ANALISIS DAN PERANCANGAN MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5 DI PT. POS INDONESIA

ANALYSIS AND DESIGN OF INFORMATION SECURITY MANAGEMENT USING THE COBIT 5 FRAMEWORK AT PT. POS INDONESIA

Satria Dwi Widiyanto, Dr. Ir. Lukman Abdurrahman, MIS[2], Rokhman Fauzi, S.T, M.T.[3]
[1]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[2]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]satriadwii@student.telkomuniversity.ac.id, [2]abdural@telkomuniversity.ac.id
[3]rokhmanfauzi@telkomuniversity.ac.id

ABSTRAK

Saat ini manajemen keamanan informasi menjadi hal yang sangat penting dalam menggunakan teknologi informasi, PT Pos Indonesia (Persero) sudah menerapkan teknologi informasi pada proses bisnisnya. Untuk melindungi asset penting pada perusahaan maka diperlukan adanya penilaian terhadap manajemen keamanan informasi yang sudah diterapkan pada PT Pos Indonesia (Persero). Analisis dan perancangan ini menggunakan kerangka kerja COBIT 5 dengan domain APO 13 (Manage Security) dan DSS05 (Manage Security Service) sebagai acuan dalam menilai keamanan informasi pada PT Pos Indonesia (Persero). Penelitian ini mengacu pada referensi dari penelitian sebelumnya yang menggunakan kerangka kerja COBIT 5 pada perusahaan lain. Metode yang digunakan dalam penelitian ini adalah dengan cara melakukan observasi, wawancara dan analisis data. Hasil penilaian berupa analisis kesenjangan, analisis risiko yang digunakan untuk menentukan prioritas risiko serta hasil dari perancangan penelitian ini yaitu rekomendasi kontrol dan berupa kebijakan keamanan informasi yang bisa dijadikan referensi untuk PT Pos Indonesia (Persero) di kemudian hari dalam mengelola keamanan informasi perusahaannya.

Kata Kunci: Keamanan Informasi, COBIT 5, Analisis Risiko, Kebijakan

ABSTRACT

Currently information security management is very important in using information technology, PT Pos Indonesia (Persero) has implemented information technology in its business processes. To protect important assets in the company, it requires obligations to information management that have been applied to PT Pos Indonesia (Persero). This analysis and design uses a framework of COBIT 5 with the domain APO 13 (Manage Security) and DSS05 (Manage Security Service) as a reference for assessing information security at PT Pos Indonesia (Persero). This study refers to references from previous studies using the COBIT 5 framework in other companies. The method used in this research is by means of observation, interviews and data analysis. The research results are in the form of risk analysis, risk analysis used to determine risk and the results of this study are control recommendations and policy policies that can be used as references for PT Pos Indonesia (Persero) in the future in its company information organization.

Keywords: Information Security, COBIT 5, Risk Analysis, Policy

1. PENDAHULUAN

Teknologi informasi merupakan ilmu yang meliputi teknologi komunikasi untuk memproses, menyimpan data dan mengirimkan informasi melalui jalur komunikasi yang cepat [1]. Dalam keamanan informasi melindungi kerahasiaan, integritas dan ketersediaan aset informasi penyimpanan, pemrosesan atau transmisi. Direalisasikan melakui kebijakan, pendidikan, pelatihan kesadaran dan penerapan teknologi hal ini yang menjadi fokus di organisasi maupun perusahaan dalam menjaga data informasi perusahaan.

Keamanan informasi penting dalam memastikan keamanan aset TI dalam suatu organisasi. Kerangka kerja yang dapat menganalisis peristiwa terkait keamanan informasi dan bagaimana kondisi tersebut bisa ditangani agar peristiwa yang terjadi dapat diantisipasi dan dapat mengontrol dampak dari risiko yang didapat.

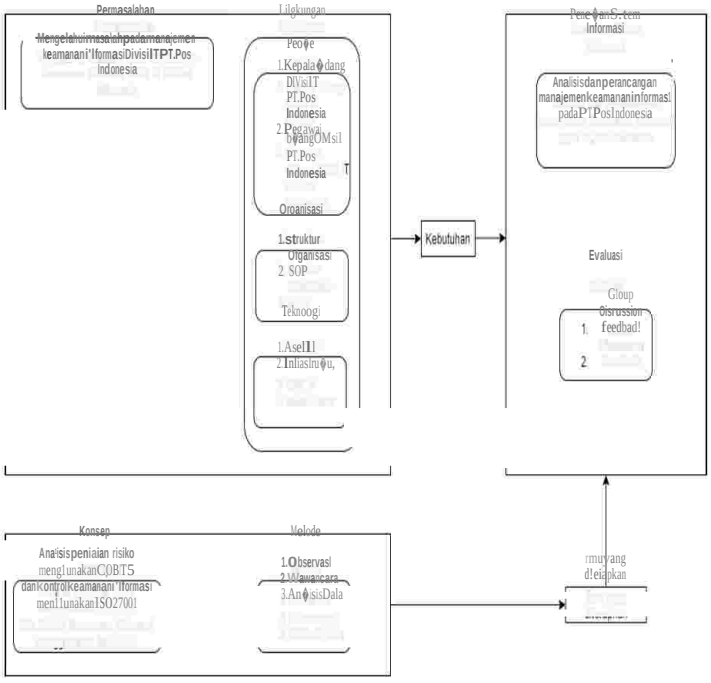
Keamanan informasi adalah melindungi informasi dari kemungkinan ancaman untuk memastikan kelangsungan bisnis, mengurangi tingkat risiko dan mempercepat atau memaksimalkan keputusan investasi dan peluang bisnis [6]. PT Pos Indonesia (Persero) perusahaan BUMN yang bergerak pada bidang layanan pos dan logistik. Data informasi pada perusahaan sangat penting sehingga harus diterapkan keamanan informasi yang dapat menjamin kerahasiaan, integritas, ketersediaan, keutuhan data tersebut. Pengamanan data perusahaan ialah cara untuk mengamankan data penting yang dimiliki oleh perusahaan baik dalam perangkat fisik maupun perangkat lunak. Penjagaan informasi perlu dilakukan pada faktor-faktor yang dapat menjadi pemicu resiko, perusahaan wajib memperhatikan faktor keamanan jaringan, faktor eksternal dan faktor penghubung pada bagian yang berkaitan langsung dengan proses pengolahan data.

COBIT 5 merupakan sekumpulan IT *best practice* untuk tata kelola IT yang dapat membantu organisasi, perusahaan, lembaga pemerintahan, perguruan tinggi, atau individual dalam menganalisa kesenjangan (gap) antara kebutuhan bisnis, kebutuhan control dan kebutuhan Teknis IT [2].

Hasil penilaian berupa analisis kesenjangan, analisis risiko yang digunakan untuk menentukan prioritas risiko serta hasil dari perancangan penelitian ini yaitu rekomendasi kontrol dan berupa kebijakan keamanan informasi yang bisa dijadikan referensi untuk PT Pos Indonesia (Persero) di kemudian hari dalam mengelola keamanan informasi perusahaannya.

2. METODE PENELITIAN

Dalam melakukan penelitian dijelaskan dalam gambar di bawah ini:



Gambar 1 Model Konseptual

Dalam model konseptual COBIT 5 pada fokus APO13 dan DSS05. Peneliti menggunakan PT Pos Indonesia (Persero) sebagai obyek untuk penelitian, Penelitian ini dimulai dengan menganalisis masalah pada manajemen keamanan informasi yang ada pada PT Pos Indonesia (Persero). Pada aspek lingkungan terdapat bagian *People* yaitu kepada bidang atau manajer divisi IT sebagai orang yang memiliki hak atas informasi terkait keamanan informasi dan pegawai divisi IT yang membantu untuk mencari masalah apa saja yang terjadi pada asset IT. Selanjutnya pada bagian organisasi terdapat struktur organisasi dan SOP, serta pada aspek teknologi terdapat asset IT dan infrastruktur yang menjadi pusat dalam menilai keamanan informasinya. Peneliti menggunakan metode observasi, wawancara, analisis data untuk mendapatkan data. Konsep yang digunakan yaitu analis penilaian risiko menggunakan COBIT 5 serta untuk kontrol keaman informasi menggunakan referensi dari ISO27001.

3. PT POS INDONESIA (Persero)

Pada tahap ini menjelaskan mengenai profil perusahaan PT. Pos Indonesia (Persero).

Pos Indonesia memiliki jaringan yang berdedikasi, sistem distribusi yang handal, pelacakan dan penelusuran, pelayanan prima, kecepatan, ketepatan dan harga yang kompetitif. Kantor pos merupakan tempat yang strategis untuk transaksi penjualan dan / atau distribusi barang dan jasa. PT Pos Indonesia terus melakukan inovasi, diantaranya pembangunan toko pos, pengembangan bisnis retail yang bertujuan untuk mengubah citra kantor pos modern dengan model one stop shopping service yaitu layanan pos berupa jasa pos, parsel, dan jasa, keuangan, penjualan barang pos stempel, prangko, produk filateli, dan layanan belanja online [3].

3.1 Visi, Misi PT Pos Indonesia (Persero)

1. **Visi**

   Menjadi pilihan utama layanan logistik dan jasa keuangan.

2. **Misi**

   a. Memberikan solusi layanan logistik e-commerce yang kompetitif
   b. Menjalankan fungsi designated operator secara profesional dan kompetitif
   c. Memberikan solusi jasa layanan keuangan terintegrasi yang kompetitif dalam rangka mendukung financial inclusion berbasis digital
   d. Memberikan solusi layanan dokumentasi dan otentikasi digital yang kompetitif

4. ANALISIS

Data yang telah didapat akan dianalisis pada identifikasi aset dan analisis risiko menggunakan COBIT 5. Berikut ini adalah tahapan dari penilaian risiko COBIT 5:

4.1 Identifikasi Asset Teknologi

Tahapan pertama melakukan identifikasi aseet perusahaan, asset dapat dilihat pada tabel 1.

Tabel 1 Identifikasi Asset

No.	Asset Perusahaan
1.	Database
2.	Server
3.	Data Centre
4.	Aplikasi
5.	Komputer/PC
6.	Anti Virus

7.	Firewall
8.	Hub
9.	Switch
10.	Bridge
11.	Router

4.2 Analisis Capability Level

Tahapan melakukan penilaian capability level, hasil capability level dapat dilihat pada tabel 2, Proses APO13 sudah mencapai 87% serta pada proses DSS05 sudah mencapai 87% yang telah berjalan sesuai rencana perusahaan.

Tabel 2 Capability Level

Proses	Capability Level	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
APO13	1	87%	F	N	N	N	N	N	N	N	N
Proses	Capability Level	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS05	1	87%	F	N	N	N	N	N	N	N	N

4.3 Analisis Risiko

Analisis risiko digunakan untuk mengetahui risiko serta penyebab risiko, dalam analisis risiko melakukan penilaian risiko untuk menangani risiko tersebut. Tabel 3 menjelaskan analisis risiko.

Tabel 3 analisis risiko

No	Kategori dalam COBIT 5	Paint Point	Level Kemungkinan	Level Dampak	Risiko	Risk Response
1	*Logical attacks*	Adanya serangan terhadap situs web.	Besar	Rendah	Tinggi	Reduction
		Adanya virus pada komputer.	Sedang	Sangat Rendah	Rendah	Reduction
2	*Network*	Kegagalan dalam mengakses data.	Kecil	Rendah	Rendah	Transfer
		Peralatan yang dapat diakses oleh pemakai yang tidak memiliki otoritas	Kecil	Menengah	Moderat	Reduction
3	*Staff operations (human error and malicious intent)*	Kesalahan karyawan dalam memberikan hak akses pada sistem.	Kecil	Menengah	Moderat	Reduction
		Password yang digunakan tidak pernah diubah dalam rentang waktu yang lama	Besar	Menengah	Tinggi	Reduction
		Peralatan TI yang rusak oleh karyawan.	Besar	Menengah	Tinggi	Reduction
		Kesalahan karyawan	Kecil	Rendah	Rendah	Reduction

		dalam penanganan insiden pada salah satu system.				
4	*Hardware*	Adanya pemindahan peralatan TI tanpa izin	Sedang	Sangat Rendah	Rendah	Reduction
5	*Software*	Teknologi yang digunakan sudah terlalu using dan belum ada pembaharuan	Kecil	Menengah	Moderat	Reduction
		Perangkat lunak yang digunakan belum baik, masih ada permasalahan seperti *bug*, *error* dll.	Kecil	Menengah	Moderat	Reduction
6	*Business ownership of IT*	Bisnis yang belum selaras dengan penggunaan TI.	Kecil	Menengah	Moderat	Reduction
7	*Malware*	Terdapat malware pada asset TI perusahaan.	Sedang	Menengah	Tinggi	Reduction
8	*IT expertise and skills*	Kurang terampilnya karyawan TI sehingga mempengaruhi kualitas keamanan layanan.	Kecil	Rendah	Rendah	Reduction
9	*Information (data breach : damage leakage and access)*	Data hilang, rusak, tidak bisa diakses.	Besar	Menengah	Tinggi	Reduction

5. REKOMENDASI KONTROL DAN REKOMENDASI KEBIJAKAN

5.1 Rekomendasi Kontrol

tahap ini menjadi landasan untuk merekomendasikan usulan mengenai kontrol risiko yang telah ditemukan sebelumnya. Rekomendasi kontrol risiko dilakukan melalui analisis menggunakan COBIT 5 dan diselaraskan dengan menggunakan ISO27001 [4]. Tabel 4 menjelaskan mengenai rekomendasi kontrol risiko.

Tabel 4 Rekomendasi Kontrol

Paint Point	Kategori dalam COBIT 5	ISO27001
Adanya serangan terhadap situs web.	*Logical attacks*	*A.12.2.1 Controls against malware* *A.13.1.2 Security of network*

		services
Adanya virus pada komputer.	*Logical attacks*	*A.12.2.1 Controls against malware* *A.12.5.1 Installation of software on operational systems*
Terdapat malware pada asset TI perusahaan.	*Malware*	*A.12.2.1 Controls against malware* *A.12.5.1*
K d h sistem.		*Information security awareness, education, and training*
Peralatan TI yang rusak oleh karyawan.	*Staff operations (human error and malicious intent)*	*A.7.2.1 Management responsibilities* *A.7.2.3*
K d i s	*Staff operations (human error and malicious intent)*	
K ka seh mem kualita layanan.	*IT expertise and*	*y* *on,*
Password ya digunakan tidak pernah diubah dalam rentang waktu yang lama	*intent)*	*A.9.4.3 ord Management System*
Bisnis yang tidak selaras dengan penggunaan TI.	*Business ownership of IT*	*A.11.2.2 Supporting utilities*
Teknologi yang digunakan sudah terlalu usang dan	*Software*	*A.14.2.7 Outsourced development*

belum ada pembaharuan		
Kegagalan dalam mengakses data.	*Network*	*A.11.2.3 Cabling security*
Adanya pemindahan peralatan TI tanpa izin	*Hardware*	*A.11.2.5 Removal of assets*
Perangkat lunak yang digunakan belum baik, masih ada permasalahan seperti *bug*, *error* dll.	*Software*	*A.11.2.4 Equipment maintenance*
Peralatan yang dapat diakses oleh pemakai yang tidak memiliki otoritas.	*Network*	*A.9.2.1 User registration and de-registration* *A.9.4.2 Secure log-on procedures* *A.9.4.3 Password management system*
Data hilang, rusak, tidak bisa diakses.	*Information (data breach : damage leakage and access)*	*A.12.3.1 Information backup*

5.2 Rekomendasi Kebijakan

Tahap rekomendasi kebijakan dilakukan untuk memberikan solusi sebagai panduan dasar dalam melakukan sebuah rencana atau pelaksanaan suatu pekerjaan dalam sebuah perusahaan atau organisasi, serta pedoman untuk menangani risiko-risiko pada asset perusahaan [5]. Tabel 5 menjelaskan mengenai rekomendasi kebijakan.

Tabel 5 Rekomendasi Kebijakan

Kebijakan Kebijakan Keamanan Informasi.
Referensi Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI Edisi: 2.0, September 2011.
Pernyataan ❖ Kebijakan keamanan informasi harus dikomunikasikan ke seluruh karyawan PT Pos Indonesia (Persero) dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi. ❖ Seluruh kelemahan keamanan informasi pada PT Pos Indonesia (Persero) yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke penanggung jawab TI terkait. ❖ PT Pos Indonesia (Persero) harus meningkatkan kepedulian *(awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi karyawan. Sosialisasi juga perlu diberkan kepada vendor, konsultan, mitra, dan pihak ketiga lainnya sepanjang diperlukan.

6 KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil kegiatan penelitian pada PT Pos Indonesia (Persero), diperoleh sebagai berikut :

Ditemukan 15 risiko dengan kriteria nilai risiko rendah 5 (lima), moderat 5 (lima), dan tinggi 5 (lima), tidak ada kasus dengan level ekstrim. Selanjutnya dilakukan respon risiko untuk memilih dan menerapkan dalam menanggulangi pengelolaan risiko yang didapat berupa mengurangi kemungkinan dan dampak *(risk reduction*) dan untuk memindahkan beberapa risiko melalui entitas lain *(risk transfer)*. Dalam mengelola keamanan informasi harus dilakukan pemeliharaan rencana keamanan informasi, mengelola risiko keamanan informasi, kontrol keamanan informasi hal ini disarankan untuk mendukung agar keamanan informasi pada perusahaan lebih baik lagi. Pada tahap rekomendasi kontrol menggunakan ISO27001 sebagai referensi dalam melakukan tindakan rekomendasi kontrol. Pada tahap rekomendasi kebijakan berupa kebijakan keamanan informasi.

6.2 Saran

Saran yang dapat penulis sampaikan adalah semoga penelitian ini dapat dijadikan evaluasi untuk PT Pos Indonesia (Persero) dikemudian hari dalam aspek manajemen keamanan informasi. Serta meningkatkan edukasi dan pelatihan kepada karyawan agar risiko dapat dikurangi atau terkontrol dengan baik.

REFERENSI

[1] ISACA. (2012). Enabling Processes. In *Cobit 5*.

[2] ISO/IEC. (2015). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management for inter-sector and. *27003:2017*, *2015*, 1–45.

[3] Informasi, D. K. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*.

[4] Indonesia, Pos(2020a). *Profil PT Pos Indonesia*. https://www.posindonesia.co.id/en/content/sejarah-pos diakses: 13-November-2020

[5] Rachmadi, T. (2020). *Teknologi Informasi*. https://play.google.com/store/books/details/Tri_Rachmadi_Pengantar_Teknologi_Informasi?id=Nor6DwAAQBAJ diakses 21-Desember-2020

[6] Retnowardhani, A. (2013). *Keamanan Informasi*. https://mmsi.binus.ac.id/2017/11/17/keamanan-informasi/ diakses: 15-Agustus-2020