

ABSTRAK

Analisis dilakukan pada Sistem *Remittance* di PT.Pos Indonesia, bertujuan untuk mengetahui apakah keamanan fisik dan lingkungan, manajemen komunikasi dan operasi serta pengendalian akses sudah diterapkan dan sesuai dengan ISO 27001:2005. Teori yang digunakan dalam analisis ini adalah ISO 27001:2005 dan teori GAP analisis. 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, melakukan wawancara serta melakukan observasi 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 keamanan fisik dan lingkungan, manajemen komunikasi dan operasi dan pengendalian akses, serta referensi penulisan dokumen ISO 27001:2005 yaitu *Policy*, *Procedure*, *Work Instruction*, dan *record Schedule*.

Kata Kunci : ISO27001:2005, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengendalian akses, PT.Pos Indonesia.

ABSTRACT

This analysis have done on remittance system at PT.Pos Indonesia have purpose to recognize whether physical and environment, communication management and operational, also access control have already applied and suitable enough with ISO 27001:2005. The method in this analysis is not only with ISO 27001:2005 but also with GAP analysis theory. The method that have used ISO 27001:2005 which are including the preparation document, give awareness questionnaire this compliant questionnaire and give document correction recommendation. This research method have done with several methods : questionnaire, interview and also with direct observation with PT.Pos Indonesia. the result of this analysis is the form of current suitability process with the procedure in ISO 27001:2005, moreover the recommendation process control to suitable with the process that already taken from the analysis research activity specifically in physical and environment security, communication management and operation, afterward access control, including the reference from the document writing in ISO 27001:2005 which are includes policy, procedure, work instruction and recorded schedule.

Keywords: Access control, communication management and operational, ISO 27001:2005, physical and environment security, PT.Pos Indonesia.

DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xiv
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	3
1.5 Sumber Data	3
1.6 Sistematika Penyajian	3
BAB 2. KAJIAN TEORI	5
2.1 Definisi Sistem	5
2.2 Definisi Informasi	5
2.3 Definisi Sistem Informasi	5
2.4 Definisi Audit	6
2.4.1 Jenis-Jenis Audit	6
2.4.2 Instrument Audit	7
2.5 Keamanan Informasi	7
2.6 Manajemen Keamanan Informasi	9
2.7 Standar Sistem Manajemen Keamanan Informasi	11
2.8 SNI ISO/IEC 27001-Persyaratan Sistem Manajemen Keamanan Informasi	12

2.9	Detail Struktur Dokumen Kontrol Keamanan ISO 27001	13
2.10	Gap Analisis	40
2.11	Perhitungan Skala Likert.....	55
2.11.1	Penentuan Skor Jawaban	55
2.11.2	Skor Ideal	55
2.11.3	<i>Rating Scale</i>	56
2.11.4	Persentase Persetujuan	57
BAB 3.	ANALISIS DAN EVALUASI.....	58
3.1	Sejarah PT Pos Indonesia	58
3.2	Visi dan Misi PT Pos Indonesia	59
3.3	Struktur organisasi	59
3.4	Fungsi dan Tujuan Aplikasi <i>Remittance</i>	60
3.5	Tahapan Dalam Menganalisis SMKl.....	60
3.5.1	Dokumen yang dibutuhkan dalam SMKl	61
3.5.2	Analisis Kuesioner <i>Awareness</i>	64
3.5.3	Analisis kuesioner <i>compliant</i>	64
3.5.4	Analisis <i>action required</i>	67
3.5.5	Analisis proses ISO 27001:2005 pada PT.Pos Indonesia	70
3.5.6	Evaluasi hasil analisis	129
3.5.7	Rekomendasi pengendalian proses	130
BAB 4.	SIMPULAN DAN SARAN.....	140
4.1	Simpulan	140
4.2	Saran.....	141
DAFTAR PUSTAKA.....		145

DAFTAR GAMBAR

Gambar 2.1 <i>Rating Scale</i>	56
Gambar 2.2 Rumus Persentase	57
Gambar 3.1 Struktur Organisasi.....	60

DAFTAR TABEL

Tabel 2.1 Detail dokumentasi ISO 27001.....	13
Tabel 2.2 Contoh <i>GAP</i> Analisis	40
Tabel 2.3 Skala Jawaban	55
Tabel 2.4 Rumus Skor Ideal	56
Tabel 2.5 Ketentuan Skala	56
Tabel 3.1 Kesimpulan Kuesioner <i>Awareness</i>	64
Tabel 3.2 Kesimpulan kuesioner <i>compliant</i>	65
Tabel 3.3 <i>Profile</i> responden	67
Tabel 3.4 Perhitungan kuesioner <i>action required</i>	68
Tabel 3.5 Batasan Parameter keamanan fisik	71
Tabel 3.6 Pengendalian entri yang bersifat fisik.....	72
Tabel 3.7 Pengamanan kantor, ruangan dan fasilitas.....	73
Tabel 3.8 Perlindungan terhadap ancaman dari luar dan lingkungan	74
Tabel 3.9 Bekerja di area yang aman.....	75
Tabel 3.10 Area akses <i>public</i> dan bongkar muat.....	76
Tabel 3.11 Penempatan dan perlindungan peralatan	77
Tabel 3.12 Sarana pendukung	78
Tabel 3.13 Keamanan kabel.....	79
Tabel 3.14 Pemeliharaan peralatan	80
Tabel 3.15 Keamanan peralatan di luar lokasi	81
Tabel 3.16 Pembuangan dan penggunaan kembali peralatan secara aman	82
Tabel 3.17 Pemindahan Barang.....	83
Tabel 3.18 Dokumentasi prosedur operasional.....	84
Tabel 3.19 Manajemen perubahan.....	84
Tabel 3.20 Pemisahan tugas.....	85
Tabel 3.21 Pemisahan fasilitas pengembangan, pengujian dan operasional	86
Tabel 3.22 Pelayanan jasa	87
Tabel 3.23 Pemantauan dan pengkajian pihak ketiga	88
Tabel 3.24 Perubahan pengelolaan terhadap jasa ketiga.....	89
Tabel 3.25 Manajemen kapasitas.....	89

Tabel 3.26 Keberterimaan sistem.....	90
Tabel 3.27 Pengendalian terhadap <i>malicious code</i>	91
Tabel 3.28 Pengendalian terhadap <i>mobile code</i>	92
Tabel 3.29 <i>Back-Up</i> indormasi	93
Tabel 3.30 Pengendalian jaringan.....	94
Tabel 3.31 Keamanan layanan jaringan.....	95
Tabel 3.32 Manajemen media yang dapat dipindahkan	95
Tabel 3.33 Pemusnahan media.....	96
Tabel 3.34 Prosedur penanganan informasi	97
Tabel 3.35 Keamanan dokumentasi sistem	98
Tabel 3.36 kebijakan dan prosedur pertukaran informasi	99
Tabel 3.37 Perjanjian pertukaran	100
Tabel 3.38 Media fisik dalam transit.....	101
Tabel 3.39 Pesan <i>electronic</i>	101
Tabel 3.40 Sistem informasi bisnis.....	102
Tabel 3.41 <i>Electronic commerce</i>	103
Tabel 3.42 Transaksi <i>online</i>	104
Tabel 3.43 informasi yang tersedia untuk umum	105
Tabel 3.44 <i>Log audit</i>	106
Tabel 3.45 Pemantauan penggunaan sistem.....	106
Tabel 3.46 Perlindungan informasi <i>log</i>	107
Tabel 3.47 <i>Log</i> administrator dan operator	108
Tabel 3.48 <i>Log</i> atas kesalahan yang terjadi.....	108
Tabel 3.49 Sinkronisasi penunjuk waktu	109
Tabel 3.50 Kebijakan pengendalian akses.....	110
Tabel 3.51 Pendaftaran pengguna	111
Tabel 3.52 Manajemen hak akses.....	111
Tabel 3.53 Manajemen <i>password</i> pengguna	112
Tabel 3.54 Tinjauan hak akses pengguna	113
Tabel 3.55 Penggunaan <i>password</i>	114
Tabel 3.56 Peralatan yang ditinggal oleh penggunanya	115
Tabel 3.57 Kebijakan <i>clear desk and clear screen</i>	116

Tabel 3.58 Kebijakan penggunaan layanan jaringan	116
Tabel 3.59 Otentikasi pengguna untuk koneksi <i>eksternal</i>	117
Tabel 3.60 Identifikasi peralatan dalam jaringan.....	118
Tabel 3.61 Perlindungan terhadap <i>remote diagnostic</i> dan <i>configuration port</i>	119
Tabel 3.62 Segregasi dalam jaringan.....	119
Tabel 3.63 Pengendalian koneksi jaringan	120
Tabel 3.64 Pengendalian <i>routing</i> jaringan.....	121
Tabel 3.65 Prosedur <i>log on</i> yang aman	122
Tabel 3.66 identifikasi dan otentikasi pengguna	123
Tabel 3.67 Sistem manajemen <i>password</i>	123
Tabel 3.68 Pengguna sistem <i>utilities</i>	124
Tabel 3.69 Sesi <i>time out</i>	125
Tabel 3.70 Pembatasan waktu koneksi.....	126
Tabel 3.71 Pembatasan akses informasi	126
Tabel 3.72 Isolasi sistem yang <i>sensitive</i>	127
Tabel 3.73 <i>Mobile computing</i> dan komunikasi	128
Tabel 3.74 Kerja jarak jauh.....	129

DAFTAR LAMPIRAN

LAMPIRAN A. Standarisasi pengujian untuk jaminan perangkat lunak.....	146
LAMPIRAN B. Pengendalian hak akses	148
LAMPIRAN C. Struktur organisasi.....	156
LAMPIRAN D. Tentang <i>Back-up</i> , pelabelan dan penghapusan	157
LAMPIRAN E. Tentang penggunaan sumber data	161
LAMPIRAN F. Penanggulangan dampak bencana terhadap infrastruktur data center di PT.Pos Indonesia	167
LAMPIRAN G. Tata cara penanganan <i>password</i>	172
LAMPIRAN H. Penerapan sistem keamanan informasi.....	175
LAMPIRAN I. Juklak Sistem Pos <i>Remittance</i>	192
LAMPIRAN J. Juknis IEMO 290312	246
LAMPIRAN K. Pengembangan sistem	256
LAMPIRAN L. Organisasi dan tata kerja	263
LAMPIRAN M. Bagan Dokumentasi ISO27001 ISMS	269
LAMPIRAN N. Hasil wawancara	270
LAMPIRAN O. Kuesioner <i>Awareness</i>	283
LAMPIRAN P. Kuesioner <i>Compliant</i>	289
LAMPIRAN Q. Rekapian isian kuesioner <i>Compliant</i>	298
LAMPIRAN R. Dokumentasi Foto	307
LAMPIRAN S. <i>Clear desk and clear screen</i>	318
LAMPIRAN T. Penulisan <i>Document Policy</i>	320
LAMPIRAN U. Referensi Penulisan <i>Document Procedure</i>	323
LAMPIRAN V. Rekomendasi Penulisan <i>Document WORK INSTRUCTION</i>	333
LAMPIRAN W. Referensi Penulisan <i>Document Record Schedule</i>	340
LAMPIRAN X Rekapian Kuesioner <i>Awareness</i>	343

DAFTAR SINGKATAN

CIA	<i>Confidentially, Integrity, Availability</i>
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
PDCA	<i>Plan, Do, Check, Act</i>
PKS	Perjanjian Kerjasama
Prantek	Perencana Teknologi
PT	Perseroan Terbatas
SIM	Sistem Informasi Manajemen
SMKI	Sistem Manajemen Keamanan Informasi
SNI	Standar Nasional Indonesia
SSP	<i>System-Spesific Policy</i>
TI	Teknologi Informasi