

ABSTRAK

Analisis dilakukan pada Sistem Tenaga Kerja Kontrak PT.Ultra Jaya, 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 Ultra Jaya. 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-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.Ultra Jaya, 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.Ultra Jaya. 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

LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	iii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iv
PRAKATA	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xiii
DAFTAR SINGKATAN	xiv
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	4
1.6 Sistematika Penyajian	5
BAB 2. KAJIAN TEORI	6
2.1 Keamanan Informasi	6
2.2 Dasar Manajemen Keamanan Informasi	7
2.2.1 Informasi Sebagai Aset	8
2.2.2 Aspek Lain Keamanan Informasi	8
2.2.3 Informasi Pelu Dilindungi Keamanannya	9
2.2.4 Manajemen	10
2.2.5 Manajemen Keamanan Informasi	11
2.3 Information Security Management System	13
2.4 Pengertian ISO 27001	15
2.4.1 ISO/IEC 2700:2009 – ISMS <i>Overview and Vocabulary</i>	17
2.4.2 SNI ISO/IEC 27001 – Persyaratan Sistem Manajemen Keamanan Informasi	17
2.4.3 ISO/IEC 27005 – <i>Information Security Risk Management</i>	20
2.4.4 ISO/IEC 27006 – <i>Requirements for Bodies Providing Audit and Certification of Information Security Management Systems</i>	20

2.5	Dokumentasi Sistem Manajemen Keamanan Informasi	20
2.6	Detail Struktur Dokumen control Keamanan ISO 27001	22
2.7	GAP Analisis.....	31
2.8	Perhitungan Skala Likert.....	38
2.8.1	Penentuan Skor Jawaban	38
2.8.2	Skor Ideal	39
2.8.3	<i>Rating Scale</i>	39
2.8.4	Persentase Persetujuan	40
BAB 3.	ANALISIS DAN RANCANGAN SISTEM.....	41
3.1	Profile Perusahaan	41
3.2	Visi Dan Misi	42
3.3	Struktur Organisasi.....	42
3.4	Tahapan Dalam Menganalisis SMKI.....	43
3.4.1	Dokumen yang dibutuhkan dalam SMKI	44
3.4.2	Analisis Kuesioner <i>Awareness</i>	45
3.4.3	Analisis Kuesioner <i>Compliant</i>	46
3.4.4	Analisis <i>Action Required</i>	48
3.4.5	Analisis Proses ISO 27001:2005 pada Divisi Teknologi Informasi PT. Ultra Jaya	50
3.4.6	Evaluasi Hasil Analisis.....	78
3.4.7	Rekomendasi Pengendalian Proses	80
BAB 4.	HASIL PENELITIAN	85
4.1	Simpulan.....	85
4.2	Saran	86
DAFTAR PUSTAKA	89

DAFTAR GAMBAR

Gambar 2.1 Elemen-elemen keamanan informasi.....	7
Gambar 2.2 ISO 27000 ISMS	15
Gambar 2.3. hubungan Antar Standar SMKI	17
Gambar 2.4 Struktur Dokumentasi SMKI.....	20
Gambar 2.5 Contoh <i>GAP</i> Analisis.....	36
Gambar 2.6 <i>Rating Scale</i>	39
Gambar 2.7 Rumus Persentase.....	40
Gambar 3.1 Struktur Organisasi PT Ultra Jaya.....	42

DAFTAR TABEL

Tabel 2.1 Peta PDCA dalam SMKI	18
Tabel 2.2 Detail Dokumentasi ISO 27001	22
Tabel 2.3 Skala Jawaban.....	38
Tabel 2.4 Rumus Skor Ideal.....	39
Tabel 2.5 Ketentuan Skala	40
Tabel 3.1 Kesimpulan Kuesioner <i>Awareness</i>	46
Tabel 3.2 Kesimpulan Kuesioner <i>Compliant</i>	46
Tabel 3.3 Kesimpulan Kuesioner <i>Action Required</i>	48
Tabel 3.4 Dokumentasi Kebijakan Keamanan Informasi.....	54
Tabel 3.5 Kajian Kebijakan Keamanan Informasi	55
Tabel 3.6 Komitmen Manajemen Terhadap Keamanan Informasi	56
Tabel 3.7 Koordinasi Keamanan Informasi	57
Tabel 3.8 Alokasi Tanggung Jawab Keamanan Informasi	58
Tabel 3.9 Proses Otorisasi Untuk Fasilitas Pengolahan Informasi.....	58
Tabel 3.10 Perjanjian Kerahasiaan	59
Tabel 3.11 Kontak Dengan Pihak Berwenang	60
Tabel 3.12 Kontak Dengan Kelompok Khusus.....	61
Tabel 3.13 Kajian Independen Terhadap Keamanan Informasi	62
Tabel 3.14 Identifikasi Resiko Terkait Pihak Eksternal.....	63
Tabel 3.15 Penekanan Keamanan Ketika Berhubungan Dengan Pelanggan	64
Tabel 3.16 Penekanan Keamanan Perjanjian	65
Tabel 3.17 Inventaris Aset	66
Tabel 3.18 Kepemilikan Aset	66
Tabel 3.19 Penggunaan Aset Yang Dapat Diterima	67
Tabel 3.20 Pedoman Klasifikasi	68
Tabel 3.21 Pelabelan dan Penanganan Informasi	69
Tabel 3.22 Peran dan Tanggung Jawab	70
Tabel 3.23 Penyaringan (<i>Screening</i>).....	71
Tabel 3.24 Syarat dan Aturan Kepegawaian.....	72
Tabel 3.25 Tanggung Jawab Manajemen	73
Tabel 3.26 Kepeduliaan, Pendidikan, dan Pelatihan Keamanan Informasi...74	
Tabel 3.27 Prosedur Pendisiplinan	75
Tabel 3.28 Tanggung Jawab Pengakhiran Pekerjaan	75
Tabel 3.29 Pengembalian Aset	76

Tabel 3.30 Penghapusan Hak Akses77

DAFTAR LAMPIRAN

LAMPIRAN A.	kebijakan informasi	93
LAMPIRAN B.	inventaris aset.....	152
LAMPIRAN C.	kepedulian, pendidikan dan pelatihan keamanan informasi	153
LAMPIRAN D.	pelabelan dan penanganan informasi.....	154
LAMPIRAN E.	penggunaan aset yang dapat diterima.....	155
LAMPIRAN F.	penyaringan (<i>Screening</i>).....	156
LAMPIRAN G.	tanggung jawab terhadap aset.....	157
LAMPIRAN H.	prosedur pendisiplinan.....	159
LAMPIRAN I.	Pihak eksternal	164
LAMPIRAN J.	Hak akses	166
LAMPIRAN K.	penekanan keamanan ketika berhubungan dengan pelanggan 168	
LAMPIRAN L.	Proses Otorisasi Untuk Fasilitas pengolahan informasi	169
LAMPIRAN M.	koordinasi keamanan informasi.....	171
LAMPIRAN N.	alokasi tanggung jawab keamanan informasi	172
LAMPIRAN O.	kuesioner <i>awarness</i>	173
LAMPIRAN P.	kuesioner <i>compliant</i>	177
LAMPIRAN Q.	isian kuesioner <i>awareness</i>	184
LAMPIRAN R.	isian kuesioner <i>compliant</i>	188
LAMPIRAN S.	lampiran Koresponden.....	236
LAMPIRAN T.	kesimpulan kuesioner <i>action required</i>	239
LAMPIRAN U.	rekapan isian kuesioner <i>compliant</i>	241
LAMPIRAN V.	wawancara.....	246
LAMPIRAN W.	hasil wawancara.....	252
LAMPIRAN X.	penulisan Dokumen <i>Policy</i>	261
LAMPIRAN Y.	referensi penulisan dokumen <i>procedure</i>	269
LAMPIRAN Z.	rekomendasi penulisan dokumen <i>work instruction</i>	299
LAMPIRAN AA.	referensi penulisan dokumen <i>record schedule</i>	309
LAMPIRAN BB.	bagan dokumentasi ISO27001 ISMS.....	314

DAFTAR SINGKATAN

CIA	: <i>Confidentially, Integrity, Availability</i>
EISP	: <i>Enterprise Information Security Policy</i>
ISO	: <i>International Organization For Standardization</i>
ISMS	: <i>Information Security Management System</i>
ISSP	: <i>Issue-Specific Security</i>
PT	: Perseroan Terbatas
PDCA	: <i>Plan, Do, Check, Act</i>
QY	: <i>Quality Yes</i>
SK	: Surat Keputusan
SIM	: Sistem Informasi Manajemen
SNI	: Standar Nasional Indonesia
SPJ	: Surat Pertanggungjawaban
SSP	: <i>System-Specific Policy</i>
SMKI	: Sistem Manajemen Keamanan Informasi
TI	: Teknologi Informasi
UHT	: <i>Ultra High Temperature</i>
TIK	: Teknologi Informasi dan Komunikasi