

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR	ii
HALAMAN PERNYATAAN KEASLIAN	iii
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xiv
ABSTRAK	xv
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Tujuan Penelitian	3
1.4 Ruang Lingkup Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Kerangka Berpikir.....	5
1.7 Sistematika Penulisan	5
BAB II.....	7
TINJAUAN PUSTAKA	7
2.1 Perancangan	7
2.2 Infrastruktur	7
2.3 Jaringan Komputer.....	7
2.3.1 Manfaat Jaringan Komputer	8
2.3.2 Topologi Jaringan	8
2.3.2.1 Topologi Star	9
2.3.2.2 Topologi Ring	9
2.3.2.3 Topologi Extended Star	9
2.3.3 Klasifikasi Jaringan Komputer	10
2.3.3.1 Berdasarkan Area.....	10
2.3.3.2 Berdasarkan Pola Operasi.....	10

2.3.3.3	Berdasarkan Media Pengantar	11
2.4	Metode Kualitatif	11
2.5	<i>System Security Engineering Capability Maturity Model (SSE-CMM)</i>	
	12	
2.5.1	Tingkat Kapabilitas SSE-CMM.....	12
2.6	Keamanan Informasi.....	14
2.6.1	Ancaman Keamanan Sistem Informasi.....	15
2.6.2	Aspek-aspek terhadap keamanan informasi	16
2.7	Sistem Manajemen Keamanan Informasi (SMKI)	17
2.8	Manajemen Risiko	18
2.8.1	Pentingnya Manajemen Risiko	19
2.8.2	Penilaian Risiko	19
2.9	ISO 27001:2013	22
2.9.1	Istilah dan definisi dalam ISO 27001:2013	22
2.9.2	Penetapan, Penerapan, Pemantauan, Peningkatan SMKI.....	23
2.9.3	Sasaran Pengendalian ISO 27001:2013	28
2.10	Perangkat Jaringan	29
2.10.1	Switch	29
2.10.2	Router.....	29
2.10.3	<i>Firewall</i>	29
2.10.4	Server	29
2.10.4.1	Sistem Operasi Server.....	30
2.10.5	Komputer Klien	30
2.10.6	Rak Server.....	30
2.11	GNS3	30
2.12	<i>Internet Control Message Protocol (ICMP)</i>	31
2.13	Desain Jaringan	31
2.13.1	Macam-Macam Desain Jaringan	31
2.13.1.1	<i>Low-level</i> Desain	31
2.13.1.2	<i>Middle-level</i> Desain	32
BAB III		33
METODOLOGI PENELITIAN		33
3.1	Tempat dan Waktu Penelitian.....	33
3.1.1	Tempat Penelitian	33

3.1.1.1	Profil PT Asuransi Jiwa BCA	33
3.1.1.2	Visi dan Misi Perusahaan	34
3.1.1.2.1	Visi PT Asuransi Jiwa BCA	34
3.1.1.2.2	Misi PT Asuransi Jiwa BCA	34
3.1.1.3	Struktur Perusahaan	35
3.1.2	Waktu Penelitian.....	35
3.2	Tahapan Penelitian.....	35
3.2.1	<i>Analysis</i>	36
3.2.2	<i>Design</i>	38
3.2.3	<i>Simulation</i>	39
3.2.4	<i>Implementation</i>	40
3.2.5	<i>Monitoring</i>	41
3.2.6	<i>Management</i>	41
3.3	Metode Pengumpulan Data.....	41
3.3.1	Studi Literatur	41
3.3.2	Wawancara.....	42
3.3.3	Kuesioner	42
3.3.4	Observasi / Studi Lapangan	42
3.3.5	Eksperimen	42
3.4	Metode Analisis Data.....	43
3.4.1	<i>Plan</i> (Merencanakan).....	43
3.4.2	<i>Do</i> (Implementasi)	46
3.4.3	<i>Check</i> (Meninjau Ulang)	46
3.4.4	<i>Act</i> (Memelihara)	46
BAB IV	47	
PEMBAHASAN	47	
4.1	Tahap Plan	47
4.1.1	Menentukan Ruang Lingkup Keamanan Informasi	47
4.1.2	Menentukan Kebijakan Keamanan Informasi	48
4.1.2.1	Tujuan	49
4.1.2.2	Kebijakan Keamanan Informasi	49
4.1.2.3	Kontrol Akses Keamanan Informasi	50
4.2	Tahap Do.....	50
4.2.1	Mengidentifikasi Risiko.....	50

4.2.1.1	Mengidentifikasi dan Menghitung Nilai Aset	50
4.2.1.2	Mengidentifikasi Kelemahan, Ancaman, dan Menilai terhadap Aset	56
4.2.2	Menganalisis dan Evaluasi Risiko	79
4.2.2.1	Menganalisis Dampak dan Risiko	79
4.2.2.2	Mengidentifikasi Tingkat Risiko	80
4.2.2.3	Penilaian Risiko	82
4.3	Tahap Check	92
4.3.1	Memilih Objektif Kontrol dan Kontrol Keamanan Informasi	92
4.3.2	Memilih Klausul dari ISO/IEC 27001:2013	92
4.3.3	Menentukan Nilai Tingkat Kemampuan.....	93
4.4	Tahap Act.....	101
4.4.1	Rekomendasi Terhadap Objektif Kontrol dan Keamanan Informasi berdasarkan ISO/IEC 27001:2013	101
4.4.2	Kesimpulan Hasil dan Pembahasan Metode PDCA	111
BAB V.....		114
PENUTUP.....		114
5.1	Kesimpulan	114
5.2	Saran	118
DAFTAR REFERENSI		120
LAMPIRAN I		122
ANALISIS RISIKO		122
LAMPIRAN II		124
ANALISIS RISIKO		124
LAMPIRAN III.....		129
LEMBAR KUESIONER		129
LAMPIRAN IV.....		137
LEMBAR PENILAIAN BIA		137
LAMPIRAN V		138
LEMBAR WAWANCARA.....		138
LAMPIRAN VI.....		144
SURAT PERMOHONAN IZIN PENELITIAN		144
LAMPIRAN VII		145
SURAT KONFIRMASI PERSETUJUAN PENELITIAN		145

DAFTAR TABEL

Tabel 2. 1 Indeks Kriteria Penilaian Tingkat Kapabilitas	13
Tabel 2. 2 Penilaian Aset Berdasarkan Kerahasiaan.....	24
Tabel 2. 3 Penilaian Aset Berdasarkan Keutuhan	25
Tabel 2. 4 Penilaian Aset Berdasarkan Ketersediaan.....	25
Tabel 2. 5 Skala Business Impact Analysis	27
Tabel 3. 1 Perangkat Jaringan yang dibutuhkan	38
Tabel 3. 2 Tabel Sasaran Pengendalian.....	43y
Tabel 4. 1 Data Aset pada Divisi IT Infrastructure	47
Tabel 4. 2 Detail Aset pada PT Asuransi Jiwa BCA.....	51
Tabel 4. 3 Nilai Aset	55
Tabel 4. 4 Daftar Kelemahan dan Ancaman Database Myportal (ITSM)	57
Tabel 4. 5 Daftar Kelemahan dan Ancaman Database Aplikasi Internal	57
Tabel 4. 6 Daftar Kelemahan dan Ancaman Laptop.....	57
Tabel 4. 7 Daftar Kelemahan dan Ancaman Personal Computer	58
Tabel 4. 8 Daftar Kelemahan dan Ancaman Server On-Premise.....	58
Tabel 4. 9 Daftar Kelemahan dan Ancaman Server On-Cloud.....	59
Tabel 4. 10 Daftar Kelemahan dan Ancaman Windows Server 2012 R2.....	59
Tabel 4. 11 Daftar Kelemahan dan Ancaman Windows 10.....	59
Tabel 4. 12 Daftar Kelemahan dan Ancaman Microsoft Office 2013	60
Tabel 4. 13 Daftar Kelemahan dan Ancaman Microsoft Office 365	60
Tabel 4. 14 Daftar Kelemahan dan Ancaman (AC) Ruang Server	60
Tabel 4. 15 Daftar Kelemahan dan Ancaman UPS Ruang Server	60
Tabel 4. 16 Daftar Kelemahan dan Ancaman Fiber Optic.....	61
Tabel 4. 17 Daftar Kelemahan dan Ancaman Kebel UTP	61
Tabel 4. 18 Daftar Kelemahan dan Ancaman CCTV	61
Tabel 4. 19 Daftar Kelemahan dan Ancaman Switch	61
Tabel 4. 20 Daftar Kelemahan dan Ancaman Router Firewall.....	62
Tabel 4. 21 Daftar Kelemahan dan Ancaman Access Point	62
Tabel 4. 22 Daftar Kelemahan dan Ancaman Aplikasi ITSM	62
Tabel 4. 23 Daftar Kelemahan dan Ancaman SSMS	63
Tabel 4. 24 Daftar Kelemahan dan Ancaman Trendmicro Antivirus	63

Tabel 4. 25 Daftar Kelemahan dan Ancaman Server Storage	63
Tabel 4. 26 Daftar Kelemahan dan Ancaman Rak Server	64
Tabel 4. 27 Daftar Kelemahan dan Ancaman Access Door.....	64
Tabel 4. 28 Daftar Kelemahan dan Ancaman Access Door Management.....	64
Tabel 4. 29 Hasil Rerata Probabilitas dan Nilai Ancaman Database Myportal	65
Tabel 4. 30 Hasil Rerata Probabilitas dan Nilai Ancaman Database Aplikasi Internal	65
Tabel 4. 31 Hasil Rerata Probabilitas dan Nilai Ancaman Laptop	66
Tabel 4. 32 Hasil Rerata Probabilitas dan Nilai Ancaman Personal Computer....	67
Tabel 4. 33 Hasil Rerata Probabilitas dan Nilai Ancaman Server On-Premise	67
Tabel 4. 34 Hasil Rerata Probabilitas dan Nilai Ancaman Server On-Cloud	68
Tabel 4. 35 Hasil Rerata Probabilitas dan Nilai Ancaman Windows Server 2012 R2	68
Tabel 4. 36 Hasil Rerata Probabilitas dan Nilai Ancaman Windows 10	69
Tabel 4. 37 Hasil Rerata Probabilitas dan Nilai Ancaman Microsoft Office 2013	69
Tabel 4. 38 Hasil Rerata Probabilitas dan Nilai Ancaman Microsoft Office 365.	70
Tabel 4. 39 Hasil Rerata Probabilitas dan Nilai Ancaman AC Ruang Server	70
Tabel 4. 40 Hasil Rerata Probabilitas dan Nilai Ancaman.....	71
Tabel 4. 41 Hasil Rerata Probabilitas dan Nilai Ancaman Fiber Optic	71
Tabel 4. 42 Hasil Rerata Probabilitas dan Nilai Ancaman.....	71
Tabel 4. 43 Hasil Rerata Probabilitas dan Nilai Ancaman CCTV	72
Tabel 4. 44 Hasil Rerata Probabilitas dan Nilai Ancaman Switch	72
Tabel 4. 45 Hasil Rerata Probabilitas dan Nilai Ancaman Router Firewall	73
Tabel 4. 46 Hasil Rerata Probabilitas dan Nilai Ancaman Access Point.....	74
Tabel 4. 47 Hasil Rerata Probabilitas dan Nilai Ancaman Aplikasi ITSM	74
Tabel 4. 48 Hasil Rerata Probabilitas dan Nilai Ancaman SSMS	75
Tabel 4. 49 Hasil Rerata Probabilitas dan Nilai Ancaman Trendmicro Antivirus	75
Tabel 4. 50 Hasil Rerata Probabilitas dan Nilai Ancaman Server Storage	76
Tabel 4. 51 Hasil Rerata Probabilitas dan Nilai Ancaman Rak Server.....	76
Tabel 4. 52 Hasil Rerata Probabilitas dan Nilai Ancaman Access Door	77
Tabel 4. 53 Hasil Rerata Probabilitas dan Nilai Ancaman Access Door Management	77

Tabel 4. 54 Kesimpulan Hasil Rerata Probabilitas dan Nilai Ancaman Aset	78
Tabel 4. 55 Hasil Nilai BIA pada Aset	80
Tabel 4. 56 Hasil Nilai Dampak Bisnis pada Aset.....	81
Tabel 4. 57 Hasil Nilai dan Tingkat Risiko pada Aset.....	82
Tabel 4. 58 Analisis Risiko Keamanan Informasi pada Aset.....	84
Tabel 4. 59 Objektif Kontrol dan Kontrol Keamanan ISO/IEC 27001: 2013	92
Tabel 4. 60 Kerangka Kerja Perhitungan Maturity Level Klausul 8	94
Tabel 4. 61 Hasil Maturity Level Klausul 8.....	95
Tabel 4. 62 Kerangka Kerja Perhitungan Maturity Level Klausul 9	95
Tabel 4. 63 Hasil Maturity Level Klausul 9.....	96
Tabel 4. 64 Kerangka Kerja Perhitungan Maturity Level Klausul 11	97
Tabel 4. 65 Hasil Maturity Level Klausul 11.....	98
Tabel 4. 66 Kerangka Kerja Perhitungan Maturity Level Klausul 12	98
Tabel 4. 67 Hasil Maturity Level Klausul 12.....	99
Tabel 4. 68 Kerangka Kerja Perhitungan Maturity Level Klausul 13	100
Tabel 4. 69 Hasil Maturity Level Klausul 13.....	100
Tabel 4. 70 Hasil Maturity Level Klausul ISO/IEC 27001:2013	101
Tabel 4. 71 Hasil Temuan dan Rekomendasi berdasarkan ISO/IEC 27001:2013	102

DAFTAR GAMBAR

Gambar 1. 1 Kerangka Berpikir	5
Gambar 2. 1 Topologi Star.....	9
Gambar 2. 2 Topologi Ring	9
Gambar 2. 3 Topologi Extended Star.....	10
Gambar 2. 4 Model PDCA yang diterapkan untuk proses SMKI.....	17
Gambar 2. 5 Firewall Fortigate	29
Gambar 2. 6 Logo GNS3	30
Gambar 2. 7 Low Level Network Design	32
Gambar 2. 8 Middle Level Network Design.....	32
Gambar 3. 1 Chase Plaza	33
Gambar 3. 2 Logo PT Asuransi Jiwa BCA	34
Gambar 3. 3 Struktur PT Asuransi Jiwa BCA	35
Gambar 3. 4 Struktur Divisi IT PT Asuransi Jiwa BCA.....	35
Gambar 3. 5 Topologi Jaringan Existing PT Asuransi Jiwa BCA	37
Gambar 3. 6 Perancangan Infrastruktur Jaringan.....	39
Gambar 3. 7 Simulasi jaringan menggunakan GNS3	40