, it can be concluded that the level of maturity of information security systems Admission in UIN Sunan Kalijaga on a scale of 2.08 (Repeatable but Intuitive). So PTIPD already have planning mechanisms, and recovery procedures in force after the attacks, but not documented. UPT PTIPD which manage admission system has not held a formal training program, which aims to communicate the procedures and responsibilities of each individual.

Keywords: Audit System, maturity level , SNI - ISO 27001, the information security.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Lebih jauh banyak pihak yang beranggapan bahwa era sekarang merupakan zaman informasi atau dikenal dengan *information based society.* Seiring dengan perkembangan teknologi informasi, berbagai bidang pekerjaan seperti pendidikan, kedokteran, lembaga pemerintahan, maupun individual telah menggunakan perangkat teknologi.

Salah satu perguruan tinggi yang mengikuti perkembangan teknologi adalah Universitas Islam Negeri Sunan Kalijaga. Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) merupakan salah satu Unit Pelaksana Teknis (UPT) atau unsur penunjang di UIN Sunan Kalijaga Yogyakarta yang mengelola seluruh aset teknologi informasi yang ada di UIN Sunan Kalijaga Yogyakarta. Salah satu sistem informasi yang dikelola PTIPD adalah Sistem Admisi. Sistem Admisi dibuat untuk mengelola pendaftaran dan penerimaan calon mahasiswa baru secara *online.* Dengan demikian dapat memudahkan bagi calon mahasiswa baru untuk melakukan pendaftaran tanpa harus mendatangi kampus tersebut.

Mengingat pentingnya informasi yang ada pada Sistem Admisi, maka diperlukan kebijakan tentang keamanan sistem informasi. Kebijakan keamanan informasi yang baik setidaknya mencakup beberapa prosedur seperti prosedur pengendalian dokumen, prosedur pengendalian rekaman, prosedur tindakan

perbaikan dan pencegahan, dan prosedur penanganan insiden / gangguan keamanan informasi.

Untuk menjamin keamanan informasi pada sistem Admisi maka diperlukan audit keamanan sistem. Salah satu standar yang sering digunakan dalam meng audit manajemen keamanan informasi adalah SNI - ISO 27001. SNI ISO 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep tata kelola keamanan informasi di dalam sebuah oraganisasi.

Oleh karena itu, dengan uraian diatas penulis mengambil tema audit keamanan sistem informasi dengan judul ***"AUDIT KEAMANAN INFORMASI BERDASARKAN STANDAR SNI-ISO 27001 PADA SISTEM ADMISI 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 penelitian yang saya ambil, terdapat beberapa poin-poin penting yang yang akan diteliti, antara lain :

a. Bagaimana memberikan penilaian tata kelola keamanan Sistem Admisi UIN Sunan Kalijaga Yogyakarta sesuai standar SNI ISO 27001?

b. Bagaimana merekomendasikan tata kelola keamanan Sistem Admisi UIN Sunan Kalijaga Yogyakarta sesuai standar SNI ISO 27001 ?

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Adapun tujuan dari penelitian yang dilakukan antara lain :

a. Menghasilkan penilaian tata kelola tingkat keamanan Sistem Admisi di UIN Sunan Kalijaga Yogyakarta sesuai standar SNI – ISO 27001.
b. Menghasilkan rekomendasi tata kelola keamanan Sistem Admisi yang baik sesuai standar SNI - ISO 27001.

1.3.2. Manfaat Penelitian

a. Memahami bagaimana audit sistem informasi dengan standar ISO 27001 yang diterapkan pada Sistem Admisi UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.
b. Memperoleh kondisi aktual tentang Sistem Manajemen Keamanan Informasi (SMKI) di Sistem Admisi di UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.
c. Mengoptimalkan pelayanan kinerja sistem dari Sistem Admisi di UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA.
d. Menghasilkan dokumen temuan dan rekomendasi dari hasil audit keamanan sistem Admisi di UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA yang dapat digunakan sebagai dokumentasi pengembangan sistem yang ada.

1.4 Batasan Penelitian

Batasan-batasan untuk penelitian yang saya lakukan, antara lain :

a. Data-data yang dilakukan dalam analisis dan pembuatan masalah adalah data yang diperoleh dari *observasi* dan wawancara.
b. Analisis yang digunakan adalah metode penilaian *(scoring)* dengan pendekatan sesuai standar ISO 27001 yaitu *maturity level* model.
c. Sasaran area kontrol pengamanan dari ISO 27001 yang digunakan adalah Kebijakan Keamanan (A.5), Manajemen Aset (A.7), Keamanan Fisik dan Lingkungan (A.9), Manajemen Komunikasi dan Operasi(A.10), Pengendalian Akses(A.11), Pemeliharaan dan perawatan sistem informasi (A.12), Manajemen kejadian keamanan informasi(A.13).
d. Tidak membahas manajemen jaringan seperti konfigurasi server, dan manajemen IP baik privat maupun public.
e. Output yang dihasilkan berupa temuan dan rekomendasi hasil audit keamanan sistem Admisi UIN SUNAN KALIJAGA.

1.5 Keaslian Penelitian

Penelitian tentang audit sistem informasi rekam medis menggunakan standar ISO 27001 sebelumnya pernah dilakukan Heri Stiawan (2015) dengan judul Audit Keamanan Sistem Informasi Rumah Sakit Menggunakan Standar ISO 27001 (Studi Kasus di RSU PKU Muhammadiyah Bantul). Penelitian ini berfokus pada keamanan sistem dengan batasan pada klausul pengelolaan aset, keamanan fisik dan lingkungan dan pengendalian akses. Penelitian ini menghasilkan nilai *maturity level* sebesar 2,2 yang berarti bahwa kontrol keamanan masih berada pada level 2 *planned and tracked* (direncanakan dan dilacak) namun keamanan sistem informasi rekam medis RSU PKU Muhamaddiyah Bantul sudah cukup baik karena sudah mengikuti prosedur keamanan sistem informasi yang ada. Tetapi belum merupakan level yang diharapkan oleh perusahaan, sehingga diperlukan peningkatan kontrol keamanan.

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

Perbedaan penelitian ini dengan yang sudah ada adalah pada penelitian sebelumnya, pengambilan studi kasus atau objek penelitian dan sasaran area kontrol pengamanan dari ISO 27001.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Kesimpulan yang peneliti hasilkan dari pross audit sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah sebagai berikut :

1. Perencanaan audit untuk kegiatan penelitian audit keamanan sistem informasi dengan standar SNI – ISO 27001 pada Sistem Admisi yang dikelola UPT PTIPD UIN Sunan Kalijaga telah berhasil dilaksanakan.
2. Peneliti telah berhasil melakukan proses audit sistem informasi yang mengambil studi kasus Sistem Admisi UIN Sunan Kalijaga dengan standar SNI – ISO 27001. Peneliti juga berhasil memberikan penilaian terhadap keamanan sistem informasi dengan nilai *maturity 2,08 (Repeatable but Intuitive).* Dengan nilai maturity yang didapatkan artinya manajemen pengamanan informasi pada Sistem Admisi belum memenuhi standar SNI ISO 27001, proses pengelolaan sistem informasi masih sebatas mengikuti pola teratur dimana prosedur serupa diikuti oleh pegawai / pengelola lainnya tanpa ada pelatihan formal sebelumnya dan tidak ada standart prosedur yang digunakan sebagai acuan dan tanggung jawab sepenuhnya dilimpahkan kepada masing – masing individu sehingga kesalahan sangat mungkin terjadi.
3. Rekomendasi audit pada Sistem Admisi untuk setiap proses klausul berhasil disusun berdasarkan analisa hasil audit.

4. Peneliti juga telah berhasil menemukan tingkat kematangan setiap klausul dan memberikan rekomendasi kepada setiap klausul yang menjdai runag lingkup untuk peningkatan keamanan Sistem Admisi. Tingkat kematangan setiap klausul sebagai berikut :
   - Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul kebijakan keamanan, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 1,6. Artinya manajemen sudah mempunyai pola kebijakan keamanan namun belum ada dokumentasi resmi, dan belum adanya pembaharuan terhadap standar yang dipakai, sehingga lamban dalam menangani serangan karena tidak ada acuan untuk pengelolaan.
   - Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul manajemen aset, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 2,11. Artinya sudah ada pengelolaan yang baik dalam mamanjemen akses *user* (admin, staff, mahasiswa) namun belum ada dokumentasi dan tanggung jawab sepenuhnya dilimpahkan kepadaindividu masing- masing sehingga sangat mungkin terjadi kesalahan.
   - Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul keamanan fisik dan lingkungan, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 1,85. Artinya pengelolaan *server* informasi sudah ditempatkan pada ruangan khusus dengan baik, sudah adanya prosedur pengecekan *hardware* namun

tidak dilakukan rutin, dan belum adanya divisi khusus dalam menangani kerusakan tersebut sehingga mengenai faktor ketersediaan terlihat belum maksimal.

- Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul manajemen komunikasi dan operasi, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 1,78. Artinya pengelolaan pengamanan jaringan belum dilakukan secara maksimal, meskipun manajemen sudah mengidentifikasi titik – titik jaringan yang rawan, namun proses pengecekan ini tidak dilakukan secara berkala dan rutin, kurangnya operator yang bertugas menangani pengelolaan jaringan, sehingga adanya serangan sangat mungkin terjadi.
- Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul pengendalian akses, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 2,18. Artinya kebijakan kontrol akses *user* sudah diterapkan dengan baik, pengguna akun sudah mempunyai *user id* untuk masing – masing personal, sudah mempunyai sistem manajemen *password*, manajemen sudah mengimplementasikan *log on* prosedur tapi belum terdokumentasi, pengelolaan pengendalian akses hanya mengikuti pola yang teratur dimana prosedur serupa diikuti karyawan dan user lainnya tetapi tidak ada pelatihan formal sebelumnya.

- Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul pemeliharaan dan perawatan sistem operasi, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 2,6. Artinya pola keamanan sistem sudah ada namun belum didokumentasikan, manajemen sudah menerapkan mekanisme pengamanan *software* namun belum didokumentasikan, hal ini hanya mengikuti pola teratur dimana prosedur serupa diikuti karyawan tetapi tidak adanya standar prosedur sebagai acuan.
- Berdasarkan analisis dan hasil pengukuran nilai *maturity level* pada klausul manajemen kejadian keamanan informasi, tingkat kematangan Sistem Admisi UIN Sunan Kalijaga Yogyakarta adalah 2,5. Artinya manajemen sudah menerapkan mekanisme pelaporan kejadian keamanan dengan baik dan dilakukan saat jam kerja, tetapi belum adanya dokumentasi resmi tentang pelaporan kejadian keamanan.

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. Seluruh manajemen , baik pimpinan dan karyawan UPT PTIPD UIN Sunan Kalijaga perlu memahami pentingnya keamanan sistem informasi dalam mendukung proses kerja guna mencapai visi misi dan tujuan UPT PTIPD UIN Sunan Kalijaga.

2. Perlu penerapan keamanan sistem informasi sesuai standar SNI – ISO 27001, secara bertahap dan secara berkala perlu dilakukan audit internal oleh pihak PTIPD dengan harapan agar PTIPD dapat menghadapi perubahan pengelolaan sistem informasi yang lebih baik.
3. Untuk penelitian lebih lanjut mengenai Sistem Admisi UIN Sunan Kalijaga diharap menggunakan klausul yang lebih menyeluruh dan mendetail sehingga diperoleh nilai keamanan sistem Admisi yang semakin akurat.

DAFTAR PUSTAKA

Sarno, Riyanarto dan Irsyat Iffano.2009. *Sistem Manajemen Keamanan Informasi*. Surabaya : ITS Press.

Ermana, Fine.2009.*Audit Keamanan Sistem Infromasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM.* Surabaya: Sekolah Tinggi Manajemen Komputer & Teknik Komputer Surabaya.

Kusuma, Riawan Arbi.2014.Skripsi. *Audit Keamanan Sistem Informasi Berdasarkan Standar Sni – Iso 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta : UIN Sunan Kalijaga Yogyakarta.

Stiawan, Heri.2015.Skripsi. *Audit Sistem Informasi Rumah Sakit Menggunakan Standar Iso 27001 (Studi Kasus Di Rsu Pku Muhammadiyah Bantul*). Yogyakarta : UIN Sunan Kalijaga Yogyakarta.

Almustafa.2014.Skripsi. *Audit Pengawasan Dan Pengelolaan Teknologi Informasi Dengan Framework Cobit Di Ptipd Uin Sunan Kalijaga Yogyakarta.* Yogyakarta : UIN Sunan Kalijaga.

Herianto, Dedi.2013.Skripsi. *Audit Pengelolaan Teknologi Informasi Menggunakan Framework Cobit Pada Domain Acquire & Implement (Studi Kasus: Pksi Uin Sunan Kalijaga Yogykarta).* Yogyakarta : UIN Sunan Kalijaga.

Badan Standarisasi Nasional.2009. *Teknologi- Informasi- Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan.* Bogor:Badan Standarisasi Nasional.

Syafrizal, Melwin.2010. *Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005.* Yogyakarta : STMIK AMIKOM.

Widodo, Nugroho Arif dan Rochim, Adian Fatchur.2009. *Perancangan Audit Internal Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan Standar ISO/IEC 27001:2005 di PT.BPR Karyajatnika Sadaya.* Semarang : Universitas Diponegoro.

Komalasari, Rizki dan Perdana, Ilham. 2014. *Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001:2009.* Bandung : Universitas Telkom Bandung.

Wakhidah, Rokhimatul, Gondokaryono, Yudi Satria dan Rosmansyah, Yusep.2013.*Tata Kelola Keamanan Informasi pada Area Transmisi PT PLN (PERSERO) P3B Jawa Bali menggunakan COBIT 5 dan ISO/ IEC 27001:2013.* Bandung : Institut Teknologi Bandung.

Utomo, Mergo, Ali, Ahmad Holil Noor and Affanfi, Irsal. 2012.*Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I.* Surabaya : Institut Teknologi Sepuluh Nopember.

Widihastuti, Ida dan Alifah, Suryani. 2009. *Audit Manajemen, Perencanaan & Organisasi Sistem Informasi di UNISSULA.* Semarang : Universitas Islam Sultan Agung Semarang.

Kristanto, Titus , Arief , Rachman dan Rozi, Nanang Fakhrur. 2014. *Perancangan Audit Keamanan Informasi Berdasarkan Standar ISO 27001:2005 (Studi Kasus : PT. ADIRA DINAMIKA MULTIFINANCE).* Surabaya : SESINDO.

Habibi, Ade Putra dan Nugroho, Aryo. 2014. Audit Keamanan Sistem Informasi Berdasarkan Standar ISO/ IEC 27001:2005 (Studi Kasus : PT. APLIKANUSA LINTASARTA). Surabaya :Universitas Narotama

https://id.m.wikipedia.org/wiki/Audit . Diakses pada hari Senin 13 Juni 2016

http://ilmuakuntansi.web.id/pengertian -auditing-menurut-ahli/ . Diakses pada hari Senin 13 Juni 2016

https://id.m.wikipedia.org/wiki/Organisasi_Internasional_untuk_Standarisasi . Diakses pada hari Senin 13 Juni 2016

Nubatonis, Meirlin S. 2013. *Audit Keamanan Informasi Pada Laboratorium Komputer Menggunakan ISO/IEC 17799 :2005 (Studi Kasus : FTIUKSW).* Salatiga:Universitas Kristen Satya Wacana.

Kemenkominfo. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik* . Jakarta : Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementrian Kominikasi dan Informatika RI.

Puspitasari, Devi.2015.Skripsi. *Audit Sistem Manajemen Keamanan Informasi Menggunakan ISO/SNI 27001 Pada Sistem Informasi Apotek Sanata Dharma.*Yogyakarta :UIN Sunan Kalijaga Yogyakarta

LAMPIRAN A : *Project Definition (PD)*

Audit Charter

Project ID : SNI – ISO 27001 – Audit – 01

Project Name : Information System Management Audit

Auditor : Dwi Indah Permatasari

Project Description :

Penelitian yang berkaitan dengan keamanan informasi menggunakan parameter SNI – ISO 27001. Berkenaan dengan maksud penelitian, dikembangkan wawancara dari SNI – ISO 27001, yang dibatasi pada 7 ruang lingkup diantaranya Kebijakan Keamanan, Manajemen Aset, Keamanan Fisik dan Lingkungan, Manajemen Komunikasi dan Operasi, Pengendalian Akses, Pemeliharaan dan Perawatan Sistem Informasi, dan Manajemen Kejadian Keamanan Informasi.

Project Schedule : Maret – Mei

Stakeholder List :

Respondent	Actual Respondent	Audit Clause
Chief Information Officer (CIO)	Agung Fatwanto, S.Si., M.Kom, Ph.D	A.5.1 A.5.2 A.7.1 A.7.2 A.9.1 A.9.2 A.11.4
Head Development (HD)	Surahmat Laguni	A.9.1 A.9.2 A.11.2 A.11.3 A.11.4 A.11.5
Head Operations (HO)	Daru Prasetyawan, S.T	A.11.1 A.11.2 A.11.4
Compliance, Audit, Risk and Security (CARS)	Agung Fatwanto, S.Si, M.Kom, Ph.D	A.10.6 A.11.5
Information System Division	Daru Prasetyawan, S.T	A.12.1 A.12.4 A.13.1

		A.13.2
Information and Technology Division	Ramadhan Gatra, S.T	A.10.6 A.11.5

Yogyakarta, 11 April 2016

Mengetahui

Kepala PTIPD UIN Sunan Kalijaga

Agung Ftawanto, S.si, M.Kom, Ph.D

NIP : 19770103 100501 003

Auditor

Dwi Indah Permatasari

NIM :12651062

LAMPIRAN B : Surat Ijin Penelitian

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Alamat : Jl. Marsda Adisucipto, No. 1 Telp. (0274) 519739 Fax (0274) 540971
Email: *fst@uin-suka.ac.id.* Yogyakarta 55281

Nomor : UIN.02/DST.1/TL.00/ 447 /2016 Yogyakarta, 10 februari 2016
Lamp : 1 bendel Proposal
Perihal : Permohonan Izin Penelitian

Kepada
Yth: Kepala Kantor Admisi
UIN Sunan Kalijaga
di
Yogyakarta

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk kelengkapan penyusunan skripsi dengan judul :

AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR SNI-ISO 27001 PADA SISTEM ADMISI UIN SUNAN KALIJAGA

diperlukan penelitian. Oleh karena itu, kami mengharap kiranya Bapak/Ibu berkenan memberi izin kepada mahasiswa kami:

Nama	:	Dwi Indah Permatasari
NIM	:	12651062
Semester	:	8
Program studi	:	Teknik Informatika
Alamat	:	Jl. Kusuma No.881 RT 78/ RW 18 Gendeng, Baciro, Gondokusuman, Yogyakarta

Untuk mengadakan penelitian di : Kantor Admisi UIN SUNAN KALIJAGA
Metode pengumpulan data : Observasi dan Wawancara
Adapun waktunya mulai tanggal : 15 Februari 2016 s.d tanggal 15 Mei 2016

Kemudian atas perkenan Bapak/Ibu kami sampaikan terima kasih.

Wassalamu'alaikum Wr.Wb.

a.n. Dekan
Wakil Dekan Bidang Akademik

Dr. Khurul Wardati, M.Si
NIP. 19660731 200003 2 001

Tembusan :
- Dekan (Sebagai Laporan)

LAMPIRAN C : *Master Control* (MC)

Document ID :MC
Document Name :Master Control
Dokumen ini digunakan sebagai acuan kontrol saat melakukan proses audit

No	KLAUSUL	KONTROL	AUDITEE
1	**A.5**	**Kebijakan keamanan**	
	A.5.1	Kebijakan keamanan Informasi	CIO
	A.5.2	Tinjauan ulang kebijakan keamanan informasi	CIO
2	**A.7**	**Manajemen aset**	
	A.7.1	Tanggung jawab terhadap aset	CIO
	A.7.2	Klasifikasi Informasi	CIO
3	**A.9**	**Keamanan fisik dan lingkungan**	
	A.9.1	Area yang aman	CIO, HD
	A.9.2	Keamanan peralatan	CIO, HD
4	**A.10**	**Manajemen komunikasi dan operasi**	
	A.10.6	Manajemen keamanan Jaringan	CARS, IT
5	**A.11**	**Pengendalian akses**	
	A.11.1	Persyaratan bisnis untuk pengendalian akses	HO
	A.11.2	Manajemen akses pengguna	HO, HD
	A.11.3	Tanggung jawab pengguna	HD
	A.11.4	Pengendalian akses jaringan	CIO, HO, HD
	A.11.5	Pengendalian akses sistem operasi	CARS, HD, IT
6	**A.12**	**Pemeliharaan dan perawatan sistem informasi**	
	A.12.1	Persyaratan keamanan sistem informasi	SI
	A.12.4	Keamanan file sistem	SI
7	**A.13**	**Manajemen kejadian keamanan informasi**	
	A.13.1	Pelaporan kejadian informasi	SI
	A.13.2	Pelaporan kelemahan keamanan	SI

LAMPIRAN D : *Master Question* (MQ)

Document ID	:MQ
Document Name	:Master Questions Dokumen ini digunakan sebagai acuan pertanyaan saat melakukan proses audit

KLAUSUL	KODE	QUESTIONS
A.5		
A.5.1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?
	Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?
	Q3	Apakah ada dokumentasi kebijakan keamanan informasi?
	Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?
	Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?
A.5.2	Q6	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?
	Q7	Apakah kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus?
	Q8	Berapa jangka waktu pengecekan keamanan informasi tersebut?
	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?
	Q10	Apakah ada pembaruan rutin pada kebijakan keamanan informasi?
A.7		
A.7.1	Q11	Apakah sudah diterapkan kebijakan pengelolaan aset ?
	Q12	Bagaimanakah kebijakan pengelolaan aset ?
	Q13	Apakah ada kendala dalam melaksanakan kebijakan penelolaan aset ?
	Q14	Apakah sudah dilakukan pembaruan rutin dari kebijakan pengelolaan aset ?

	Q15	Bagaimana prosedur inventarisasi aset ?
	Q16	Siapakah yang bertanggung jawab terhadap inventarisasi aset ?
	Q17	Berapa jangka waktu pengecekan inventarisasi aset secara berkala ?
A.7.2	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user sistem Admisi ?
	Q19	Bagaimana prosedur pengklasifikasian data tersebut ?
A.9		
A.9.1	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?
	Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?
	Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?
	Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?
	Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?
	Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?
	Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?
	Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?
	Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?
	Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya ?
	Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?
A.9.2	Q31	Apakah ada prosedur untuk pengecekan hardware ?
	Q32	Bagaimana prosedur pengecekan hardware ?

	Q33	Berapa jangka waktu pengecekan hardware secara berkala ?
	Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?
	Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?
	Q36	Bagaimana anda menangani kerusakan itu ?
A.10		
A.10.6	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?
	Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?
	Q39	Sudah adakah kebijakan pengamanan jaringan?
	Q40	Apakah sudah terdokumentasi ?
	Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?
	Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?
	Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?
	Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?
	Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?
A.11		
A.11.1	Q46	Apakah sudah ada dokumentasi control akses?
	Q47	Apakah sudah ada kebijakan dalam mengatur kontrol akses?
	Q48	Apakah ada kendala dalam melaksanakan kebijakan pengendalian akses ?
	Q49	Apakah dilakukan pembaruan rutin kebijakan pengendalian akses ?

	Q50	Siapakah yang bertanggung jawab terhadap pengendalian akses ?
	Q51	Apakah sudah sesuai kebijakan pengendalian akses dengan kondisi riil di lapangan ?
A.11.2	Q52	Apakah user sistem Admisi diberikan user id dan password ?
	Q53	Apakah user memahami keamanan user id dan password ?
	Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)
	Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?
	Q56	Apakah sudah ada alokasi penggunaan hak akses kepada user?
	Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?
	Q58	Berapa lama jangka waktu anda mengganti password ?
	Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?
A.11.3	Q60	Bagaimana cara user mendapatkan password akun?
	Q61	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?
	Q62	Apakah ada sosialisasi dalam pemilihan password yang baik?
	Q63	Apakah user mengubah password dalam sistem tersebut?
	Q64	Adakah ada petunjuk untuk membuat kombinasi password yang baik?
	Q65	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?
	Q66	Apakah anda pernah memberikan password ke orang lain ?
	Q67	Apakah anda pernah meninggalkan komputer tanpa logout dari sistem admisi ?
	Q68	Apa yang terjadi dengan komputer anda ?
A.11.4	Q69	Apakah ada kebijakan layanan jaringan ?
	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?

	Q71	Apakah ada prosedur pengamanan jaringan ?
	Q72	Bagaimanakan prosedur pengamanan jaringan ?
	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?
	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?
A.11.5	Q75	Apakah sudah ada prosedur log on?
	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?
	Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?
	Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?
	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?
	Q80	Apkakah ada kendala dalam penggunaan komputer ini?
	Q81	Apakah kendala tersebut?
	Q82	Bagaimana cara menangani kendala tersebut?
	Q83	Apakah sudah ada sistem manajemen password?
	Q84	Apakah ada sosialisasi password yang interaktif?
	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?
	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?
	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?
A.12		
A.12.1	Q88	Pada saat perancangan sistem, apakah keamanan dalam sistem informasi yang dibangun sudah termasuk dalam bussiness statements?
	Q89	Bagaimana prosedur tersebut?
	Q90	Apakah ada kesulitan saat menerapkan prosedur tersebut?

	Q91	Pada saat sistem informasi berjalan, apakah rancangan keamanan sistem admisi sudah terimplementasi?
	Q92	Pada tahap perancangan sistem admisi, apakah keamanan sistem informasi yang dibangun sudah termasuk dalam perancangan?
	Q93	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem?
	Q94	Apabila terjadi serangan sistem, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?
	Q95	Apakah ada monitoring manajemen terhadap mekanisme sistem informasi?
	Q96	Apakah sudah ada dokumentasi mekanisme pengamanan sistem?
	Q97	Apakah petugas selalu mengidentifikasi titik kelemahan sistem ?
	Q98	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?
A.12.4	Q99	Apakah sudah ada Standar Operation Procedure pada sistem admisi?
	Q100	Sudah berapa lama prosedur tersebut diterapkan?
	Q101	Apakah petugas selalu mengontrol program source code sistem tersebut?
	Q102	Berapa jangka waktu pengecekan sistem tersebut?
A.13		
A.13.1	Q103	Apakah pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat?
	Q104	Apakah petugas selalu melaporkan temuan kelemahan sistem?
	Q105	Seperti apakah temuan tersebut?
A.13.2	Q106	Apakah solusi yang diberikan pada saat sistem terkena serangan?
	Q107	Apakah manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?

	Q108	Apakah sudah ada pembaharuan mekanisme sistem keamanan?
	Q109	Apakah petugas selalu memonitor terhadap penanganan insiden?
	Q110	Apabila terjadi insiden , apakah sudah ada kebijakan dokumentasi untuk insiden tersebut?

LAMPIRAN E : *Form Questions* (FQ)

Document ID	: FQ
Document Name	: Form Question Dokumen ini digunakan sebagai acuan pemetaan pertanyaan yang akan digunakan saat proses audit.

Form Question 1 (FQ1_CIO) : CIO
Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q69, Q70, Q71, Q72, Q73, Q74.

Form Question 2 (FQ2_HD) : Head Development
Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q65, Q66, Q67, Q68, Q69, Q70, Q71, Q72, Q73, Q74, Q75, Q76, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86, Q87

Form Question 3 (FQ3_HO) : Head Operations
Q46, Q47, Q48, Q49, Q50, Q51, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q69, Q70, Q71, Q72, Q73, Q74.

Form Question 4 (FQ4_SI) : Information System Division
Q88, Q89, Q90, Q91, Q92, Q93, Q94, Q95, Q96, Q97, Q98, Q99, Q100, Q101, Q102, Q103, Q104, Q105, Q106, Q107, Q108, Q109, Q110

Form Question 5 (FQ5_CARS) : Compliance Audit Risk and Security
Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q75, Q76, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86, Q87

Form Question 6 (FQ6_IT) : Information and Technology Division
Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q75, Q76, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86, Q87

LAMPIRAN F : *Form Questions 1* (FQ1_CIO)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID : FQ1_CIO

Project Name : Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta

Auditor : Dwi Indah Permatasari

Auditee : Agung Fatwanto, S.Si, M.Kom., Ph.D

Audit Function : Chief Information Officer (CIO)

Description : Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga

Date :

Approved by Auditor

Agung Fatwanto, S.Si, M.Kom., Ph.D Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?		
2	Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?		
3	Q3	Apakah ada dokumentasi kebijakan keamanan informasi?		
4	Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?		
5	Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?		
6	Q6	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?		
7	Q7	Apakah kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus?		
8	Q8	Berapa jangka waktu pengecekan keamanan informasi tersebut?		
9	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?		
10	Q10	Apakah ada pembaruan rutin pada kebijakan keamanan informasi?		
11	Q11	Apakah sudah diterapkan kebijakan pengelolaan aset ?		

12	Q12	Bagaimanakah kebijakan pengelolaan aset ?		
13	Q13	Apakah ada kendala dalam melaksanakan kebijakan penelolaan aset ?		
14	Q14	Apakah sudah dilakukan pembaruan rutin dari kebijakan pengelolaan aset ?		
15	Q15	Bagaimana prosedur inventarisasi aset ?		
16	Q16	Siapakah yang bertanggung jawab terhadap inventarisasi aset ?		
17	Q17	Berapa jangka waktu pengecekan inventarisasi aset secara berkala ?		
18	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user sistem Admisi ?		
19	Q19	Bagaimana prosedur pengklasifikasian data tersebut ?		
20	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?		
21	Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?		
22	Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?		
23	Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit		

		pendaftaran ?		
24	Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?		
25	Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?		
26	Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?		
27	Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?		
28	Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?		
29	Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya ?		
30	Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?		
31	Q31	Apakah ada prosedur untuk pengecekan hardware ?		
32	Q32	Bagaimana prosedur pengecekan hardware ?		
33	Q33	Berapa jangka waktu pengecekan hardware secara berkala ?		
34	Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?		

35	Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?		
36	Q36	Bagaimana anda menangani kerusakan itu ?		
37	Q69	Apakah ada kebijakan layanan jaringan ?		
38	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?		
39	Q71	Apakah ada prosedur pengamanan jaringan ?		
40	Q72	Bagaimanakah prosedur pengamanan jaringan ?		
41	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?		
42	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?		

LAMPIRAN G : *Form Questions 2* (FQ2_HD)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ2_HD
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Surahmat Laguni
Audit Function	: Head Development
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by Auditor

Surahmat Laguni Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?		
2	Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?		
3	Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?		
4	Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?		
5	Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?		
6	Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?		
7	Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?		
8	Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?		
9	Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?		
10	Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan		

		lainya ?		
11	Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?		
12	Q31	Apakah ada prosedur untuk pengecekan hardware ?		
13	Q32	Bagaimana prosedur pengecekan hardware ?		
14	Q33	Berapa jangka waktu pengecekan hardware secara berkala ?		
15	Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?		
16	Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?		
17	Q36	Bagaimana anda menangani kerusakan itu ?		
18	Q52	Apakah user sistem Admisi diberikan user id dan password ?		
19	Q53	Apakah user memahami keamanan user id dan password ?		
20	Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)		
21	Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?		
22	Q56	Apakah sudah ada alokasi penggunaan hak akses		

		kepada user?		
23	Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?		
24	Q58	Berapa lama jangka waktu anda mengganti password ?		
25	Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?		
26	Q60	Bagaimana cara user mendapatkan password akun?		
27	Q61	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?		
28	Q62	Apakah ada sosialisasi dalam pemilihan password yang baik?		
29	Q63	Apakah user mengubah password dalam sistem tersebut?		
30	Q64	Adakah ada petunjuk untuk membuat kombinasi password yang baik?		
31	Q65	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?		
32	Q66	Apakah anda pernah memberikan password ke orang lain ?		
33	Q67	Apakah anda pernah		

		meninggalkan komputer tanpa logout dari sistem admisi ?		
34	Q68	Apa yang terjadi dengan komputer anda ?		
35	Q69	Apakah ada kebijakan layanan jaringan ?		
36	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?		
37	Q71	Apakah ada prosedur pengamanan jaringan ?		
38	Q72	Bagaimanakan prosedur pengamanan jaringan ?		
39	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?		
40	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?		
41	Q75	Apakah sudah ada prosedur log on?		
42	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?		
43	Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?		
44	Q78	Apakah saat anda mengganti password ada kombinasi		

		yang unik ?		
45	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?		
46	Q80	Apkakah ada kendala dalam penggunaan komputer ini?		
47	Q81	Apakah kendala tersebut?		
48	Q82	Bagaimana cara menangani kendala tersebut?		
49	Q83	Apakah sudah ada sistem manajemen password?		
50	Q84	Apakah ada sosialisasi password yang interaktif?		
51	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?		
52	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?		
53	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?		

LAMPIRAN H : *Form Questions 3* (FQ3_HO)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ3_HO
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Daru Prasetyawan, S.T
Audit Function	: Head Operations (HO)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by Auditor

Daru Prasetyawan, S.T. Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q46	Apakah sudah ada dokumentasi control akses?		
2	Q47	Apakah sudah ada kebijakan dalam mengatur kontrol akses?		
3	Q48	Apakah ada kendala dalam melaksanakan kebijakan pengendalian akses ?		
4	Q49	Apakah dilakukan pembaruan rutin kebijakan pengendalian akses ?		
5	Q50	Siapakah yang bertanggung jawab terhadap pengendalian akses ?		
6	Q51	Apakah sudah sesuai kebijakan pengendalian akses dengan kondisi riil di lapangan ?		
7	Q52	Apakah user sistem Admisi diberikan user id dan password ?		
8	Q53	Apakah user memahami keamanan user id dan password ?		
9	Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)		
10	Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?		
11	Q56	Apakah sudah ada alokasi penggunaan hak akses		

		kepada user?		
12	Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?		
13	Q58	Berapa lama jangka waktu anda mengganti password ?		
14	Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?		
15	Q69	Apakah ada kebijakan layanan jaringan ?		
16	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?		
17	Q71	Apakah ada prosedur pengamanan jaringan ?		
18	Q72	Bagaimanakan prosedur pengamanan jaringan ?		
19	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?		
20	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?		

LAMPIRAN I : *Form Questions 4* (FQ4_SI)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ4_SI
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Daru Prasetyawan, S.T
Audit Function	: Information System Division (SI)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by Auditor

Daru Prasetyawan, S.T. Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q88	Pada saat perancangan sistem, apakah keamanan dalam sistem informasi yang dibangun sudah termasuk dalam bussiness statements?		
2	Q89	Bagaimana prosedur tersebut?		
3	Q90	Apakah ada kesulitan saat menerapkan prosedur tersebut?		
4	Q91	Pada saat sistem informasi berjalan, apakah rancangan keamanan sistem admisi sudah terimplementasi?		
5	Q92	Pada tahap perancangan sistem admisi, apakah keamanan sistem informasi yang dibangun sudah termasuk dalam perancangan?		
6	Q93	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem?		
7	Q94	Apabila terjadi serangan sistem, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?		
8	Q95	Apakah ada monitoring manajemen terhadap mekanisme sistem informasi?		
9	Q96	Apakah sudah ada		

		dokumentasi mekanisme pengamanan sistem?		
10	Q97	Apakah petugas selalu mengidentifikasi titik kelemahan sistem ?		
11	Q98	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?		
12	Q99	Apakah sudah ada Standar Operation Procedure pada sistem admisi?		
13	Q100	Sudah berapa lama prosedur tersebut diterapkan?		
14	Q101	Apakah petugas selalu mengontrol program source code sistem tersebut?		
15	Q102	Berapa jangka waktu pengecekan sistem tersebut?		
16	Q103	Apakah pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat?		
17	Q104	Apakah petugas selalu melaporkan temuan kelemahan sistem?		
18	Q105	Seperti apakah temuan tersebut?		
19	Q106	Apakah solusi yang diberikan pada saat sistem terkena serangan?		
20	Q107	Apakah manajemen memberikan respon yang cepat terhadap laporan		

		keamanan sistem informasi?		
21	Q108	Apakah sudah ada pembaharuan mekanisme sistem keamanan?		
22	Q109	Apakah petugas selalu memonitor terhadap penanganan insiden?		
23	Q110	Apabila terjadi insiden , apakah sudah ada kebijakan dokumentasi untuk insiden tersebut?		

LAMPIRAN J : *Form Questions 5* (FQ5_ CARS)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ5_ CARS
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Agung Fatwanto, S.Si, M.Kom., Ph.D
Audit Function	: Compliance, Audit, Risk and Security (CARS)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Auditor

Agung Fatwanto, S.Si, M.Kom., Ph.D

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?		
2	Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?		
3	Q39	Sudah adakah kebijakan pengamanan jaringan?		
4	Q40	Apakah sudah terdokumentasi ?		
5	Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?		
6	Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?		
7	Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?		
8	Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?		
9	Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?		
10	Q75	Apakah sudah ada prosedur log on?		

11	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?		
12	Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?		
13	Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?		
14	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?		
15	Q80	Apkakah ada kendala dalam penggunaan komputer ini?		
16	Q81	Apakah kendala tersebut?		
17	Q82	Bagaimana cara menangani kendala tersebut?		
18	Q83	Apakah sudah ada sistem manajemen password?		
19	Q84	Apakah ada sosialisasi password yang interaktif?		
20	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?		
21	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?		
22	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?		

LAMPIRAN K : *Form Questions 6* (FQ6_IT)

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID : FQ6_IT

Project Name : Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta

Auditor : Dwi Indah Permatasari

Auditee : Ramadhan Gatra, S.T

Audit Function : Information and Technology Division (IT)

Description : Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga

Date :

Approved by Auditor

Ramadhan Gatra, S.T Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?		
2	Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?		
3	Q39	Sudah adakah kebijakan pengamanan jaringan?		
4	Q40	Apakah sudah terdokumentasi ?		
5	Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?		
6	Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?		
7	Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?		
8	Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?		
9	Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?		
10	Q75	Apakah sudah ada prosedur log on?		

11	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?		
12	Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?		
13	Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?		
14	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?		
15	Q80	Apkakah ada kendala dalam penggunaan komputer ini?		
16	Q81	Apakah kendala tersebut?		
17	Q82	Bagaimana cara menangani kendala tersebut?		
18	Q83	Apakah sudah ada sistem manajemen password?		
19	Q84	Apakah ada sosialisasi password yang interaktif?		
20	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?		
21	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?		
22	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?		

LAMPIRAN L : Lembar Evaluasi Audit (LEA)

Dokumen ID : LEA

Dokumen Name : Lembar Evaluasi Audit

Dokumen berikut digunakan sebagai pedoman perhitungan nilai *maturity* proses audit.

CIO :
HD :
HO:
SI:
CARS
IT:

NO	KLAUSUL	CODE	QUESTIONS	FORM QUESTIONS						SCORE MATURITY	MATURITY	RATA - RATA SISTEM
				CIO	HD	HO	SI	CARS	IT			
1	A.5											
	A.5.1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?									
		Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?									
		Q3	Apakah ada dokumentasi kebijakan keamanan informasi?									

		Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?									
		Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?									
	A.5.2	Q6	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?									
		Q7	Apakah kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus?									
		Q8	Berapa jangka waktu pengecekan keamanan informasi tersebut?									
		Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?									
		Q10	Apakah ada pembaruan rutin pada kebijakan keamanan informasi?									
2	A.7											
	A.7.1	Q11	Apakah sudah diterapkan kebijakan pengelolaan aset ?									
		Q12	Bagaimanakah kebijakan pengelolaan aset ?									
		Q13	Apakah ada kendala dalam melaksanakan kebijakan penelolaan aset ?									
		Q14	Apakah sudah dilakukan pembaruan rutin dari kebijakan pengelolaan aset ?									
		Q15	Bagaimana prosedur inventarisasi aset ?									
		Q16	Siapakah yang bertanggung jawab terhadap inventarisasi aset ?									
		Q17	Berapa jangka waktu pengecekan inventarisasi aset secara berkala ?									

	A.7.2	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user sistem Admisi ?										
		Q19	Bagaimana prosedur pengklasifikasian data tersebut ?										
3	A.9												
	A.9.1	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?										
		Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?										
		Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?										
		Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?										
		Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?										
		Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?										
		Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?										
		Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?										
		Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?										
		Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya ?										
		Q30	Apakah anda mudah mengoperasikan										

			sistem admisi ini ?										
	A.9.2	Q31	Apakah ada prosedur untuk pengecekan hardware ?										
		Q32	Bagaimana prosedur pengecekan hardware ?										
		Q33	Berapa jangka waktu pengecekan hardware secara berkala ?										
		Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?										
		Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?										
		Q36	Bagaimana anda menangani kerusakan itu ?										
4	A.10												
	A.10.6	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?										
		Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?										
		Q39	Sudah adakah kebijakan pengamanan jaringan?										
		Q40	Apakah sudah terdokumentasi ?										
		Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?										
		Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?										
		Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan										

			terhadap serangan ?										
		Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?										
		Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?										
5	A.11												
	A.11.1	Q46	Apakah sudah ada dokumentasi control akses?										
		Q47	Apakah sudah ada kebijakan dalam mengatur kontrol akses?										
		Q48	Apakah ada kendala dalam melaksanakan kebijakan pengendalian akses ?										
		Q49	Apakah dilakukan pembaruan rutin kebijakan pengendalian akses ?										
		Q50	Siapakah yang bertanggung jawab terhadap pengendalian akses ?										
		Q51	Apakah sudah sesuai kebijakan pengendalian akses dengan kondisi riil di lapangan ?										
	A.11.2	Q52	Apakah user sistem Admisi diberikan user id dan password ?										
		Q53	Apakah user memahami keamanan user id dan password ?										
		Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)										
		Q55	Apakah ada prosedur pencabutan akses ke										

			seluruh sistem admisi?										
		Q56	Apakah sudah ada alokasi penggunaan hak akses kepada user?										
		Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?										
		Q58	Berapa lama jangka waktu anda mengganti password ?										
		Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?										
	A.11.3	Q60	Bagaimana cara user mendapatkan password akun?										
		Q61	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?										
		Q62	Apakah ada sosialisasi dalam pemilihan password yang baik?										
		Q63	Apakah user mengubah password dalam sistem tersebut?										
		Q64	Adakah ada petunjuk untuk membuat kombinasi password yang baik?										
		Q65	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?										
		Q66	Apakah anda pernah memberikan password ke orang lain ?										
		Q67	Apakah anda pernah meninggalkan komputer tanpa logout dari sistem admisi ?										
		Q68	Apa yang terjadi dengan komputer anda ?										

	A.11.4	Q69	Apakah ada kebijakan layanan jaringan ?										
		Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?										
		Q71	Apakah ada prosedur pengamanan jaringan ?										
		Q72	Bagaimanakan prosedur pengamanan jaringan ?										
		Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?										
		Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?										
	A.11.5	Q75	Apakah sudah ada prosedur log on?										
		Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?										
		Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?										
		Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?										
		Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?										
		Q80	Apkakah ada kendala dalam penggunaan komputer ini?										
		Q81	Apakah kendala tersebut?										
		Q82	Bagaimana cara menangani kendala tersebut?										

		Q83	Apakah sudah ada sistem manajemen password?									
		Q84	Apakah ada sosialisasi password yang interaktif?									
		Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?									
		Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?									
		Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?									
6	A.12											
	A.12.1	Q88	Pada saat perancangan sistem, apakah keamanan dalam sistem informasi yang dibangun sudah termasuk dalam bussiness statements?									
		Q89	Bagaimana prosedur tersebut?									
		Q90	Apakah ada kesulitan saat menerapkan prosedur tersebut?									
		Q91	Pada saat sistem informasi berjalan, apakah rancangan keamanan sistem admisi sudah terimplementasi?									
		Q92	Pada tahap perancangan sistem admisi, apakah keamanan sistem informasi yang dibangun sudah termasuk dalam perancangan?									
		Q93	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem?									

		Q94	Apabila terjadi serangan sistem, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?									
		Q95	Apakah ada monitoring manajemen terhadap mekanisme sistem informasi?									
		Q96	Apakah sudah ada dokumentasi mekanisme pengamanan sistem?									
		Q97	Apakah petugas selalu mengidentifikasi titik kelemahan sistem ?									
		Q98	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?									
	A.12.4	Q99	Apakah sudah ada Standar Operation Procedure pada sistem admisi?									
		Q100	Sudah berapa lama prosedur tersebut diterapkan?									
		Q101	Apakah petugas selalu mengontrol program source code sistem tersebut?									
		Q102	Berapa jangka waktu pengecekan sistem tersebut?									
7	A.13											
	A.13.1	Q103	Apakah pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat?									
		Q104	Apakah petugas selalu melaporkan temuan kelemahan sistem?									
		Q105	Seperti apakah temuan tersebut?									
	A.13.2	Q106	Apakah solusi yang diberikan pada saat sistem terkena serangan?									

		Q107	Apakah manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?									
		Q108	Apakah sudah ada pembaharuan mekanisme sistem keamanan?									
		Q109	Apakah petugas selalu memonitor terhadap penanganan insiden?									
		Q110	Apabila terjadi insiden , apakah sudah ada kebijakan dokumentasi untuk insiden tersebut?									

LAMPIRAN M : Hasil Wawancara Audit

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ1-C10
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Agung Fatwanto, S.Si, M.Kom., Ph.D
Audit Function	: Chief Information Officer (CIO)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Agung Fatwanto, S.Si, M.Kom., Ph.D

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?	Sudah, secara umum sudah ada level pengaksesan untuk masing2 user	2
2	Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?	Sudah	1
3	Q3	Apakah ada dokumentasi kebijakan keamanan informasi?	Sebagian sudah ada dokumentasi kebijakan keamanan	1
4	Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?	Ya, kadang-kadang yang bertugas yaitu divisi TI	2
5	Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?	Prosedurnya diturunkan dari SOP umum pelaksanaan penerimaan maba oleh unit	2
6	Q6	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	CIO	3
7	Q7	Apakah kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus?	Sebagian sudah sesuai	2
8	Q8	Berapa jangka waktu pengecekan keamanan informasi tersebut?	Untuk sekarang jarang dilakukan pengecekan, paling tidak sebulan sekali	1
9	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	Sebagian sudah sesuai dg aturan yang berlaku	1
10	Q10	Apakah ada pembaruan rutin pada kebijakan keamanan informasi?	Ada, tapi tergantung pas penerimaan mahasiswa baru	1
11	Q11	Apakah sudah diterapkan	Sudah	2

		kebijakan pengelolaan aset?		
12	Q12	Bagaimanakah kebijakan pengelolaan aset ?	Data dimonitor secara berkala yaitu pada saat jam kerja	2
13	Q13	Apakah ada kendala dalam melaksanakan kebijakan penelolaan aset ?	Kadang, wewenang orang yg diberi hak tetapi memberi kredensial pada orang lain untuk pekerjaan dia	2
14	Q14	Apakah sudah dilakukan pembaruan rutin dari kebijakan pengelolaan aset ?	Sudah	1
15	Q15	Bagaimana prosedur inventarisasi aset ?	Sudah diterapkan, tapi belum didokumentasi	2
16	Q16	Siapakah yang bertanggung jawab terhadap inventarisasi aset ?	CIO	3
17	Q17	Berapa jangka waktu pengecekan inventarisasi aset secara berkala ?	Sebulan sekali	1
18	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user sistem Admisi ?	Ada, diterapkan level hak akses user	3
19	Q19	Bagaimana prosedur pengklasifikasian data tersebut ?	Misal level hak akses admin untuk staf dan mahasiswa	3
20	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?	Ada	3
21	Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?	Data disimpan diruang server dengan suhu tertentu, dan hanya pihak yg berkepentingan yang boleh masuk	3
22	Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?	Sudah aman	1

23	Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?	Karena sifatnya online jadi sudah aman	1
24	Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?	Sampai saat ini belum meneliti, tetapi dg adanya sistem admisi sudah sangat membantu	2
25	Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?	Bisa karena bersifat online	3
26	Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?	Ya, hanya yang berkepentingan misalnya staff IT	3
27	Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?	Ya, nyaman	2
28	Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?	Belum pernah sejauh ini	3
29	Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya ?	Ya, nyaman	3
30	Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?	Mudah, karena sudah memahami sistem tersebut	2
31	Q31	Apakah ada prosedur untuk pengecekan hardware ?	Ada	2
32	Q32	Bagaimana prosedur pengecekan hardware ?	Melihat mesin yang sering dipakai	1
33	Q33	Berapa jangka waktu pengecekan hardware secara berkala ?	Sebulan sekali	1

34	Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?	Teknisi kemudian CIO	2
35	Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?	Tidak ada, biasanya langsung diservice	1
36	Q36	Bagaimana anda menangani kerusakan itu ?	Ditangani secara manual atau diservice	1
37	Q69	Apakah ada kebijakan layanan jaringan ?	Sudah	2
38	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?	Divisi infrastruktur kemudian lanjut ke CIO	3
39	Q71	Apakah ada prosedur pengamanan jaringan ?	Ada	2
40	Q72	Bagaimanakah prosedur pengamanan jaringan ?	Network management, (pembuangan media, pembatasan akses. dll)	2
41	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?	Kerusakan jaringan untuk saat ini sporadik atau tidak tentu	2
42	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?	Pernah	1

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ2_ HD
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Surahmat Laguni
Audit Function	: Head Development
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Surahmat Laguni

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?	Ya ada tempat khusus	3
2	Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?	Tidak tahu	0
3	Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?	Belum	0
4	Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?	Terpisah dari unit admin	1
5	Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?	Ya, sudah	3
6	Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?	Ya, karena sifatnya online bukan dekstop	3
7	Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?	Ya	3
8	Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?	Ya, tertata dengan baik	2
9	Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?	tidak pernah	3
10	Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya	Ya	3

		?		
11	Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?	Ya	3
12	Q31	Apakah ada prosedur untuk pengecekan hardware ?	Ya	2
13	Q32	Bagaimana prosedur pengecekan hardware ?	tidak tahu karena tidak berwenang	0
14	Q33	Berapa jangka waktu pengecekan hardware secara berkala ?	tidak tahu, tidak punya wewenang dalam hal itu	0
15	Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?	tidak tahu	0
16	Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?	Ada, saat itu komputer bagian CS pernah meledak	1
17	Q36	Bagaimana anda menangani kerusakan itu ?	Diteparasi secara manual	1
18	Q52	Apakah user sistem Admisi diberikan user id dan password ?	Peserta PMB dari Ya, bank Admisi dari sistem kepegawaian	3
19	Q53	Apakah user memahami keamanan user id dan password ?	Ya	2
20	Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)	Melalui pembayaran Ya, ke bank maka akan terdaftar user dan passwordnya	2
21	Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?	Ya	2
22	Q56	Apakah sudah ada alokasi penggunaan hak akses	Ya	3

		kepada user?		
23	Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?	Ya	3
24	Q58	Berapa lama jangka waktu anda mengganti password ?	tidak pernah diganti	1
25	Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?	ya	3
26	Q60	Bagaimana cara user mendapatkan password akun?	Membayar ke bank sesuai kode bayar setiap jalur PMB yg diinginkan	3
27	Q61	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?	Ya	2
28	Q62	Apakah ada sosialisasi dalam pemilihan password yang baik?	Tidak tahu, mungkin di sistem kepegawaian	1
29	Q63	Apakah user mengubah password dalam sistem tersebut?	User calon maba tidak, tetapi si admin dari sistem kepegawaian	2
30	Q64	Adakah ada petunjuk untuk membuat kombinasi password yang baik?	tidak ada di sistem admisi	0
31	Q65	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?	Ya	3
32	Q66	Apakah anda pernah memberikan password ke orang lain ?	Tidak	3
33	Q67	Apakah anda pernah	Tidak, sistem sudah	

		meninggalkan komputer tanpa logout dari sistem admisi ?	Ada session time out. Otomatis logout pada detik tertentu	3
34	Q68	Apa yang terjadi dengan komputer anda ?	aman. aman saja	2
35	Q69	Apakah ada kebijakan layanan jaringan ?	ya, ada	2
36	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?	divisi jaringan	3
37	Q71	Apakah ada prosedur pengamanan jaringan ?	ada	2
38	Q72	Bagaimanakan prosedur pengamanan jaringan ?	kurang tau, karena tidak berwenang	0
39	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?	tidak tahu, karena tidak berwenang dalam hal itu.	0
40	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?	kadang - kadang, karena bermasalahan pada sistem sering dilakukan pelaporan pada medsos	2
41	Q75	Apakah sudah ada prosedur log on?	ya	3
42	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?	ya	3
43	Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?	tidak tahu	0
44	Q78	Apakah saat anda mengganti password ada kombinasi	ya	2

		yang unik ?		
45	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?	Kurang tau karena sejauh ini aman-aman saja dg sifat sistem yang online	3
46	Q80	Apkakah ada kendala dalam penggunaan komputer ini?	kurang tau	0
47	Q81	Apakah kendala tersebut?	kurang tau	0
48	Q82	Bagaimana cara menangani kendala tersebut?	kurang tau	0
49	Q83	Apakah sudah ada sistem manajemen password?	Ya di sistem bayar dan sistem kepegawaian	2
50	Q84	Apakah ada sosialisasi password yang interaktif?	Belum ada	0
51	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?	kurang tau, masih aman sejauh ini	1
52	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?	Setiap ada kesalahan langsung dilakukan perbaikan	3
53	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?	ya	4

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ3_ HO
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Daru Prasetyawan, S.T
Audit Function	: Head Operations (HO)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di *UIN* Sunan Kalijaga
Date	:

Approved by

Daru Prasetyawan, S.T.

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q46	Apakah sudah ada dokumentasi control akses?	Ada	3
2	Q47	Apakah sudah ada kebijakan dalam mengatur kontrol akses?	Ada	3
3	Q48	Apakah ada kendala dalam melaksanakan kebijakan pengendalian akses ?	Tidak ada	3
4	Q49	Apakah dilakukan pembaruan rutin kebijakan pengendalian akses ?	Belum dilakukan	1
5	Q50	Siapakah yang bertanggung jawab terhadap pengendalian akses ?	Head Operations (Mas Daru)	3
6	Q51	Apakah sudah sesuai kebijakan pengendalian akses dengan kondisi riil di lapangan ?	Sejauh ini sudah sesuai	3
7	Q52	Apakah user sistem Admisi diberikan user id dan password ?	Sudah. ID & password yg dipakai saat login WIFI	3
8	Q53	Apakah user memahami keamanan user id dan password ?	Sudah	3
9	Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)	Ada, masukkan ID dan password	3
10	Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?	Ada	3
11	Q56	Apakah sudah ada alokasi penggunaan hak akses kepada user?	Sudah, admin, karyawan & mahasiswa	3
12	Q57	Apakah sudah ada sistem / program / aplikasi yang	Sudah ada. admin.akademik-uin-suka.ac.id	3

		digunakan untuk mengelola hak akses user?		
13	Q58	Berapa lama jangka waktu anda mengganti password ?	Tergantung masing-masing user	2
14	Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?	Sejauh ini belum ada, dan sering dikerjakan oleh staff	2
15	Q69	Apakah ada kebijakan layanan jaringan ?	ada, secara universal	2
16	Q70	Siapakah yang bertanggung jawab terhadap layanan jaringan ?	Divisi TI (Mas Gatra)	3
17	Q71	Apakah ada prosedur pengamanan jaringan ?	Sudah	2
18	Q72	Bagaimanakan prosedur pengamanan jaringan ?	Sesuai SOP, sistem tertentu hanya boleh diakses oleh intranet UIN u/ setiap firewall	3
19	Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?	Sistem admisi ~~bit~~nya tinggi, jadi pas penutupan pendaftaran sering terjadi gangguan jaringan	2
20	Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?	Pernah, karena dipakai untuk pelaporan permasalahan sistem	2

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ4_SI
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Daru Prasetyawan, S.T
Audit Function	: Information System Division (SI)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Daru Prasetyawan, S.T.

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q88	Pada saat perancangan sistem, apakah keamanan dalam sistem informasi yang dibangun sudah termasuk dalam bussiness statements?	Sudah	2
2	Q89	Bagaimana prosedur tersebut?	Model dan procedur yang ada di Agilee	3
3	Q90	Apakah ada kesulitan saat menerapkan prosedur tersebut?	Tidak ada	3
4	Q91	Pada saat sistem informasi berjalan, apakah rancangan keamanan sistem admisi sudah terimplementasi?	Sudah	2
5	Q92	Pada tahap perancangan sistem admisi, apakah keamanan sistem informasi yang dibangun sudah termasuk dalam perancangan?	Sudah	2
6	Q93	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem?	Ada 2. Divisi software dan divisi infrastruktur	3
7	Q94	Apabila terjadi serangan sistem, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?	Sudah	3
8	Q95	Apakah ada monitoring manajemen terhadap mekanisme sistem informasi?	Ada	2
9	Q96	Apakah sudah ada dokumentasi mekanisme pengamanan sistem?	Sudah, di divisi infrastruktur	3
10	Q97	Apakah petugas selalu mengidentifikasi titik kelemahan sistem ?	Ya, setiap hari pada jam kerja.	3
11	Q98	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?	Ya	2
12	Q99	Apakah sudah ada Standar Operation Procedure pada sistem admisi?	Sudah	2

13	Q100	Sudah berapa lama prosedur tersebut diterapkan?	3 tahun, dari 2013 - 2016	3
14	Q101	Apakah petugas selalu mengontrol program source code sistem tersebut?	Ya, setiap jam kerja	3
15	Q102	Berapa jangka waktu pengecekan sistem tersebut?	Ya, setiap hari	3
16	Q103	Apakah pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat?	Ya	3
17	Q104	Apakah petugas selalu melaporkan temuan kelemahan sistem?	Ya	3
18	Q105	Seperti apakah temuan tersebut?	Kesalahan data, kesalahan sistem.	2
19	Q106	Apakah solusi yang diberikan pada saat sistem terkena serangan?	Dianalisis dahulu kemudian ditangani	2
20	Q107	Apakah manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?	Ya, cepat	3
21	Q108	Apakah sudah ada pembaharuan mekanisme sistem keamanan?	Belum	1
22	Q109	Apakah petugas selalu memonitor terhadap penanganan insiden?	Selalu	3
23	Q110	Apabila terjadi insiden, apakah sudah ada kebijakan dokumentasi untuk insiden tersebut?	Ya, bisa jadi akhir bulan biasanya.	2

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQS_CARS
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Agung Fatwanto, S.Si, M.Kom., Ph.D
Audit Function	: Compliance, Audit, Risk and Security (CARS)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Agung Fatwanto, S.Si, M.Kom., Ph.D

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?	Ada, dg monitoring rutin terhadap lalu lintas jaringan.	1
2	Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?	Iya seminggu sekali	1
3	Q39	Sudah adakah kebijakan pengamanan jaringan?	Sudah ada	3
4	Q40	Apakah sudah terdokumentasi ?	Sudah, di divisi IT	1
5	Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?	Sudah, pengaturan hak akses dan pengaturan fitur yg diakses secara internal	3
6	Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?	Belum, masih menggunakan versi yang lama	1
7	Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?	Belum, karena operator yg ditugaskan untuk mengelola belum cukup	1
8	Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?	Sudah dokumennya di staff IT	3
9	Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?	Belum ada serangan, jadi belum ada mekanisme recovery	1
10	Q75	Apakah sudah ada prosedur log on?	Ada	3
11	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?	Ya	3
12	Q77	Apakah user diberikan pelatihan	Tidak diberikan	0

		penggunaan sistem informasi yang benar dan aman ?		
13	Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?	Ya	2
14	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?	Tidak perlu pengamanan dikomputer karena bersifat online	3
15	Q80	Apkakah ada kendala dalam penggunaan komputer ini?	Tidak ada	2
16	Q81	Apakah kendala tersebut?	Tidak ada	2
17	Q82	Bagaimana cara menangani kendala tersebut?	Tergantung kerusakan	2
18	Q83	Apakah sudah ada sistem manajemen password?	Sudah	3
19	Q84	Apakah ada sosialisasi password yang interaktif?	Belum	0
20	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?	Karena sistemnya online jadi aman terhadap flasdisk	3
21	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?	Setiap ada kesalahan langsung diperbaiki	2
22	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?	Sudah, default server	3

Lembar Kertas Kerja

Audit Keamanan Sistem Informasi Berdasarkan Standar SNI – ISO 27001

Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Document ID	: FQ6_IT
Project Name	: Audit Keamanan Sistem Informasi Berdasarkan Standar SNI ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogayakarta
Auditor	: Dwi Indah Permatasari
Auditee	: Ramadhan Gatra, S.T
Audit Function	: Information and Technology Division (IT)
Description	: Lembar kertas kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja ini digunakan untuk mengetahui keamanan sistem Admisi di UIN Sunan Kalijaga
Date	:

Approved by

Ramadhan Gatra, S.T

Auditor

Dwi Indah Permatasari

No	Kode	Pertanyaan	Respon	Score
1	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?	Belum ada	0
2	Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?	Iya, traffic jaringan dikontrol selalu	2
3	Q39	Sudah adakah kebijakan pengamanan jaringan?	Sudah	2
4	Q40	Apakah sudah terdokumentasi ?	Belum ada	0
5	Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?	Sudah, kontrol di sistem jaringan misal firewallnya	2
6	Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?	Ya, jika ada notif serangan kemudian dicek secara berkala	2
7	Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?	Sudah, pada akses kontrolnya	2
8	Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?	Sudah	3
9	Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?	Sudah, apabila sistem down akan dialihkan ke sistem ke 2	4
10	Q75	Apakah sudah ada prosedur log on?	Sudah, misal log file	3
11	Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?	Ada, untuk admin, karyawan dan mahasiswa	3
12	Q77	Apakah user diberikan pelatihan		

		penggunaan sistem informasi yang benar dan aman ?	Ya, untuk pegawai kalau untuk admisi belum ada	2
13	Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?	Ya	2
14	Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?	Tidak perlu, karena sifatnya online	3
15	Q80	Apkakah ada kendala dalam penggunaan komputer ini?	Tidak ada kendala	2
16	Q81	Apakah kendala tersebut?	Tidak ada	2
17	Q82	Bagaimana cara menangani kendala tersebut?	Tidak ada	2
18	Q83	Apakah sudah ada sistem manajemen password?	Sudah	3
19	Q84	Apakah ada sosialisasi password yang interaktif?	Belum ada	0
20	Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?	Sistem admisi Sifatnya online jadi aman	3
21	Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?	Membuat sub domain yg baru tetapi yang lama dibiarkan aktif	3
22	Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?	Sudah, kira-kira ± 5 menit	3

LAMPIRAN N : Hasil Evaluasi Audit

Dokumen ID : LEA

Dokumen Name : Lembar Evaluasi Audit

Dokumen berikut digunakan sebagai pedoman perhitungan nilai *maturity* proses audit.

CIO :
HD :
HO:
SI:
CARS
IT:

NO	KLAUSUL	CODE	QUESTIONS	FORM QUESTIONS						SCORE MATURITY	MATURITY	RATA - RATA SISTEM
				CIO	HD	HO	SI	CARS	IT			
1	A.5											
	A.5.1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?	2						1,6	Repeatable but Intuitive	2,0890926
		Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?	1								
		Q3	Apakah ada dokumentasi kebijakan keamanan informasi?	1								
		Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?	2								

		Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?	2								
	A.5.2	Q6	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	3								
		Q7	Apakah kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus?	2								
		Q8	Berapa jangka waktu pengecekan keamanan informasi tersebut?	1								
		Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	1								
		Q10	Apakah ada pembaruan rutin pada kebijakan keamanan informasi?	1								
2	A.7											
	A.7.1	Q11	Apakah sudah diterapkan kebijakan pengelolaan aset ?	2						2,111111111	Repeatable but Intuitive	
		Q12	Bagaimanakah kebijakan pengelolaan aset ?	2								
		Q13	Apakah ada kendala dalam melaksanakan kebijakan penelolaan aset ?	2								
		Q14	Apakah sudah dilakukan pembaruan rutin dari kebijakan pengelolaan aset ?	1								
		Q15	Bagaimana prosedur inventarisasi aset ?	2								
		Q16	Siapakah yang bertanggung jawab terhadap inventarisasi aset ?	3								
		Q17	Berapa jangka waktu pengecekan inventarisasi aset secara berkala ?	1								
	A.7.2	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user sistem Admisi ?	3								

		Q19	Bagaimana prosedur pengklasifikasian data tersebut ?	3								
3	A.9											
	A.9.1	Q20	Apakah ada tempat khusus untuk penempatan server sistem informasi ?	3	3					1,852941176	Repeatable but Intuitive	
		Q21	Bagaimanakah kondisi ruangan khusus untuk server tersebut ?	3	1							
		Q22	Apakah sistem Admisi di area publik sudah aman misal di unit pendaftaran ?	1	1							
		Q23	Bagaimana kondisi tempat untuk sistem Admisi di unit pendaftaran ?	1	1							
		Q24	Apakah penempatan sistem Admisi sudah membuat nyaman user ?	2	3							
		Q25	Apakah anda bisa mengcopy data menggunakan flash diskdisk di komputer ini ?	3	3							
		Q26	Apakah hanya karyawan unit sistem admisi yang dapat mengakses pintu masuk ke sistem admisi?	3	3							
		Q27	Apakah anda merasa nyaman dengan penempatan sistem admisi ini ?	2	2							
		Q28	Apakah anda pernah mengalami kecelakaan kerja terkait sistem admisi misal terkena listrik ?	3	3							
		Q29	Apakah anda merasa aman jika bekerja di ruangan ini terkait kabel, cpu, dan lainya ?	3	3							
		Q30	Apakah anda mudah mengoperasikan sistem admisi ini ?	2	3							
	A.9.2	Q31	Apakah ada prosedur untuk pengecekan	2	2							

			hardware ?									
		Q32	Bagaimana prosedur pengecekan hardware ?	1	0							
		Q33	Berapa jangka waktu pengecekan hardware secara berkala ?	1	0							
		Q34	Siapakah yang bertanggung jawab terhadap pengecekan hardware ?	2	0							
		Q35	Adakah tempat khusus yang sering terjadi kerusakan hardware ?	1	1							
		Q36	Bagaimana anda menangani kerusakan itu ?	1	1							
	A.10											
4	A.10.6	Q37	Apakah ada perawatan khusus untuk mencegah terjadinya serangan?					1	0	1,777777778	Repeatable but Intuitive	
		Q38	Apakah sistem admisi selalu dikontrol secara secara berkala oleh petugas?					1	2			
		Q39	Sudah adakah kebijakan pengamanan jaringan?					3	2			
		Q40	Apakah sudah terdokumentasi ?					1	0			
		Q41	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?					3	2			
		Q42	Adakah pembaharuan yang dilakukan terhadap strategi pencegahan pada jaringan sistem ?					1	2			
		Q43	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?					1	2			

		Q44	Apakah manajemen sudah menerapkan SNMP dalam upaya menjaga sekuritas jaringan?					3	3			
		Q45	Jika setelah terjadi serangan, apakah ada mekanisme recovery jaringan yang sudah diterapkan?					1	4			
5	A.11											
	A.11.1	Q46	Apakah sudah ada dokumentasi control akses?			3				2,181818182	Repeatable but Intuitive	
		Q47	Apakah sudah ada kebijakan dalam mengatur kontrol akses?			3						
		Q48	Apakah ada kendala dalam melaksanakan kebijakan pengendalian akses ?			3						
		Q49	Apakah dilakukan pembaruan rutin kebijakan pengendalian akses ?			1						
		Q50	Siapakah yang bertanggung jawab terhadap pengendalian akses ?			3						
		Q51	Apakah sudah sesuai kebijakan pengendalian akses dengan kondisi riil di lapangan ?			3						
	A.11.2	Q52	Apakah user sistem Admisi diberikan user id dan password ?		3	3						
		Q53	Apakah user memahami keamanan user id dan password ?		2	3						
		Q54	Apakah ada prosedur registrasi untuk user ? (karyawan dan mahasiswa)		2	3						
		Q55	Apakah ada prosedur pencabutan akses ke seluruh sistem admisi?		2	3						
		Q56	Apakah sudah ada alokasi penggunaan		3	3						

			hak akses kepada user?									
		Q57	Apakah sudah ada sistem / program / aplikasi yang digunakan untuk mengelola hak akses user?		3	3						
		Q58	Berapa lama jangka waktu anda mengganti password ?		1	2						
		Q59	Apakah ada divisi tertentu dalam mengelola hak akses user?		3	2						
	A.11.3	Q60	Bagaimana cara user mendapatkan password akun?		3							
		Q61	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?		2							
		Q62	Apakah ada sosialisasi dalam pemilihan password yang baik?		1							
		Q63	Apakah user mengubah password dalam sistem tersebut?		2							
		Q64	Adakah ada petunjuk untuk membuat kombinasi password yang baik?		0							
		Q65	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?		3							
		Q66	Apakah anda pernah memberikan password ke orang lain ?		3							
		Q67	Apakah anda pernah meninggalkan komputer tanpa logout dari sistem admisi ?		3							
		Q68	Apa yang terjadi dengan komputer anda ?		2							
	A.11.4	Q69	Apakah ada kebijakan layanan jaringan ?	2	2	2						
		Q70	Siapakah yang bertanggung jawab	3	3	3						

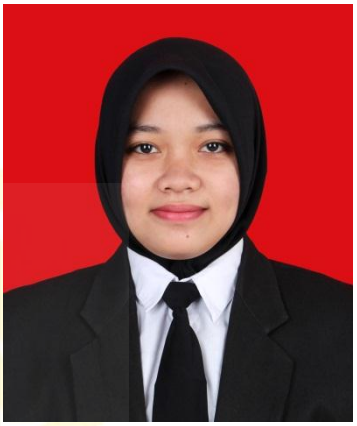
			terhadap layanan jaringan ?									
		Q71	Apakah ada prosedur pengamanan jaringan ?	2	2	2						
		Q72	Bagaimanakan prosedur pengamanan jaringan ?	2	0	3						
		Q73	Dimanakah sering terjadi kerusakan atau gangguan jaringan ?	2	0	2						
		Q74	Apakah anda pernah membuka media sosial dengan komputer ini saat jam kerja ?	2	2	2						
	A.11.5	Q75	Apakah sudah ada prosedur log on?		3			3	3			
		Q76	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?		3			3	3			
		Q77	Apakah user diberikan pelatihan penggunaan sistem informasi yang benar dan aman ?		0			0	2			
		Q78	Apakah saat anda mengganti password ada kombinasi yang unik ?		2			2	2			
		Q79	Bagaimana mengamankan aplikasi sistem Admisi dari media luar user misal flash disk ?		3			3	3			
		Q80	Apkakah ada kendala dalam penggunaan komputer ini?		0			2	2			
		Q81	Apakah kendala tersebut?		0			2	2			
		Q82	Bagaimana cara menangani kendala tersebut?		0			2	2			
		Q83	Apakah sudah ada sistem manajemen password?		2			3	3			

		Q84	Apakah ada sosialisasi password yang interaktif?		0			0	0			
		Q85	Bagaimana mengamankan aplikasi sistem admisi dari media luar user misal flash disk ?		1			3	3			
		Q86	Bagaimana prosedur maintanance aplikasi sistem admisi ?		3			2	3			
		Q87	Apakah sistem admisi sudah menerapkan mekanisme session time out?		3			3	3			
6	A.12											
	A.12.1	Q88	Pada saat perancangan sistem, apakah keamanan dalam sistem informasi yang dibangun sudah termasuk dalam bussiness statements?				2			2,6	Repeatable but Intuitive	
		Q89	Bagaimana prosedur tersebut?				3					
		Q90	Apakah ada kesulitan saat menerapkan prosedur tersebut?				3					
		Q91	Pada saat sistem informasi berjalan, apakah rancangan keamanan sistem admisi sudah terimplementasi?				2					
		Q92	Pada tahap perancangan sistem admisi, apakah keamanan sistem informasi yang dibangun sudah termasuk dalam perancangan?				2					
		Q93	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem?				3					
		Q94	Apabila terjadi serangan sistem, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?				3					

		Q95	Apakah ada monitoring manajemen terhadap mekanisme sistem informasi?				2						
		Q96	Apakah sudah ada dokumentasi mekanisme pengamanan sistem?				3						
		Q97	Apakah petugas selalu mengidentifikasi titik kelemahan sistem ?				3						
		Q98	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?				2						
	A.12.4	Q99	Apakah sudah ada Standar Operation Procedure pada sistem admisi?				2						
		Q100	Sudah berapa lama prosedur tersebut diterapkan?				3						
		Q101	Apakah petugas selalu mengontrol program source code sistem tersebut?				3						
		Q102	Berapa jangka waktu pengecekan sistem tersebut?				3						
7	A.13												
	A.13.1	Q103	Apakah pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat?				3				2,5	Repeatable but Intuitive	
		Q104	Apakah petugas selalu melaporkan temuan kelemahan sistem?				3						
		Q105	Seperti apakah temuan tersebut?				2						
	A.13.2	Q106	Apakah solusi yang diberikan pada saat sistem terkena serangan?				3						
		Q107	Apakah manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?				3						
		Q108	Apakah sudah ada pembaharuan				1						

			mekanisme sistem keamanan?									
		Q109	Apakah petugas selalu memonitor terhadap penanganan insiden?				3					
		Q110	Apabila terjadi insiden , apakah sudah ada kebijakan dokumentasi untuk insiden tersebut?				2					

CURRICULUM VITAE



Nama	: Dwi Indah Permatasari
Tempat, Tanggal Lahir	: Ngawi, 15 Januari 1994
Jenis Kelamin	: Perempuan
Status	: Belum menikah
Agama	: Islam
Nama Ayah	: Bakrun
Nama Ibu	: Umu Basiroh
Alamat	: Jalan Kresno no.76 RT 01 RW 04 Ds.Walikukun, Kec. Widodaren, Kab. Ngawi
No.HP	: 085736320495
Email	: ipermata78@gmail.com

Riwayat Pendidikan :

2000-2006	: SD N Widodaren 4
2006-2009	: SMP N 1 Widodaren
2009-2012	: SMA N 1 Widodaren
2012-2016	: Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta