PERANCANGAN KEAMANAN INFORMASI BERDASARKAN PENILAIAN RISIKO KEAMANAN INFORMASI DI PT. MULTI TERMINAL INDONESIA

KARYA AKHIR
Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Teknologi Informasi

AAN AL BONE
0706308004

UNIVERSITAS INDONESIA
PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDONESIA
JAKARTA
JUNI 2009

PERANCANGAN KEAMANAN INFORMASI BERDASARKAN PENILAIAN RISIKO KEAMANAN INFORMASI DI PT. MULTI TERMINAL INDONESIA

KARYA AKHIR

AAN AL BONE
0706308004

UNIVERSITAS INDONESIA
PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDONESIA
JAKARTA
JUNI 2009

HALAMAN PERNYATAAN ORISINALITAS

Karya Akhir ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	**:** AAN ALBONE
NPM	**:** 0706308004
Tanda tangan	:
Tanggal	: 29 Juni 2009

HALAMAN PENGESAHAN

Karya Akhir diajukan oleh

Nama **:** AAN ALBONE

NPM **:** 0706308004

Program Studi : Magister Teknologi Informasi

Judul Karya Akhir : Perancangan Keamanan Informasi berdasarkan Penilaian Risiko Keamanan di PT. Multi Terminal Indonesia.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Teknologi Informasi pada Program Studi Magister Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Budi Yuwono, PhD ( )

Penguji : Dana Indra Sensuse, Ph.D ( )

Penguji : Dr. Ahmad Nizar Hidayanto ( )

Ditetapkan di :

Tanggal :

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah,inayah serta berkahnya maka penelitian dan laporan penelitian yang berjudul, Perancangan Keamanan Informasi berdasarkan Penilaian Risiko Keamanan Informasi di PT. Multi Terminal Indonesia, dapat diselesaikan.

Adapun penelitian dan laporan penelitian ini dilaksanakan dan disusun sebagai syarat untuk mendapatkan gelar Magister Teknologi Informasi di Universitas Indonesia. Kendala, masalah dan tantangan yang dihadapi penulis dapat dilalui berkat dukungan, bimbingan dan motivasi dari berbagai pihak, dan oleh karena itu penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada

1. Bapak Budi Yuwono, PhD. selaku dosen pembimbing, yang telah bersedia menyediakan waktu dan pikirannya untuk memberi bimbingan, arahan dan saran selama penelitian dan proses penyusunan laporan penelitian.
2. Bapak Dr. Ahmad Nizar Hidayanto selaku Ketua Program Magister Teknologi Informasi.
3. Bapak Suwondo Widjatmoko S.Kom, selaku Manager Sistem Informasi & Pengadaan di PT. Multi Terminal Indonesia.
4. Bapak Dahlan. S.Kom Supervisor Teknologi Informasi di PT Multi Terminal Indonesia.

Akhirul kalam, penulis menyadari bahwa penelitian ini masih jauh dari sempurna oleh karena itu penulis dengan senang hati menerima kritikan dan saran yang membangun untuk penyempurnaan penelitian ini. Semoga apa yang telah dilakukan dan ditulis dalam laporan ini dapat bermanfaat. Terima kasih.

Jakarta, 29 Juni 2009

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Undonesia, saya yang bertandatangan dibawah ini:

Nama : AAN AL BONE
NPM : 0706308004
Program Studi : Magister Teknologi Informasi
Departemen :
Fakultas : Fakultas Ilmu Komputer
Jenis Karya : Karya Akhir

Demi pengembangan ilmi pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Nonekslusif (*Non-exclusive Royalty Right*) atas karya ilmiah saya yang berjudul:

Perancangan Keamanan Informasi berdasarkan
Penilaian Risiko Keamanan Informasi di PT. Multi Terminal Indonesia.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-ekskutif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database). Merawat, dan mempublikasikan karya akhir saya tanpa meminta izin dari saya selama tetap mencantumkan saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di :
Pada tanggal :

Yang menyatakan

(Aan AlBone)

ABSTRACT

Name **:** AAN ALBONE

Study Program : Masters in Information Technology

Title : Designing Information Security based on Information Security Risk Assessment in PT. Multi Terminal Indonesia.

Awareness of the importance of security controls to protect company assets, which include data and information, has been increasing. Media more open at this time, and the freedom to speak, causing interference security information. Companies still have a perception that, by using the advanced technology of information security, the security of certain information obtained. While the organization and personnel are factors that determine the achievement of information security. Development of information security controls in the PT. Multi Terminal Indonesia (PT.MTI) is still based on the needs and budget, without any risk assessment first, and selection strategies mitigate risks, so security has not been built to protect information effectively and efficiently.

Based on the problems, the design must be based on the information security risk assessment. Information security risk assessment is the beginning of the process of risk management, which needs to be done to find out potential threats and risks. And proposed strategies to mitigate risks, as important recommendations for the design of a comprehensive information security, based on risk assessment.

Risk assessment will be followed by risk mitigation, which provides a comprehensive evaluation of security and control strategies should be implemented by PT. MTI, in order to achieve the goals and objectives of information security.

Key word: Risk assessment, Risk mitigation, Enterpise Information Security Planning.
x + 231 peges; 26 figures, 64 table.

ABSTRAK

Nama **:** AAN ALBONE

Program Studi : Magister Teknologi Informasi

Judul : Perancangan Keamanan Informasi berdasarkan Penilaian Risiko Keamanan Informasi di PT. Multi Terminal Indonesia.

Kesadaran pentingnya kontrol keamanan dalam melindungi aset perusahaan, yang berupa data dan informasi, telah semakin meningkat. Media yang bersifat terbuka saat ini dan kebebasan orang berbicara, menyebabkan kekhawatiran terganggunya kerahasiaan informasi. Perusahaan masih memiliki persepsi bahwa, dengan menggunakan teknologi canggih keamanan informasi, maka keamanan informasi pasti diperoleh. Padahal faktor organisasi dan personil adalah faktor yang sangat menentukan tercapainya keamanan informasi. Pembangunan kontrol keamanan informasi di PT. Multi Terminal Indonesia (PT.MTI), yang bergerak dalam bidang logistik, masih berdasarkan anggaran dan kebutuhan sementara, tanpa ada penilaian risiko terlebih dahulu, dan pemilihan strategi meredakan risiko, sehingga kontrol keamanan informasi yang dibangun belum dapat melindungi informasi secara efektif dan efisien.

Dengan permasalahan tersebut perlu dilakukannya perancangan keamanan berdasarkan hasil penilaian risiko. Penilaian risiko keamanan informasi (*information security risk assesment*) merupakan awal dari proses pengelolaan risiko (*risk management*), yang perlu dilakukan untuk mengetahui potensi ancaman dan risiko. Selanjutnya akan diusulkan strategi untuk meredakan risiko (*risk mitigation*), sebagai rekomendasi penting bagi perancangan keamanan informasi yang komprehensif, berdasarkan penilaian risiko.

Dengan melakukan penilaian risiko (*risk assessment*), dan dilanjutkan mitigasi risiko (*risk mitigation*), akan dapat melakukan perancangan keamanan informasi yang komprehensif tentang strategi dan kontrol keamanan apa yang harus diimplementasikan oleh perusahaan, untuk mencapai tujuan dan sasaran keamanan informasi.

Kata Kunci: Penilaian risiko, *Risk mitigation, Enterpise Information Security Planning.*
x + 231 halaman; 26 gambar, 64 tabel.

DAFTAR ISI

Halaman

HALAMAN PERNYATAAN ORISINALITAS..... i
HALAMAN PENGESAHAN..... ii
KATA PENGANTAR..... ii
HALAMAN PERNYATAAAN PERSETUJUAN PUBLIKASI..... iv
ABSTRACT..... iii
ABSTRAK..... iv
DAFTAR ISI..... v
DAFTAR GAMBAR..... xii
DAFTAR TABEL..... xiii
DAFTAR LAMPIRAN..... xv

BAB 1 PENDAHULUAN.....1
1.1 Latar Belakang..... 1
1.2 Perumusan Masalah..... 4
1.3 Pertanyaan Penelitian..... 5
1.4 Ruang Lingkup Penelitian 5
1.5 Tujuan dan Manfaat Hasil Penelitian..... 6
1.6 Sistematika Penulisan..... 7

BAB 2 TINJAUAN TEORI..... 9
2.1 Teori Risiko..... 9
2.2 Pengelolaan Risiko (Risk Management)..... 13
2.3 Penilaian Risiko (Risk Assessment)..... 16
2.3.1 Analisis Risiko..... 19
2.3.2 Analisis Risiko Kuantitatif..... 21
2.3.3 Analisis Risiko Kualitatif..... 23
2.3.4 Analisis Risiko Kuantitatif dan Kualitatif..... 26
2.4 Mitigasi Risiko (Risk Mitigation)..... 29
2.4.1 Cost-Benefit Analysis 32
2.4.2 Cost-Effectiveness Analysis..... 34
2.4.3 Kebijakan Keamanan Informasi..... 36
2.5 Perancangan Keamanan Informasi..... 38
2.6 Tatakelola Keamanan Informasi..... 42

BAB 3 DESAIN DAN METODOLOGI PENELITIAN.....44
3.1 Desain Penelitian..... 44
3.2 Metodologi Penelitian..... 46
3.3 Tahapan Penilaian Risiko TI..... 48
3.4 Tahapan Mitigasi Risiko.....51
3.5 Tahapan Perancangan Keamanan Informasi.....54

BAB 4 PROFIL DAN PENILAIAN RISIKO……57
4.1 Profil Perusahaan……. 57
4.1.1 Sekilas Perusahaan……57
4.1.2 Visi dan Misi Perusahaan…….. 59
4.1.3 Struktur Organisasi…… 59
4.1.4 Bisnis Inti…….. 60
4.2 Penentuan Tujuan dan Sasaran Rancangan Keamanan Informasi….. 62
4.3 Kegiatan Penilaian Risiko……64
4.4 Karakteristik Sistem……..65
4.4.1 Pengelolaan Kebijakan Keamanan Informasi……69
4.4.2 Pengelolaan Aset Perusahaan…… 71
4.4.2.1 Aset Perangkat Keras……71
4.4.2.2 Aset Perangkat Lunak……74
4.4.2.3 Aset Jaringan dan Komunikasi…….. 77
4.4.2.4 Aset Informasi……... 81
4.4.2.5 Aset Personil…… 82
4.4.2.6 Aset Sarana Pendukung…… 84
4.4.3 Pengelolaan Sumber Daya Manusia TI…… 85
4.4.4 Pengelolaan Fisik dan Lingkungan……86
4.4.5 Pengelolaan Komunikasi dan Operasional…… 88
4.4.6 Pengelolaan Pembangunan Sistem dan Pemeliharan……89
4.4.7 Pengelolaan Insiden Keamanan Informasi……90
4.4.8 Pengelolaan Keberlangsungan Bisnis……91
4.5 Identifikasi Ancaman…… 91
4.6 Identifikasi Kelemahan/Kerawanan (Vulnerabilities)…….. 95
4.6.1 Sumber Kelemahan……95
4.6.2 Pembangunan Kebutuhan Keamanan……...100
4.7 Analisis Kontrol 104
4.7.1 Analisis berdasarkan Kategori Kontrol……104
4.7.2 Hasil Analisis Kontrol…….. 108
4.8 Penilaian Kecenderungan (Likelihood) dan Analisis Dampak……110
4.9 Pengenalan dan Tingkat Risiko……115
4.10 Rekomendasi Kontrol……...119

BAB 5 MITIGASI RISIKO……...124
5.1 Penentuan Prioritas Aksi…….....124
5.2 Evaluasi Rekomendasi Kontrol…… ...129
5.2.1 Evaluasi Kontrol Kebijakan dan Prosedur…… 130
5.2.2 Evaluasi Kontrol Pelabelan Informasi yang sensitif…….. 138
5.2.3 Evaluasi Kontrol Perjanjian Kerja……..139
5.2.4 Evaluasi Kontrol Pelatihan Security Awareness……141
5.2.5 Evaluasi Kontrol Pemeriksaan Latar Belakang……..142
5.2.6 Evaluasi Kontrol Scanning terhadap virus……143

5.2.7 Evaluasi Kontrol Penggunaan call back system……144
5.2.8 Evaluasi Kontrol Pembatasan Fungsi dan Informasi……..145
5.2.9 Evaluasi Kontrol Enkripsi……...146
5.2.10 Evaluasi Kontrol Penyimpanan backup……..147
5.2.11 Evaluasi Kontrol Pemasangan Anti Petir dan Grounding……... 148
5.2.12 Evaluasi Kontrol Pemasangan Firewall……..149
5.2.13 Evaluasi Kontrol Increased Supervisions…….. 150
5.2.14 Evaluasi Kontrol Sharing Responsibilities…… 151
5.2.15 Evaluasi Kontrol Job Rotation…….. 153
5.2.16 Evaluasi Kontrol Violation Report…….154
5.2.17 Evaluasi Kontrol Audit Trail Information……..155
5.2.18 Evaluasi Kontrol Intrusion Detection System……157
5.2.19 Hasil Evaluasi Rekomendasikan Kontrol……...158
5.3 Analisis Cost-Benefit Kontrol Keamanan……..…..160
5.3.1 Analisis Cost-Benefit Kontrol Kebijakan dan Prosedur…….160
5.3.2 Analisis Cost-Benefit Kontrol Pelabelan informasi sensitif……...161
5.3.3 Analisis Cost-Benefit Kontrol Perjanjian Kerja……... 162
5.3.4 Analisis Cost-Benefit Kontrol Pelatihan Security Awarness…….164
5.3.5 Analisis Cost-Benefit Kontrol Pemeriksaan Latar Belakang…….165
5.3.6 Analisis Cost-Benefit Kontrol Scanning terhadap virus…….167
5.3.7 Analisis Cost-Benefit Kontrol Penggunaan call back system……168
5.3.8 Analisis Cost-Benefit Kontrol Pembatasan Fungsi dan Informasi 169
5.3.9 Analisis Cost-Benefit Kontrol Enkripsi…….170
5.3.10 Analisis Cost-Benefit Kontrol Penyimpanan backup…….171
5.3.11 Analisis Cost-Benefit Kontrol Pemasangan Anti Petir dan Ground……172
5.3.12 Analisis Cost-Benefit Kontrol Pemasangan Firewall…….173
5.3.13 Analisis Cost-Benefit Kontrol Increase Supervisions……174
5.3.14 Analisis Cost-Benefit Kontrol Sharing Responsibilites…….175
5.3.15 Analisis Cost-Benefit Kontrol Job Rotation……..177
5.3.16 Analisis Cost-Benefit Kontrol Violation report…….178
5.3.17 Analisis Cost-Benefit Kontrol Audit Trail Information…….179
5.3.18 Analisis Cost-Benefit Kontrol Intrusion Detection System……...180
5.4 Analisis Cost-effectiveness Kontrol Keamanan……..……181
5.5 Pemilihan Kontrol…….185
5.6 Rancangan Implementasi Pengamanan dan Penugasan……..……186

BAB 6 PERANCANGAN KEAMANAN INFORMASI PERUSAHAAN…….190
6.1 Pendahuluan Rancangan Keamanan……...……190
6.2 Ancaman dan Kelemahan…….192
6.3 Aturan dan Tanggungjawab……..195
6.4 Tujuan dan Sasaran Rancangan Keamanan Informasi…….200
6.4.1 Sasaran: Dapat menentuan Kebijakan……...201
6.4.2 Sasaran: Dapat mengidentifikasi kebutuhan SDM TI……. 202
6.4.3 Sasaran: Dapat mengidentifikasi pembangunan sistem……. 203

6.4.4 Sasaran: Dapat mengidentifikasi aset-aset kritikal perusahaan……203
6.4.5 Sasaran: Dapat mengidentifikasi insiden keamanan informasi…….204
6.4.6 Sasaran: Dapat mengidentifikasi pengelolaan fisik dan lingkungan 204
6.4.7 Sasaran: Dapat mengidentifikasi pengelolaan komunikasi……...205
6.4.8 Sasaran: Dapat melakukan audit dan korektif……...205
6.4.9 Sasaran: Dapat mengidentifikasi pengelolaan keberlanjutan bisnis 206
6.5 Strategi……...……...207
6.5.1 Strategi: Menyusun kebijakan, prosedur dan standard……..208
6.5.2 Strategi: Memperbaiki pola rekruitmen dan pelatihan SDM TI……208
6.5.3 Strategi: Mengimplementasikan perangkat preventive dan detection……..209
6.5.4 Strategi:Menerapkan pola pemeriksaan dan evaluasi operasiona TI…….210
6.6 Kontrol Keamanan…….210
6.7 Rancangan Implementasi Kontrol Keamanan……..214
6.7.1 Rancangan Implementasi Kebijakan Keamanan Informasi……...215
6.7.2 Rancangan Implementasi Pelabelan informasi sensitif…….218
6.7.3 Rancangan Implementasi Penyimpanan backup data pada tempat aman……..219
6.7.4 Rancangan Implementasi Pemeriksaan latar belakang……..219
6.7.5 Rancangan Implementasi Perjanjian Kerja……220
6.7.6 Rancangan Implementasi Pelatihan Security Awarness……... 221
6.7.7 Rancangan Implementasi Sharing Responsibility…….221
6.7.8 Rancangan Implementasi Scanning terhadap virus……...222
6.7.9 Rancangan Implementasi Pemasangan anti petir dan grounded…… 223
6.7.10 Rancangan Implementasi Pemasangan Firewall……223
6.7.11 Rancangan Implementasi IDS……224
6.7.12 Rancangan Implementasi Enkripsi…….224
6.7.13 Rancangan Implementasi Pembatasan fungsi dan informasi……..225
6.7.14 Rancangan Implementasi Increased supervision……225
6.7.15 Rancangan Implementasi Job rotation……226
6.7.16 Rancangan Implementasi Penggunaan call back system……226
6.7.17 Rancangan Implementasi Violation report…….227
6.7.18 Rancangan Implementasi Audit trail……..228

BAB 7 PENUTUP 229
7.1 Kesimpulan……229
7.2 Saran…… 230

DAFTAR PUSTAKA……...231

LAMPIRAN……L-1

DAFTAR GAMBAR

Gambar 2.1 Hubungan risiko, ancaman, kerawanan, dan nilai aset……. 9
Gambar 2.2 Risk Diagram……. 12
Gambar 2.3Risk Management Life Cycle……. 14
Gambar 2.4 Fase pada Risk Management dan Risk Assessment……. 16
Gambar 2.5 Fase pada IT Risk Assessment……. 17
Gambar 2.6 Analisis Risiko Kuantitatif dan Penilaian Risiko…….. 22
Gambar 2.7 Analisis Risiko Kualitatif dan Penilaian Risiko…….25
Gambar 2.8 Penanganan Serangan…… 31
Gambar 2.9 Skema Tahapan Analisis Cost Benefit…….. 33
Gambar 2.10 AHP Hierarchy……..... 34
Gambar 2.11 CIA triangle……. 39
Gambar 2.12 People, policy and technology model……..40
Gambar 2.13 Konsep Tatakelola Keamanan Informasi…… 43
Gambar 3.1 Desain Penelitian …… 44
Gambar 3.2 Metodologi Penelitian……46
Gambar 3.3 Tahapan Risk Assessment…… 50
Gambar 3.4 Tahapan Risk Mitigation…….. 52
Gambar 3.5 Tahapan Rancangan Keamanan Informasi…… 55
Gambar 4.1 Struktur Organisasi PT. Multi Terminal Indonesia……... 60
Gambar 4.2 Topologi Jaringan Komputer Perusahaan…… 77
Gambar 4.3 Matriks Tingkat Risiko……. 118
Gambar 6.1Kerangka Rancangan Keamanan Informasi…….. 190
Gambar 6.2 Tanggungjawab dan aturan fungsional……. 196
Gambar 6.3 Rekomendasi Struktur Organiasi Keamanan Informasi (L)……. 198
Gambar 6.4 Rekomendasi Struktur Organisasi Keamanan Informasi (S)…….. 198
Gambar 6.5 Struktur Organisasi PT. Multi Terminal Indonesia (saat ini)……... 199

DAFTAR TABEL

Tabel 2.1 Skala Nilai Perbandingan (NIST Standard)..... 35
Tabel 4.1 Kebijakan Keamanan Informasi Perusahaan..... 69
Tabel 4.2 Spesifikasi Server..... 72
Tabel 4.3 Spesifikasi PC..... 73
Tabel 4.4 Sistem Operasi yang digunakan..... 74
Tabel 4.5 Perangkat lunak perkantoran yang digunakan..... 75
Tabel 4.6 Perangkat lunak pendukung bisnis yang digunakan..... 76
Tabel 4.7 Perangkat Jaringan Komputer..... 78
Tabel 4.8 Fasilitas Internet yang digunakan..... 79
Tabel 4.9 Penggunaan Protokol Internet..... 79
Tabel 4.10 Firewall yang digunakan..... 80
Tabel 4.11 Identifikasi Informasi yang Sensitif dan Kritikal..... 81
Tabel 4.12 Komposisi Pekerja Berdasarkan Jabatan (Company Profile PT. MTI).. 82
Tabel 4.13 Komposisi Pekerja Berdasarkan Pendidikan..... 83
Tabel 4.14 Sarana Pendukung..... 84
Tabel 4.15 Pengguna Sistem Aplikasi pendukung bisnis..... 85
Tabel 4.16 Pembagian Ruang TI..... 86
Tabel 4.17 Lingkungan Lokasi Server/Data Center..... 87
Tabel 4.18 Kontrol Fisik yang digunakan..... 89
Tabel 4.19 Ancaman Aktif..... 92
Tabel 4.20 Ancaman Aktif (2)..... 93
Tabel 4.21 Ancaman Pasif..... 93
Tabel 4.22 Kelemahan (1)..... 96
Tabel 4.23 Kelemahan (2)..... 97
Tabel 4.24 Kelemahan (3)..... 98
Tabel 4.25 Kelemahan (4)..... 99
Tabel 4.26 Hasil Pemeriksaan Kriteria Keamanan Informasi (1)..... 101
Tabel 4.27 Hasil Pemeriksanaan Kriteria Keamanan Informasi (2)..... 102
Tabel 4.28 Tabel Kombinasi Kontrol (1)..... 105
Tabel 4.29 Tabel Kombinasi Kontrol (2)..... 106
Tabel 4.30 Tingkatan Likelihood..... 110
Tabel 4.31 Ukuran dari Dampak..... 111
Tabel 4.32 Kecenderungan dan Dampak (1)..... 112
Tabel 4.33 Kecenderungan dan Dampak (2)..... 113
Tabel 4.34 Kecenderungan dan Dampak (3)..... 114
Tabel 4.35 Risk Scale and Necessary Actions..... 115
Tabel 4.36 Identifikasi Tingkat Risiko (1)..... 116
Tabel 4.37 Identifikasi Tingkat Risiko (2)..... 117
Tabel 4.38 Analisis Kuantitatif pada Risiko akibat Gangguan Petir..... 118
Tabel 4.39 Recomendasi kontrol (1)..... 121
Tabel 4.40 Recomendasi kontrol (2)..... 122

Tabel 4.41 Recomendasi kontrol (3)…… 123
Tabel 5.1 Keterlibatan dalam Kontrol Kebijakan dan Prosedur (1)……..131
Tabel 5.2 Keterlibatan dalam Kontrol Kebijakan dan Prosedur (2)……..132
Tabel 5.3 Keterlibatan dalam Kontrol Kebijakan dan Prosedur (3)……..133
Tabel 5.4 Evaluasi Kontrol Keamanan (1)……134
Tabel 5.5 Evaluasi Kontrol Keamanan (2)……135
Tabel 5.6 Evaluasi Kontrol Keamanan (3)……136
Tabel 5.7 Evaluasi Kontrol Keamanan (4)……137
Tabel 5.8 Ukuran Tingkat Evaluasi Rekomendasi Kontrol…….. 158
Tabel 5.9 Hasil Evaluasi Rekomendasi Kontrol……... 159
Tabel 5.10Cost Effectiveness-Tahap 1……181
Tabel 5.11Cost-effectiveness– Tahap 2……183
Tabel 5.12 Cost-effectiveness– Tahap 3……...184
Tabel 5.13 Pemilihan Kontrol……...185
Tabel 5.14 Rancangan Kontrol Keamanan (1)…… 187
Tabel 5.15 Rancangan Kontrol Keamanan (2)……..188
Tabel 6.1 Ancaman dan Kelemahan (1)……192
Tabel 6.2 Ancaman dan Kelemahan (2)……192
Tabel 6.3 Ancaman dan Kelemahan (3)……193
Tabel 6.4 Tujuan dan Sasaran……...200
Tabel 6.5 Tujuan , Sasaran dan Strategi……207
Tabel 6.6 Strategi dan Kontrol Keamanan……211
Tabel 6.7 Rancangan Implementasi Kontrol……214

DAFTAR LAMPIRAN

Lampiran 1	Materi Observasi dan wawancara	L-2
Lampiran 2	Daftar Pertanyaan	L-3
Lampiran 3	Hasil Observasi dan Wawancara	L-5