

DAFTAR ISI

HALAMAN SAMPUL	i
ABSTRAK	iii
<i>ABSTRACT</i>	iv
LEMBAR PENGESAHAN PEMBIMBING	v
LEMBAR PERNYATAAN ORISINALITAS	vi
PAKTA INTEGRITAS PROGRAM STUDI MAGISTER SISTEM INFORMASI UNIVERSITAS TELKOM.....	vii
HALAMAN PENGESAHAN KAPRODI, PEMBIMBING DAN PENGUJI	viii
LEMBAR PERNYATAAN PERSETUJUAN AKADEMIS	ix
COPYRIGHT TESIS MAGISTER.....	x
HALAMAN PENGAKUAN	xi
HALAMAN DAFTRA PUBLIKASI	xii
KATA PENGANTAR	xiii
DAFTAR ISI.....	xiv
DAFTAR TABEL.....	xix
DAFTAR GAMBAR	xx
DAFTAR LAMPIRAN.....	xxii
BAB I PENDAHULUAN.....	1
I.1 <i>State of Art</i>	1
I.2 Latar Belakang	2
I.3 Rumusan Masalah	7
I.4 Tujuan Penelitian.....	7
I.5 Pertanyaan Penelitian	8
I.6 Lingkup Penelitian	8
I.7 Kesenjangan Penelitian	9
I.8 Rasionalisme Penelitian	10
I.9 Ekspektasi Penelitian.....	11
I.10 Signifikansi Penelitian.....	12
I.11 Pertimbangan Penelitian.....	13
I.12 Peran Peneliti.....	14
I.13 Sistematika Penulisan.....	15

BAB II LANDASAN TEORI	17
II.1 Metode <i>Review</i>	17
II.2 Hasil <i>Review</i>	20
II.3 Perspektif Teori	25
II.3.1 Pusat Kendali Keamanan/ <i>Security Operation Centre</i>	25
II.3.2 Lima Aspek Layanan Utama SOC	29
II.3.3 Kriteria Rancangan SOC	34
II.3.4 Keamanan SOC	35
II.3.5 Authentication	35
II.3.6 Serangan Terhadap Sistem Informasi Organisasi	36
II.3.7 <i>Intrusion Detection System (IDS)</i>	37
II.3.8 Indeks KAMI	38
II.4 <i>Framework</i> Yang Relevan	38
II.4.1 ISO/IEC 27005	38
II.4.2 NIST	40
II.4.3 NIST SP 800-30	41
II.5 Isu dan Tren Penelitian	42
II.6 Motivasi Penelitian	43
II.6.1 Pemilihan Teori	43
II.6.2 Pemilihan <i>Framework</i>	47
II.6.3 Pemilihan Isu dan Tren	49
BAB III METODOLOGI PENELITIAN	51
III.1 Perancangan Penelitian	51
III.1.1 <i>Planning</i>	52
III.1.2 <i>Conduction</i>	52
III.1.3 <i>Reporting</i>	55
III.2 Model Konseptual	55
III.3 Sistematika Penelitian	56
III.3.1 Tahap Identifikasi Masalah dan Pengumpulan Data (Data Collection)	57
III.3.2 Tahap Studi Literatur (Review)	58
III.3.3 Tahap Analisis Data (Data Analysis)	59
III.3.4 Tahap Interpretasi Data dan Pembentukan <i>Framework</i> Baru (Data Interpretation)	59

III.3.5 Tahap Kesimpulan dan Saran.....	60
III.4 Asumsi atau Premis	61
III.5 Sumber Data Penelitian	61
III.6 Pertimbangan Etika	62
III.7 Instrumen Penelitian.....	62
III.8 Prosedur Seleksi	63
III.9 Bias Penelitian.....	64
III.10 Uji Keabsahan Data	64
III.10.1 Uji Kreadibilitas.....	64
III.10.2 Uji Keterikatan.....	65
III.10.3 Uji Konfirmasi	65
III.10.4 Uji Transferabilitas	65
BAB IV PENGUMPULAN DATA.....	67
IV.1 Metode Pengumpulan Data.....	67
IV.1.1 Pertimbangan Etika	68
IV.1.2 Prosedur Seleksi	68
IV.1.3 Uji Keabsahan Data.....	68
IV.1.4 Dokumen Yang Digunakan	69
IV.2 Gambaran Umum.....	77
IV.2.1 Objek Penelitian	77
IV.2.2 Persiapan Penelitian	78
IV.2.3 Kondisi Saat Ini.....	78
IV.2.4 Kajian Bisnis	80
IV.2.5 Pelaksanaan Penelitian	82
IV.2.6 Analisis PESTLE	83
IV.3 Studi Pendahuluan	88
IV.4 Hasil Deskriptif.....	93
IV.4.1 Proses Bisnis	93
IV.4.2 Struktur SOC di PT NBFC.....	95
IV.4.3 Pembagian Kerja Tim SOC PT NBFC.....	100
IV.4.4 Kerangka Pengelolaan Penanganan Insiden Keamanan Informasi	101
IV.4.5 Standar/ <i>Framework</i>	101
IV.4.6 Pengembangan dari Kolaborasi <i>Framework</i>	105

IV.5	Hasil Validasi.....	106
IV.5.1	SOC Menurut <i>National Institute Standards Technology</i> (NIST) ..	106
IV.5.2	Perbedaan Pemahaman Pada ISO 27001 Dengan NIST	106
IV.5.3	Perbedaan Kompleksitas SOC	112
IV.5.4	Pentingnya <i>People</i> pada Instrumen SOC	113
IV.5.5	Parameter Dalam <i>Assessment Security</i>	114
IV.5.6	Control Dalam ISO dan NIST.....	118
BAB V ANALISA DATA		123
V.1	Implementasi <i>Grounded Theory</i>	123
V.2	Pengembangan Model Data.....	125
V.3	Uji Instrumen Data	125
V.3.1	Rekomendasi SOC Modern	128
V.3.2	Roadmap Dasar Transformasi SOC	137
V.3.3	Evaluasi SOC	139
V.3.4	Strategi Keamanan	142
V.4	Penilaian <i>Framework</i>	146
V.4.1	Penilaian <i>Framework</i> ISO 27005	147
V.4.2	Penilaian <i>Framework</i> NIST SP 800-30	148
V.4.3	Penilaian <i>Framework</i> Usulan.....	149
V.5	Perancangan.....	150
V.6	Implementasi	151
V.3.1	<i>Cyber Security</i>	152
V.3.2	Parameter <i>Assessment</i> Sistem Informasi <i>SOC</i>	152
V.3.3	<i>Research Assessment</i>	154
V.3.4	<i>Risk Assessment</i>	158
V.3.5	<i>Risk Treatment and Risk Acceptance Strategy</i>	165
V.3.6	<i>Monitoring</i>	166
V.3.7	<i>Assessment SOC</i>	166
V.7	Hasil Uji Keabsahan Data	166
V.8	Implikasi Penelitian	168
BAB VI KESIMPULAN		169
VI.1	Metode Interpretasi	169
VI.2	Kesimpulan	171

VI.3	Kritik dan Saran	173
VI.4	Rekomendasi.....	174
DAFTAR PUSTAKA		175
LAMPIRAN.....		183