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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

CIA	*Confidentially, Integrity, Availability*
CMMI	*Capability Maturity Model Integration*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ISMS	*Information Security Management System*
ITIL	*Information Technology Infrastructure Library*
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

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