

## ABSTRAK

Kata Kunci: PT. Pos Bandung, ancaman, aset, keamanan, kontrol.

Sistem Informasi sangat berperan penting dalam berbagai kegiatan, termasuk PT. Pos Bandung. Banyak kemudahan yang diberikan dengan adanya sistem informasi yang berjalan dengan baik. Dibalik kemudahan yang ditawarkan oleh sistem informasi terdapat banyak ancaman yang sewaktu-waktu dapat menyerang yang dapat menimbulkan masalah dan kerugian terhadap aset yang ada pada PT. Pos Bandung. Aset sistem informasi dapat dibagi menjadi dua bagian yaitu, aset fisik yang terdiri dari personil, perangkat keras, fasilitas dan penunjang dan aset logis yang terdiri dari perangkat lunak, sistem operasi dan aplikasi perangkat lunak. Ancaman yang dapat menyerang aset PT. Pos seperti, gempa bumi, kebakaran, banjir, ancaman teroris, peperangan, pemalsuan data, kesalahan input data, personil yang kurang latihan, pencurian terhadap aset, pemadaman listrik, korsleting listrik, ketidak stabilan arus listrik dan virus. Jika aset sistem informasi PT. Pos Bandung mengalami ancaman atau masalah maka sistem informasi di PT. Pos Bandung tidak akan berjalan baik atau bahkan tidak berjalan sama sekali. Untuk mengatasi masalah dan ancaman, PT. Pos Bandung membutuhkan sebuah kontrol terhadap manajemen keamanan sistem yang berfungsi untuk mengontrol aset sistem informasi pada PT. Pos Bandung jika terjadi suatu ancaman. Dengan kontrol ini diharapkan dapat mengurangi atau mencegah kerugian yang dialami oleh PT. Pos Bandung atau kerugian yang dialami masih pada tahap level yang masih dapat diterima.

## ABSTRACT

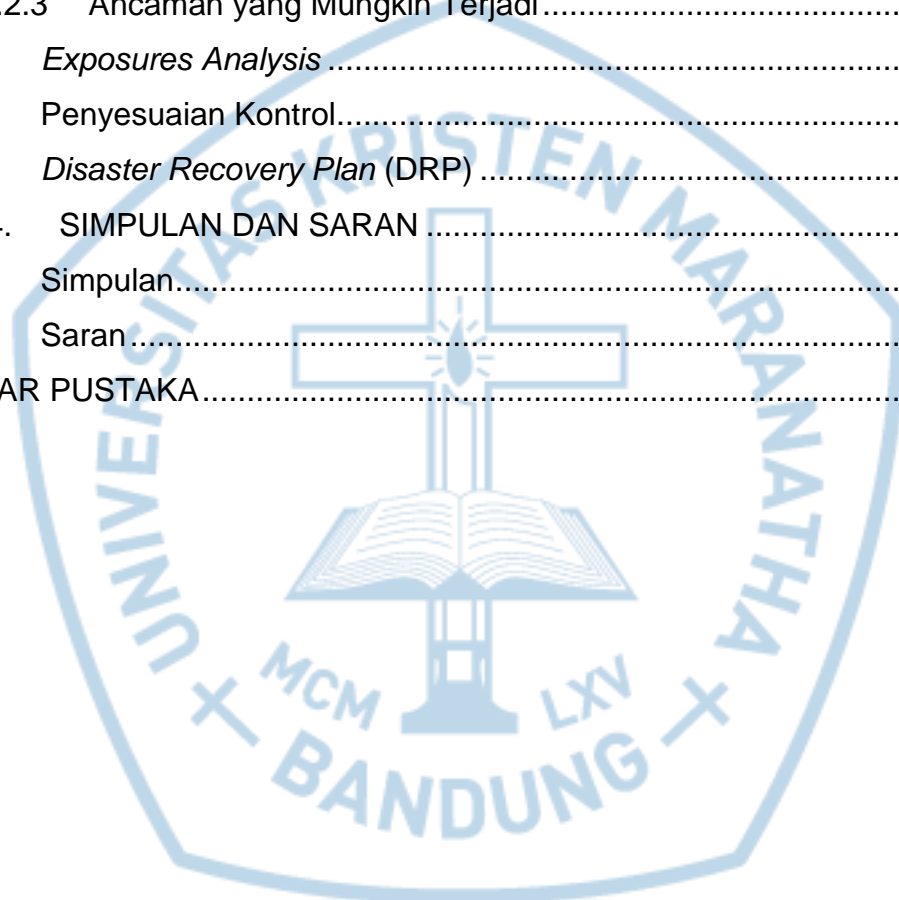
*Keywords: PT. Pos Bandung, assets, control , security, threats.*

*Information system plays important role in every activities, including for PT. Pos Bandung's. Simplicity is offered along with a good information system available. Behind the ease and simplicity offered, there are many threats which may potentially cause problems and inflict loses on PT. Pos Bandung's assets. Information system's assets can be divided into two parts: The physical assets including personel, hardware, facilities and supporting facilities, and The logical assets including software, operating system and software applications. Threats which can attack PT. Pos Bandung's assets including earthquake, fire, flood, terrorist attack, war, data fabrication, data input failure, personel's lack of training, stolen assets, electrical black-out, electrical shorting, electrical instability and virus. If the PT. Pos Bandung's information system's assets experience threats or problems, the system will not run effectively or even stop working. To counter problems and threats, PT. Pos Bandung's needs a control over the system's security management which controls PT. Pos Bandung's information system's assets should there be any threats posed. By the control, it is hoped that it may reduce or event preventthe loss faced by PT. Pos Bandung's or keep the loss on an acceptable level.*

## DAFTAR ISI

LEMBAR PENGESAHAN .....	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN .....	i
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN .....	i
PRAKATA .....	i
ABSTRAK .....	ii
ABSTRACT .....	iii
DAFTAR ISI .....	iv
DAFTAR GAMBAR .....	vi
DAFTAR TABEL .....	vii
DAFTAR LAMPIRAN .....	viii
DAFTAR SINGKATAN .....	ix
BAB 1. PENDAHULUAN .....	1
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	2
1.3 Tujuan Pembahasan .....	2
Ruang Lingkup Kajian .....	3
1.4 Sumber Data .....	3
1.5 Sistematika Penyajian .....	3
BAB 2. KAJIAN TEORI .....	4
2.1 Kontrol .....	4
Tipe-Tipe Kontrol (Perbaikan) .....	4
2.2 <i>Security Management</i> .....	5
2.2.1 Aset–Aset .....	6
2.2.2 Ancaman .....	7
2.3 <i>Exposures Analysis</i> .....	10
2.4 <i>Disaster Recovery Plan (DRP)</i> .....	12
BAB 3. ANALISIS DAN HASIL PENELITIAN .....	13
3.1 Identifikasi Aset .....	13

3.1.1	Aset Fisik.....	13
3.1.2	Aset Logik .....	22
3.2	Identifikasi Ancaman.....	23
3.2.1	Identifikasi Ancaman terhadap Aset Fisik PT. Pos Bandung....	23
3.2.2	Identifikasi Ancaman Aset Logik PT. Pos Bandung.....	25
3.2.3	Ancaman yang Mungkin Terjadi.....	25
3.3	<i>Exposures Analysis</i> .....	26
3.4	Penyesuaian Kontrol.....	43
3.5	<i>Disaster Recovery Plan (DRP)</i> .....	49
BAB 4.	SIMPULAN DAN SARAN .....	55
4.1	Simpulan.....	55
4.2	Saran.....	56
DAFTAR PUSTAKA	.....	57



## DAFTAR GAMBAR

Gambar 2.1 Kategori Aset Sistem Informasi .....	6
Gambar 2.2 Tahapan <i>Exposure Analysis</i> .....	11
Gambar 3.1 Gedung PT. Pos Bandung .....	18
Gambar 3.2 Ruang Kerja di Gedung Wahana Bhakti Pos .....	19
Gambar 3.3 Ruang Rapat di salah satu lantai Gedung Wahana Bakti Pos ..	20
Gambar 3.4 Gudang PT. Pos Bandung .....	20
Gambar 3.5 Ruang Tamu di salah satu lantai Gedung Wahana Bhakti Pos.	21
Gambar 3.6 Ruang genset dan pengaturan PT. Pos Bandung.....	21



## DAFTAR TABEL

Tabel 2.1 Skenario <i>exposure analysis</i> .....	11
Tabel 3.1 Aset <i>Hardware</i> PT. Pos Bandung .....	17
Tabel 3.2 <i>Software</i> Aplikasi PT Pos Bandung .....	22
Tabel 3.3 <i>System Software</i> PT. Pos Bandung .....	23
Tabel 3.4 Analisa peluang ancaman .....	26
Tabel 3.5 Analisa ancaman gempa bumi .....	27
Tabel 3.6 Analisa ancaman banjir .....	30
Tabel 3.7 Analisa ancaman kebakaran .....	32
Tabel 3.8 Analisa ancaman kerusakan <i>hardware</i> .....	34
Tabel 3.9 Analisa ancaman pencurian .....	35
Tabel 3.10 Analisa ancaman listrik padam/listrik tidak stabil .....	36
Tabel 3.11 Analisa ancaman software error .....	38
Tabel 3.12 Analisa ancaman <i>virus</i> .....	39
Tabel 3.13 Analisa ancaman <i>spam</i> .....	40
Tabel 3.14 Analisa ancaman <i>hacking</i> .....	41
Tabel 3.15 Analisa ancaman <i>employee errors</i> .....	42
Tabel 3.16 Penyesuaian kontrol kerusakan <i>hardware</i> .....	44
Tabel 3.17 Penyesuaian kontrol ancaman pencurian .....	45
Tabel 3.18 Penyesuaian kontrol listrik padam/listrik tidak stabil .....	46
Tabel 3.19 Penyesuaian kontrol <i>software error</i> .....	47
Tabel 3.20 Penyesuaian kontrol ancaman virus .....	47
Tabel 3.21 Penyesuaian kontrol ancaman <i>spam</i> .....	48
Tabel 3.22 Penyesuaian kontrol ancaman <i>hacking</i> .....	48
Tabel 3.23 Penyesuaian kontrol ancaman <i>employee errors</i> .....	49
Tabel 3.24 <i>Disaster Recovery Plan</i> ancaman gempa bumi .....	50
Tabel 3.25 <i>Disaster Recovery Plan</i> ancaman banjir .....	51
Tabel 3.26 <i>Disaster Recovery Plan</i> ancaman kebakaran .....	53

## DAFTAR LAMPIRAN

LAMPIRAN A. pHasil Wawancara.....	58
LAMPIRAN B. Gambar-Gambar.....	63



## DAFTAR SINGKATAN

PT.POS	BUMN yang bergerak dibidang logistik,pengiriman barang.
UPS	Uninterruptible Power Supply
CCTV	Closed Circuit Television
SPV	Supervisor
Provider	Penyedia layanan jasa

