AUDIT HUMAN RESOURCES SECURITY, ACCESS CONTROL, DAN PHYSICAL AND ENVIRONMENTAL SECURITY PADA SISTEM INFORMASI PT. TASPEN (PERSERO) KCU BANDUNG MENGGUNAKAN ISO 27001

AUDIT OF HUMAN RESOURCES SECURITY, ACCESS CONTROL, AND PHYSICAL AND ENVIRONMENTAL SECURITY ON INFORMATION SYSTEM PT. TASPEN (PERSERO) KCU BANDUNG USING ISO 27001

Vica Firlia

Prodi S1 Manajemen Bisnis Telekomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom
vicafirlia@gmail.com

Abstrak

Pada perkembangan teknologi komputasi dan komunikasi dewasa ini, sistem informasi perusahaan hampir dapat dikatakan sangat mengandalkan dukungan teknologi informasi (TI). PT TASPEN (Persero) sebagai salah satu perusahaan BUMN Indonesia merasakan hal yang sama akan pentingnya teknologi informasi. Untuk memastikan apakah sistem informasi telah dirancang dan diterapkan sesuai dengan prosedur dan standar yang telah diterapkan, perlu dilakukan audit terhadap sistem informasi. Audit juga dilakukan untuk memastikan apakah pengendalian yang telah ada sudah memadai sesuai ISO 27001: 2013.

Jenis penelitian yang digunakan adalah deskriptif kualitatif. Tehnik pengumpulan data yang digunakan adalah wawancara, observasi, dan studi dokumentasi. Dan tehnik keabsahan menggunakan triangulasi tehnik. Setelah data di dapat, selanjutnya dilakukan analisis data dengan melakukan Gap Analysis. Dan untuk mengukur tingkat kematangan, penelitian ini menggunakan *System Security Engineering Capability Maturity Model* (SSECMM).

Hasil penelitian ini menunjukkan bahwa tingkat kematangan klausul Human *Resource Security* mencapai level level 1 (*Performed Informally*), klausul *Access Control* mencapai level 2 (*planned and tracked*), sedangkan klausul *Physical and Environmental Security* sudah mencapai level 3 *(well defined).*

Kata kunci*:* audit, keamanan sistem informasi, ISO 27001, *maturity level*

Abstract

In the development of computing and communication technology today, enterprise information system almost can be said to rely heavily on the support of information technology (IT). TASPEN PT (Persero) as one of the Indonesian state-owned companies feel the same way about the importance of information technology. To ascertain whether the information system has been designed and implemented in accordance with the procedures and standards that have been applied, there should be an audit of the information system. Audits are also conducted to ascertain whether existing controls are adequate according to ISO 27001: 2013.

This type of research is descriptive qualitative. Data collection techniques used were interviews, observation, and study documentation. And the validity of using the technique of triangulation techniques. Once the data is in the can, then analyzed the data by conducting Gap Analysis. And to measure the level of maturity, this study uses the System Security Engineering Capability Maturity Model (SSECMM). Based on the research results, level of maturity clause Human Resource Security reached a level 1 (Performed Informally), clause Access Control reaches level 2 (planned and tracked), whereas clauses of Physical and Environmental Security has reached level 3 (well-defined).

Keywords: audit, information systems security, ISO 27001, maturity level

1. PENDAHULUAN

Pada perkembangan teknologi komputasi dan komunikasi dewasa ini, sistem informasi perusahaan hampir dapat dikatakan sangat mengandalkan dukungan teknologi informasi (TI). Paradigma lama memandang sistem informasi sebagai pengolah data secara elektronik untuk menyediakan informasi bagi manajemen dalam membuat keputusan. Paradigma baru

mengungkapkan teknologi menempati posisi strategis dalam pencapaian keunggulan kompetitif dalam perencanaan strategis perusahaan [1].

PT TASPEN (Persero) sebagai salah satu perusahaan BUMN Indonesia merasakan hal yang sama akan pentingnya teknologi informasi. Karenanya, perseroan memberikan perhatian yang sangat besar terhadap pengembangan aspek teknologi informasi, baik yang berkaitan dengan internal perusahaan maupun yang berhubungan dengan peserta.

Pengalaman di berbagai organisasi dalam pemanfaatan sistem informasi, salah satu hal yang dibutuhkan adalah bagaimana setiap organisasi dapat memastikan bahwa sistem informasi yang ada memiliki sistem pengamanan dan pengendalian yang [2].

Oleh karena itu, suatu sistem yang baik seharusnya selalu dilengkapi dengan mekanisme kontrol internal. Selanjutnya untuk menjamin bahwa segala sesuatunya berjalan seperti yang seharusnya, maka secara periodik diperlukan adanya pemeriksaan/ audit sistem, penggunaannya maupun pengguna itu sendiri, dengan kata lain adalah sistem dan *user*-nya.

Berdasarkan hasil wawancara, masalah yang berkaitan keamanan sistem informasi terutama keamanan sumber daya manusia di PT TASPEN (Persero) KCU Bandung menjadi ancaman terbesar. Pernah menjadi temuan jika terdapat *user* yang pernah mencoba untuk menghidupkan kembali atau mengubah keterangan akun nasabah yang sudah tidak ada wali yang berhak menerima uang pensiun, namun karena ada kerja samanya dengan pihak bank akun tersebut diubah keterangannya dan dana pensiun itu ia yang terima. Dari kasus tersebut dapat disimpulkan bahwa masih kurangnya pengguna atau *human* itu untuk menyadari tanggung jawabnya sebagai *user* dari sistem informasi dan dari kasus tersebut juga didapat bahwa penerapan keamanan kontrol akses yang ada di PT TASPEN (Persero) KCU Bandung belum sempurna penerapannya untuk melindungi kerahasiaan, integritas dan ketersediaan informasi. Selain itu, dari observasi yang dilakukan, didapat bahwa ruang *data center* PT TASPEN (Persero) KCU Bandung yang berada di ruang divisi teknologi informasi hanya dilindungi dengan kunci password. Dan ruangan tersebut dapat dilihat dari kejauhan karena hanya kaca yang menutup/melindungi ruangan tersebut.

Dan berdasarkan permasalahan diatas, maka dilakukan audit pada *Human Resources Security, Access Control, Physical and Environmental Security,* dan *Communication Security* sistem informasi PT TASPEN (Persero) KCU Bandung, untuk memberikan penilaian terhadap tingkat kematangan keamanan sistem informasi yang dijalankan. Metode pengukuran tingkat kematangan yang digunakan adalah SSE-CMM. Dan hasil dari audit ini berupa laporan temuan dan rekomendasi sebagai acuan kinerja TI yang baik menurut standar ISO/IEC 27001.

2. DASAR TEORI DAN METODOLOGI

2.1 Sistem Informasi

Pengertian sistem informasi adalah sebuah sistem yang menggunakan teknologi informasi (TI) untuk menangkap, mentransmisikan, menyimpan, mendapatkan, memanipulasi, atau menampilkan informasi yang dibutuhkan oleh satu atau lebih proses bisnis. Agar dapat berdaya guna, maka sistem informasi seharusnya merupakan rangkaian prosedur formal yang melakukan pengelompokam data, pemrosesan dan pendistribusian kepada pengguna [3].

2.2 Audit Sistem Informasi

An MIS audit examines the firm.s overall security environment as well as controls governing individual information system [4]. Dari pengertian diatas dijelaskan bahwa audit sistem informasi manajemen memeriksa keseluruhan keamanan lingkungan perusahaan sebaik mengontrol sistem informasi individu sendiri.

2.3 ISO 27001

ISO 27001 adalah standar yang dikeluarkan oleh *International Organization for Standarization* (ISO) dan *International Electrotechnical Commission* (IEC). ISO 27001 ini memfokuskan diri pada keamanan sistem informasi suatu organisasi. ISO/IEC 27001 : 2013 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *information Security Management System* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan. Secara umum terdapat 14 aspek yang seharusnya ada dalam setiap perusahaan dalam usahanya mengimplementasikan konsep keamanan informasi tersebut [5].

2.4 *Maturity Level*

System Security Engineering Capability Maturity Model (SSE-CMM) menjelaskan karakteristik penting dari proses rekayasa keamanan organisasi yang harus ada untuk memastikan teknik keamanan yang baik. *System Security Engineering Capability Maturity Model* (SSE-CMM). SSE-CMM adalah standar karakteristik yang menggambarkan karakteristik dasar

pencapaian tingkat diterimanya keamanan informasi dalam organisasi. SSE-CMM berorientasi pada proses keamanan sistem informasi dan fokus pada pelaksanaan daripada dari hasil, karena hasil diukur dari pelaksanaannya. Model kematangan SSE-CMM terdiri dari 5 tingkat kematangan [6].

2.5 Metodologi penelitian

Pada penelitian ini, tahap awal dari penelitian adalah mengidentifikasi masalah atau fenomena yang ada dari berbagai sumber. Setelah masalah atau fenomena ini diketahui maka disusunlah rumusan masalah dan dilanjutkan penyusunan tujuan dan manfaat penelitian untuk mengetahui kegunaan dari penelitian ini. Sebelum masuk ke tahapan mengurus surat perijinan, tahapan berikutnya adalah wawancara dengan orang yang dianggap sangat menguasai tentang sistem informasi perusahaan. Setelah ada kesepatan bahwa bersedia untuk dilaksanakannya audit, tahapan selanjutnya adalah mengurus perijian untuk melakukan penelitian pada objek penelitian yang ditentukan. Setelah perijinan didapatkan, selanjutnya adalah studi literatur dan referensi yang berhubungan degan permasalahan yang diangkat. Selanjutnya adalah dilakukannya audit sistem informasi dengan pengumpulan bukti-bukti guna memperkuat penelitian. Setelah audit dilaksanakan dan bukti tekumpul selanjutnya dilakukan analisis data.

Langkah-langkah analisi data adalah sebagai berikut:

a. Reduksi Data
   Hasil wawancara yang didapat, akan diubah dan dijabarkan kedalam bentuk verbatim dan juga catatan lapangan, selanjutnya diubah kembali kedalam bentuk Deskripsi Fenomenal Individu (DFI). Data yang sudah diubah menjadi bentuk DFI tadi, akan dilakukan pengkodean (coding) dengan format" nama peneliti-nama informan/urutan wawancara/baris pernyataan DFI" dan katagorisasi beserta pemaknaan agar lebih mudah untuk dipahami.
b. Penyajian Data
   Langkah selanjutnya adalah menjelaskan hasil temuan ke dalam tabel *work paper gap analysis,* kemudian dilakukan penilaian *maturity level* terhadap klausul yang diteliti. Selanjutnya akan digambarkan dalam bentuk grafik nilai *maturity level* hasil penelitian, dengan standar *maturity level* BUMN dan juga harapan atau target maturity level organisasi.
c. Kesimpulan/verifikasi
   Tahap terakhir adalah kesimpulan dari hasil yang didapat, agar dapat menjawab rumusan masalah yang dibuat.

Dan hasil akhir dari penelitian ini adalah berupa rekomendasi untuk PT TASPEN (Persero) KCU Bandung guna meningkatkan keamanan sistem informasinya.

3. PEMBAHASAN

3.1 *Work Paper Gap Analysis*

Berdasarkan hasil wawancara, observasi dan studi dokumentasi yang dilakukan pada PT TASPEN (Persero) KCU Bandung, maka didapat *evidence* dan temuan. Temuan-temuan hasil audit keamanan sistem informasi PT TASPEN (Persero) KCU Bandung didapat *gap* antara hasil audit dengan standar ISO 27001 tahun 2013. Contoh dari *Work paper gap analysis* audit keamanan sistem informasi PT TASPEN (Persero) KCU Bandung ditunjukkan pada **Tabel 1** berikut:

Tabel 1 *Work Paper Gap Analysis*

Kontrol	Pertanyaan	Ya	Tidak	*Evidence*	Temuan	*Gap*
Klausul A.7 *Human Resources Security*						
7.2 *During Employment*						
7.2.1 *Management Responsibility*	Apakah manajemen sudah menerapkan langkah-langkah untuk memperkecil kemungkinan resiko keamanan informasi oleh pengguna?	√		Terdapat pada dokumen Nomor : SK-24/DIR/2006	-	Sesuai dengan standar
	Apakah tanggung jawab terhadap keamanan dan penggunaan fasilitas pemrosesan informasi sudah ditetapkan?	√		Terdapat pada dokumen Nomor : SK-24/DIR/2006 subbab 2.4.1 Tugas dan tanggung jawab	-	Sesuai dengan standar
	Apakah kebijakan dan prosedur tersebut sudah didokumentasikan?	√		SK-24/DIR/2006	Kebijakan penerapan langkah-langkah memang sudah didokumentasikan, tetapi untuk prosedur belum ada.	Berdasarkan sasaran kontrol 7.2.1 seharusnya kebijakan dan prosedur dipersiap-kan guna mendukung keamanan organisasi untuk memper-kecil kemungkin-an resiko keamanan
	Apakah sudah dievaluasi secara berkala atau ketika terjadi perubahan?	√		Terdapat pada dokumen Nomor : SK-24/DIR/2006 Bab 5 tentang audit	-	Sesuai dengan standar
	Apakah sudah dilakukan perbaikan terus menerus?	√		Terdapat pada dokumen Nomor : SK-24/DIR/2006 Bab 5 tentang audit	-	Sesuai dengan standar

3.2 Penilaian *Maturity Level* Tiap Kontrol

Penilaian *Maturity Level* dilakukan terhadap masing-masing kontrol sesuai dengan hasil audit yang dilakukan, berdasarkan kriteria penilaian mulai dari skor 0 sampai 5. Pada penelitian ini, daftar pertanyaan sudah diurutkan berdasarkan kriteria penilaian, dan tiap kriteria penilaian sudah disesuaikan dengan standar ISO 27001.

Setiap pertanyaan kontrol dari klausul yang diteliti dimulai dengan tingkatan 1 hingga tingkatan 5. Skor 0 akan diberikan apabila pada pertanyaan penelitian tingkat pertama berisi jawaban tidak. Untuk tingkat selanjutnya, pemberian nilai atau skor *Maturity Level* diberikan dengan mempertimbangkan temuan yang ada di lapangan.

Nilai *Maturity Level* tiap kontrol dari klausul yang didapat menggambarkan kondisi keamanan sistem informasi PT TASPEN (Persero) KCU Bandung. Contoh penilaian *Maturity Level* akan ditunjukkan pada **Tabel 2** berikut:

Tabel 2 Penilaian *Maturity Level* Tiap Kontrol

Kontrol		Pertanyaan	Ya	Tidak	Temuan	*Hasil Pengujian Maturity Level Tiap Kontrol*
Klausul A.7 *Human Resources Security*						
7.2 *During Employment*						
7.2.1 *Management Responsibility*	1	Apakah manajemen sudah menerapkan langkah-langkah untuk memperkecil kemungkinan resiko keamanan informasi oleh pengguna?	√			**2**
	2	Apakah tanggung jawab terhadap keamanan dan penggunaan fasilitas pemrosesan informasi sudah ditetapkan?	√			
	3	Apakah kebijakan dan prosedur tersebut sudah didokumentasikan?	√		√	
	4	Apakah sudah dievaluasi secara berkala atau ketika terjadi perubahan?	√			
	5	Apakah sudah dilakukan perbaikan terus menerus?	√			

Tabel 3 Ringkasan *Maturity Level*

Klausul	Rata-rata per klausul	Keterangan
A.7 *Human Resources Security*	**1,66**	*Performed informally*
A.9 *Access Control*	**2,10**	*Planned and Tracked*
A.11 *Physical and Environmental Security*	**3**	*Well-Defined*
Rata-rata	**2,25**	***Planned and Tracked***

3.3 Analisis *Maturity Level*

Hasil dari penilaian akhir *Maturity Level* PT TASPEN (Persero) KCU Bandung menunjukkan pencapaian praktik keamanan sistem informasi yang dimiliki berdasarkan ISO 27001: 2013. Hasil dari tingkatan *Maturity Level* tersebut akan digambarkan dan dianalisis dengan grafik, yang akan dibandingkan dengan standar tingkatan *Maturity Level* BUMN berdasarkan peraturan menteri BUMN Nomor : PER-02/MBU/2013 dan juga tingkatan *Maturity Level* yang diharapkan atau ditargetkan oleh perwakilan bidang Sistem Informasi, yaitu Senior Network Administrator.

Berikut adalah simbol yang akan digunakan dalam grafik *Maturity Level* :

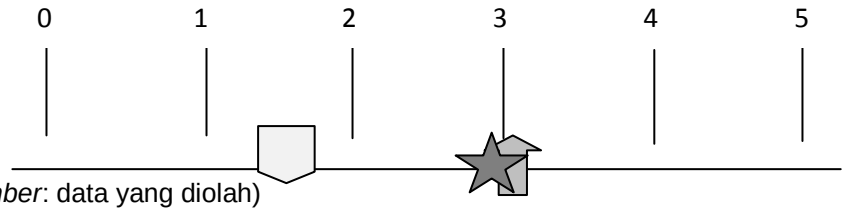
Maturity Level keamanan sistem informasi saat ini

Standar *Maturity Level* BUMN

Target *Maturity Level* PT TASPEN (Persero) KCU Bandung

Berikut ini adalah grafik *Maturity Level* PT TASPEN (Persero) KCU Bandung :

a. Grafik *Maturity Level* Klausul A.7 *Human Resources Security*



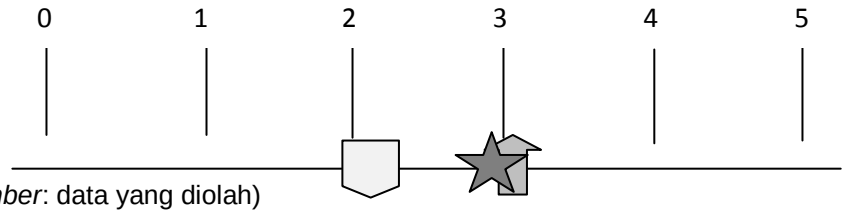
(*Sumber*: data yang diolah)

Gambar 1

Grafik *Maturity Level* Klausul A.7 *Human Resources Security*

Terlihat pada **Gambar 1** bahwa keamanan sistem informasi PT TASPEN (Persero) KCU Bandung yang berkaitan dengan keamanan sumber daya manusia berada pada level 1 (*Performed informally*). Hal ini menunjukkan bahwa keamanan sumber daya manusia yang ada masih dijalankan secara informal. Namun hal ini masih jauh dari harapan dan standar BUMN. Hal ini dikarenakan masih banyaknya kontrol yang dilaksanakan secara informal, tanpa ada aturan atau kebijakan atau prosedur untuk acuan pelaksanaan.

b. Grafik *Maturity Level* Klausul A.9 *Access Control*



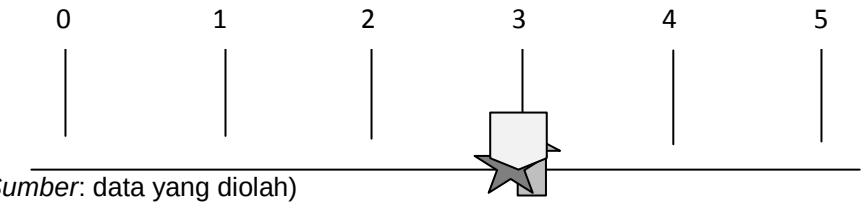
(*Sumber*: data yang diolah)

Gambar 2

Grafik *Maturity Level* Klausul A.9 *Access Control*

Terlihat pada **Gambar 2** bahwa keamanan sistem informasi PT TASPEN (Persero) KCU Bandung yang berkaitan dengan keamanan akses kontrol berada pada level 2 (*planned and tracked*). Hal ini menunjukkan bahwa keamanan akses kontrol yang ada sudah terencanakan, meskipun belum sesuai dengan harapan dan standar BUMN. Hal ini bisa dikarenakan belum adanya prosedur yang didokumentasikan sebagai panduan pelaksanaan, meskipun ada kebijakan yang mengatur.

c. Grafik *Maturity Level* Klausul A.11 *Physical and Environmental Security*



(*Sumber*: data yang diolah)

Gambar 3

Grafik *Maturity Level* Klausul A.11 *Physical and Environmental Security*

Terlihat pada **Gambar 3** bahwa keamanan sistem informasi PT TASPEN (Persero) KCU Bandung yang berkaitan dengan keamanan fisik dan lingkungan berada pada level 3 (*well defined*). Hal ini menunjukkan bahwa keamanan akses kontrol yang ada sudah didefinisikan dengan baik. yang artinya pendokumentasi sudah dilakukan dengan baik, meskipun masih banyak temuan yang didapat. Level yang dicapai juga sudah sesuai dengan harapan dan standar BUMN

4 KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, audit keamanan sistem informasi pada klausul A.7 *Human Resouces Security*, A.9 *Access Control,* dan A.*11 Physical and Environmental Security* pada PT TASPEN (Persero) KCU Bandung menggunakan ISO 27001, maka dapat diambil kesimpulan sebagai berikut:

a. Tingkat kematangan/ *Maturity Level* pada klausul *Human Resouces Security* telah mencapai level 1 (*Performed informally*), yang berarti belum sesuai dengan target PT TASPEN (Persero) KCU Bandung dan standar BUMN.
b. Tingkat kematangan/ *Maturity Level* pada klausul *Access Control* telah mencapai level 2 (*Planned and tracked*), dan belum sesuai dengan target PT TASPEN (Persero) KCU Bandung dan standar BUMN.
c. Tingkat kematangan/ *Maturity Level* pada klausul *Physical and Environmental Security* telah mencapai level 3 (*well defined*). M eskipun sudah sesuai dengan target dan standar BUMN, namun masih didapat temuan dilapangan yang berkaitan dengan pelaksanaan keamanan dan juga prosedur.

DAFTAR PUSTAKA

[1] Elitan, Lena & Anatan, Lina. (2009). *Sistem Informasi Manajemen Konsep dan Praktis.* Bandung: Alfabeta.

[2] Darmawan, Deni dan Fauzi, Kunkun Nur. (2013). Sistem Informasi Manajemen. Bandung: Remaja Rosdakarya.

[3] Sarno, Riyanarto. (2009). *Audit Sistem & Teknologi Informasi.* Surabaya: ITSPress.

[4] Rainer, Kelly., & Turban, Efraim. (2009). *Introduction to Information System.* Asia: ISBN

[5] International Standart ISO/IEC 27001. (2013). *Information Technology – Security Techniques – Information Security Management Systems – Requirement.* ISO/IEC 2013.

[6] Stevanovic, Boris (2011). *Maturity Models in Information Security*. Vol 1 No 2, 2-3. International Journal of Information and Communication Technology Research.