

ABSTRAK

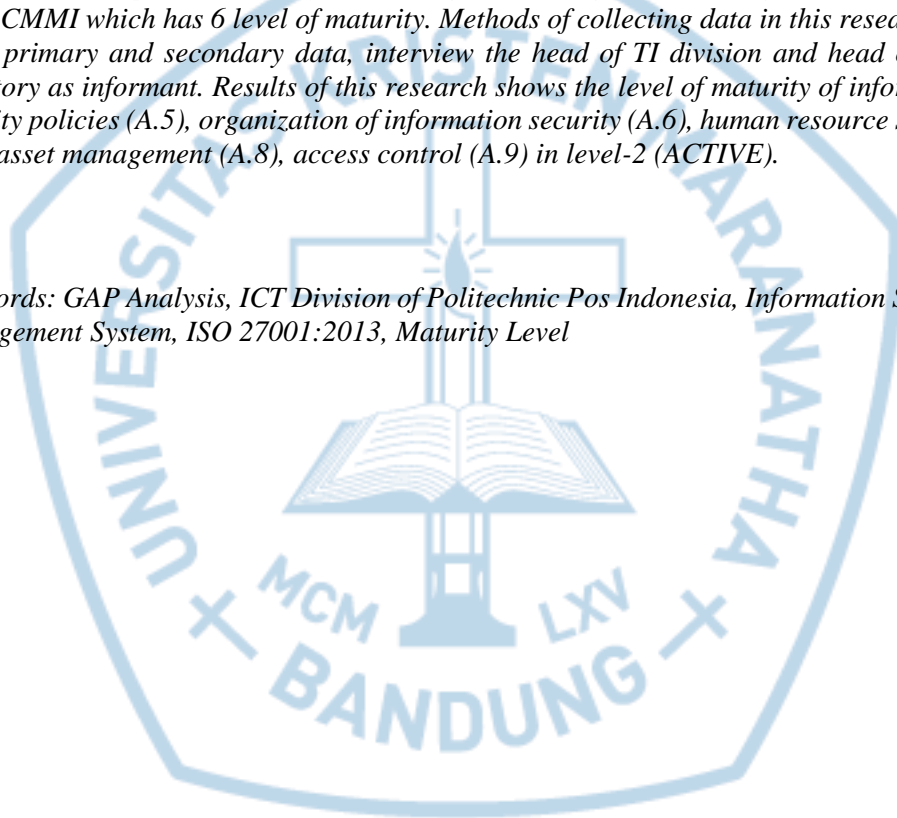
Informasi adalah salah satu aset penting dan sangat berharga bagi suatu organisasi ataupun institusi. Salah satu elemen penting dalam tata kelola organisasi yang baik adalah keamanan informasi. Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisir risiko bisnis (*reduce business risk*) dan memaksimalkan, serta mempercepat pengembalian investasi dan peluang bisnis. Hal tersebut diatur dalam sebuah sistem manajemen keamanan informasi yang menjamin tiga aspek penting yang dikenal dengan sebutan CIA, yaitu *Confidentiality*, *Integrity*, *Availability*. Untuk memastikan apakah sistem informasi yang telah dirancang dan diterapkan sesuai dengan prosedur dan standar yang telah ditetapkan berdasarkan ISO 27001:2013, maka Divisi TIK Politeknik Pos Indonesia perlu melakukan analisis untuk menentukan tingkat kematangan terhadap sistem informasi yang ada dengan menggunakan enam tingkat kematangan CMMI. Penelitian bersifat deskriptif kualitatif, dilakukan analisis pada 5 annex ISO 27001:2013 dengan teknik pengumpulan data primer dan sekunder, wawancara yang dilakukan dengan Kepala Divisi TIK dan Ketua Inventaris Aset sebagai narasumber. Dari hasil penelitian yang dilakukan, diketahui tingkat kematangan *information security policies* (annex 5), *organization of information security* (annex 6), *human resource security* (annex 7), *asset management* (annex 8), *access control* (annex 9) berada pada tingkat 2 – AKTIF.

Kata kunci: *GAP Analysis*, ISO 27001:2013, Sistem Manajemen Keamanan Informasi, Tingkat Kematangan, Divisi TIK Politeknik Pos Indonesia

ABSTRACT

Information is one of the important assets which is very valuable to an organization or institution. One of important elements in good corporate governance is technology information organization, including governance of information security. Information security is the practice of defending information from all possible threats in an attempt to ensure or guarantee the continuity of business, minimizes and maximizes the risk of business and accelerates a return on investments and business opportunities. Information security management systems in an organization must be guarantee the most three important aspects called CIA namely Confidentiality, Integrity and Availability. To make sure whether the information system has been designed and implemented, TI division of Pos Indonesia Polytechnic need to analyze them in accordance with the procedures and standards that have been applied according to ISO 27001: 2013. This research is using qualitative descriptive method by conducting an auditing on 5 annex of ISO 27001:2013, using CMMI which has 6 level of maturity. Methods of collecting data in this research are using primary and secondary data, interview the head of TI division and head of asset inventory as informant. Results of this research shows the level of maturity of information security policies (A.5), organization of information security (A.6), human resource security (A. 7)asset management (A.8), access control (A.9) in level-2 (ACTIVE).

Keywords: GAP Analysis, ICT Division of Politechnic Pos Indonesia, Information Security Management System, ISO 27001:2013, Maturity Level



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 SINGKATAN	xii
DAFTAR ISTILAH	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup.....	3
1.5 Sumber Data.....	5
1.6 Sistematika Penyajian	5
BAB 2 KAJIAN TEORI	7
2.1 Data	7
2.2 Informasi	7
2.3 Sistem Manajemen Keamanan Informasi	8
2.3.1 Struktur Dokumentasi Sistem Manajemen Keamanan Informasi.....	8
2.4 Manajemen Keamanan Informasi	10

2.5 Keamanan Informasi	10
2.6 Prinsip Keamanan Informasi.....	11
2.7 Ruang Lingkup Keamanan Informasi	13
2.8 ISO 27000	14
2.9 ISO 27001	15
2.10 Maturity Level Model	16
BAB 3 ANALISIS DAN HASIL PENELITIAN.....	20
3.1 Analisis Studi Kasus	20
3.1.1 Divisi TIK Politeknik Pos Indonesia	20
3.1.2 Visi Dan Misi	20
3.1.3 Struktur Divisi TIK	21
3.1.3.1 Bagan Struktur Divisi TIK Politeknik Pos Indonesia	21
3.1.3.2 Uraian Tugas	22
3.1.4 Karakteristik Responden	23
3.1.4.1 Karakteristik Responden Berdasarkan Jobdesk	23
3.2 Hasil Wawancara	24
3.3 Hasil Analisis	26
BAB 4 SIMPULAN DAN SARAN.....	40
4.1 Simpulan	40
4.2 Saran.....	43
DAFTAR PUSTAKA	44
LAMPIRAN A – DAFTAR PERTANYAAN.....	A-1
LAMPIRAN B – BUKTI FOTO.....	B-1

DAFTAR GAMBAR

Gambar 2-1 Struktur Dokumentasi SMKI	9
Gambar 2-2 Ruang Lingkup Keamanan Informasi	14
Gambar 2-3 Hubungan Antar Standar Keluarga SMKI.....	15
Gambar 2-4 Hubungan Tingkat Kematangan dan Kelengkapan Pengamanan.....	17
Gambar 3-1 Bagan Struktur Divisi TIK Politeknik Pos Indonesia.....	21



DAFTAR TABEL

Tabel 3-1 Uraian Tugas Pada Divisi TIK Politeknik Pos Indonesia.....	22
Tabel 3-2 Annex 5 <i>Information Security Policies</i>	26
Tabel 3-3 Annex 6 <i>Organization of Information Security</i>	27
Tabel 3-4 Annex 7 <i>Human Resource Security</i>	29
Tabel 3-5 Annex 8 <i>Asset Management</i>	32
Tabel 3-6 Annex 9 <i>Access Control</i>	35
Tabel 4-1 Penilaian Tingkat Kematangan (Maturity Level)	40



DAFTAR SINGKATAN

CIA	<i>Confidentially, Integrity, Availability</i>
CMMI	<i>Capability Maturity Model Integration</i>
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
ISMS	<i>Information Security Management System</i>
ITIL	<i>Information Technology Infrastructure Library</i>
Poltekpos	Politeknik Pos Indonesia
SDM	Sumber Daya Manusia
SI	Sistem Informasi
SMKI	Sistem Manajemen Keamanan Informasi
TIK	Teknologi Informasi Komunikasi
YPBPI	Yayasan Pendidikan Bhakti Pos Indonesia



DAFTAR ISTILAH

<i>Evidence</i>	Sesuatu yang menyatakan kebenaran suatu peristiwa; keterangan nyata; tanda.
<i>Stakeholder</i>	Seseorang yang mempunyai minat dan kepentingan dalam perusahaan; seperti kepentingan finansial dan sebagainya.
<i>Single Sign On</i>	teknologi yang mengizinkan pengguna jaringan atau <i>user</i> agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja.

