

## DAFTAR ISI

PERNYATAAN.....	iii
PRAKATA.....	iv
DAFTAR SINGKATAN .....	vi
ABSTRACT.....	vii
INTISARI.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xiii
DAFTAR TABEL.....	xiv
BAB I PENDAHULUAN.....	1
<b>1.1 Latar Belakang</b> .....	1
<b>1.2 Perumusan Masalah</b> .....	4
<b>1.3 Batasan Masalah</b> .....	5
<b>1.4 Keaslian Penelitian</b> .....	5
<b>1.5 Tujuan Penelitian</b> .....	11
<b>1.6 Manfaat Penelitian</b> .....	11
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI .....	13
<b>2.1 Tinjauan Pustaka</b> .....	13
<b>2.2 Landasan Teori</b> .....	20
<b>2.2.1 Aspek Keamanan Informasi</b> .....	20
<b>2.2.1.1 Ruang Lingkup Keamanan Informasi</b> .....	22
<b>2.2.1.2 Failure Modes and Effects Analysis (FMEA)</b> .....	24
<b>2.2.1.3 Ancaman Kemanan Informasi</b> .....	25
<b>2.2.2 Kerentanan Yang Terjadi Pada Jaringan Komputer</b> .....	26

2.2.3 Jenis-jenis Serangan yang Sering Terjadi Melalui Jaringan .....	29
2.2.4 Manajemen Risiko dan Penilaian Risiko .....	34
2.2.5 Kerangka Kerja Manajemen Risiko .....	35
2.2.6 Manajemen Risiko Keamanan Informasi .....	36
2.2.7 Berbagai Framework-Framework Manajemen Risiko Keamanan Informasi .....	37
2.2.7.1 OCTAVE Allegro[7] .....	38
2.2.7.2 Framework NIST Special Publication 800-30 .....	42
2.2.8 Disaster Recovery Plan (DRP) .....	44
2.3    Pertanyaan Penelitian .....	48
BAB III METODOLOGI PENELITIAN .....	49
3.1 Jenis Penelitian .....	49
3.2 Alat dan Bahan Penelitian .....	49
3.2.1 Alat Penelitian .....	49
3.2.2 Bahan Penelitian .....	50
3.3 Jalannya Penelitian .....	50
3.3.1 Mendata Kondisi Eksisting .....	52
3.3.2 Menetapkan kriteria pengukuran Risiko .....	54
3.3.3 Mengembangkan Profil Aset Informasi .....	56
3.3.4 Mengidentifikasi Container Aset Informasi .....	58
3.3.5 Mengidentifikasi <i>area of concern</i> .....	59
3.3.6 Mengidentifikasi Skenario Ancaman .....	60
3.3.7 Mengidentifikasi Risiko .....	62
3.3.8 Menganalisis Risiko .....	64
3.3.9 Memilih Pendekatan Mitigasi .....	65

<b>3.3.10 Validasi Data</b> .....	67
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....	68
<b>4.1 Kondisi Sistem Saat ini</b> .....	68
<b>4.1.1 Kebijakan Terkait Pelaksanaan Manajemen Risiko</b> .....	68
<b>4.1.2 Rencana Strategis Dinas KOMINFO Kulonprogo</b> .....	69
<b>4.1.3 Kajian Layanan Aplikasi</b> .....	73
<b>4.1.4 Infrastruktur Jaringan</b> .....	75
<b>4.1.5 Sistem Server</b> .....	78
<b>4.1.6 Kelemahan Teknologi Saat Ini</b> .....	80
<b>4.2 Menetapkan Kriteria Pengukuran Risiko</b> .....	81
<b>4.3 Mengembangkan Profil Aset Informasi</b> .....	83
<b>4.4 Mengidentifikasi <i>Container</i> Aset Informasi</b> .....	86
<b>4.5 Mengidentifikasi Area Masalah (<i>Area of Concern</i>)</b> .....	88
<b>4.4 Mengidentifikasi Skenario Ancaman</b> .....	91
<b>4.5 Mengidentifikasi Risiko</b> .....	93
<b>4.6 Menganalisis Risiko</b> .....	95
<b>4.7 Memilih Pendekatan Mitigasi</b> .....	98
<b>4.8 Pembahasan</b> .....	100
<b>4.8.1 Mitigasi Risiko I</b> .....	100
<b>4.8.2 Mitigasi Risiko II</b> .....	101
<b>4.8.3 Mitigasi Risiko III</b> .....	102
<b>4.8.4 Mitigasi Risiko IV</b> .....	103
<b>4.8.5 Rekomendasi Strategi Proteksi</b> .....	104
<b>4.8.6 Keterbatasan Penelitian</b> .....	109
<b>4.8.7 Kelebihan Penelitian</b> .....	109

BAB V KEMPULAN DAN SARAN .....	111
<b>5.1 Kesimpulan</b> .....	111
<b>5.2 Saran</b> .....	112
DAFTAR PUSTAKA .....	113
LAMPIRAN .....	117
<b>Profil Pemerintah Kabupaten Kulonprogo</b> .....	117
<b>Sejarah Profil Daerah</b> .....	117
<b>Visi Dan Misi</b> .....	120
<b>Organisasi Di Pemerintah Kabupaten Kulonprogo</b> .....	123
<b>Profil Dinas Komunikasi Dan Informatika Pemerintah Kabuten     Kulonprogo</b> .....	126

## DAFTAR GAMBAR

Gambar 1.1 Fishbone diagram manajemen risiko keamanan informasi .....	6
Gambar 2. 1 Fase OCTAVE .....	14
Gambar 2. 2 Tujuan Kaskade penelitian[18] .....	16
Gambar 2. 3 Tahapan OCTAVE Allegro[7] .....	19
Gambar 2. 4 Elemen Keamanan Informasi [23] .....	22
Gambar 2. 5 Aspek Keamanan Informasi .....	23
Gambar 2. 6 Siklus FMEA.....	24
Gambar 2. 7 Siklus manajemen dan evaluasi risiko keamanan informasi[22] .....	37
Gambar 2. 8 Langkah-langkah OCTAVE Allegro .....	39
Gambar 3. 1 Allegro Road Map (Caralli et.al., 2007)[7].....	51
Gambar 3. 2 Workflow Penelitian Menggunakan Metode OCTAVE Allegro.....	52
Gambar 4. 1 Tampilan utama portal layanan aplikasi Pemkab Kulonprogo .....	73
Gambar 4. 2 Topologi Jaringan Pemerintah Kabupaten Kulonprogo.....	76
Gambar 4. 3 Denah Ruang divisi TI dan UPTD. ....	80
Gambar 4. 4 Asset Information Container .....	86
Gambar 4. 4 Kabupaten Kulonprogo Dalam Peta.....	118
Gambar 4. 5 Struktur Organisasi Pemerintah Kabupaten Kulonprogo.....	124

## DAFTAR TABEL

Tabel 2. 1 Rincian Tahapan Metode OCTAVE Allegro[20] .....	17
Tabel 2. 2 Mitigation Approach .....	20
Tabel 2. 3 Description of Threat Trees Threat [7] .....	41
Tabel 3. 1 Impact Area Reputasi Kepercayaan Pelanggan .....	55
Tabel 3. 2 Impact Area Reputasi Kepercayaan Pelanggan .....	56
Tabel 3. 3 Informasi Aset.....	57
Tabel 3. 4 Information Asset Risk Environment Map .....	59
Tabel 3. 5 <i>Area of Concern</i> .....	60
Tabel 3. 6 Information Asset Risk Worksheets .....	61
Tabel 3. 7 Graphical Representation of Threat Trees .....	62
Tabel 3. 8 Contoh Identifikasi Risiko .....	63
Tabel 3. 9 Score Terhadap Impact Area.....	65
Tabel 3. 10 Matriks Risiko Relatif dengan Probabilitas Ancaman .....	66
Tabel 3. 11 Pendekatan dan Pengurangan Risiko .....	67
Tabel 4. 1 Tujuan, Sasaran, Strategi, dan Kebijakan .....	71
Tabel 4. 2 Penentuan Alternatif Strategi Meningkatkan Tata Kelola Pemerintahan .....	72
Tabel 4. 3 Data Layanan Aplikasi.....	74
Tabel 4. 4 Spesifikasi Server.....	78
Tabel 4. 8 Kelemahan teknologi terkini.....	80
Tabel 4. 6 Impact Area – Reputasi dan Kepercayaan Pelanggan .....	82
Tabel 4. 7 Skala Prioritas Impact Area .....	82
Tabel 4. 8 Aset-aset kritis untuk portal layanan aplikasi .....	84
Tabel 4. 9 Information Asset Profiling – Transaksi Layanan Informasi .....	84
Tabel 4. 10 Information Asset Risk Environment (Technical) – Transaksi Layanan Informasi .....	87
Tabel 4. 11 Information Asset Risk Environment (Physical) – Transaksi Layanan Informasi .....	87
Tabel 4. 12 Information Asset Risk Environment (People) – Transaksi Layanan Informasi .....	88

Tabel 4. 13 area of concern .....	89
Tabel 4. 14 Information Asset Risk Worksheets .....	91
Tabel 4. 15 Identifikasi Risiko Ancaman.....	94
Tabel 4. 16 score of impact area .....	95
Tabel 4. 17 Score of impact area – area of concern 1 .....	95
Tabel 4. 18 Score of impact area – area of concern 2 .....	96
Tabel 4. 19 Score of impact area – area of concern 3 .....	96
Tabel 4. 20 Score of impact area – area of concern 4 .....	97
Tabel 4. 21 Relative Risk Matrix .....	98
Tabel 4. 22 Mitigation Approach .....	99