

**AUDIT MANAJEMEN KEAMANAN INFORMASI DI RUMAH SAKIT  
ISLAM YOGYAKARTA PDHI MENGGUNAKAN  
ISO/IEC 27001:2013**

**SKRIPSI**



Disusun oleh

**Adinda Amaliyah**

**14.11.7831**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**AUDIT MANAJEMEN KEAMANAN INFORMASI DI RUMAH SAKIT  
ISLAM YOGYAKARTA PDHI MENGGUNAKAN  
ISO/IEC 27001:2013**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Sistem Informasi



Disusun oleh

**Adinda Amaliyah**

**14.11.7831**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

# PERSETUJUAN

## SKRIPSI

**AUDIT MANAJEMEN KEAMANAN INFORMASI DI RUMAH SAKIT  
ISLAM YOGYAKARTA PDHI MENGGUNAKAN  
ISO/IEC 27001:2013**


yang dipersiapkan dan disusun oleh

**Adinda Amaliyah**

14.11.7831

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 1 Mei 2017

Dosen Pembimbing,

  
**Sudarmawan, S.T., M.T.**  
NIK. 190302035

# PENGESAHAN

## SKRIPSI

**AUDIT MANAJEMEN KEAMANAN INFORMASI DI RUMAH SAKIT  
ISLAM YOGYAKARTA PDHI MENGGUNAKAN  
ISO/IEC 27001:2013**

yang dipersiapkan dan disusun oleh

**Adinda Amalyah**  
14.11.7831

telah dipertahankan di depan Dewan Penguji  
pada tanggal 25 April 2018

### Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Hastari Utama, M.Cs  
NIK. 190302230

Sri Ngudi Wahyuni, S.T., M.Kom  
NIK. 190302060

Melwin Syafrizal, S.Kom., M.Eng.  
NIK. 190302105



Skrripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 3 Mei 2018



## PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri(ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Instusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 03 Mei 2018



(Azzahra Hanafiyah)

NIM. 14.11.7831

## MOTTO

Menyia-nyiakan waktu lebih buruk dari kematian. Karena kematian memisahkanmu dari dunia sementara menyia-nyiakan waktu memisahkanmu dari Allah.

(Imam bin Al Qayim)

Karunia Allah yang paling lengkap adalah kehidupan yang didasarkan pada ilmu pengetahuan.

(Ali bin Abi Thalib)

Seseorang yang bertindak tanpa ilmu ibarat bepergian tanpa petunjuk. Dan sudah banyak yang tahu kalau orang seperti itu sekiranya akan hancur, bukan selamat.

(Hasan Al Basri)

## PERSEMBAHAN

*Laahawlawalaaquwwataillabillah*, tidak ada daya dan kekuatan kecuali Allah yang Maha Tinggi dan Maha Agung. Puji syukur kehadiran Allah yang Maha Pengasih dan Penyayang. Sholawat semoga tercurah pada junjungan Nabi Muhammad *Shallallahu`alaihi Wa Sallam*. Alhamdulillah dengan kasih sayang dan pertunjuk-Nya, saya dapat menyelesaikan penelitian ini. Terelesaikannya penelitian ini, tidak lepas dari doa dan dukungan banyak pihak. Maka, melalui kesempatan ini, saya mengucapkan terimakasih setulus hati kepada:

1. Bapak Safri Zen Effendi dan Ibu Nurhayati selaku orang tuaku, terimakasih untuk semua kasih sayang dan pengorbananmu. Tidak ada kata yang bisa mewakili betapa besar rasa terimakasihku. Semoga Allah senantiasa melimpahkan kasih sayang, rahmat dan barokah serta kemuliaan hidup dunia dan akhirat. *Love you mom and dad, you always be my hero.*
2. Abang Dayat, Kak Rahma, dan Mbak Tari selaku kakak yang selalu memberikan dukungan dan motivasi kepada adeknya agar tidak menyerah dalam keadaan apapun. Terimakasih untuk semua bantuan dan dukungan yang telah kalian berikan.
3. Dinda Asri Aisyah, *best childhood* karena kami tumbuh dan berjuang bersama. Yang selalu bersedia menemani saya dalam berproses di segala hal.
4. Teman-teman 14-S1TI-04, akan ada yang kita rindukan *guys*.
5. Teman-teman FOSSIL yang memberikan saya banyak pengalaman dalam sebuah organisasi.

Terimakasih yang luar biasa penulis ucapkan untuk kalian.

## KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan penulis. Tidak lupa sholawat serta salam penulis haturkan pada junjungan umat yaitu Nabi besar Muhammad SAW.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa UNIVERSITAS AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komunikasi.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada :

1. Krisnawati, S Si, M.T selaku dekan UNIVERSITAS AMIKOM Yogyakarta.
2. Bapak Sudarmawan,S.T.,M.T selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
3. Semua keluarga besar penulis terutama untuk kedua orang tua yang tidak bosan – bosannya memberikan dukungan, semangat, motivasi dan tentunya doa kepada penulis.
4. Seluruh Staff IT Rumah Sakit Islam Yogyakarta PDHI yang telah bersedia membantu penulis dalam proses penyelesaian skripsi.
5. Teman – teman saya yang telah membantu dan mendukung saat penulis menyusun skripsi ini.
6. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu baik dukungan moriil maupun materiil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penulis tentunya menyadari bahwa pembuatan skripsi ini masih banyak kekurangan dan kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun, penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta 06 Mei 2018

Penulis



## DAFTAR ISI

HALAMAN JUDUL.....	ii
PERSETUJUAN .....	iii
PENGESAHAN .....	iv
PERNYATAAN.....	v
MOTTO .....	vi
PERSEMBAHAN .....	vii
KATA PENGANTAR .....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xii
DAFTAR TABEL.....	xiii
DAFTAR LAMPIRAN.....	xv
INTI SARI.....	xvi
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Maksud dan Tujuan Penelitian .....	3
1.5 Metode penelitian .....	4
1.5.1 Metode Pengumpulan Data .....	4
1.5.2 Metode Analisa.....	4
1.5.3 Metode Perancangan.....	5
1.6 Sistematika Penulisan.....	5
<b>BAB II LANDASAN TEORI .....</b>	<b>7</b>
2.1 Tinjauan Pustaka .....	7
2.2 Keamanan Informasi.....	8
2.3 Alasan Diperlukan Keamanan Informasi .....	12
2.4 Dasar Manajemen Keamanan Informasi .....	14
2.5 Audit.....	15

2.5.1	Tahapan Audit .....	16
2.5.1.1	Scoping and Pre-audit Survey.....	16
2.5.1.2	Planning and Preparation .....	17
2.5.1.3	Fieldwork .....	17
2.5.1.4	Analisis .....	18
2.5.1.5	Reporting .....	18
2.5.1.6	Closure.....	19
2.6	Pengertian Analisa Sistem .....	19
2.7	IEC.....	20
2.8	ISO.....	20
2.8.1	Kegiatan ISO .....	21
2.8.2	Bagaimana ISO Mengembangkan Standar .....	21
2.9	Standar .....	23
2.9.1	Keuntungan Standarisasi Internasional ISO .....	23
2.9.2	Untuk Bisnis .....	23
2.9.3	Untuk Masyarakat .....	24
2.9.4	Untuk Pemerintah .....	24
2.10	Standard ISO 27000 .....	25
2.11	ISO/IEC 27001:2013 .....	29
2.12	Pembobotan .....	31
<b>BAB III METODE PENELITIAN.....</b>		<b>34</b>
3.1	Deskripsi Perusahaan.....	34
3.1.1	Sejarah .....	34
3.1.2	Struktur Organisasi .....	36
3.2	Tahapan Audit .....	36
3.2.1	<i>Scoping and Pre-audit</i> .....	36
3.2.2	<i>Planning and Preparation</i> .....	37
3.2.3	<i>Fieldwork</i> .....	40
3.2.4	<i>Analisis</i> .....	41
3.2.5	Reporting .....	43
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>45</b>

4.1	Scoping and Pre-audit Survey .....	45
4.1.1	Hasil Tujuan, Ruang Lingkup dan Resiko.....	45
4.1.2	Hasil Klausul, Obyektif dan Kontrol.....	46
4.2	Planning and Preparation.....	46
4.2.1	Hasil Pernyataan.....	47
4.2.2	Hasil Penilaian.....	48
4.2.3	Membuat Pertanyaan .....	50
4.3	Fieldwork.....	51
4.3.1	Informasi security policies .....	52
4.3.2	Asset Management.....	53
4.3.3.	Access Control .....	54
4.3.3	Physical and environmental security.....	63
4.3.4	Operations Security.....	70
4.3.5	Communications Security .....	78
4.3.6	Information security incident management.....	79
4.3.7	Information security aspectc of business continuity management .....	82
4.4	Analisis .....	84
4.4.1	Hasil Checklist .....	84
4.4.2	Penyusunan Temuan dan Rekomendasi.....	85
4.4.3	Konfirmasi Temuan dan Rekomendasi .....	86
4.5	Reporting .....	86
<b>BAB V PENUTUP.....</b>		<b>91</b>
5.1	Kesimpulan.....	91
5.2	Saran .....	92
Daftar Pustaka .....		93
LAMPIRAN.....		95

## DAFTAR GAMBAR

Gambar 2.1 <i>People, Process, dan Tecknolog</i> .....	8
Gambar 2.2 <i>Confidentiality, Integrity, dan Availability</i> .....	9
Gambar 2.3 Hubungan Resiko .....	10
Gambar 2.4 <i>Information Security Breaches Survey 2017</i> .....	12
Gambar 2.5 Tahapan Audit.....	14
Gambar 2.6 ISO27K <i>Timeline</i> .....	21
Gambar 2.7 Struktur ISO .....	24
Gambar 3.1 Logo RS Islam Yogyakarta PDHI.....	27
Gambar 3.2 Struktur Organisasi.....	28
Gambar 4.1 <i>File List</i> .....	42
Gambar 4.2 <i>User List</i> .....	44
Gambar 4.3 <i>User Group</i> .....	45
Gambar 4.4 <i>SNMP Settings</i> .....	46
Gambar 4.5 Terminal .....	48
Gambar 4.6 <i>IP Service List</i> .....	49
Gambar 4.7 <i>Fingerprint</i> .....	50
Gambar 4.8 <i>Live Camera</i> .....	51
Gambar 4.9 Kabel LAN .....	53
Gambar 4.10 <i>Package List</i> .....	57
Gambar 4.11 <i>Logging</i> .....	59
Gambar 4.12 <i>SNMP Client</i> .....	60
Gambar 4.13 <i>Neighbor List</i> .....	62

## DAFTAR TABEL

Tabel 2.1 Tingkat Kepentingan dalam Pembobotan pertanyaan .....	26
Tabel 3.1 Kebutuhan Data Audit .....	30
Tabel 3.2 Pernyataan.....	30
Tabel 3.3. Penilaian Resiko.....	31
Tabel 3.4 Pertanyaan.....	31
Tabel 3.5 Tingkat Keamanan Informasi .....	33
Tabel 3.5 Daftar Temuan Audit .....	34
Tabel 4.1 Pernyataan.....	37
Tabel 4.2 Tingkat Kepentingan dalam Penilaian Pertanyaan .....	38
Tabel 4.3 Pembobotan pernyataan Audit keamanan Informasi .....	38
Tabel 4.4 Tabel Pertanyaan.....	40
Tabel 4.5 Kebijakan keamanan informasi.....	41
Tabel 4.6 Klasifikasi informasi.....	43
Tabel 4.7 Pengguna registrasi dan deregistrasi .....	43
Tabel 4.8 Ketersediaan Pengguna.....	44
Tabel 4.9 Pengelolaan hak akses istimewa .....	45
Tabel 4.10 Pengelolaan otentikasi rahasia informasi pengguna .....	46
Tabel 4.11 Pengelolaan otentikasi rahasia informasi pengguna .....	47
Tabel 4.12 Prosedur <i>log-on</i> yang aman.....	48
Tabel 4.13 Sistem manajemen <i>password</i> .....	49
Tabel 4.14 Penggunaan Utilitas Sistem .....	50
Tabel 4.15 Perimeter keamanan fisik sistem.....	51
Tabel 4.16 Kontrol masuk fisik.....	52
Tabel 4.17 Penempatan dan perlindungan peralatan.....	52
Tabel 4.18 Keamanan Kabel .....	53

Tabel 4.19 Pemeliharaan peralatan .....	54
Tabel 4.19 Penghapusan aset .....	54
Tabel 4.20 Pelepasan atau penggunaan kembali peralatan yang aman.....	55
Tabel 4.21 Prosedur operasi terdokumentasi .....	55
Tabel 4.22 Manajemen perubahan .....	56
Tabel 4.23 Manajemen kapasitas .....	57
Tabel 4.24 Informasi <i>backup</i> .....	58
Tabel 4.25 <i>Event logging</i> .....	58
Tabel 4.26 Perlindungan informasi <i>log</i> .....	59
Tabel 4.27 <i>Log</i> operator dan administrator .....	60
Tabel 4.28 Sinkronisasi penunjuk waktu .....	61
Tabel 4.29 Pengelolaan kerentanan teknik.....	61
Tabel 4.30 Kontrol jaringan .....	62
Tabel 4.31 Tanggung jawab dan prosedur .....	63
Tabel 4.32 Pelaporan peristiwa keamanan informasi .....	63
Tabel 4.33 Belajar dari insiden keamanan informasi.....	64
Tabel 4.34 Merencanakan kontinuitas keamanan informasi.....	65
Tabel 4.35 Melaksanakan kontinuitas keamanan informasi .....	65
Tabel 4.36 Memverifikasi, meninjau dan mengevaluasi .....	66
kelangsungan keamanan informasi	
Table 4.37 Tingkat keamanan informasi.....	67
Tabel 4.38 Daftar temuan Audit.....	69

## DAFTAR LAMPIRAN

1.	Pernyataan .....	95
2.	Pertanyaan .....	98
3.	Checklist .....	104
4.	Daftar Temuan Audit .....	109



## INTI SARI

Rumah Sakit Islam Yogyakarta PDHI yaitu sebuah perusahaan yang bergerak di bidang kesehatan dan menggunakan TI sebagai pendukung proses pelayanan berlangsung. Perusahaan ini memiliki sistem informasi kantor yang menghubungkan setiap komputer dengan *server* yang terdapat dilingkungan kantor dan saling terhubung pada setiap departemen. Hal ini tentu saja membutuhkan sebuah standar manajemen keamanan informasi yang optimal karena bila diabaikan akan menyebabkan pelayanan pada perusahaan terganggu. Sehingga perlu dilakukan audit keamanan informasi pada router yang digunakan untuk mengetahui keamanan informasi pada Rumah Sakit Islam Yogyakarta PDHI.

Penelitian dilakukan berdasarkan standar internasional ISO/IEC 27001:2013. Dimana terdapat 14 domain di dalam ISO/IEC 27001:2013. Penelitian ini akan menggunakan 8 domain yang diantaranya *router policy, administrator authentication, router management, configuration management, bussiniss continuity, physical security, log managemnet and incident handling*.

Setelah dilakukan audit di bagian router terdapat tingkat keamanan informasi pada router baru memenuhi 12 *checklist* yang berarti kategori beresiko tinggi, setelah dilakukan audit dan telah memberikan rekomendasi yang sesuai dengan ISO/IEC 27001:2013 setiap tindakan yang ada diharapkan router bisa berada di posisi aman.

**Kata-kunci :** ISO/IEC 27001:2013, Standarisasi, Keamanan, Audit, Informasi.



## **ABSTRACT**

*Islam Hospital Yogyakarta PDHI is a company engaged in the field of health and use IT as a supporter of the process of service takes place. The company has an office information system that connects each computer to a server that is located in an office environment and connected to each department. This of course requires an optimal standard of information security management because if ignored it will cause service to the company disrupted. So it is necessary to do an information security audit on router which is used to know information security at Islam Hospital of PDHI.*

*The research was conducted based on international standard ISO / IEC 27001: 2013. Where there are 14 domains in ISO / IEC 27001: 2013. This research will use 8 domains such as router policy, administrator authentication, router management, configuration management, bussiness continuity, physical security, log managemnet and incident handling.*

*After the audit on the router side there is a level of information security on the new router meet 12 checklist which means high risk category, after the audit and has provided recommendations in accordance with ISO / IEC 27001: 2013 every action is expected router can be in a safe position.*

**Keywords:** *ISO / IEC 27001: 2013, Standardization, Security, Audit, Information*