

DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN SURAT PERNYATAAN.....	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN.....	xvi
RINGKASAN	xvii
<i>ABSTRACT</i>	xviii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah.....	1
B. Perumusan Masalah.....	6
C. Batasan Penelitian.....	6
D. Tujuan Penelitian.....	6
E. Manfaat Penelitian.....	6
BAB II TINJAUAN PUSTAKA	
A. Konsep Dasar Sistem Informasi.....	8
B. Aset Informasi.....	16
C. Keamanan Informasi.....	17
D. Manajemen Risiko.....	21
E. Fungsi Manajemen Risiko.....	22

F. Proses Manajemen Risiko.....	23
G. OCTAVE-S.....	25
H. Kelebihan OCTAVE-S.....	32
I. Hasil OCTAVE-S.....	33
J. Penelitian Sebelumnya.....	34
BAB III METODE PENELITIAN	
A. Tempat dan Waktu Penelitian.....	39
B. Metode Pengumpulan Data.....	39
C. Alat dan Bahan Penelitian.....	41
D. Konsep Penelitian.....	42
BAB IV PEMBAHASAN	
A. Gambaran Objek Penelitian.....	45
B. Hasil Analisis Metode OCTAVE-S.....	47
1. Fase 1 Membangun Aset Berbasis Profil Ancaman.....	47
a. Proses 1: Identifikasi Informasi Organisasi.....	47
b. Proses 2: Membuat Profil Ancaman.....	79
2. Fase 2 Identifikasi Kerentanan Infrastruktur.....	88
a. Proses 3: Melakukan Perhitungan Aset Kritis yang Berhubungan dengan Aset Organisasi.....	88
3. Fase 3 Mengembangkan Strategi Keamanan dan Rencana Mitigasi.....	90
a. Proses 4: Mengidentifikasi dan Menganalisis Risiko.....	90
b. Proses 5: Mengembangkan Perlindungan Strategi dan Rencana Mitigasi	97
C. Rekomendasi.....	103
BAB V PENUTUP	
A. Kesimpulan.....	106
B. Saran.....	107

DAFTAR PUSTAKA
LAMPIRAN



DAFTAR TABEL

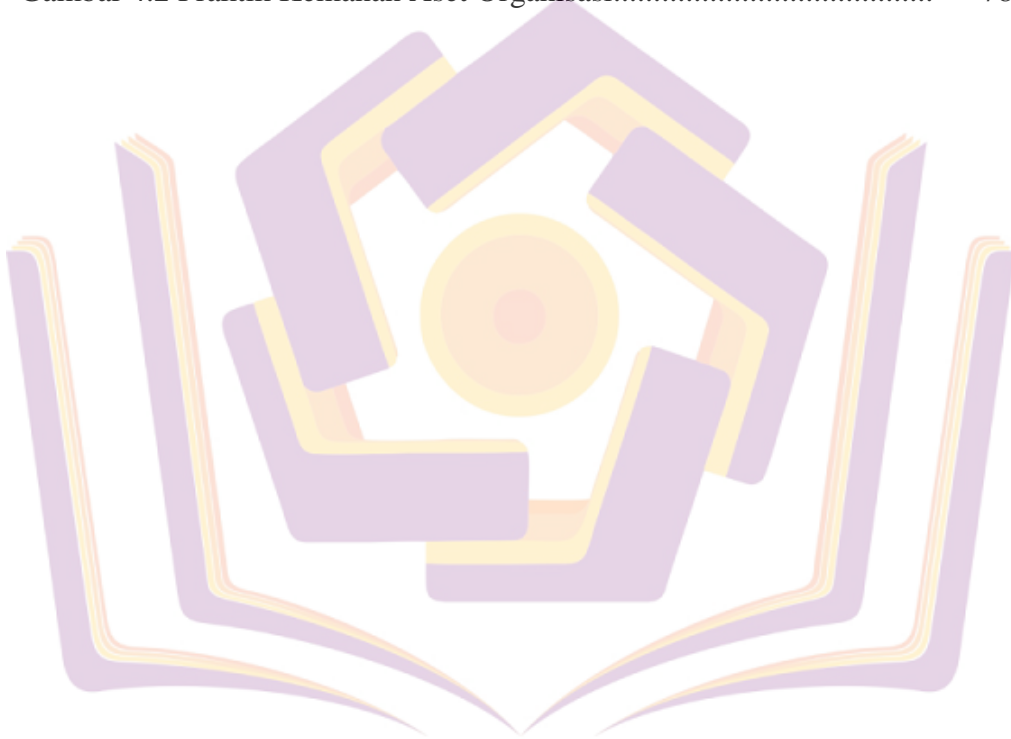
Tabel 2.1 Fase, Proses dan aktivitas metode OCTAVE-S.....	27
Tabel 2.2 Perbandingan Penelitian Sebelumnya.....	36
Tabel 4.1 Kriteria Evaluasi Dampak Secara Umum.....	48
Tabel 4.2 Kriteria Evaluasi Dampak Terhadap Sistem	51
Tabel 4.3 Identifikasi Aset Informasi.....	54
Tabel 4.4 Identifikasi Aset Perangkat Keras.....	55
Tabel 4.5 Identifikasi Aset Pengguna.....	56
Tabel 4.6 Kesadaran dan Pelatihan Keamanan.....	57
Tabel 4.7 Strategi Keamanan.....	59
Tabel 4.8 Manajemen Keamanan.....	59
Tabel 4.9 Peraturan dan Kebijakan Keamanan.....	61
Tabel 4.10 Kolaborasi Manajemen Keamanan.....	62
Tabel 4.11 Rencana Kemungkinan/Pemulihan Bencana.....	63
Tabel 4.12 Pengendalian Akses Fisisk.....	65
Tabel 4.13 Pemantauan dan Audit Keamanan.....	67
Tabel 4.14 Manajemen Jaringan dan Sistem.....	68
Tabel 4.15 Pemantauan dan Audit Keamanan IT.....	70
Tabel 4.16 Pengesahan dan Otorisasi.....	71
Tabel 4.17 Manajemen <i>Vulnerability</i>	72
Tabel 4.18 <i>Enkripsi</i>	73
Tabel 4.19 Desain dan Arsitektur Keamanan.....	75
Tabel 4.20 Manajemen Insiden.....	76
Tabel 4.21 Keamanan Aset Organisasi.....	77
Tabel 4.22 Risiko Sistem Informasi pada Rumah Sakit Wishnu Husada Banyumas.....	85

Tabel 4.23 Risiko <i>Hardware</i> pada Rumah Sakit Wishnu Husada Banyumas.....	86
Tabel 4.24 Risiko Keamanan pada Rumah Sakit Wishnu Husada Banyumas.....	87
Tabel 4.25 Rekomendasi.....	103



DAFTAR GAMBAR

Gambar 1.1 Perbandingan Metode Manajemen Risiko.....	5
Gambar 2.1 Proses Metode OCTAVE-S.....	26
Gambar 3.1 Konsep Penelitian.....	42
Gambar 4.1 Struktur Organisasi.....	46
Gambar 4.2 Praktik Keamanan Aset Organisasi.....	78



DAFTAR LAMPIRAN

Lampiran 1 Data Wawancara

Lampiran 2 Dokumen Manajemen Risiko Menggunakan Metode OCTAVE-S

Lampiran 3 Keterangan Penelitian

Lampiran 4 Kartu Bimbingan Skripsi

Lampiran 5 Dokumentasi

