

ABSTRAK

Sebagai dinas yang memiliki peranan penting di bidang komunikasi, informatika dan hubungan masyarakat di kota Bandung, DISKOMINFO memiliki aset-aset sistem informasi yang dapat menunjang tugas dan tanggung jawab yang ada. Aset-aset sistem informasi yang terdiri dari aset fisik dan aset logik perlu mendapatkan kontrol yang tepat agar keamanan aset-aset dari ancaman yang terjadi dapat terjamin. Menjamin adanya keamanan terhadap aset-aset sistem informasi diperlukan identifikasi aset, identifikasi ancaman, dan identifikasi kontrol yang diterapkan dalam DISKOMINFO Kota Bandung sehingga kontrol-kontrol yang seharusnya diterapkan pun dapat teridentifikasi. Dengan teridentifikasinya aset, ancaman, dan kontrol yang ada, maka ditemukan masih lemahnya kontrol di beberapa kejadian-kejadian yang dapat menjadi ancaman bagi aset-aset sistem informasi. Oleh karena itu, DISKOMINFO Kota Bandung diharapkan segera menerapkan kontrol-kontrol yang tepat untuk menjaga aset-aset sistem informasi yang dimiliki dari kejadian-kejadian yang dapat menjadi ancaman.

Kata Kunci: ancaman, aset, DISKOMINFO Bandung, keamanan, kontrol

ABSTRACT

As a government department, DISKOMINFO consists of communication sector, information sector, and public relations sector has information systems assets that can support the tasks and responsibilities. Information systems assets of DISKOMINFO Bandung consists of Physical assets and logic assets. the assets needs to get proper control to ensure the security of assets. To ensure the security of assets, necessary identification of assets, identification of the threats, identification of the control of DISKOMINFO Bandung, so the control should be applied can be identified. With the identification of assets, threats, and existing controls, it was found weak controls in some event that could be threaten the information systems assets. Therefore, DISKOMINFO Bandung expected to implement the proper controls soon to protect the information systems assets of DISKOMINFO Bandung from the threats.

Keywords: assets, control, DISKOMINFO, security, threats

DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xii
DAFTAR SINGKATAN	xiii
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup Kajian	3
1.5 Sumber Data	3
1.6 Sistematika Penyajian	3
BAB 2. KAJIAN TEORI	4
2.1 Kontrol	4
2.1.1 Tipe-Tipe Kontrol	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	28

3.2	Identifikasi Ancaman.....	30
3.2.1	Identifikasi Ancaman terhadap Aset Fisik DISKOMINFO Kota Bandung	30
3.2.2	Identifikasi Ancaman terhadap Aset Logik DISKOMINFO Kota Bandung	30
3.2.3	Ancaman yang Mungkin Terjadi.....	31
3.3	<i>Exposures Analysis</i>	32
3.4	Penyesuaian Kontrol.....	48
3.5	<i>Disaster Recovery Plan (DRP)</i>	54
BAB 4.	SIMPULAN DAN SARAN	59
4.1	Simpulan.....	59
4.2	Saran	60
	DAFTAR PUSTAKA.....	61

DAFTAR GAMBAR

Gambar 2.1 Kategori Aset Sistem Informasi	6
Gambar 2.2 Tahapan <i>Exposure Analysis</i>	11
Gambar 3.1 Gedung DISKOMINFO Kota Bandung	25
Gambar 3.2 Ruang Server pada Bidang Telematika	26
Gambar 3.3 Ruang Server pada Bidang Telematika	26
Gambar 3.4 Ruang Bidang Telematika DISKOMINFO Kota Bandung.....	27
Gambar 3.5 Ruang Bidang Telematika DISKOMINFO Kota Bandung.....	27
Gambar 3.6 Ruang Diseminasi Informasi DISKOMINFO Kota Bandung	28

DAFTAR TABEL

Table 2.1 Skenario <i>exposure analysis</i>	11
Table 3.1 Aset <i>Hardware</i> DISKOMINFO Kota Bandung	22
Table 3.2 <i>Software</i> Aplikasi DISKOMINFO Kota Bandung	29
Table 3.3 <i>System Software</i> DISKOMINFO Kota Bandung.....	29
Table 3.4 Analisa ancaman gempa bumi	32
Table 3.5 Analisa ancaman banjir	35
Table 3.6 Analisa ancaman kebakaran	36
Table 3.7 Analisa ancaman kerusakan <i>hardware</i>	39
Table 3.8 Analisa ancaman pencurian.....	40
Table 3.9 Analisa ancaman listrik padam/listrik tidak stabil	42
Table 3.10 Analisa ancaman software error	43
Table 3.11 Analisa ancaman virus	44
Table 3.12 Analisa ancaman <i>spam</i>	45
Table 3.13 Analisa ancaman <i>hacking</i>	46
Table 3.14 Analisa ancaman <i>employee errors</i>	47
Table 3.15 Penyesuaian kontrol kerusakan <i>hardware</i>	49
Table 3.16 Penyesuaian kontrol ancaman pencurian	49
Table 3.17 Penyesuaian kontrol listrik padam/listrik tidak stabil	51
Table 3.18 Penyesuaian kontrol <i>software error</i>	51
Table 3.19 Penyesuaian kontrol ancaman virus	52
Table 3.20 Penyesuaian kontrol ancaman <i>spam</i>	53
Table 3.21 Penyesuaian kontrol ancaman <i>hacking</i>	53
Table 3.22 Penyesuaian kontrol ancaman <i>employee errors</i>	54
Table 3.23 <i>Disaster Recovery Plan</i> ancaman gempa bumi	55
Table 3.24 <i>Disaster Recovery Plan</i> ancaman banjir	56
Table 3.25 <i>Disaster Recovery Plan</i> ancaman kebakaran	57

DAFTAR LAMPIRAN

LAMPIRAN A. Hasil Wawancara.....	62
LAMPIRAN B. Gambar-Gambar.....	69

DAFTAR SINGKATAN

DISKOMINFO	Dinas Komunikasi dan Informatika
SKPD	Satuan Kerja Perangkat Daerah
UPS	Uninterruptible Power Supply
CCTV	Closed Circuit Television