

ABSTRAK

Analisis dilakukan pada Sistem Tenaga Kerja Kontrak PT. Pos Indonesia, bertujuan untuk mengetahui apakah Kebijakan Keamanan Informasi, Organisasi Keamanan Informasi, Pengelolaan Aset, dan Keamanan Sumber Daya Manusia sudah diterapkan dengan baik dan sesuai dengan ISO 27001:2005. Teori yang digunakan dalam pembahasan adalah ISO 27001:2005 dan teori GAP Analisis ISO 27001:2005. Metode yang digunakan berdasarkan proses pada ISO 27001:2005 yaitu persiapan dokumen, memberikan kuesioner *awareness*, memberikan kuesioner *compliant*, menentukan *action required*, memberikan komentar, dan memberikan rekomendasi perbaikan dokumen. Teknik penelitian dilakukan dengan memberikan kuesioner dan melakukan wawancara secara langsung kepada pihak PT. Pos Indonesia. Hasil analisis adalah berupa kesesuaian proses saat ini dengan proses di dalam ISO 27001:2005, rekomendasi pengendalian proses agar sesuai dengan proses yang diambil dalam kegiatan analisis yaitu Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset, dan Keamanan Sumber Daya Manusia, serta referensi penulisan dokumen ISO 27001:2005 yaitu *Policy*, *Procedure*, *Work Instruction*, dan *record Schedule*.

Kata Kunci: ISO 27001:2005, GAP Analisis, Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset, Keamanan Sumber Daya Manusia

ABSTRACT

Analysis was performed on Contracted Employee system at PT. Pos Indonesia, Aiming at determining if the Information Security Policy , Organization of Information Security , Asset Management , Human Resources and Security had been implemented properly and in accordance with ISO 27001:2005. Theories applied for the study were ISO 27001:2005 and ISO 27001:2005 GAP Analysis theory. The Implemented method was based on the ISO 27001:2005's process; document preparation, delivering awareness questionnaire, delivering compliant questionnaire, determining action required , giving comment, and providing document improvement recommendation. Study methods were conducted by questionnaire delivering and directly conducted interviews to the party of PT. Pos Indonesia. The outcomes of the analysis were, compatibility process between ISO 27001:2005 with current process and process controlling recommendations to match the process studied in analysis activities; Security Policy, Information Security Organization , Asset Management , and Human Resources Security , as well as ISO 27001:2005 document writing reference; Policy , Procedure , Work Instruction , and Schedule record .

Keywords: ISO 27001:2005, GAP Analysis, Security Policy, Organization of Information Security, Asset Management, Human Resource Security

DAFTAR ISI

PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	i
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA	iv
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xiii
DAFTAR SINGKATAN	xv
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup Kajian	2
1.5 Sumber Data	3
1.6 Sistematika Penyajian	4
BAB 2. KAJIAN TEORI	5
2.1 Pengertian Sistem, Informasi, dan Manajemen	5
2.2 Manajemen Keamanan Informasi	7
2.3 Standar Sistem Manajemen Keamanan Informasi	9
2.3.1 ISO/IEC 27000:2009 – <i>ISMS Overview and Vocabulary</i>	9
2.3.2 SNI ISO/IEC 27001 – Persyaratan Sistem Manajemen Keamanan Informasi	10
2.3.3 ISO/IEC 27005 – <i>Information Security Risk Management</i>	12
2.3.4 ISO/IEC 27006 – <i>Requirements for Bodies Providing Audit and Certification of Information Security Management Systems</i>	12
2.4 Dokumentasi Sistem Manajemen Keamanan Informasi	12
2.5 Detail Struktur Dokumen Kontrol Keamanan ISO 27001	14
2.6 GAP Analisis	23

2.7	Perhitungan Skala Likert.....	28
2.7.1	Penentuan Skor Jawaban	28
2.7.2	Skor Ideal.....	29
2.7.3	<i>Rating Scale</i>	29
2.7.4	Persentase Persetujuan	30
BAB 3.	ANALISIS DAN EVALUASI.....	31
3.1	Profil Perusahaan.....	31
3.2	Visi dan Misi	32
3.2.1	Visi	32
3.2.2	Misi.....	32
3.3	Struktur Organisasi	32
3.4	Fungsi dan Tujuan Aplikasi TKK.....	33
3.5	Tahapan Dalam Menganalisis SMKI.....	34
3.5.1	Dokumen yang dibutuhkan dalam SMKI	35
3.5.2	Analisis Kuesioner <i>Awareness</i>	36
3.5.3	Analisis Kuesioner <i>Compliant</i>	37
3.5.4	Analisis <i>Action Required</i>	39
3.5.5	Analisis Proses ISO 27001:2005 pada PT. Pos Indonesia	41
3.5.6	Evaluasi Hasil Analisis.....	72
3.5.7	Rekomendasi Pengendalian Proses	75
BAB 4.	SIMPULAN DAN SARAN.....	79
4.1	Simpulan	79
4.2	Saran.....	80
DAFTAR PUSTAKA.....		83

DAFTAR GAMBAR

Gambar 2.1 Hubungan Antar Standar SMKI	9
Gambar 2.2 Struktur Dokumentasi SMKI	12
Gambar 2.3 Contoh <i>GAP</i> Analisis	27
Gambar 2.4 <i>Rating Scale</i>	29
Gambar 2.5 Rumus Persentase	30
Gambar 3.1 Struktur Organisasi PT. Pos Indonesia	33

DAFTAR TABEL

Tabel 2.1 Peta PDCA dalam SMKI.....	10
Tabel 2.2 Detail Dokumentasi ISO 27001	14
Tabel 2.3 Skala Jawaban	28
Tabel 2.4 Rumus Skor Ideal	29
Tabel 2.5 Ketentuan Skala	30
Tabel 3.1 Kesimpulan Kuesioner <i>Awareness</i>	37
Tabel 3.2 Kesimpulan Kuesioner <i>Compliant</i>	37
Tabel 3.3 Kesimpulan Kuesioner <i>Action Required</i>	39
Tabel 3.4 Dokumentasi Kebijakan Keamanan Informasi	42
Tabel 3.5 Kajian Kebijakan Keamanan Informasi	43
Tabel 3.6 Komitmen Manajemen Terhadap Keamanan Informasi	45
Tabel 3.7 Koordinasi Keamanan Informasi	46
Tabel 3.8 Alokasi Tanggung Jawab Keamanan Informasi.....	47
Tabel 3.9 Proses Otorisasi Untuk Fasilitas Pengolahan Informasi	48
Tabel 3.10 Perjanjian Kerahasiaan	49
Tabel 3.11 Kontak Dengan Pihak Berwenang	50
Tabel 3.12 Kontak Dengan Kelompok Khusus.....	51
Tabel 3.13 Kajian Independen Terhadap Keamanan Informasi	52
Tabel 3.14 Identifikasi Resiko Terkait Pihak Eksternal	53
Tabel 3.15 Penekanan Keamanan Ketika Berhubungan Dengan Pelanggan.....	55
Tabel 3.16 Penekanan Keamanan Perjanjian.....	56
Tabel 3.17 Inventaris Aset.....	57
Tabel 3.18 Kepemilikan Aset.....	58
Tabel 3.19 Penggunaan Aset Yang Dapat Diterima	59
Tabel 3.20 Pedoman Klasifikasi	60
Tabel 3.21 Pelabelan dan Penanganan Informasi	61
Tabel 3.22 Peran dan Tanggung Jawab	62
Tabel 3.23 Penyaringan (<i>Screening</i>).....	64
Tabel 3.24 Syarat dan Aturan Kepegawaian.....	65
Tabel 3.25 Tanggung Jawab Manajemen	66

Tabel 3.26 Kepeduliaan, Pendidikan, dan Pelatihan Keamanan Informasi..	67
Tabel 3.27 Prosedur Pendisiplinan.....	68
Tabel 3.28 Tanggung Jawab Pengakhiran Pekerjaan	69
Tabel 3.29 Pengembalian Aset	70
Tabel 3.30 Penghapusan Hak Akses	71

DAFTAR LAMPIRAN

LAMPIRAN A.	SISTEM MANAJEMEN KEAMANAN INFORMASI	87
LAMPIRAN B.	TATA CARA PENANGANAN <i>PASSWORD</i>	104
LAMPIRAN C.	PENGENDALIAN HAK AKSES	107
LAMPIRAN D.	PENERAPAN <i>CLEAN DESK</i> DAN <i>CLEAR SCREEN</i>	115
LAMPIRAN E.	STRUKTUR ORGANISASI	117
LAMPIRAN F.	PERJANJIAN KERAHASIAAN	127
LAMPIRAN G.	<i>MINUTES OF MEETING (MOM) DETAILING SALESFORCE</i>	133
LAMPIRAN H.	PELATIHAN PENYUSUNAN KEBIJAKAN DAN <i>STRATEGY CYBER SECURITY NATIONAL</i>	138
LAMPIRAN I.	PROSEDUR, KLASIFIKASI, <i>BACKUP</i> , PELABELAN, DAN PENGHAPUSAN DATA ELEKTRONIK	144
LAMPIRAN J.	SK PENGANGKATAN DAN PEMBEBASAN JABATAN ..	148
LAMPIRAN K.	JUKLAK SIM ASET	151
LAMPIRAN L.	KUESIONER <i>AWARENESS</i>	176
LAMPIRAN M.	KUESIONER <i>COMPLIANT</i>	180
LAMPIRAN N.	ISIAN KUESIONER <i>AWARENESS</i>	187
LAMPIRAN O.	ISIAN KUESIONER <i>COMPLIANT</i>	190
LAMPIRAN P.	<i>PROFILE</i> RESPONDEN	250
LAMPIRAN Q.	KESIMPULAN KUESIONER ACTION REQUIRED	253
LAMPIRAN R.	REKAPAN ISIAN KUESIONER <i>COMPLIANT</i>	255
LAMPIRAN S.	WAWANCARA	261
LAMPIRAN T.	HASIL WAWANCARA	267
LAMPIRAN U.	PENULISAN DOKUMEN <i>POLICY</i>	277
LAMPIRAN V.	REFERENSI PENULISAN DOKUMEN <i>PROCEDURE</i>	282
LAMPIRAN W.	REKOMENDASI PENULISAN DOKUMEN <i>WORK INSTRUCTION</i>	312
LAMPIRAN X.	REFERENSI PENULISAN DOKUMEN <i>RECORD SCHEDULE</i>	322

LAMPIRAN Y. BAGAN DOKUMENTASI ISO27001 ISMS.....	327
--	-----

DAFTAR SINGKATAN

CIA	: <i>Confidentially, Integrity, Availability</i>
Datakom	: Data Komunikasi
EISP	: <i>Enterprise Information Security Policy</i>
ISO	: <i>International Organization For Standarization</i>
ISMS	: <i>Information Security Management System</i>
ISSP	: <i>Issue-Spesific Security</i>
Juklak	: Petunjuk Pelaksana
MOM	: <i>Minutes Of Meeting</i>
PN	: Perusahaan Negara
PT	: Perseroan Terbatas
PTT	: <i>Post, Telegraph, and Telephone</i>
PKS	: Perjanjian Kerjasama
PHL	: Pekerja Harian Lepas
PDCA	: <i>Plan, Do, Check, Act</i>
PKWT	: Perjanjian Kerja Untuk Waktu Tertentu
Prantek	: Perencana Teknologi
QY	: <i>Quality Yes</i>
SK	: Surat Keputusan
SIM	: Sistem Informasi Manajemen
SNI	: Standar Nasional Indonesia
SPJ	: Surat Pertanggungjawaban
SSP	: <i>System-Spesific Policy</i>
SMKI	: Sistem Manajemen Keamanan Informasi
TI	: Teknologi Informasi
TIK	: Teknologi Informasi dan Komunikasi
TKK	: Tenaga Kerja Kontrak
TKPP	: Tenaga Kerja Kontrak <i>Professional</i> Perusahaan