

**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN
SNI – ISO 27001 PADA SISTEM INFORMASI AKADEMIK
UNIVERSITAS PEMBANGUNAN NASIONAL
“VETERAN” JAKARTA**

Tugas Akhir



Diajukan Oleh

Darma Yanto Putra

1610512074

Kepada

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UPN “VETERAN” JAKARTA

2019



**AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN SNI – ISO
27001 PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS
PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

DISUSUN OLEH:

DARMA YANTO PUTRA

1610512074

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI S1 SISTEM INFORMASI

2020

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar

Nama : Darma Yanto Putra

NIM : 1616512074

Tanggal : 02 Agustus 2020

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan di proses sesuai dengan ketentuan yang berlaku.

Jakarta, 02 Agustus 2020

Yang Menyatakan,



(Darma Yanto Putra)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Darma Yanto Putra

NIM : 1610512074

Fakultas : Ilmu Komputer

Program Studi : Sistem Informasi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

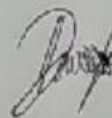
Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional "Veteran" Jakarta

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 02 Agustus 2020

Yang menyatakan,



(Darma Yanto Putra)

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Darma Yanto Putra

NIM : 1610512074

Program Studi : S1 Sistem Informasi

Judul : Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO
27001 Pada Sistem Informasi Akademik Universitas
Pembangunan Nasional “Veteran” Jakarta

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Erly Krisnanik, S.Kom, MM.

Ketua Penguji



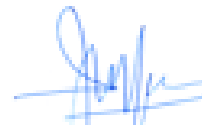
Tri Rahayu, S.Kom., MM.

Anggota Penguji



Theresia Wati, S.Kom., MTI

Pembimbing I



I Wyan Widi Pradnyana, S.Kom., MTI.

Pembimbing II



Dr. Ermatita, M.Kom

Dekan



Ati Zaidiah, S.Kom., MTI

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 23 Juli 2020



ABSTRAK

Darma Yanto Putra – 1610512074, Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional “Veteran Jakarta”. dibawah bimbingan **Theresiawati,S.Kom,MTI** dan **I Wayan Widi P.,S.Kom.,MM**

Terjadinya kerusakan pada aset sistem informasi, tidak memiliki kebijakan tentang keamanan informasi yang memiliki keharusan diterapkan didalam keamanan juga pengawasan aset pelayanan informasi akademik, juga kemungkinan ancaman dan risiko terhadap dukungan sistem informasi. Penelitian ini memiliki tujuan untuk perencanaan Sistem Manajemen Keamanan Informasi (SMKI) dimana penggunaannya sebagai pedoman terhadap kebijakan keamanan informasi di UPT TIK UPN “Veteran” Jakarta. Bahasan dalam penelitian ini adalah analisis Sistem Manajemen Keamanan Informasi (SMKI) dengan ISO/IEC 27001 pada sistem informasi akademik UPT TIK UPN “Veteran” Jakarta. Penelitian ini menggunakan metode *Plan, Do, Check, dan Act* dalam kegiatan mengumpulkan, menganalisis, dan mengolah data. Hasil penelitian ini adalah tingkat kematangan ISO 27001 dengan rata – rata berada di level dua, diharapkan penelitian ini sangat membantu memberikan rekomendasi terhadap kontrol keamanan informasi sebagai pedoman dan prosedur untuk menerapkan kebijakan keamanan informasi.

Kata kunci: ISO 27001, Sistem Manajemen Keamanan Informasi (SMKI), *Plan, Do, Check, Act*

ABSTRACT

Darma Yanto Putra – 1610512074, Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional “Veteran Jakarta”. Under the guidance of **Theresiawati,S.Kom,MTI** and **I Wayan Widi P.,S.Kom.,MM**.

The occurrence of damage to information system assets, do not have information system security policy that must be applied in security also supervision of information academic service assets, the possibility of threat and risk against information system support. This research have a purpose to plan Information Security Management System (ISMS) with its use as guidelines of information system policy in UPT TIK UPN “Veteran” Jakarta. The main discussion in this research is Information Security Management System (ISMS) analysis using

ISO/IEC 27001 to UPT TIK UPN “Veteran” Jakarta Information Academic System. This research using Plan, Do, Check, and Act methods in collecting, analyze, and processing data. The result of this research is maturity level of ISO 27001 with average located in level two, be expected this research would be helpfull to provide a rekomendasi to control information security as guidance and procedure for implementation of information security policy.

Keywords: ISO 27001, Information Security Management System (ISMS), *Plan, Do, Check, Act*

Daftar Isi

BAB I	1
PENDAHULUAN	1
1.1 LATAR BELAKANG	1
1.2 RUMUSAN MASALAH	3
1.3 RUANG LINGKUP.....	3
1.4 TUJUAN PENELITIAN	4
1.5 MANFAAT PENELITIAN	5
1.6 BATASAN MASALAH.....	6
1.7 METODOLOGI PENELITIAN.....	6
1.8 LUARAN YANG DIHARAPKAN.....	7
1.9 SISTEMATIKA PENULISAN	8
BAB II	9
LANDASAN TEORI	9
2.1 KONSEP SISTEM INFORMASI.....	9
2.2 SMKI.....	10
2.2.1 KEAMANAN INFORMASI.....	10
2.2.2 SMKI	13
2.2.4.1 IDENTIFIKASI ASET.....	17
2.2.4.2 IDENTIFIKASI ANCAMAN	17
2.2.4.3 IDENTIFIKASI KELEMAHAN	18
2.2.4.4 MENENTUKAN KEMUNGKINAN ANCAMAN	19
2.2.4.5 ANALISA DAMPAK (IMPACT ANALISIS).....	19
2.2.4.6 MENENTUKAN NILAI RISIKO	20
2.3 MANAJEMEN ASET	21
2.3.1 ASET	21
2.3.1 PENGERTIAN MANAJEMEN ASET	21
2.4 KEAMANAN FISIK DAN LINGKUNGAN	22
2.4.1 KONTROL ADMINISTRATIF	23
2.5 ISO/IEC 27000 SERIES	24
2.6 THE CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT).....	28
2.7 ISO/IEC 27001	29
2.7.1 KLAUSUL ISO/IEC 27001	30
2.8 PLAN – DO – CHECK – ACT (PDCA)	32
2.8.1 PLAN.....	32
2.8.2 DO	33
2.8.3 CHECK.....	39
2.8.4 ACT	39
2.9 ANALISIS SMKI.....	40
2.10 KEGIATAN AUDIT.....	40
2.11 AUDIT BERBASIS RISIKO	41
2.12 SERTIFIKASI	41

2.13	PENELITIAN TERDAHULU	42
2.14	SYSTEM, SECURITY, ENGINEERING, CAPABILITY, MATURITY, MODEL (SSE – CMM)	44
2.14.1	RUANG LINGKUP SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL (SSE – CMM)	44
2.14.2	TINGKATAN KAPABILITAS SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL (SSE – CMM)	44
2.15	METODE PERHITUNGAN	46
2.16	PENGUMPULAN DATA	47
BAB III	49
METODE PENELITIAN	49
3.1	TAHAP PLAN.....	49
3.1.1	OBSERVASI	49
3.1.2	WAWANCARA.....	49
3.1.3	KUESIONER.....	49
TABEL 20 DAFTAR KUESIONER	54
3.1.4	MENENTUKAN RUANG LINGKUP.....	56
3.1.5	MENENTUKAN KEBIJAKAN	57
3.2	TAHAP DO	57
3.3	TAHAP CHECK.....	57
3.4	TAHAP ACT	58
3.5	TAHAP PENELITIAN.....	59
BAB IV	60
HASIL DAN PEMBAHASAN	60
4.1	KONSEP PDCA.....	60
4.2	TAHAP PLAN	60
4.2.1	MENGIDENTIFIKASI PROSES BISNIS	60
4.2.1.1	GAMBARAN, UMUM, INSTANSI, DAN, ORGANISASI	60
4.2.1.1.1	UPN “VETERAN” JAKARTA.....	60
4.2.1.1.1.1	VISI DAN MISI UPN “VETERAN” JAKARTA	61
4.2.1.1.2.1	VISI	61
4.2.1.1.2.2	MISI	61
4.2.1.1.2.3	UNIT PELAKSANA TEKNIK (UPT) TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) UPN “VETERAN” JAKARTA	61
4.2.1.1.2.3	STRUKTUR ORGANISASI UPT TIK UPN “VETERAN” JAKARTA.....	62
4.2.1.1.2.4	RUANG LINGKUP KEAMANAN INFORMASI	62
4.2.2	MENENTUKAN KEBIJAKAN KEAMANAN INFORMASI	62
4.2.3	AUDITEE SISTEM INFORMASI AKADEMIK	64
4.2.4	INDIKATOR PENGUKURAN KEAMANAN INFORMASI.....	64
4.2.5	HUKUM KEAMANAN INFORMASI	65
4.3	TAHAP DO.....	65
4.3.1	DAFTAR KEBIJAKAN YANG SUDAH DIBUAT DAN DIRESMIKAN.....	65
4.3.2	MELAKSANAKAN AUDIT	66
4.3.2.1	MANAJEMEN ASET	66
4.3.2.2	PERALATAN	67
4.3.2.3	PROSEDUR DAN TANGGUNG JAWAB OPERASIONAL	68
4.3.2.4	KENDALI PERANGKAT LUNAK OPERASIONAL.....	68
4.4	TAHAP CHECK.....	70

4.3.1 PEMILIHAN OBJEKTIF KONTROL DAN KONTROL KEAMANAN INFORMASI	70
4.4.2 PEMILIHAN SEBAGIAN KLAUSUL DARI ISO/IEC 27001:2013	70
4.4.3 PENENTUAN ANALISIS SSE – CMM	71
4.4.4 PENENTUAN NILAI TINGKAT KEMAMPUAN UNTUK SYSTEM SECURITY ENGINEERING	71
CAPABILITY MATURITY MODEL (SSE – CMM)	71
4.5 TAHAP ACT	85
4.5.1 REKOMENDASI OBYEKTIF KONTROL DAN KEAMANAN INFORMASI BERDASARKAN METODE SSE - CMM ISO/IEC 27001:2013	86
4.6 KESIMPULAN DAN PEMBAHASAN	103
BAB V	106
PENUTUP	106
5.1 KESIMPULAN	107
5.2 SARAN	109

Gambar 2.1 Kehilangan Kerahasiaan Data	25
Gambar 2-1 Kehilangan Keutuhan Data	25
Gambar 2-2 Komponen Keamanan Informasi (Tipton & Krause, 2016)	27
Gambar 2-3 PDCA Model (ISO/IEC 27001, 2005).....	28
Gambar 2.5 CIA (netsec.id)	37
Gambar 2.6 Plan, do, check, act (asq.org)	49
Gambar 3-1 Tahapan Penelitian.....	76
Gambar 4-1 Tahapan Penelitian.....	79
Gambar 4.2 Maturity Level Klausul A.5	90
Gambar 4.3 Maturity Level Klausul A.8	93
Gambar 4.4 Maturity Level Klausul A.10	94
Gambar 4.5 Maturity Level Klausul A.11	98
Gambar 4.6 Maturity Level Keseluruhan	100
Gambar 4.7 Maturity Level Keseluruhan	100

Daftar Tabel

TABEL 1 PENILAIAN RISIKO	17
TABEL 2 IDENTIFIKASI ANCAMAN	18
TABEL 3 IDENTIFIKASI KELEMAHAN	19
TABEL 4 ANALISA DAMPAK.....	20
TABEL 5 ANCAMAN BERDASARKAN CIA.....	22
TABEL 6 SERI ISO 27000	28
TABEL 7 IDENTIFIKASI ASET.....	33
TABEL 8 PENILAIAN <i>CONFIDENTIALITY</i>	33
TABEL 9 PENILAIAN <i>INTEGRITY</i>	34
TABEL 10 PENILAIAN <i>AVAILABILITY</i>	34
TABEL 11 ANCAMAN.....	35
TABEL 12 PROBABILITY OF OCCURENCE.....	37
TABEL 13 BIA	38
TABEL 14 LEVEL PROBABILITAS ANCAMAN	38
TABEL 15 LEVEL DAMPAK BISNIS	39
TABEL 16 JENIS STANDAR SERTIFIKASI	42
TABEL 17 PENELITIAN TERDAHULU	43
TABEL 18 TINGKAT KEMAMPUAN	47
TABEL 19 WAWANCARA	49
TABEL 20 DAFTAR KUESIONER	54
TABEL 21 PEMILIHAN KLAUSUL.....	56
TABEL 22 TINGKAT KEMAMPUAN	58
TABEL 23 AUDITEE SISTEM INFORMASI	64
TABEL 24 PENERIMA KUESIONER SSE - CMM	64
TABEL 25 DAFTAR KEBIJAKAN POB	65
TABEL 26 DAFTAR KEBIJAKAN SOP.....	66
TABEL 27 AUDIT MANAJEMEN ASET	67
TABEL 28 AUDIT PERALATAN	67
TABEL 29 AUDIT PROSEDUR DAN TANGGUNG JAWAB OPERASIONAL	68
TABEL 30 AUDIT KENDALI PERANGKAT LUNAK OPERASIONAL.....	69
TABEL 31 PEMILIHAN KLAUSUL.....	71

TABEL 32 PENENTUAN AUDIT	71
TABEL 33 TINGKAT KEMAMPUAN KLAUSUL 5	73
TABEL 34 MATURITY LEVEL KLAUSUL 5	73
TABEL 35 TINGKAT KEMAMPUAN KLAUSUL 8	75
TABEL 36 MATURITY LEVEL KLAUSUL 8	75
TABEL 37 TINGKAT KEMAMPUAN KLAUSUL 10	77
TABEL 38 MATURITY LEVEL KLAUSUL 10	77
TABEL 39 TINGKAT KEMAMPUAN KLAUSUL 11	80
TABEL 40 MATURTY LEVEL KLAUSUL 11	81
TABEL 41 TABEL KESELURUHAN MATURITY LEVEL	83
TABEL 42 TINGKAT KEMATANGAN KLAUSUL	85
TABEL 43 A.5 KEBIJAKAN KEAMANAN INFORMASI	87
TABEL 44 A.8 MANAJEMEN ASET	88
TABEL 45 A.8 MANAJEMEN ASET	89
TABEL 46 A.8 MANAJEMEN ASET	89
TABEL 47 A.8 MANAJEMEN ASET	90
TABEL 48 A.10 KRIPTOGRAFI.....	91
TABEL 49 A.10 KRIPTOGRAFI.....	92
TABEL 50 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	93
TABEL 51 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	94
TABEL 52 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	95
TABEL 53 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	96
TABEL 54 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	98
TABEL 55 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	98
TABEL 56 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	99
TABEL 57 A.11 KEAMANAN FISIK DAN LINGKUNGAN.....	101
TABEL 58 REKOMENDASI ASET	102