

AUDIT MANAJEMEN JARINGAN WIFI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA
MENGGUNAKAN STANDAR SNI-ISO 27001

Skripsi

Untuk Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1

Program Studi Teknik Informatika



Disusun Oleh:

Muhammad Haedar Zhafran Hidayatullah

(13650019)

PRODI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2017



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1347/Un.02/DST/PP.00.9/08/2017

Tugas Akhir dengan judul : Audit Manajemen Jaringan Wifi Universitas Islam Negeri Sunan Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001

yang dipersiapkan dan disusun oleh:

Nama : MUHAMMAD HAEDAR ZHAFRAN
HIDAYATULLAH
Nomor Induk Mahasiswa : 13650019
Telah diujikan pada : Senin, 14 Agustus 2017
Nilai ujian Tugas Akhir : A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Sumarsono, S.T., M.Kom.
NIP. 19710209 200501 1 003

Pengaji I

Aulia Faqih Rifa'i, M.Kom
NIP. 19860306 2011011 009

Pengaji II

Dr. Bambang Sugiantoro, MT.
NIP. 19751024 200912 1 002

Yogyakarta, 14 Agustus 2017

UIN Sunan Kalijaga

Fakultas Sains dan Teknologi

D E K A N

Dr. Murtono, M.Si

NIP. 19691212 200003 1 001





SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hai : Permohonan
Lamp : -

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

Assalamu'alaikum wr. wb.

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

Nama : Muhammad Haedar Zhafran Hidayatullah
NIM : 13650019
Judul Skripsi : Audit Manajemen Jaringan Wifi Universitas Islam Negeri Yogyakarta
Menggunakan Standar SNI-ISO 27001

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, 7 Agustus 2017

Pembimbing

Sumarsono, S.T., M.Kom.

NIP. 19710209 200501 1 003

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama : Muhammad Haedar Zhafran Hidayatullah
NIM : 13650019
Program Studi : Teknik Informatika
Fakultas : Sains dan teknologi

Menyatakan bahwa skripsi dengan judul "**Audit Manajemen Jaringan Wifi Universitas Islam Negeri Sunan Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001**" tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Yogyakarta, 7 Agustus 2017

Yang menyatakan,



Muhammad Haedar Zhafran H
NIM: 13650019

KATA PENGANTAR

Segala puji syukur penulis panjatkan hanya bagi Allah SWT. 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 Manajemen Jaringan Wifi UIN Sunan Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001”**.

Skripsi atau tugas akhir ini diselesaikan untuk memenuhi salah satu syarat guna mencapai gelar sarjana pada program studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Selesainya tugas akhir ini tentunya tidak lepas dari dorongan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih sebesar-besarnya kepada :

1. Allah SWT, Tuhan Semesta Alam yang telah memberikan kelancaran dan ridho dalam penyusunan skripsi ini, tanpa kehendak-Nya penyusunan skripsi ini tidak akan terlaksana dengan baik.
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. Dr. Bambang Sugiantoro, MT., selaku Kepala Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
5. Bapak Nurochman, M.Kom., selaku Dosen Pembimbing Akademik.

6. Bapak Sumarsono, S.T., M.Kom. selaku Dosen Pembimbing Skripsi, yang telah banyak memberi arahan, dukungan, masukan, dan motivasi untuk keberhasilan penyusunan skripsi ini.
7. Seluruh Dosen Program Studi Teknik Informatika yang telah memberi banyak ilmu pengetahuan kepada penulis, semoga ilmu yang didapat bisa bermanfaat dan menjadi amal jariyah.
8. Ayahanda Muhammad Ridwan, Ibuku Hidayah Puji Triyani, dan Adekku Meutia Anissabrina Zhafirah, serta seluruh anggota keluarga atas segala doa, perhatian, dukungan moril maupun materil, serta kasih saying yang tak ternilai harganya.
9. Teman-teman Program Studi Teknik Informatika 2013 Reguler maupun Mandiri yang telah banyak memberi arahan untuk penyusunan dan penelitian ini.
10. Fitri Alfianti yang tak henti-henti memberikan support serta solusi untuk keberhasilan penyusunan skripsi ini.
11. Teman-teman kerjaku di PrivyID yang banyak mengajariku bagaimana menjadi seorang pekerja yang disiplin dan bertanggung jawab, dengan adanya kalian saya bisa lebih tau tentang dunia kerja dan cara menanggulangi setiap masalah.
12. Teman-teman kerja di Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) yang telah banyak membantu meluangkan waktunya untuk membantu penyusunan skripsi.
13. Seluruh teman-teman band The Salvatory, Lumena, Silangkata, Nuswantara Project, Last Day Adventist, Elevans Project, atas dukungannya.

14. Serta semua pihak yang tidak dapat disebutkan satu persatu, yang telah memberikan banyak dukungan, motivasi, inspirasi, dan membantu dalam proses penyelesaian skripsi ini.

Pada akhirnya penulis hanya dapat bersyukur kepada Allah SWT semoga dalam proses penyusunan skripsi ini menjadi amal di dunia dan akhirat nanti. Penulis menyadari masih banyak sekali kekurangan dalam penelitian ini, Akhir kata semoga penelitian ini dapat menjadi panduan serta referensi yang sangat berguna bagi pembaca dan dapat dimanfaatkan dalam pengembangan ilmu pengetahuan.

Yogyakarta, 7 Agustus 2017

Penulis,

Muhammad Haedar Zhafran H

NIM: 13650019

HALAMAN PERSEMBAHAN

Alhamdulillahirrabbil'alamin. Dengan mengucap segala rasa syukur sehingga penulis dapat menyelesaikan tugas akhir atau skripsi ini. Kupersembahkan tugas akhir ini untuk:

1. Orang tuaku tercinta, Ayahanda Muhammad Ridwan dan Ibuku Hidayah Puji Triyani, yang tak henti-hentinya memanjatkan doa, perhatian, dukungan moril maupun materil, serta kasih sayang yang tak ternilai harganya. Kedua malaikatku yang tak pernah bosan mendoakan dan menyanyangiku dan terus mendukungku sampai sejauh ini. Semoga orangtuaku panjang umur, sehat selalu, dan bisa melihatku menjadi anak yang sukses, yang bisa membanggakan keluarga suatu hari nanti. Serta Adekku Meutia Anissabrina Zhafirah yang sangat baik. Semoga Allah memberikan berkah kepada kalian.
2. Semua jajaran keluarga besar Teknik Informatika, khususnya kepada Bapak Sumarsono, S.T., M.Kom selaku Dosen Pembimbing Skripsi yang selalu sabar, menerima, dan mengarahkan yang benar tentang penyusunan dan sistematika dalam penyusunan ini. Semoga bapak selalu bahagia panjang umur, selalu menjadi kebanggaan keluarga, dan sehat selalu.
3. Pihak-pihak yang memberikan doa, bantuan, semangat, dan motivasi baik secara langsung maupun tidak langsung yang tidak dapat penulis sebutkan namanya satu-persatu.

MOTTO

“Sesuatu akan menjadi kebanggan, jika sesuatu itu dikerjakan, dan bukan hanya dipikirkan. Sebuah cita-cita akan menjadi kesuksesan, jika kita awali dengan bekerja untuk mencapainya. Bukan hanya menjadi impian”



DAFTAR ISI

HALAMAN JUDUL.....	i
PENGESAHAN SKRIPSI	ii
PERSETUJUAN SKRIPSI	iii
PERNYATAAN KEASLIAN SKRIPSI.....	iv
KATA PENGANTAR	v
HALAMAN PERSEMBAHAN	viii
MOTTO	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN	xvi
DAFTAR SINGKATAN	xviii
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	2
1.2 Rumusan Masalah	4
1.3 Batasan Penelitian	5
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5

1.6 Keaslian Penelitian.....	6
BAB II.....	7
2.1 Tinjauan Pustaka	7
2.2 Landasan Teori.....	10
2.2.1 Definisi Audit.....	10
2.2.2 Definisi Sistem.....	13
2.2.3 Dasar Manajemen Keamanan Informasi	16
2.2.4 Definisi CIA	17
2.2.4.1 Confidentiality	17
2.2.4.2 Integrity	18
2.2.4.3 Availability	18
2.2.5 Pengertian Captive Portal	19
2.2.6 Definisi ISO/IEC 27001	20
2.2.7 Definisi SNI-ISO 27001	21
2.2.8 Definisi Maturity Model	26
BAB III METODE PENELITIAN.....	28
3.1 Objek Penelitian.....	28
3.2 Perangkat Penelitian.....	28
3.2.1 Hardware	29
3.2.2 Software	29
3.3 Metode Penelitian.....	29
3.3.1 Studi Literatur	29

3.3.2 Penentuan Ruang Lingkup Audit.....	29
3.3.3 Prosedur Audit	30
3.3.4 Uji Kepatutan	31
3.3.5 Evaluasi Hasil Audit	31
3.3.6 Laporan Audit	31
BAB IV PERENCANAAN AUDIT	33
4.1 Tujuan Audit	33
4.2 Lingkup Audit	34
4.2.1 Gambaran Umum PTIPD.....	34
4.2.2 Penentuan Ruang Lingkup	40
4.3 Perencanaan Audit	42
4.3.1 Jadwal Pelaksanaan Audit.....	43
4.3.2 Tim Audit.....	44
4.4 Mekanisme Audit	46
4.4.1 Observasi.....	46
4.4.2 Lembar Kerja Audit	46
4.4.3 Penentuan Target Auditee.....	47
4.5 Pengumpulan Data	48
4.5.1 Wawancara.....	48
4.6 Pengolahan Data.....	49
4.6.1 Analisis Maturity Level	49
4.6.2 Scoring	49

4.7 Laporan Audit	51
4.7.1 Hasil Audit	51
4.7.2 Temuan dan Rekomendasi Audit	52
BAB V HASIL DAN PEMBAHASAN.....	53
5.1 Proses Audit	53
5.1.1 Audit Chief Information Officer (CIO)	54
5.1.2 Audit Head Operations (HO)	55
5.1.3 Audit Complicance, Audit, Risk, and Security (CARS).....	56
5.2 Analisis dan Hasil Audit	57
5.2.1 Analisa Hasil Audit Kebijakan Keamanan	59
5.2.2 Analisa Hasil Audit Manajemen Aset.....	60
5.2.3 Analisa Hasil Audit Pengendalian Akses.....	61
5.2.4 Analisa Hasil Audit Keamanan Fisik dan Lingkungan.....	63
5.2.5 Analisa Hasil Audit Manajemen Komunikasi	64
5.2.6 Analisa Hasil Audit Pemeliharaan dan Perawatan Sistem.....	65
5.2.7 Analisa Hasil Audit Manajemen Kejadian Keamanan	66
5.3 Hasil Rekomendasi Audit	67
5.3.1 Hasil Audit	68
5.3.2 Rekomendasi Audit.....	69
BAB VI	73
6.1 Kesimpulan	73
6.2 Saran.....	74

DAFTAR TABEL

2.1 Tabel Sasaran Pengendalian SNI-ISO 27001	21
4.1 Tabel Sasaran kontrol audit.....	41
4.2 Tabel Jadwal Pelaksanaan Audit.....	43
4.3 Tabel Tim Audit.....	44
4.4 Tabel Target Auditee.....	47
4.5 Tabel Interval Index Penilaian	50
5.1 Tingkat Kematangan Setiap Klausul.....	58



DAFTAR GAMBAR

5.1 Hasil Kematangan Setiap Klausul..... 69



DAFTAR LAMPIRAN

LAMPIRAN A Surat Izin Penelitian
LAMPIRAN B Project Definition (Audit Charter).....
LAMPIRAN C Master Control.....
LAMPIRAN D Detail Control.....
LAMPIRAN E Form Questions.....
LAMPIRAN F Maturity Model
LAMPIRAN G Hasil Wawancara Audit.....
LAMPIRAN H Hasil Evaluasi Audit.....



DAFTAR SINGKATAN

SNI	: Standar Nasional Indonesia
ISO	: International Organization for Standardization
IEC	: International Electrotechnical Commission
SNMP	: Simple Network Management Protocol
PTIPD	: Pusat Teknologi Informasi dan Pangkalan Data
CIA	: Confidentiality, Integrity, and Availability
SOP	: Standar Operation Procedure
TI	: Teknologi Informasi
SI	: Sistem Informasi
SMKI	: Sistem Manajemen Keamanan Informasi
CIO	: Chief Information Officer
HO	: Head Operation
CARS	: Complicance, Audit, Risk, and Security
FQ	: Form Question
MC	: Master Control

Audit Manajemen Jaringan Wifi
Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Menggunakan Standar SNI-ISO 27001

Muhammad Haedar Zhafran Hidayatullah

NIM: 13650019

INTISARI

Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) merupakan salah satu unit pelaksana teknis yang mengelola seluruh aset teknologi informasi yang ada di Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Salah satu pemanfaatan teknologi yang dikelola PTIPD adalah layanan wifi. Dengan adanya layanan wifi akan mempermudah seluruh civitas akademika untuk mengakses internet dan seluruh sistem online yang ada di UIN Sunan Kalijaga Yogyakarta, tanpa adanya jaringan wifi, sistem online tidak dapat berjalan. Namun dengan adanya sistem jaringan wifi yang diterapkan tentunya perlu dilakukan pengamanan sistem yang dimiliki oleh PTIPD.

Oleh karena itu, untuk mendapatkan data tentang sejauh mana manajemen jaringan wifi UIN Sunan Kalijaga perlu adanya audit dengan menggunakan Standar SNI ISO 27001. Standar ini secara resmi yang digunakan oleh pemerintah Indonesia dan adopsi otentik dari standar ISO 27001. Maturity Model digunakan untuk mengukur manajemen jaringan wifi dengan tujuan untuk melihat tingkat kematangan sistem dari kondisi saat ini.

Dari hasil penelitian ini, dapat disimpulkan bahwa tingkat kematangan keamanan jaringan wifi di UIN Sunan Kalijaga Yogyakarta pada skala 2,6 (*Defined Process*). Jadi Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) telah mempunyai mekanisme perencanaan keamanan sistem, inventaris aset, standar operasional kerja yang berlaku, dan *recovery* data.

Kata Kunci: Audit Sistem Jaringan Wifi, SNI-ISO 27001, Maturity Level.

**AUDIT WIFI SERVICE MANAGEMENT IN
ISLAMIC UNIVERSITY OF SUNAN KALIJAGA YOGYAKARTA
USING SNI-ISO 27001 STANDARD**

Muhammad Haedar Zhafran Hidayatullah

NIM: 13650019

ABSTRACT

Information Technology and Data Center is one of technical support units who manage all IT assets in Islamic State University of Sunan Kalijaga Yogyakarta. Wifi service is one of their facilities to facilitate all their online system. Without wifi service, their online system can't works. Therefore, they need to do high security to secure their IT and Data Center.

To knows how secure their security system, they need an audit to fit their wifi service by using SNI ISO 27001 standard. SNI standard is officially used by Indonesian Government and authenticity of ISO 27001 standard. Maturity model is used to measure the security performance of their current wifi network system.

Result of this research, we have 2.21 (Repeatable but intuitive) as their maturity level score in their wifi network system security.

we can conclude that Information Technology and Database Center has mechanism for their security system, assets inventory, operational standard, and data recovery.

Keywords: Wifi Service, Audit, SNI-ISO 27001, Maturity Level.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi yang semakin pesat saat ini ternyata memberikan dampak yang besar bagi kehidupan masyarakat terutama bagi proses penyampaian informasi. Dimana proses penyampaian informasi tersebut dapat diperoleh melalui jaringan internet dan tentunya tidak terlepas dari adanya sistem komputerisasi. Hal tersebut dipengaruhi oleh kecepatan, ketepatan maupun keamanan suatu jaringan yang dikelola agar mampu bekerja lebih baik.

Dalam era dimana semuanya serba mobile, peranan wireless device semakin penting dan menjadi kebutuhan utama bagi sebagian masyarakat. Oleh karena itu setiap pemilik tempat yang mempunyai layanan wifi dapat mengimplementasikan keamanan data agar tidak semua orang dapat menggunakannya tanpa memiliki username dan password. Salah satu lembaga yang menerapkan layanan wifi dengan kemanan data adalah perguruan tinggi, karena perguruan tinggi harus memberikan layanan terbaik dengan memanfatkan teknologi untuk memberikan informasi yang cepat, tepat, dan akurat. Proses tersebut harus didukung oleh beberapa aktifitas penunjang untuk keberhasilan proses yang ada di perguruan tinggi. Kemanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola informasi akan terganggu jika informasi mengalami suatu masalah kemanan informasi yang

menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

Salah satu penunjang vital pada perguruan tinggi adalah sistem pelayanan internet yang mempunyai mekanisme prosedur keamanan data yang baik sehingga perlu adanya standar keamanan sistem untuk tercapainya pelayanan akademik yang baik. Salah satu perguruan tinggi yang menerapkan pelayanan internet adalah UIN Sunan Kalijaga Yogyakarta. UIN menggunakan layanan internet untuk memberikan pelayanan terbaik kepada civitas akademika dan membantu terlaksananya kegiatan unit kerja yang ada di dalam kampus.

Sistem login wifi UIN Sunan Kalijaga Yogyakarta telah menerapkan sistem keamanan data dengan captive portal. Captive portal merupakan suatu teknik autentikasi dan pengamanan data yang membuat user atau pengguna suatu jaringan harus melalui satu halaman web khusus sebelum dapat mengakses internet. Captive portal merupakan mesin router atau gateway yang memanfaatkan web browser sebagai sarana atau perangkat autentikasi yang aman dan terkendali dalam mengijinkan adanya trafik hingga user melakukan registrasi. Hal ini dilakukan untuk mencegah semua paket berupa data dalam bentuk apapun dan kemanapun, sampai user membuka web browser dan mencoba untuk mengakses internet. Browser telah diarahkan ke suatu web khusus yang telah ditentukan untuk melakukan otentikasi, atau sekedar menampilkan halaman yang berlaku dan mengharuskan pengguna untuk menyetujuinya.

Mengingat pentingnya informasi data yang terdapat pada suatu *account* wifi, maka kebijakan tentang pengamanan informasi harus mencakup tentang prosedur

pengendalian dokumen, prosedur pengendalian rekaman, prosedur tindakan perbaikan, prosedur pencegahan, prosedur penanganan informasi, prosedur penanganan insiden, dan prosedur pemantauan penggunaan fasilitas teknologi informasi. Dalam perguruan tinggi UIN Sunan Kalijaga Yogyakarta setiap civitas akademika (rektor, dosen, staff, dan mahasiswa) diberikan satu *account* untuk mengakses ke semua sistem, antara lain akademik, learning, pustaka, surat, pegawai (khusus bagi pegawai UIN Sunan Kalijaga), dan mail.

Diperlukan audit manajemen jaringan wifi UIN Sunan Kalijaga untuk memastikan standar keamanan data yang baik. Standar yang digunakan adalah SNI-ISO 27001. Karena audit manajemen jaringan wifi UIN Sunan Kalijaga belum pernah dilakukan. Maka penulis ingin melaksanakan audit manajemen jaringan wifi UIN Sunan Kalijaga dengan menggunakan standar SNI-ISO 27001. Standar tersebut memuat prinsip-prinsip dasar *Information Security Management Systems* (Sistem Manajemen Kemanan Informasi-SMKI), yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan atau instansi dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di dalam perusahaan atau intansi tersebut. Karena tujuan dari audit ini adalah untuk dapat mewujudkan manfaat TI yang diharapkan, menggunakan dan memaksimalkan manfaat tersebut, mewujudkan penggunaan sumber daya TI yang bertanggung jawab, dan dapat mengelola risiko yang terkait dengan TI.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan di atas, permasalahan yang dapat diangkat yaitu:

1. Bagaimana merencanakan audit manajemen jaringan wifi UIN Sunan Kalijaga dengan menggunakan metode SNI-ISO 27001.
2. Bagaimana melaksanakan audit manajemen jaringan wifi UIN Sunan Kalijaga terhadap faktor CIA (*confidentiality, integrity, availability*).
3. Bagaimana mengetahui tingkat keamanan jaringan wifi UIN Sunan Kalijaga menggunakan standar SNI-ISO 27001.
4. Bagaimana menyusun rekomendasi hasil audit manajemen jaringan wifi UIN Sunan Kalijaga dengan menggunakan standar SNI-ISO 27001.

1.3 Batasan Penelitian

Berdasarkan penelitian yang dilakukan dalam audit ini, yaitu:

1. Penelitian ini dilakukan dengan standar SNI-ISO 27001.
2. Penelitian difokuskan pada manajemen wifi UIN Sunan Kalijaga.
3. Data yang didapatkan adalah hasil dari wawancara pengguna wifi UIN Sunan Kalijaga dan karyawan Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) UIN Sunan Kalijaga.
4. Audit ini difokuskan dalam hal pengelolaan dan penerapan sistem keamanan wifi UIN Sunan Kalijaga menggunakan standar SNI-ISO 27001.

5. Audit ini menggunakan checklist yang ada dalam panduan standar SNI-ISO 27001.
6. Output yang dihasilkan berupa hasil temuan dan rekomendasi hasil audit.

1.4 Tujuan Penelitian

1. Membuat perencanaan audit manajemen jaringan wifi UIN Sunan Kalijaga.
2. Melaksanakan audit manajemen jaringan wifi UIN Sunan Kalijaga terhadap faktor CIA (confidentiality, integrity, availability).
3. Mengetahui tingkat keamanan wifi UIN Sunan Kalijaga menggunakan standar SNI-ISO 27001.
4. Menyusun rekomendasi hasil audit manajemen wifi UIN Sunan Kalijaga dengan melakukan evaluasi terhadap fakta-fakta yang ada, memberikan saran dan informasi tentang tindakan apa saja yang harus dilakukan mengingat pentingnya sistem kemanan yang telah digunakan UIN Sunan Kalijaga, mendokumentasikan hasil audit dan menyusun laporan hasil audit.

1.5 Manfaat Penelitian

Manfaat penelitian yang ingin dicapai dalam audit ini, yaitu:

1. Mengidentifikasi hal apa saja yang perlu dilakukan dan dibenahi untuk meningkatkan kinerja manajemen yang telah ada.
2. Memperoleh hasil dan kondisi yang aktual tentang sistem manajemen wifi yang ada di UIN Sunan Kalijaga.

3. Menghasilkan rekomendasi hasil audit, yang dapat digunakan untuk pengembangan sistem yang ada, sebagai dasar acuan pengembangan sistem dan pelayanan apa yang perlu dilakukan dan dibenahi untuk meningkatkan kinerja manajemen wifi UIN Sunan Kalijaga.
4. Memberikan rekomendasi agar memperhatikan pentingnya manajemen jaringan wifi UIN Sunan Kalijaga serta dapat membantu manajemen tata kelola keamanan jaringan wifi untuk melakukan pengelolaan sesuai standar tata kelola yang baik dan benar.

1.6 Keaslian Penelitian

Penelitian tentang sistem manajemen sudah banyak dilakukan sebelumnya. Namun menggunakan standar dan objek yang berbeda. Sedangkan penelitian tentang Audit Manajemen Jaringan Wifi UIN Sunan Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001 belum pernah dilakukan oleh mahasiswa manapun sebelumnya.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan proses penelitian yang telah dilakukan dari perencanaan hingga didapatkannya hasil penelitian, maka kesimpulan yang dapat peneliti simpulkan dari proses Audit manajemen jaringan wifi UIN Sunan Kalijaga adalah:

1. Peneliti berhasil melakukan kegiatan audit terhadap manajemen jaringan wifi dengan menggunakan standar SNI ISO 27001
2. Peneliti berhasil melakukan proses audit sistem jaringan wifi dengan mengambil studi kasus di Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Peneliti berhasil memberikan penilaian terhadap manajemen jaringan wifi dengan dengan tingkat kematangan 2.6 (Defined Process), yang artinya artinya proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan, dan dikomunikasikan melalui pelatihan. Proses berada pada keadaan diamanatkan namun kecil kemungkinan penyimpangan dapat terdeteksi.
4. Rekomendasi hasil audit pada sistem jaringan wifi Universitas Islam Negeri Sunan Kalijaga Yogyakarta berhasil disusun dan diberikan pada setiap klausul berdasarkan analisa hasil audit untuk memperbaiki sistem pengelolaan yang ada.

6.2 Saran

Dari keseluruhan penelitian yang telah dilakukan tentunya tidak terlepas dari kekurangan dan kelamahan yang harus diperbaiki dan ditingkatkan, termasuk peneliti mungkin masih banyak kesalahan dalam melakukan penelitian. Oleh karena itu untuk jangka waktu selanjutnya penulis menyarankan beberapa hal sebagai berikut:

1. Dilakukan audit internal menggunakan standar SNI ISO 27001 secara rutin oleh pihak manajemen Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Seluruh Manajemen, baik pimpinan dan karyawan Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas Islam Negeri Sunan Kalijaga Yogyakarta perlu lebih memahami pentingnya manajemen dalam mendukung proses kerja guna mencapai visi misi dan tujuan dari PTIPD.
3. Untuk penelitian lebih lanjut mengenai manajemen jaringan wifi diharapkan menggunakan klausul yang lebih menyeluruh dan mendetail sehingga diperoleh nilai keamanan yang semakin akurat.

DAFTAR PUSTAKA

- 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.
- Permatasari, Dwi.2016.Skripsi. Audit Keamanan Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Yogyakarta : UIN Sunan Kalijaga Yogyakarta.
- Juhdan.2016.Skripsi. *Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001.* Yogyakarta : UIN Sunan Kalijaga Yogyakarta.
- Badan Standarisasi Nasional.2009. *Teknologi- Informasi- Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan.* Bogor:Badan Standarisasi Nasional.
- Komalasari, Rizky dan Perdana, Ilham. 2014. *Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001: 2009.* Bandung

LAMPIRAN A: SURAT IZIN PENELITIAN





KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA
FAKULTAS SAINS DAN TEKNOLOGI
Alamat: Jln. Marsda Adisucipto telepon 0274519739 fax 0274540971
<http://saintek.uin-suka.ac.id> Yogyakarta 55281

Nomor : B-967/Un.02/DST.1/PN.01.1/07/2017

26 Juli 2017

Sifat : Penting

Lamp. : 1 bendel proposal

Hal : Permohonan Izin Penelitian

Kepada:

Yth. Kepala PTIPD

UIN Sunan Kalijaga Yogyakarta

di Jln.Marsda Adisucipto 55281 Yogyakarta

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk memenuhi penyusunan tugas akhir/skripsi yang berjudul "ADIT KEAMANAN SISTEM CAPTIVE PORTAL WIFI UIN SUNAN KALIJAGA YOGYAKARTA MENGGUNAKAN STANDAR SNI-ISO 27001" diperlukan penelitian.

Oleh karena itu, kami Mmengharap kiranya Bapak/Ibu berkenan memberikan izin kepada mahasiswa kami :

Nama : Muhammad Haedar zhafran Hidayatullah

NIM : 13650019

Program Studi : Teknik Informatika

Alamat : Pengkok,Patuk,Gunungkidul,Yogyakarta

untuk melakukan penelitian di PTIPD,dengan metode penelitian SNI-ISO 27001 yang dijadwalkan pada tanggal 31 juli 2017 s/d 2 agustus 2017

Sebagai bahan pertimbangan bersama ini kami lampirkan :

1. Proposal Skripsi
2. Fotocopy Kartu Tanda Mahasiswa (KTM)
3. Fotocopy Kartu Rencana Studi (KRS)

Demikian surat permohonan ini disampaikan, atas diperkenankannya diucapkan terimakasih.

Wassalamu'alaikum Wr.Wb.

a.n. Dekan,

Wakil Dekan Bidang Akademik,



Tembusan:

Dekan (sebagai laporan)

LAMPIRAN B: PROJECT DEFINITION (AUDIT CHARTER)



Audit Charter

Project ID : SNI-ISO 27001-Audit-01

Project Name : Management Audit

Auditor : Muhammad Haedar Zhafran Hidayatullah

Project Description :

Penelitian yang berkaitan dengan manajemen jaringan wifi ini menggunakan parameter SNI-ISO 27001. Penelitian ini berfokus pada klausul kebijakan keamanan informasi, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengendalian akses, dan akuisisi pengembangan dan pemeliharaan.

Project Schedule : Juni – Agustus

Stakeholder List :

Jabatan	Responden	Audit Clause
Chief Information Officer (CIO)	Dr. Shofwatul 'Uyun, S.T., M.Kom.	Kebijakan Keamanan A.5.1 A.5.2 Manajemen A.7.1 A.7.2
Head Operations (HO)	Hendra Hidayat, S.Kom.	Pengendalian Akses A.11.1 A.11.2 A.11.3 A.11.4 A.11.5
Compliance, Audit,	Rahmadhan Gatra, S.T.	Keamanan Fisik dan

Risk, and Security (CARS)		Lingkungan A.9.1 A.9.2 Manajemen Komunikasi A.10.6 Pemeliharaan dan Perawatan Sistem A.12.1 A.12.4 Manajemen Kejadian Keamanan A.13.1 A.13.2
------------------------------	--	--

Yogyakarta, 1 Agustus 2017

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Mengetahui, Kepala PTIPD
UIN Sunan Kalijaga




Dr. Shofwatul Uyun, S.T., M.Kom.
NIP: 19820511 2006042 002

Auditor
Muhammad Haedar Zhafran Hidayatullah
NIM: 13650019

LAMPIRAN C: CONTROL OBJECTIVE



No.	Klausul	Deskripsi	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	CARS
	A.9.2	Keamanan Peralatan	CARS
4.	A.10	Manajemen Komunikasi	
	A.10.6	Manajemen Keamanan Jaringan	CARS
5.	A.11	Pengendalian Akses	
	A.11.1	Persyaratan Bisnis untuk Pengendalian Akses	HO
	A.11.2	Manajemen Akses Pengguna	HO
	A.11.3	Tanggung Jawab Pengguna	HO
	A.11.4	Pengendalian Akses Jaringan	HO
	A.11.5	Pengendalian Akses Sistem Operasi	HO
6.	A.12	Pemeliharaan dan Perawatan Sistem	
	A.12.2	Pengolahan Yang Benar Dalam Aplikasi	CARS
	A.12.3	Melindungi dengan Kriptografi	CARS
	A.12.4	Keamanan File Sistem	CARS
7.	A.13	Manajemen Kejadian Keamanan	
	A.13.1	Pelaporan Kejadian	CARS
	A.13.2	Pelaporan Kelemahan Keamanan	CARS

LAMPIRAN D: DETAIL OF CONTROL OBJECTIVE



Klausul	Kode
A.5 Kebijakan keamanan	
A.5.1	Q1
	Q2
	Q3
	Q4
	Q5
A.5.2	Q6
	Q7
	Q8
	Q9
	Q10
A.7 Manajemen Aset	
A.7.1	Q11
	Q12
	Q13
	Q14
	Q15
	Q16
	Q17
A.7.2	Q18
	Q19
A.9 Keamanan Fisik dan Lingkungan	
A.9.1	Q20
	Q21
	Q22
	Q23
	Q24
	Q25
	Q26

	Q27
	Q28
	Q29
	Q30
A.9.2	Q31
	Q32
	Q33
	Q34
	Q35
	Q36
A.10 Manajemen Komunikasi	
A.10.6	Q37
	Q38
	Q39
	Q40
	Q41
	Q42
	Q43
	Q44
	Q45
A.11 Pengendalian Akses	
A.11.1	Q46
	Q47
	Q48
	Q49
	Q50
	Q51
A.11.2	Q52
	Q53
	Q54

	Q55
	Q56
	Q57
	Q58
	Q59
A.11.3	Q60
	Q61
	Q62
	Q63
	Q64
	Q65
	Q66
	Q67
	Q68
A.11.4	Q69
	Q70
	Q71
	Q72
	Q73
	Q74
SUNAN KALIJAGA YOGYAKARTA	Q75
	Q76
	Q77
	Q78
	Q79
A.11.5	Q80
	Q81
	Q82
	Q83
	Q84

	Q85
	Q86
	Q87
A.12 Pemeliharaan dan Perawatan Sistem	
A.12.2	Q88
	Q89
	Q90
	Q91
	Q92
	Q93
	Q94
	Q95
	Q96
	Q97
	Q98
A.12.3	Q99
	Q100
	Q101
	Q102
A.12.4	Q103
	Q104
	Q105
	Q106
A.13 Manajemen Kejadian Keamanan	
A.13.1	Q107
	Q108
	Q109
A.13.2	Q110
	Q111
	Q112

	Q113
	Q114



LAMPIRAN E: FORM QUESTIONS



Pemetaan Pertanyaan yang Akan Digunakan Saat Proses Audit

Form Questions 1 (FQ1) : CIO

Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19

Form Questions 2 (FQ2) : HO

Q46, Q47, Q48, Q49, Q50, Q51, 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 Questions 3 (FQ3) : CARS

Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q88, Q89, Q90, Q91, Q92, Q93, Q94, Q95, Q96, Q97, Q98, Q99, Q100, Q101, Q102, Q103, Q104, Q105, Q106, Q107, Q108, Q109, Q110, Q111, Q112, Q113, Q114

LAMPIRAN F: MATURITY MODEL



No	Tingkat Kematangan	Definisi
1	0 – (Non-Existent)	Proses manajemen tidak diterapkan sama sekali. Semua proses tidak dapat diidentifikasi dan dikenali. Status kesiapan keamanan informasi tidak diketahui.
2	1 – (Initial/Ad Hoc)	Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi. Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan resiko yang ada, tanpa alur komunikasi, dan kewenangan yang jelas dan tanpa pengawasan, Kelemahan teknis dan nonteknis tidak teridentifikasi dengan baik, pihak yang terlibat tidak menyadari tanggung jawab mereka.
3	2 – (Repeatable but Intuitive)	Proses mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainnya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing-masing dan kesalahan sangat mungkin terjadi.
4	3 – (Defined Process)	Proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan, dan dikomunikasikan melalui pelatihan.

		Proses berada pada keadaan diamanatkan namun kecil kemungkinan penyimpangan dapat terdeteksi. Prosedur yang ada hanya formalisasi praktek yang ada.
5	4 – (Managed and Measurable)	Monitor dari manajemen dan mengukur kepatuhan prosedur dan mengambil tindakan apabila diperlukan. Selalu ada proses pembaharuan yang konstan dan berkala dan memberikan pelaksanaan yang baik. Otomasi dan alat-alat yang digunakan diakses secara terbatas dan sudah terfragmentasi
6	5 – (Optimized)	Praktek yang baik diikuti dan secara otomatis. Proses telah disempurnakan ke tingkat pelaksanaan yang baik, berdasarkan hasil dari peningkatan berkelanjutan dan maturity pemodelan dengan informasi lainnya tentang perusahaan. TI digunakan secara terpadu untuk mengotomatisasi alur kerja, menyediakan alat untuk meningkatkan kualitas dan efektivitas.

LAMPIRAN G: HASIL WAWANCARA AUDIT



LEMBAR KERTAS KERJA AUDIT

Audit Manajemen Jaringan Wifi

Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Menggunakan Standar SNI-ISO 27001

Document ID : FQ1-CIO

Project Name : Audit Manajemen Jaringan Wifi Universitas Islam Negeri Sunan
Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001

Auditor : Muhammad Haedar Zhafran Hidayatullah

Audite : Dr. Shofwatul 'Uyun, S.T., M.Kom.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian
tugas akhir mahasiswa Program Studi Teknik Informatika,
Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar
kerja audit ini digunakan untuk mengevaluasi manajemen yang
diterapkan oleh pengelola Wifi Universitas Islam Negeri Sunan
Kalijaga Yogyakarta

Date :

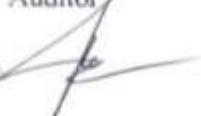
Responsible : Chief Information Officer (CIO)

Approved by



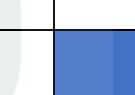
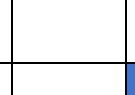
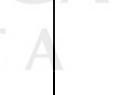
Dr. Shofwatul 'Uyun, S.T., M.Kom.

Auditor



Muhammad Haedar Zhafran H.

No	Code	Questions	Score Maturity					
			0	1	2	3	4	5
1	Q1	Sudah diterapkan kebijakan keamanan informasi					5	
2	Q2	Kebijakan keamanan informasi sudah terdokumentasi				4		
3	Q3	Kebijakan tersebut sudah dipublikasikan kepada seluruh pihak terkait			3			
4	Q4	Petugas selalu mengontrol keamanan informasi secara berkala		2				
5	Q5	Kebijakan tersebut sudah disosialisasikan dalam bentuk yang lebih relevan, mudah diakses, dan dapat dimengerti			1			
6	Q6	Adanya petugas yang bertanggung jawab terhadap kebijakan keamanan informasi				5		
7	Q7	Kebijakan keamanan informasi sudah sesuai dengan kondisi riil di kampus				4		

8	Q8	Terdapat estimasi waktu pengecekan keamanan informasi							
9	Q9	Kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku							
10	Q10	Adanya tinjauan rutin pada kebijakan keamanan informasi							
11	Q11	Diterapkan kebijakan pengelolaan inventaris aset							
12	Q12	Inventaris aset perlu didokumentasikan							
13	Q13	Semua inventaris aset seperti informasi, piranti lunak, fisik, dan layanan sudah terdokumentasi							
14	Q14	Klasifikasi lokasi keamanan didokumentasikan (contoh dokumen hilang atau kerugian)							
15	Q15	Sudah diidentifikasi nilai dan tingkat kepentingan aset							
16	Q16	Adanya petugas yang bertanggung jawab untuk mengontrol dan memelihara terhadap semua inventaris							
17	Q17	Adanya pengecekan inventarisasi aset secara berkala							

18	Q18	Adanya pengklasifikasian data yang dapat diakses oleh user						
19	Q19	Adanya prosedur pengklasifikasian data tersebut						



LEMBAR KERTAS KERJA AUDIT

Audit Manajemen Jaringan Wifi

Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Menggunakan Standar SNI-ISO 27001

Document ID : FQ2-HO

Project Name : Audit Manajemen Jaringan Wifi Universitas Islam Negeri Sunan
Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001

Auditor : Muhammad Haedar Zhafran Hidayatullah

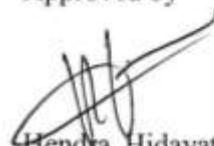
Audite : Hendra Hidayat, S.Kom.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian
tugas akhir mahasiswa Program Studi Teknik Informatika,
Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar
kerja audit ini digunakan untuk mengevaluasi manajemen yang
diterapkan oleh pengelola Wifi Universitas Islam Negeri Sunan
Kalijaga Yogyakarta

Date :

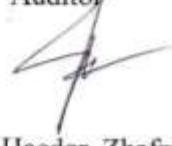
Responsible : Head Officer (HO)

Approved by



Hendra Hidayat, S.Kom.

Auditor



Muhammad Haedar Zhafran H

No	Code	Questions	Score Maturity					
			0	1	2	3	4	5
1	Q46	Adanya dokumentasi control akses					5	
2	Q47	Adanya kebijakan dalam mengatur kontrol akses					5	
3	Q48	Ditemukan kendala dalam melaksanakan kebijakan pengendalian akses		5				
4	Q49	Kebijakan pengendalian akses dilakukan pembaruan rutin					5	
5	Q50	Ada petugas yang bertanggung jawab terhadap pengendalian akses					5	
6	Q51	Kebijakan pengendalian akses sudah sesuai dengan kondisi riil di lapangan					5	
7	Q52	Adanya klasifikasi user jaringan wifi						5
8	Q53	User memahami keamanan bahwa user id hanya milik personal						5
9	Q54	Jika user mempunyai tunggakan atau hal yang belum terselesaikan user ID tersebut mengalami suspend lock/terkunci sementara					5	

10	Q55	Adanya prosedur pencabutan akses ke seluruh sistem						
11	Q56	Adanya alokasi penggunaan hak akses kepada user						
12	Q57	Adanya sistem/program /aplikasi yang digunakan untuk mengelola hak akses user						
13	Q58	Adanya batasan jumlah dalam mengganti password						
14	Q59	Adanya divisi tertentu dalam mengelola hak akses user						
15	Q60	Adanya prosedur validasi data pengguna						
16	Q61	Petugas selalu meninjau ulang terhadap hak akses user secara berkala						
17	Q62	Sudah ada sistem manajemen password dan sistem pengelola password untuk mengelola kwalitas password						
18	Q63	Password default setiap user ID tidak ada yang sama dengan user ID lain						
19	Q64	User interface ketika login jaringan wifi mudah dimengerti dan mudah diakses oleh seluruh civitas akademika						

20	Q65	Ketika mengisi password, sudah diterapkan ada sistem clear screen password						
21	Q66	Password default mudah diingat dengan ukuran yang standar						
22	Q67	Pembenahan sistem error pada layanan jaringan wifi (misal gateway, stack, atau force closed)						
23	Q68	Jaringan wifi sudah membatasi dari konten yang tidak semestinya diakses						
24	Q69	Adanya kebijakan dan prosedur layanan jaringan						
25	Q70	Adanya petugas yang bertanggung jawab terhadap layanan jaringan						
26	Q71	Diterapkan proses pengamanan jaringan sebagai upaya pencegahan serangan						
27	Q72	Diterapkan pengamanan sistem dengan kriptografi, contohnya 2FA (Two Factor Authentication)						
28	Q73	Adanya pembaharuan secara berkala untuk terus mengevaluasi dan membangun sistem agar lebih baik						

29	Q74	Mengatasi sumberdaya untuk melakukan pembaharuan sistem						
30	Q75	Adanya prosedur log-on yang aman						
31	Q76	Membatasi kegagalan percobaan log-on						
32	Q77	Seluruh civitas akademika memiliki user ID yang berbeda						
33	Q78	Setiap user ID sudah dibatasi untuk penggunaan pribadi (dari segi kuota)						
34	Q79	Adanya pengamanan jaringan wifi dari pengguna luar						
35	Q80	Penempatan access point sudah sesuai untuk mencakup seluruh lokasi akses						
36	Q81	Adanya sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password						
37	Q82	Ada prosedur batasan jangka waktu pemakaian akun user						

38	Q83	Adanya prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang						
39	Q84	Menggunakan program utility sehingga mampu meminimalisir overriding						
40	Q85	Menggunakan sesi time-out						
41	Q86	Diterapkan prosedur maintenance (misalnya listrik padam) pada sistem jaringan wifi						
42	Q87	Alat penunjang pencegahan maintenance selalu siap dan selalu dipantau						



LEMBAR KERTAS KERJA AUDIT

Audit Manajemen Jaringan Wifi

Universitas Islam Negeri Sunan Kalijaga Yogyakarta

Menggunakan Standar SNI-ISO 27001

Document ID : FQ3-CARS

Project Name : Audit Manajemen Jaringan Wifi Universitas Islam Negeri Sunan
Kalijaga Yogyakarta Menggunakan Standar SNI-ISO 27001

Auditor : Muhammad Haedar Zhafran Hidayatullah

Audite : Rahmadhan Gatra, S.T.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian
tugas akhir mahasiswa Program Studi Teknik Informatika,
Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar
kerja audit ini digunakan untuk mengevaluasi manajemen yang
diterapkan oleh pengelola Wifi Universitas Islam Negeri Sunan

Date :

Responsible : Complience, Audit, Risk, and Security (CARS)

Approved by



Rahmadhan Gatra, S.T.

Auditor



Muhammad Haedar Zhafran H

No	Code	Questions	Score Maturity					
			0	1	2	3	4	5
1	Q20	Adanya tempat khusus untuk penempatan server jaringan						
2	Q21	Komputer dan peralatan informasi lainnya seperti server, sudah di tempatkan pada tempat yang aman						
3	Q22	Adanya sistem pengamanan (misal kartu control atau sidik jari) di pintu masuk ruang server						
4	Q23	Adanya kontrol akses fisik atau ruang sebagai tempat menerima tamu						
5	Q24	Bahan berbahaya dan mudah meledak sudah disimpan diwilayah aman						
6	Q25	Mempertimbangkan kebijakan tentang makan, minum dan merokok disekitar ruangan server						
7	Q26	Adanya perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya						

8	Q27	Penempatan ruang sistem informasi sudah termasuk dalam area yang aman					 	
9	Q28	Penempatan posisi ruang server sudah membuat nyaman pengelola dan pegawai					 	
10	Q29	Pekerja yang berasal dari luar PTIPD akan dilakukan pengawasan dan di pantau (misal perbaikan dan peralatan) di ruang server					 	
11	Q30	Diterapkan mekanisme pengawasan					 	
12	Q31	Adanya prosedur untuk pengecekan peralatan				 		
13	Q32	Keamanan peralatan sudah tidak ada peluang akses oleh pihak yang tidak berwenang					 	
14	Q33	Peralatannya sudah dilindungi dari kegagalan catu daya listrik					 	
15	Q34	Tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan					 	
16	Q35	Kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman					 	

17	Q36	Pembaruan alat-alat yang mengalami kerusakan ditangani dengan cepat						
18	Q37	Menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan						
19	Q38	Maintenance server selalu dikontrol secara berkala oleh petugas						
20	Q39	Back-up data sudah di pelihara serta sudah dilakukan sesuai prosedur						
21	Q40	Back-up data sudah terdokumentasi						
22	Q41	Adanya petugas atau pegawai yang khusus menangani keamanan jaringan						
23	Q42	Manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan						
24	Q43	Apabila serangan telah terjadi, mekanisme recovery yang sudah diterapkan						
25	Q44	Manajemen sudah menerapkan SNMP (<i>Simple Network Management Protocol</i>) dalam upaya menjaga sekuritas jaringan						

26	Q45	Untuk melindungi hak akses tanpa ijin pada jaringan, tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer					 	
27	Q88	Keamanan dalam sistem yang dibangun sudah termasuk dalam business statements				 		
28	Q89	Prosedur business statement sudah berjalan				 		
29	Q90	Kerusakan sistem karena ada kesalahan bisa dideteksi oleh sistem		 				
30	Q91	Pada saat sistem wifi berjalan, rancangan keamanan wifi sudah terimplementasi				 		
31	Q92	Keamanan wifi saat ini sudah dirasa cukup aman					 	
32	Q93	Klasifikasi pembagian tugas dalam penanganan serangan sistem		 				
33	Q94	Apabila terjadi serangan sistem sudah diterapkan mekanisme penanganan sesuai serangannya		 				
34	Q95	Adanya monitoring manajemen terhadap mekanisme sistem wifi		 				
35	Q96	Adanya dokumentasi mekanisme pengamanan sistem		 				

36	Q97	Petugas selalu mengidentifikasi titik kelemahan sistem						
37	Q98	Petugas melakukan pengujian titik kelemahan sistem yang sudah teridentifikasi						
38	Q99	Sistem keamanan dengan kriptografi dapat digunakan dalam sistem jaringan wifi kampus						
39	Q100	Sistem sudah dilindungi dengan sistem kriptografi						
40	Q101	Integritas data user tidak diketahui oleh user lain						
41	Q102	Keamanan sistem telah diterapkan, dan dirasa aman, dan tidak ada masalah penyerangan sejauh ini						
42	Q103	Adanya Standar Operation Procedure pada penggunaan sistem wifi						
43	Q104	Sudah berjalan dan telah diterapkannya Standar Operation Procedure						
44	Q105	Petugas selalu mengontrol sistem						
45	Q106	Adanya estimasi waktu pengecekan						
46	Q107	Pelaporan keamanan sistem sudah dilaporkan dengan baik dan cepat						

47	Q108	Petugas selalu melaporkan temuan kelemahan sistem				 		
48	Q109	Temuan tersebut segera dilakukan proses perbaikan				 	 	
49	Q110	Adanya dokumentasi perbaikan		 				
50	Q111	Memberikan solusi dengan cepat dan tanggap terhadap sistem yang terkena serangan					 	
51	Q112	Adanya pembaharuan mekanisme sistem keamanan						
52	Q113	Petugas selalu memonitor terhadap penanganan setiap insiden					 	
53	Q114	Apabila terjadi insiden, ada kebijakan dokumentasi untuk insiden tersebut				 		

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

LAMPIRAN H: HASIL EVALUASI AUDIT



Klausul	Kode	Score	Score Maturity
A.5 Kebijakan keamanan			
A.5.1	Q1	4	2.4
	Q2	3	
	Q3	2	
	Q4	1	
	Q5	2	
A.5.2	Q6	4	
	Q7	3	
	Q8	1	
	Q9	3	
	Q10	1	
A.7 Manajemen Aset			
A.7.1	Q11	1	2.6
	Q12	3	
	Q13	4	
	Q14	1	
	Q15	1	
	Q16	4	
	Q17	1	
A.7.2	Q18	5	
	Q19	4	
A.9 Keamanan Fisik dan Lingkungan			
A.9.1	Q20	5	3.4
	Q21	4	
	Q22	1	
	Q23	0	
	Q24	3	

A.9.2	Q25	4	
	Q26	3	
	Q27	4	
	Q28	5	
	Q29	4	
	Q30	4	
A.10.6	Q31	3	3.1
	Q32	4	
	Q33	4	
	Q34	5	
	Q35	4	
	Q36	1	
A.10 Manajemen Komunikasi			
A.11.1	Q37	5	3.1
	Q38	1	
	Q39	3	
	Q40	1	
	Q41	4	
	Q42	4	
	Q43	3	
	Q44	3	
	Q45	4	
A.11 Pengendalian Akses			
A.11.1	Q46	4	3.1
	Q47	4	
	Q48	1	
	Q49	4	

	Q50	4	
	Q51	4	
A.11.2	Q52	5	
	Q53	5	
	Q54	4	
	Q55	4	
	Q56	4	
	Q57	0	
	Q58	3	
	Q59	4	
A.11.3	Q60	4	
	Q61	3	
	Q62	4	
	Q63	3	
	Q64	4	
	Q65	1	
	Q66	3	
	Q67	3	
	Q68	4	
A.11.4	Q69	2	
	Q70	4	
	Q71	3	
	Q72	1	
	Q73	3	
	Q74	3	
A.11.5	Q75	4	
	Q76	3	

	Q77	5	
	Q78	4	
	Q79	4	
	Q80	3	
	Q81	4	
	Q82	1	
	Q83	0	
	Q84	1	
	Q85	1	
	Q86	4	
	Q87	4	
A.12 Pemeliharaan dan Perawatan Sistem			
A.12.2	Q88	3	
	Q89	3	
	Q90	1	
	Q91	3	
	Q92	4	
	Q93	1	
	Q94	1	
	Q95	1	
	Q96	1	
	Q97	1	
A.12.3	Q98	2	1.7
	Q99	1	
	Q100	1	
	Q101	3	

	Q102	3	
A.12.4	Q103	1	
	Q104	1	
	Q105	1	
	Q106	1	
A.13 Manajemen Kejadian Keamanan			
A.13.1	Q107	4	
	Q108	3	
	Q109	4	
A.13.2	Q110	2	
	Q111	4	
	Q112	5	
	Q113	4	
	Q114	3	
Total Maturity			2.6

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

CURRICULUM VITAE

Data Pribadi

Nama : Muhammad Haedar Zhafran Hidayatullah
Tempat Tanggal Lahir : Sleman, 6 Maret 1996
Jenis Kelamin : Laki-laki
Umur : 20 tahun
Tinggi Badan : 167 cm
Berat Badan : 65 kg
Agama : Islam
Alamat : Patuk, Gunungkidul
Status : Lajang
Telepon/WA : 081904104115
Email : mazhaedar@gmail.com

Latar Belakang Pendidikan

SD N 1 Pengkok, Gunungkidul
SMP N 1 Patuk, Gunungkidul
SMA N 1 Banguntapan, Bantul
Teknik Informatika UIN Sunan Kalijaga
Yogyakarta

Pengalaman Organisasi

Panitia Open Suse Asia Summit 2016
Team Lendabook.co Indonesia di Singapura
Panitia Seminar Internet of Things 2016 di
Gunungkidul
FMKP (Forum Mahasiswa Kecamatan Patuk)

Pengalaman Kerja

Software Analyst di Alim Studio
Call Center Indihome PT Telkom Indonesia
Help Desk Verifikasi PT Telkom Indonesia
Verifikator di PrivyID

Prestasi

Juara 1 FCDC Drum Competition Jawa-Bali
Juara 2 GRSD Drum Competition Nasional
Juara 2 Yamaha Campus Competition
Juara 3 Class Mild Band Competition
Best Drummer se Kabupaten Sleman
Best Volunteer di acara Open Suse Asia 2016
Lendabook di acara Foss Asia Singapura

PORTOFOLIO



Muhammad Haedar Zhafran Hidayatullah

mazhaedar@gmail.com | HP/Whatsapp (081904104115) | Sleman, 6 Maret 1996 | Laki-laki | Islam | 20 tahun | Belum Menikah | 167 cm | 65 kg | Yogyakarta, Indonesia

Ringkasan

Selama studi, saya mengikuti beberapa aktivitas diantaranya Open Suse Asia Summit 2016, FOSS Asia di Singapura.

Hingga saat resume ini dibuat, saya telah bekerja antara lain di Alim Studio, PT Telkom Indonesia, dan PrivyID, dan Pusat Informasi Teknologi dan Pangkalan Data (PTIPD). Saya berharap nilai network yang luas dan ketrampilan menejerial yang saya peroleh dari pengalaman kerja dapat membantu saya bekerja dengan optimal di perusahaan.

Kemampuan

Design analyst, software analyst, verifikasi data, call center, musik, dapat bertanggung jawab

Pendidikan

SD N 1 Pengkok, Gunungkidul

SMP N 1 Patuk, Gunungkidul

SMA N 1 Banguntapan, Bantul

Teknik Informatika UIN Sunan Kalijaga Yogyakarta