

ABSTRAK

Analisis Keamanan Sistem Informasi merupakan hal yang penting bagi sebuah perusahaan, terutama bagi perusahaan yang memiliki sistem berskala besar dan memiliki hubungan dengan pihak luar, dimana keamanan lingkungan serta manajemen operasi dan pengendalian akses pada data dan informasi menjadi susah untuk dipantau. Pemahaman ini dapat digunakan untuk melakukan penilaian terhadap proses – proses yang dilakukan perusahaan dalam melakukan pengamanan data dan informasi. Masalah yang dibahas adalah mengenai analisis keamanan informasi pada unit IT yang berada di PT.KAI daerah operasi Bandung. Teori yang digunakan adalah standar berdasarkan ISO 27001 klausul keamanan fisik dan lingkungan, manajemen komunikasi operasi dan pengendalian akses. Sumber data yang didapat merupakan hasil dari wawancara yang dilakukan dengan orang yang memiliki wewenang dan melakukan observasi langsung ke PT.KAI daerah operasi Bandung. Metode penelitian yang dilakukan dengan cara melakukan pemahaman tentang ISO 27001 dan melakukan teknik penelitian dengan tinjauan langsung dan wawancara.

Kata kunci : ISO, Keamanan, SMKI

ABSTRACT

Analysis of the security of information systems is crucial for a company, especially for companies that have large-scale systems and have relationships with outside parties, where the security environment as well as the management of operations and control of access to data and information being difficult to monitor. This understanding can be used to do an assessment of the processes that made the company the security of data and information. The problem being discussed is about information security analysis on the unit IT was in PT.KAI area of operations. The theory is based on the ISO 27001 standard physical security and environmental clauses, manajemen communications operations and access control. Source data obtained as the result of interviews conducted with people who have the authority and perform direct observation of PT.KAI area of operations. Methods of research done by an understanding of ISO 27001 and do research techniques with direct review and interviews.

Keywords : ISO, Security, ISMS

DAFTAR ISI

ABSTRAK.....	i
<i>ABSTRACT</i>	ii
DAFTAR ISI.....	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	vi
DAFTAR LAMPIRAN	viii
DAFTAR SINGKATAN.....	ix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	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	3
BAB II KAJIAN TEORI	5
2.1 Analisis Sistem	5
2.2 Proses Bisnis.....	5
2.3 Manajemen.....	6
2.4 Keamanan Sistem Informasi.....	7
2.4 Manajemen Keamanan Informasi	10
2.4.1 Planning.....	10
2.4.2 Programs	12
2.4.3 Policy	12
2.4.4 People	13
2.4.5 Protection	13
2.4.6 Project Management.....	13
2.8 Standar Sistem Manajemen Keamanan Informasi	14
2.9 Information Security Management System	14
2.10 ISO 27000	16

2.11	<i>ISO/IEC 27000:2009 – ISMS Overview and Vocabulary</i>	17
2.11.1	SNI <i>ISO/IEC 27001</i> - Persyaratan Sistem Manajemen Keamanan Informasi.	18
2.11.2	<i>ISO/IEC 27005 – Information Security Risk Management</i>	21
2.11.3	<i>ISO/IEC 27006 – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems</i>	21
2.12	Dokumentasi Sistem Manajemen Keamanan Informasi	21
2.13	Detail Struktur Dokumen Kontrol Keamanan <i>ISO 27001</i>	23
2.14	<i>Gap Analysis</i>	38
BAB III ANALISIS DAN EVALUASI		43
3.1	Latar Belakang Perusahaan	43
3.2	Visi dan Misi	44
3.3	Struktur Organisasi	44
3.4	Tujuan dan Fungsi Unit TI pada Perusahaan.....	46
3.5	Tahapan Dalam Menganalisis SMKI	47
3.5.1	Persiapan Dokumen	48
3.5.2	Analisis Kuesioner <i>Awareness</i>	52
3.5.3	Analisis Kuesioner <i>Compliant</i>	52
3.5.4	Analisis Kuesioner <i>Required</i>	55
3.5.5	Pemberian Komentar	57
BAB IV SIMPULAN DAN SARAN		102
4.1	Simpulan	102
4.2	Saran dan Rekomendasi	102
DAFTAR PUSTAKA.....		113
RIWAYAT HIDUP PENULIS		260

DAFTAR GAMBAR

Gambar 1 Elemen-elemen keamanan informasi	8
Gambar 2 Hubungan antar standar SMKI	18
Gambar 3 Struktur dokumentasi SMKI	22
Gambar 4 Gap Analysis & Audit Tools	41
Gambar 5 Struktur organisasi PT.KAI	45
Gambar 6 Struktur Organisasi Unit Sistem Informasi	46
Gambar 8 Dokumentasi ISO27001 ISMS	49

DAFTAR TABEL

Tabel I PDCA MODEL	19
Tabel II Detail dokumentasi ISO 27001.....	23
Tabel III Kuisisioner Awareness	52
Tabel IV Kuisisioner Compliant.....	52
Tabel V Kuisisioner Required	55
Tabel VI Perimeter keamanan fisik	57
Tabel VII Pengendalian entri yang bersifat fisik	58
Tabel VIII Mengamankan kantor, ruangan dan fasilitas.....	58
Tabel IX Perlindungan terhadap ancaman eksternal dan lingkungan.....	59
Tabel X Bekerja di area yang aman	60
Tabel XI Area akses publik dan bongkar muat	60
Tabel XII Penempatan dan perlindungan peralatan	61
Tabel XIII Sarana Pendukung	61
Tabel XIV Keamanan Kabel.....	62
Tabel XV Pemeliharaan Peralatan	62
Tabel XVI Keamanan peralatan di luar lokasi	63
Tabel XVII Pembuangan atau penggunaan kembali peralatan secara aman	63
Tabel XVIII Pemindahan barang	64
Tabel XIX Prosedur operasi terdokumentasi.....	65
Tabel XX Manajemen perubahan	65
Tabel XXI Pemisahan Tugas	66
Tabel XXII Pemisahan fasilitas pengembangan, pengujian dan operasional.....	66
Tabel XXIII Pelayanan Jasa.....	67
Tabel XXIV Pemantauan dan Pengkajian Data.....	67
Tabel XXV Pengelolaan Perubahan Terhadap Jasa Pihak Ketiga	68
Tabel XXVI Manajemen Kapasitas	68
Tabel XXVII Keberterimaan Sistem	69
Tabel XXVIII Perlindungan Terhadap <i>Malicious Code</i>	69
Tabel XXIX Perlindungan Terhadap <i>Mobile Code</i>	70
Tabel XXX <i>Back-Up</i> Informasi	71
Tabel XXXI Pengendalian Jaringan	71
Tabel XXXII Keamanan Layanan Jaringan	72
Tabel XXXIII Manajemen Media yang dapat Dipindahkan	72
Tabel XXXIV Pemusnahan Media.....	73
Tabel XXXV Prosedur Penanganan Informasi	73
Tabel XXXVI Keamanan Dokumentasi Sistem.....	74
Tabel XXXVII Kebijakan dan Prosedur Pertukaran Informasi.....	74

Tabel XXXVIII Perjanjian Pertukaran	75
Tabel XXXIX Pesan Elektronik.....	75
Tabel XL Sistem Informasi Bisnis	75
Tabel XLI <i>Electronic Commerce</i>	76
Tabel XLII Transaksi <i>Online</i>	76
Tabel XLIII Informasi yang Tersedia untuk umum	77
Tabel XLIV Log Audit.....	77
Tabel XLV Pemantauan Penggunaan Sistem.....	78
Tabel XLVI Perlindungan Informasi Log.....	78
Tabel XLVII Log Administrator dan Operator	79
Tabel XLVIII Log atas Kesalahan yang Terjadi	79
Tabel XLIX Sinkronisasi Penunjuk Waktu	80
Tabel L Kebijakan Pengendalian Akses.....	80
Tabel LI Pendaftaran Pengguna	81
Tabel LII Manajemen Hak Khusus	81
Tabel LIII Manajemen Password Pengguna.....	82
Tabel LIV Tinjauan Terhadap Hak Akses.....	82
Tabel LV Penggunaan Password.....	83
Tabel LVI Peralatan yang ditinggalkan oleh Pengguna.....	83
Tabel LVII Kebijakan Clear desk and screen	84
Tabel LVIII Kebijakan Penggunaan Layanan	84
Tabel LIX Otentikasi Pengguna untuk Koneksi Eksternal.....	85
Tabel LX Identifikasi Peralatan dalam Jaringan	85
Tabel LXI Perlindungan terhadap remote diagnostic dan configuration port.....	86
Tabel LXII Segregasi dalam Jaringan	86
Tabel LXIII Pengendalian Koneksi Jaringan.....	86
Tabel LXIV Pengendalian routing jaringan.....	87
Tabel LXV Prosedur Log-on yang aman	87
Tabel LXVI Identifikasi dan otentifikasi pengguna	88
Tabel LXVII Sistem manajemen password.....	88
Tabel LXVIII Pengguna sistem utilities	89
Tabel LXIX Sesi time out	89
Tabel LXX Pembatasan waktu koneksi.....	90
Tabel LXXI Pembatasan akses informasi	90
Tabel LXXII Isolasi sistem yang sensitif	91
Tabel LXXIII Mobile computing dan komunikasi.....	91
Tabel LXXIV Kerja jarak jauh	92

DAFTAR LAMPIRAN

LAMPIRAN A KUESIONER <i>COMPLIANT</i>	117
LAMPIRAN B KUESIONER AWARENESS	118
LAMPIRAN C DOKUMEN POLICY ISO 27001	121
LAMPIRAN D PROSEDUR ISO 27001	123
LAMPIRAN E WORKLIST ISO 27001	183
LAMPIRAN E SCHEDULE OF AUDIT LOG REQUIREMENT	208
LAMPIRAN F RECORD ISO 27001	228
LAMPIRAN G HAK AKSES	238
LAMPIRAN H AKSES PINTU.....	239
LAMPIRAN I KERJA SAMA PIHAK KETIGA.....	240
LAMPIRAN J TATA KELOLA TI	241
LAMPIRAN K WAWANCARA.....	245

DAFTAR SINGKATAN

Singkatan Istilah	Arti Istilah
<i>Doc</i>	Dokumen
PT.KAI	PT.Kereta Api Indonesia (Persero)
SMKI	Sistem Manajemen Keamanan Informasi
TI	Teknologi informasi
TIK	Teknologi Informasi Komunikasi