Abstrak

Informasi merupakan salah satu aset yang sangat penting untuk PT.KAI. Dengan perkembangan teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan terhadap keamanan informasi semakin meningkat. Untuk itu, PT.KAI harus dapat menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki. Laporan ini membahas tentang analisis pengendalian manajemen keamanan informasi berbasis ISO/IEC 27001:2005. Hasil analisis yang didapat di antaranya adalah masalah pemahaman proses-proses dalam mengelola dokumentasi kebijakan informasi sudah dapat dijelaskan dengan baik, serta dapat memastikan kesesuaian, kecakupan, dan keefektifan secara berkelanjutan. Pemahaman dalam mengelola keamanan informasi di dalam ataupun di luar organisasi sudah ada, tetapi penerapan pada pihak internal perusahaan masih kurang baik. Unit TI pada PT.KAI sudah memahami tentang pentingnya pemeliharaan aset serta perlindungan terhadap aset. Aset sudah diidentifikasi dengan baik, hanya saja metode yang kurang baik menyebabkan aset masih ada yang tidak *valid*. Unit TI pada PT.KAI sudah memahami pengelolaan sumber daya manusia sebelum dipekerjakan, selama bekerja, ataupun yang sudah diberhentikan serta perubahan pekerjaan.

Kata Kunci : GAP Analisis, SMKI, ISO 27001:2005, Teknologi Informasi

Abstract

Information is one of the most important assets for PT.KAI. With the development of information technology very rapidly, the possibility of disruption to information security is increasing. For that PT.KAI should be able to apply appropriate policies to protect information assets owned. One of the policies that can be taken by the company to overcome the interference problem is to implement information security Information Security Management Systems (ISMS) ISO 27001:2005 on. This report discusses the Information Security Management Control Analysis Based on Policy, Organization, assets and human resources PT.KAI Unit Based on ISO / IEC 27001:2005, which includes some of the processes in the ISO include Security Policy, Organization of Information Security, Asset Management and Security Human Resources. Understanding of the processes in managing policy documentation can be explained by the information already good, and can ensure compliance, reach and effectiveness on an ongoing basis. Understanding in managing information security inside and outside the organization already exists, but the application of the internal party companies are still not good. IT units PT.KAI already aware of the importance of asset preservation and protection of assets. Assets already identified by either method just is not good cause there asset invalid. IT units PT.KAI already understand how human resource management, pre-employment, for work or who are laid off or change jobs.

Keyword : GAP Analysis, ISMS, ISO 27001:2005, Information Technology

Daftar Isi

Prakata i
Abstrak ii
Abstract iii
Daftar Isi iv
Daftar Gambar vii
Daftar Tabel viii
Daftar Lampiran x
Daftar Singkatan xi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 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 4
BAB II KAJIAN TEORI 6
2.1 Definisi Analisis Sistem 6
2.2 Kebijakan dan Strategi 9
2.3 Proses dan Manajemen Keamanan 9
2.4 Standar Keamanan Informasi 14
2.5 Tata Kelola Keamanan Informasi 14
2.6 Sistem Manajemen Keamanan Informasi (SMKI) 15

2.6.1 ISO/IEC 27000 *ISMS- Overview and Vocabulary* 16

2.6.2 SNI ISO/IEC 27001- Persyaratan Sistem Manajemen Keamanan Informasi 17

2.6.3 ISO/IEC 27002 – *Code of Practice for ISMS* 20

2.6.4 ISO/IEC 27003- *Information Security Management System Implementation Guidance* 24

2.6.5 ISO/IEC 27004 - *Information Security Management Measurement* 24

2.6.6 ISO/IEC27005 - *Information Security Risk Management* 25

2.6.7 ISO/IEC 27006 - *Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.* 25

2.7 Dokumentasi Sistem Manajemen Keamanan Informasi 25

2.8 Manfaat dan Kendala Implementasi ISO 27001:2005:2005 27

2.9 Standar Pengelolaan Keamanan Informasi Sesuai ISO 27001:2005 dan ISO 27002:2005 29

2.10 Sasaran Pengendalian dan Pengendalian 31

2.11 GAP Analisis 37

BAB III ANALISIS 41

3.1 Lingkungan Bisnis Serta Visi dan Misi Perusahaan 41

3.2 Unit TI pada PT.KAI 41

3.3 Strategi Penerapan TI pada PT.KAI 43

3.4 Tujuan Pengembangan Sistem dan TI 45

3.5 Tahapan Dalam Menganalisis SMKI 45

3.5.1 Dokumen yang dibutuhkan dalam SMKI 46

3.5.2 Analisis Kuesioner *Awareness* 49

3.5.3 Analisis Kuesioner *Compliant* 50

3.5.4 Analisis *Action Required* 51

3.6 Analisis Proses ISO 27001:2005 pada PT.KAI 53
3.6.1 Analisis Kebijakan Kemanan 54
3.6.2 Analisis Organisasi Keamanan Informasi (Pihak Internal) 56
3.6.3 Analisis Organisasi Keamanan Informasi (Pihak Eksternal) 64
3.6.4 Analisis Tanggung Jawab Terhadap Aset..... 67
3.6.5 Analisis Klasifikasi Informasi..... 70
3.6.6 Analisis Keamanan Sumber Daya Manusia (Sebelum Dipekerjakan)..... 72
3.6.7 Analisis Keamanan Sumber Daya Manusia (Selama Bekerja)..... 75
3.6.8 Analisis Sumber Daya Manusia Saat Pengakhiran atau Perubahan Pekerjaan..... 78
3.7 Evaluasi Hasil Analisis..... 81
3.8 Rekomendasi Pengendalian Proses..... 84
BAB IV SIMPULAN DAN SARAN 88
4.1 Simpulan 88
4.2 Saran..... 89
DAFTAR PUSTAKA..... 92
DAFTAR LAMPIRAN 97
RIWAYAT HIDUP PENULIS 232

Daftar Gambar

Gambar 1 Hubungan Antar Standar SMKI 17
Gambar 2 Struktur Dokumentasi SMKI 26
Gambar 3 Contoh GAP Analisis 39
Gambar 4 Struktur Organisasi Pusat Sistem informasi..... 42
Gambar 5 Proses Pengembangan Sistem dan TI 44
Gambar 6 Bagan Dokumentasi ISO27001 ISMS 47

Daftar Tabel

Tabel I Istilah Dan Definisi Dokumen 7
Tabel II Komponen Resiko 10
Tabel III Peta PDCA Dalam SMKI 18
Tabel IV Sasaran Pengendalian Dan Pengendalian 31
Tabel V Dokumentasi ISO 27001:2005 Lanjutan 36
Tabel VI Kesimpulan Kuesioner *Awareness* 49
Tabel VII Kesimpulan Kuesioner *Compliant* 50
Tabel VIII Kesimpulan Kuesioner *Action Required* 52
Tabel IX Dokumentasi Kebijakan Keamanan Informasi 55
Tabel X Kajian Kebijakan Keamanan Informasi 56
Tabel XI Komitmen Manajemen Terhadap Keamanan Informasi 57
Tabel XII Koordinasi Keamanan Informasi 58
Tabel XIII Alokasi Tanggung Jawab Keamanan Informasi 59
Tabel XIV Proses Otorisasi Untuk Fasilitas Pengolahan Informasi 60
Tabel XV Perjanjian Kerahasiaan 61
Tabel XVI Kontak Dengan Pihak Berwenang 62
Tabel XVII Kontak Dengan Kelompok Khusus (*Special Interest*) 63
Tabel XVIII Kajian Independen Terhadap Keamanan Informasi 64
Tabel XIX Identifikasi Resiko Terkait Pihak Ekstenal 65
Tabel XX Penekanan Keamanan Ketika Berhubungan Dengan Pelanggan. 66
Tabel XXI Penekanan Keamanan Perjanjian 67
Tabel XXII Inventaris Aset 68
Tabel XXIII Kepemilikan Aset 69
Tabel XXIV Penggunaan Aset Yang Dapat Diterima 70
Tabel XXV Pedoman Klasifikasi 71
Tabel XXVI Pelabelan Dan Penanganan Informasi 72
Tabel XXVII Peran Dan Tanggung Jawab 73
Tabel XXVIII Penyaringan (*Screening*) 74
Tabel XXIX Syarat Dan Aturan Kepegawaian 75
Tabel XXX Tanggung Jawab Manajemen 76

Tabel XXXI Kepedulian, Pendidikan Dan Pelatihan Keamanan Informasi....77
Tabel XXXII Prosedur Pendisiplinan 78
Tabel XXXIII Tanggung Jawab Pengakhiran Pekerjaan.....79
Tabel XXXIV Pengembalian Aset 80
Tabel XXXV Penghapusan Hak Akses 81

Daftar Lampiran

Lampiran A Kebijakan Keamanan Informasi..... 97

Lampiran B Kebijakan dan Prosedur Teknologi Informasi..... 100

Lampiran C Hak Akses..... 104

Lampiran D Kebijakan Umum Tata Kelola Teknologi Informasi 105

Lampiran E Data Aset 112

Lampiran F Monitoring Server dan Aset 113

Lampiran G Aset Aplikasi..... 114

Lampiran H Konsultasi Sertifikasi ISO 27001:2005 120

Lampiran I Surat Perjanjian Kerja Sama..... 122

Lampiran J Surat Pengesahan Perjanjian..... 123

Lampiran K Perubahan dan Tambahan Organisasi dan Tata Laksana Unit Sistem Informasi..... 124

Lampiran L Struktur Organisasi Pusat Sistem Informasi..... 128

Lampiran M Kedudukan, Tugas Pokok, Tanggung Jawab dan Tata Laksana Unit Sistem Informasi..... 133

Lampiran N Surat Perubahan Perjanjian..... 162

Lampiran O Wawancara..... 166

Lampiran P Kuesioner Awareness..... 173

Lampiran Q Kuesioner *Compiant*..... 175

Lampiran R Referensi Penulisan dokumen *Policy*..... 181

Lampiran S Referensi Penulisan Dokumen *Procedure*..... 186

Lampiran T Rekomendasi Penulisan Dokumen *Work Instruction*..... 216

Lampiran U Referensi Penulisan *Dokumen Schedule* 226

Daftar Singkatan

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