PENGEMBANGAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO 27001:2013 MENGGUNAKAN KONTROL *ANNEX* : STUDI KASUS DATA CENTER PT. XYZ

THE DEVELOPMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION BASED ON ISO 27001: 2013 USING ANNEX CONTROL : IN PT. XYZ CASE STUDY DATA CENTER

Boying Panjaitan[1], Lukman Abdurrahman[2], Rahmat Mulyana[3]

[1,2,3] Program Studi S1 Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
[1]boyingpanjaitan@telkomuniversity.ac.id, [2]abdural@telkomuniversity.ac.id,
[3]rahmatmoelyana@telkomuniversity.ac.id

Abstrak

PT. XYZ merupakan perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak di bidang industri manufaktur alat utama sistem persenjataan serta komersial dan industri. Informasi elektronik adalah salah satu aset yang berharga bagi perusahaan, sering kali perusahaan melakukan pengelolaan informasi yang kemudian hasilnya disimpan atau dibagikan. Sebagai parameter untuk menjamin keselarasan TI dengan tujuan bisnis korporasi dan kebijakan strategis maka dapat dilakukan pendekatan salah satunya dengan menerapkan keamanan informasi menggunakan standar ISO/IEC 27001:2013 sesuai peraturan menteri komunikasi dan informatika nomor 4 tahun 2016 tentang sistem manajemen pengamanan informasi. Penelitian ini dilakukan dengan menganalisis kondisi saat ini pada perusahaan Berdasarkan hasil penelitian yang dilakukan ditemukan beberapa klausul dan kontrol Annex yang belum terpenuhi di PT. XYZ yang dapat berdampak pada sistem manajemen keamanan informasi dan mempengaruhi kinerja dan proses bisnis pada PT. XYZ. Oleh karena itu, diperlukan implementasi standarisasi sesuai ISO 27001:2013 sebagai referensi arahan dalam menjaga informasi sensitif bagi PT. XYZ serta penelitian ini dapat digunakan untuk meminimalisasi risiko dan sebagai bentuk kepatuhan terhadap regulasi, hukum dan undang-undang terkait keamanan informasi. Hasil penelitian ini juga dapat dijadikan sebagai acuan yang dapat digunakan untuk meningkatkan efektivitas pengamanan informasi perusahaan.

Kata Kunci: informasi, informasi elektronik, penilaian risiko, ISO 27001:2013

Abstract

PT. XYZ is a state-owned company (BUMN) which is engaged in the manufacturing of the main weaponry systems as well as commercial and industrial equipment. Electronic information is one of the most valuable assets for the company, often the company manages the information and the results are stored or shared. As a parameter to ensure the alignment of IT with corporate business objectives and strategic policies, one approach can be made by implementing information security using the ISO / IEC 27001: 2013 standard according to the regulation of the minister of communication and informatics number 4 of 2016 concerning information security management systems. This research was conducted by analyzing the current condition of the company. Based on the results of the research, it was found that several Annex clauses and controls had not been fulfilled at PT. XYZ which can have an impact on the information security management system and affect the performance and business processes at PT. XYZ. Therefore, it is necessary to implement standardization according to ISO 27001: 2013 as a reference direction in maintaining sensitive information for PT. XYZ and this research can be used to minimize risk and as a form of compliance with regulations, laws and laws related to information security. The results of this study can also be used as a reference that can be used to increase the effectiveness of securing company information.

Keywords: information, electronic information, risk assessment, ISO 27001:2013

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) saat ini menjadi bagian yang sangat penting bahkan hampir semua bidang kehidupan. Perkembangan teknologi informasi dapat menunjang organisasi dalam memenuhi kegiatan organisasi menjadi proses dalam mencapai tujuan, bahkan di kehidupan kita tidak lepas dari teknologi. Dengan kemajuan teknologi dapat membantu kita untuk menangani berbagai masalah dan memudahkan kita dalam pembelajaran.

Di era milenial saat ini, perkembangan TI sudah berpengaruh terhadap proses bisnis utama , yaitu dalam pengambilan keputusan yang dilakukan oleh manajemen (-Prahani, 2012). Dengan adanya TI peran dari setiap manajerial dalam melakukan pengambilan keputusan dapat memberikan keputusan yang berdasarkan informasi yang tepat, terpercaya serta akurat dan mempertimbangkan *risk* yang akan terjadi.

ISO 27001:2013 merupakan dokumen standar sistem manajemen keamanan informasi (SMKI), sering kali digunakan oleh perusahaan untuk menerapkan keamanan sistem informasi, dengan menerapkan standar ISO 27001:2013 perusahaan dapat melindungi, memelihara kerahasiaan, integritas dan ketersediaan informasi serta untuk mengelola dan mengendalikan risiko keamanan informasi pada organisasi perusahaan. Dalam penelitian ini penerapan yang dipakai untuk manajemen keamanan informasi PT. XYZ adalah ISO 27001:2013.

PT. XYZ merupakan perusahaan yang bergerak dibidang industri manufaktur alat utama sistem persenjataan (alutsista) serta produk komersial dan industrl adalah satu aset yang berharga bagi perusahaan, sering kali perusahaan melakukan pengelolaan informasi yang kemudian hasil nya disimpan atau dibagikan. Untuk mencegah risiko dalam keamanan informasi, dalam penerapannya, perusahaan menggunakan ISO 27001:2013 sebagai kerangka kerjanya.

Berdasarkan hasil observasi dan wawancara yang sudah penulis lakukan bahwa pengelolaan TI pada PT XYZ ditemukan beberapa kontrol pada klausul *annex* yang masih belum terpenuhi sesuai ISO 27001:2013 yang berdampak pada manajemen keamanan informasi PT XYZ dan dapat mempengaruhi kinerja dari perusahaan.

Dengan adanya permasalahan tersebut mendorong untuk merancang rekomendasi pengamanan informasi berdasarkan standard ISO 27001:2013 di PT XYZ untuk membuat perancangan sistem manajemen keamanan informasi yang difokuskan pada kontrol *annex* manajemen aset, kontrol akses, kriptografi, pengamanan fisik dan lingkungan, keamanan informasi, keamanan komunikasi, akuisisi dan pengembangan sistem agar proses bisnis perusahaan dapat berjalan sesuai dengan tujuan dari organsisasi.

2. LANDASAN TEORI

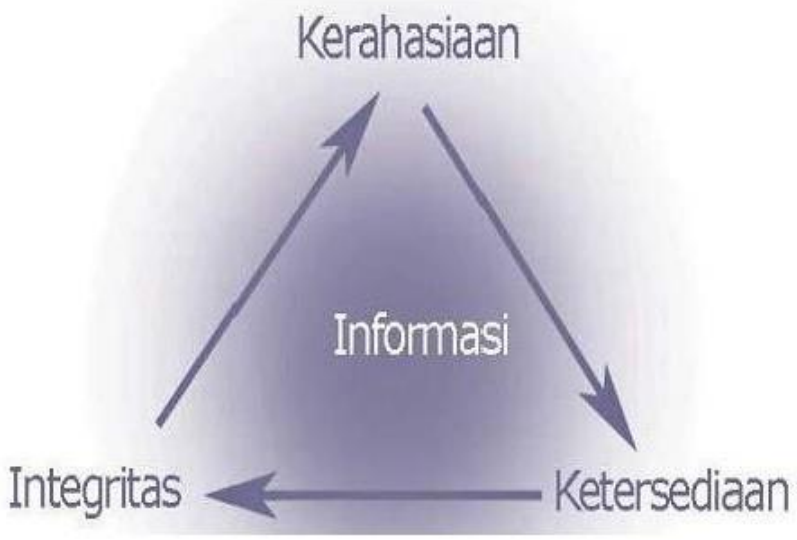
2.1 Sistem Manajemen Keamanan Informasi

Sistem manajemen keamanan informasi (SMKI) merupakan salah satu area fokus dari tata kelola teknologi informasi yaitu *Risk Management* yang berfokus pada bagaimana melakukan identifikasi kemungkinan risiko – risiko yang ada, serta bagaimana mengatasi dampak dari risiko – risiko tersebut.

Sistem manajemen keamanan informasi (SMKI) atau yang biasa disebut *Information Management Security System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan *(Plan),* Mengimplementasikan *(Do),* memonitor dan meninjau ulang *(Check),* dan memelihara *(Act)* terhadap keamanan informasi perusahaan. Keamanan informasi ditunjukkan untuk menjaga aspek kerahasiaan *(Confidentiality),* Integritas *(Integrity),* dan Ketersediaan *(Avaibility)* dari informasi (Sarno, 2009).

2.2 Aspek-Aspek Keamanan Informasi

Dalam menentukan aspek-aspek keamanan informasi perlu diperhatikan hal-hal yang merupakan aset yang berharga bagi perusahaan. Keamanan sistem informasi memiliki perlindungan terhadap aspek-aspek(-Chazar, 2016)



Gambar 1 Aspek Keamanan Informasi

1. *Confidentiality* (Kerahasiaan)

Aspek yang menjamin kerahasiaan informasi dan data, memastikan bahwa data dan informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang telah dikirim, diterima maupun di simpan.

2. *Integrity* (Integritas)

Aspek yang menjamin bahwa data tidak diubah tanpa ada izin dari pihak yang berwenang, serta menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas.

3. *Availability* (Ketersediaan)

Aspek yang menjamin bahwa data yang dibutuhkan akan tersedia serta memastikan *user* yang berhak menggunakan informasi dan perangkat terkait.

2.3 *Framework* Sistem Manajemen Keamanan Informasi

Framework tata kelola TI adalah kerangka kerja yang berfungsi untuk meningkatkan koordinasi dan rencana layanan TI dengan bisnis atau organisasi dan mengoptimalkan pencapaian value dari penyelenggaraan TI untuk internal manajemen dan pelayanan.

Ada beberapa framework yang menjadi acuan dalam perancangan tata kelola TI yang menjadi best practice dalam penggunaanya, berikut beberapa contoh framework tata kelola TI :

1. COBIT 5 *for Information Security* lebih ditekankan pada keamanan informasi dan memberikan gambaran secara detail dan praktis tentang panduan bagi para profesional keamanan informasi dan orang-orang

yang merupakan bagian dari *enterprise* yang memiliki ketertarikan bidang keamanan informasi.

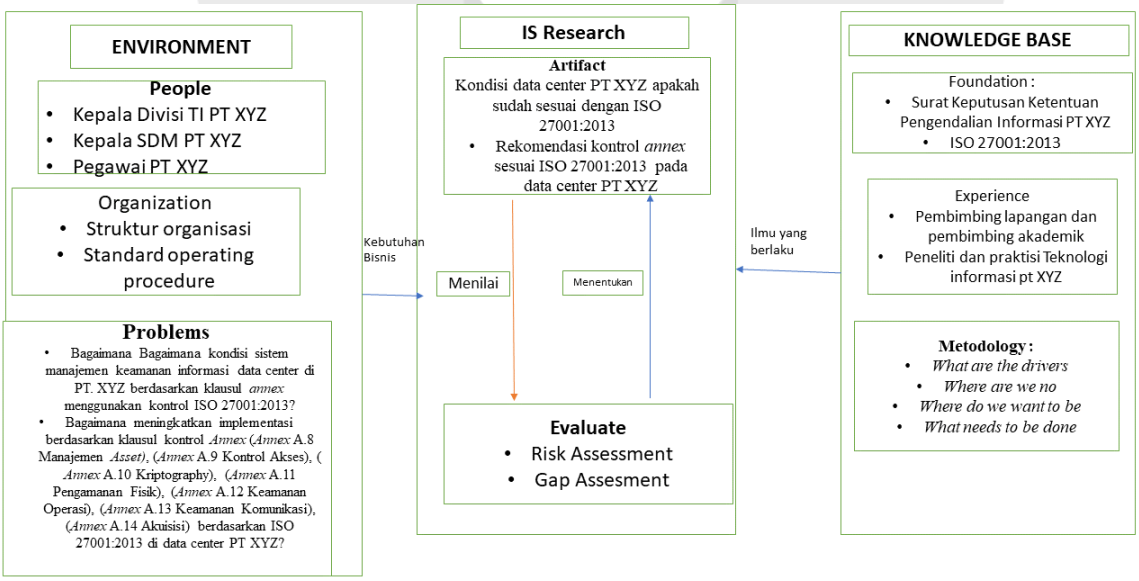
2. ISO *International Organization for Standardization* (ISO) adalah suatu organisasi internasional non-pemerintah untuk standardisasi. *International Electrotechnical Commission* (IEC) adalah suatu organisasi standardisasi internasional yang menyiapkan serta mempublikasikan standar internasional untuk semua teknologi elektrik, elektronika, dan teknologi yang terkait, yang juga dikenal sebagai elektroteknologi. Standardisasi digunakan untuk memberikan inovasi serta memberikan solusi (Chazar, 2015)
3. ISO 27001:2013

   ISO 27001:2013 merupakan dokumen standar sistem manajemen keamanan informasi (SMKI) atau *Information Security Management System* (ISMS) adalah memberikan suatu gambaran untuk mengimplementasikan konsep – konsep keamanan informasi di suatu perusahaan. ISO 27001:2013 menjelaskan keperluan – keperluan untuk sistem manajemen keamanan informasi yang baik dan memelihara serta melindungi terhadap gangguan yang akan terjadi pada aktivitas bisnis dan memberikan perlindungan terhadap gangguan keamanan informasi yang mengakibatkan kerugian (Jim Macellaro, 2016).

3. METODOLOGI PENELITIAN

3.1 Model Konseptual

Metode Konseptual suatu kerangka kerja yang menerangkan keterlibatan individu, kelompok, dan kejadian terhadap suatu ilmu dan pengembangannya. Suatu konseptual yang menunjukkan hubungan logis antara *factor/ variable* yang telah diidentifikasi untuk menganalisis masalah penelitian.



Gambar 2Model Konseptual

3.2 Sistematika Penelitian

Masalah yang terdapat pada penelitian ini membutuhkan cara penyelesaian masalah yang teratur. Sistematika penyelesaian masalah akan membantu penelitian yang dilakukan dengan memiliki tahapan yang akan dilalui pada proses penelitian.

a. *What are the drivers*

Pada tahap ini dimulai dengan melakukan identifikasi masalah melalui observasi lapangan dan juga studi pustaka. Setelah melakukan identifikasi dan merumuskan masalah . Perumusan masalah ini mempertimbangkan batasan penelitian dan juga menjadi tujuan dari pelaksanaan penelitian.

b. *Where are now*

Pada Tahap pengumpulan data, sebelum melakukan wawancara berdasarkan Penilaian Kesenjangan ISO/IEC 27001:2013 kontrol yang ada di *Annex* yaitu Manajemen Aset, Kontrol Akses, Kriptografi, Pengamanan Fisik dan Lingkungan, Keamanan Komunikasi, Akuisisi, Pengembangan dan Pemeliharaan Sistem. Setelah itu mengisi Penilaian Kesenjangan IS/IEC 27001:2013 jika semua kontrol telah terisi maka akan dilakukan verifikasi terhadap data yang telah di isi pada Kuesioner Indeks KAMI

c. *Where do we want to be*

Pada tahap ini dilakukan guna menentukan perumusan masalah yang nantinya menjadi tujuan dari pada penelitian serta menjadi Batasan penelitian. Tahap ini dilakukan guna mendukung studi pustaka dan studi lapangan. Langkah awal pada tahap ini adalah wawancara mengenai kondisi sistem informasi pada PT. XYZ Data yang diperoleh digunakan untuk mengetahui permasalahan apa saja yang ada pada sistem manajemen keamanan informasi pada PT. XYZ, sehingga dari permasalahan tersebut dapat menentukan *scope* sistem manajemen keamanan informasi pada PT. XYZ kemudian menerapkan sistem keamanan informasi berdasarkan standar ISO 27001:2013 guna mencapai target yang diinginkan.

4. PENGUMPULAN DATA DAN HASIL ANALISIS *RISK ASSESSMENT*

4.1 Gap *Assessment*

Gap *Assessment* merupakan proses penilaian yang dilakukan dibagi menjadi 2 kriteria yaitu penelitian pada kondisi saat ini dan kondisi pada yang ideal berdasarkan ISO 27001:2013 yang akan membantu untuk mengetahui sudah sampai di mana tingkat pencapaian tujuan PT XYZ. Penilaian kesenjangan ini didapatkan dengan melakukan penelitian setiap kontrol *Annex* sesuai ISO 27001:2013.

4.1.1 Hasil Gap *Assessment*

Penilaian kesenjangan ini didapatkan dengan melakukan penelitian setiap kontrol *Annex* sesuai ISO 27001:2013.

Tabel 1 Hasil Penilaian Kesenjangan ISO 27001:2013

No	Area Dalam Standar	Jumlah Persyaratan Pada SECTION Ini	Jumlah Persyaratan Yang Terpenuhi	% *Conformant*
1.	A.8 Manajemen Aset (*Asset Management*)	10	8	80%
2.	A.9 Kontrol Akses (*Access Control*)	14	10	71%
3.	A.10 Kriptografi (*Cryptography*)	2	0	0%
4.	A.11 Pengamanan Fisik Dan Lingkungan (*Physical and Environmental Security*)	15	12	86%
5.	A.12 Keamanan Operasional (*Operational Security*)	14	10	71%
6.	A.13 Keamanan Komunikasi (*Communications Security*)	7	7	100%
7.	A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem (*System Acquisition, Development and Maintenance*)	13	10	77%
	Total	**74**	**57**	

4.1.2 Identifikasi Kontrol *Annex* yang tidak terpenuhi

Identifikasi risiko pada bagian ini adalah segala kejadian yang kemungkinan bisa terjadi pada suatu hari dan akan memberikan dampak buruk pada proses bisnis organisasi. Tujuan dari identifikasi risiko adalah untuk mengetahui daftar klausul yang tidak terpenuhi sesuai dengan kontrol ISO 27001:2013.

Tabel 0-2 Identifikasi klausul yang tidak terpenuhi

No	Kategori dalam ISO 27001	Temuan
1.	A.8.3.2 Penghancuran Media	belum memiliki prosedur terkait media yang tidak dibutuhkan atau telah digunakan.

No	Kategori dalam ISO 27001	Temuan
2.	A. 8.3.3 Pemindahan Media Fisik	belum memiliki prosedur terkait informasi yang telah dilindungi terhadap akses illegal, penyalahgunaan atau pun rusak.
3.	A.9.4.2 Prosedur *secure log-on*	Belum memiliki Prosedur terkait *secure log-on* pada aplikasi yang digunakan
4.	A.9.4.3 Sistem Pengelolaan *Password*	Sudah memiliki Pengelolaan password dengan baik, namun masih terpancing dengan kejadian *phising* dan penyalahgunaan akun.
5.	A.9.4.5 Kontrol akses terhadap *source code*	Tidak ada pembatasan terhadap *sourcecode* pada aplikasi
6.	A.10.1.1 Kebijakan Kontrol penggunaan kriptografi	Sudah memiliki rancangan terhadap kontrol kriptografi namun belum diterapkan
7.	A.10.1.2 Manajemen Kunci	Terkait penggunaan proteksi kunci-kunci kriptografi sudah memiliki rancangan namun belum diterapkan
8.	A.11.2.3 Pengamanan kabel	Belum adanya prosedur terkait pengamanan kabel di lingkungan organisasi
9.	*A.11.2.5 Pemindahan Aset*	*Prosedur pemindahan aset, alat, informasi atau software belum di terapkan namun sudah memiliki rancangan di dalam organisasi pt xyz*
10.	A.11.2.6 Pengamanan peralatan dan aset di luar kantor	Belum memiliki prosedur terkait penggunaan aset di luar kantor
11.	A.12.1.1 Prosedur operasi yang terdokumentasi	Belum memiliki prosedur operasi yang terdokumentasi
12	A.12.2.1 Kontrol terhadap *malware*	Belum memiliki Kebijakan terkait *Anti-Malware*

No	Kategori dalam ISO 27001	Temuan
13.	A.12.5.1 Instalasi *software* pada sistem operasional	Belum memiliki prosedur mengenai kontrol instalasi *software* pada sistem operasional yang telah diimplementasikan.
14.	A.12.6.2 Pembatasan instalasi *software*	belum memiliki aturan pembatasan terhadap instalasi *software*.
15.	A.14.2.4 Pembatasan perubahan pada *software package*	prosedur *software package* masih belum dijalankan dengan baik.
16.	A.14.2.5 Prinsip sistem keteknikan yang aman	sistem pengembangan keteknikan yang aman secara umum pada *Data Center* PT. XYZ telah diatur dalam dokumen SMKI perusahaan PT XYZ namun belum diterapkan.
17.	A.14.2.6 Lingkungan pengembangan yang aman	ruang *data center* PT XYZ belum menerapkan proteksi pada lingkungan pengembangan sistem

4.2 *Risk Assessment*

Proses *risk assessment* adalah penilaian risiko pada pusat data PT XYZ. Proses ini diharapkan dapat memunculkan proses prioritas instansi menurut aset yang dilihat dari berbagai macam risiko yang pernah dan sedang terjadi pada data center PT XYZ. Penulis melakukan observasi dan wawancara dengan pihak terkait mengenai beberapa skenario risiko dari berbagai kategori ISO 27001:2013 serta melakukan analisa kriteria risiko yang sering terjadi dan menjadi prioritas untuk ditangani. Dalam melakukan *risk assessment* penulis melakukan beberapa tahapan di antaranya pencarian mengidentifikasi risiko, *threats*/ancaman, analisis risiko yang sesuai dengan proses ISO 27001 dan harus diprioritaskan serta berkaitan dengan solusi dari penyelesaian risiko tersebut.

4.2.1 Identifikasi Aset

Identifikasi aset berguna dalam menentukan aset yang terhubung dengan pusat data PT XYZ. Berdasarkan hasil observasi yang dilakukan maka aset yang sudah teridentifkasi dapat dilihat pada tabel berikut ini.

Tabel 1 Identifikasi Aset

Kategori Aset	Sub Kategori	Aset
Infrastruktur Data Center	Perusahaan	Anggaran
		Rencana perusahaan
		Kebijakan perusahaan
	Pegawai	Data pelanggan
		Data pegawai PT XYZ
		Data Pelatihan pegawai
Organisasi		PT XYZ
Perangkat Keras	Peralatan Tetap	PC
		Server
		Storage
		Laptop
		Rak Server
		UPS
		Router
		Sistem Pendingin
Perangkat Lunak	Sistem Operasi	Software Monitoring
		Office
	Perangkat Jaringan	Intranet
		Kabel LAN (*Local Area Network*)
		Router

4.2.2 Identifikasi *threats* dan Kerentanan

Identifikasi ancaman atau *threats* merupakan kegiatan yang dapat membahayakan informasi atau tahap dilakukannya penggabungan informasi yang diperoleh ketika melakukan observasi langsung, wawancara yang telah dilakukan dengan mencari ancaman apa saja yang muncul pada gap *assessment* yang tidak terpenuhi. Identifikasi kerentanan merupakan cara untuk menimbulkan ancaman atau *pen test* adalah serangan simulasi yang dilakukan untuk mengeksploitasi prosedur kontrol fisik, Teknik , keamanan informasi, atau kontrol lainnya, berdasarkan hasil dari temuan pada gap *assessment* yang tidak terpenuhi berikut analisa ancaman yang dapat pada tabel berikut ini.

Tabel 2 identifikasi *threats* dan ancaman

No	Gap	Deskripsi Risiko		
		Aset	**Kerentanan (V)**	**Ancaman (T)**
1.	Belum adanya Prosedur terkait *secure log-on* pada aplikasi yang digunakan	*Website*	Belum memiliki arahan dalam pembuatan *secure log-on*	Terjadinya *spam bot*
2.	Sudah memiliki sistem pengelolaan password, namun masih ada kejadian *phising* dan penyalahgunaan akun	informasi	Terpedaya dengan *phising* dan penyalahgunaan penggunaan akun serta password	Pencurian data informasi.
3.	Tidak adanya pembatasan terhadap *sourcecode* pada	Sistem Aplikasi	Terjadi kesalahan pada saat melakukan perubahan *source code* pada aplikasi	Kerusakan pada aplikasi
4.	Belum memiliki prosedur terkait pengamanan kabel di internal data center PT XYZ	Infrastruktur dan layanan TI	Rentan terjadi kehilangan, kerusakan serta kebakaran pada kabel.	Sabotase, pencurian, kebakaran serta kerusakan pada kabel.
5.	Belum memiliki prosedur terkait penggunaan aset di luar kantor	Laptop	Belum ada aturan terkait penggunaan aset diluar kantor	Kehilangan perangkat dan isi data didalam nya.
6.	Belum memiliki prosedur operasi yang terdokumentasi	Dokumentasi operasional	Tidak adanya instruksi kerja dan standar dalam pelaksanaan kegiatan operasional.	Kesalahan dalam pemrosesan.

No	Gap	Deskripsi Risiko		
		Aset	Kerentanan (V)	Ancaman (T)
7.	Belum memiliki kebijakan terkait *anti-malware*	Software	Terjadi penyebaran malware di perusahaan.	Malware.
8.	Belum memiliki prosedur mengenai kontrol instalasi *software* pada sistem operasional yang telah diimplementasikan	software	Terjadi penggunaan *software* bajakan	Audit software berlisensi
9.	Prosedur *software package* masi belum dijalankan dengan baik.	software	Terjadi penggunaan software *package* yang tidak tepat dan masih ada bug	Kerusakan pada *software* dari versi yang belum stabil.

4.3 Analisis Risiko

Proses dalam melakukan analisa risiko terhadap kemungkinan dan *impact* yang sudah ditetapkan dan menetapkan level dari risiko berdasarkan *risk apptetite* yang telah ditentukan. Dalam menentukan analisis risiko peneliti membuat kesepakatan dengan objek penelitian mengenai *risk appetite* atau batas toleransi risiko yang dilihat dari sisi organisasi PT XYZ.

4.3.1 Kriteria level risiko

Kriteria risiko merupakan ukuran standar dalam menentukan seberapa besar dampak yang akan terjadi dan seberapa besar kemungkinan atau frekuensi risiko akan terjadi. Dalam membuat kriteria risiko, penulis menggunakan tabel *probability* dan *impact* ukuran 5x5 yang terdiri dari 5 level kemungkinan dan 5 level dampak/*impact* dapat dilihat pada gambar di bawah ini

Rating Kemungkinan	Rating Dampak				
	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sangat Tinggi	Rendah	Sedang	Tinggi	Sangat Tinggi	Sangat Tinggi
Tinggi	Rendah	Sedang	Sedang	Tinggi	Sangat Tinggi
Sedang	Sangat Rendah	Rendah	Sedang	Tinggi	Tinggi
Rendah	Sangat Rendah	Rendah	Rendah	Sedang	Tinggi
Sangat Rendah	Sangat Rendah	Sangat Rendah	Rendah	Sedang	Sedang

Gambar 3 Level Risiko berdasarkan *likehood* dan *impact*

No	Temuan	Tingkat Risiko
1.	Belum adanya Prosedur terkait *secure log-on* pada aplikasi yang digunakan	*Medium*
2.	Sudah memiliki sistem pengelolaan password yang baik, masih ada kejadian *phising* dan penyalahgunaan akun	*Medium*
3.	Tidak adanya pembatasan terhadap *sourcecode* pada aplikasi	*Medium*
4.	Belum memiliki prosedur terkait pengamanan kabel di internal organisasi	*Medium*
5.	Belum memiliki prosedur terkait penggunaan aset diluar kantor	*Low*
6.	Sudah memiliki prosedur clear desk dan clear screen, namun user masih tidak disiplin dalam menerapakan 5R	*Medium*
7.	Belum memiliki prosedur operasi yang terdokumentasi	*Medium*
8.	Belum memiliki kebijakan anti *malware*	*Medium*
9.	Belum memiliki prosedur mengenai kontrol instalasi software pada sistem operasional yang telah diimplementasikan.	*Medium*
10.	Belum memiliki aturan pembatasan terhadap instalasi software.	*Medium*
11.	Prosedur *software package* masih belum dijalankan dengan baik	*Medium*

5. PERANCANGAN SMKI

Perancangan SMPI dilakukan berdasarkan penilaian yang telah dilakukan sesuai dengan ISO 27001:2013 dengan kontrol *Annex* sebagai pendukung dalam melakukan rekomendasi untuk perancangan SMPI tersebut. Perancangan yang didapatkan berupa perancangan people, process, dan technology.

5.1 Perancangan *people*

Perancangan *people* merupakan perancangan yang didapat dari *risk assessment* yang telah membahas kontrol tentang organisasi, kompetensi serta kemampuan. Perancangan *people* yang dilakukan akan menghasilkan rekomendasi struktur organisasi baru pada kompetensi dan kemampuan menghasilkan rekomendasi sumber daya yang harus dimiliki oleh setiap organisasi berdasarkan kebutuhan dan pelaksanaan proses.

5.2 Perancangan *process*

Perancangan proses merupakan hasil dari perancangan yang didapat berdasarkan pada kondisi *data center* PT.XYZ. perencanaan proses yang dilakukan menghasilkan rekomendasi kebijakan sistem manajemen keamanan informasi untuk data center serta diterapkan sesuai prosedur SMKI yang berlaku pada ruang lingkup data center pt xyz. Berikut ini tabel pemetaan terhadap *risk treatment* plan terhadap perancangan *process*

5.3 Perancangan *technology*

Perancangan *technology* adalah hasil dari perancangan yang didapat berdasarkan dari perancangan *risk assessment* yang telah dianalisis. Perancangan teknologi akan menghasilkan rekomendasi aplikasi dan *tools* yang akan digunakan untuk menunjang kebutuhan pelaksanaan proses.

6. KESIMPULAN

Berdasarkan hasil dari penelitian ini kesimpulan yang dapat diambil dalam melakukan perancangan SMKI pada data center PT . XYZ yang dilakukan berdasarkan *risk assessment* dan *gap assessment* adalah masih kurangnya persyaratan yang harus dipenuhi berdasarkan standard ISO 27001:2013 dan dapat disimpulkan bahwa :

1. Berdasarkan hasil penilaian kesenjangan pada *Annex* A.8 sampai dengan A.14 berdasarkan ISO 27001:2013 terdapat beberapa persyaratan yang belum dipenuhi pada data center PT. XYZ.
2. Dalam penilaian risiko, terdapat 17 temuan dengan 3 temuan merupakan kategori *low* dan 14 temuan dengan kategori *medium* dan pada temuan tersebut opsi penanganan yang didapat adalah *mitigate, accept, transfer,* dan *avoid.*
3. Dalam rekomendasi perancangan *people* adanya penambahan deskripsi kerja dengan melakukan pelatihan dan sertifikasi pada data center pt xyz.

Reference

[1] Chazar, C. (2016). *MODEL PERENCANAAN KEAMANAN SISTEM INFORMASI MENGGUNAKAN PENDEKATAN METODE OCTAVE DAN ISO 27001:2005.*

[2] Fania1, I. ,. (2020). *ANALISIS DAN PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA KANTOR IMIGRASI KELAS 1 TPI PONTIANAK MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ISO/IEC 27001:2013.*

[3] Hevner, A. R., & Chatterjee, S. (2010). *Design research in information systems : theory and practice.* New York; London.

[4] Macellaro, J. (2016). *Implementing an ISMS to Support ISO 27001 and ISO 27001 Certification.*

[5] MUHAMMAD BAHRUDIN2, F. (2018). *Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001.*

[6] NIST. (2012). *NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments.*

[7] Ritzkal Ritzkal, A. G. (2016). *IMPLEMENTASI ISO/IEC 27001:2013 UNTUK SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) PADA FAKULTAS TEKNIK UIKA-BOGOR.*

[8] Shenton, A. K. (2004). Education for Information. *Strategies for Ensuring Trustworthiness in Qualitative Research Projects*, 63-75.