Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005

I Putu Narario Sastra [1] Haryanto Tanuwijaya [2] Erwin Sutomo
Program Studi/Jurusan Sistem Informasi
Institut Bisnis Dan Informatika Stikom Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)narario31@gmail.com, 2)haryanto@stikom.edu, 3)sutomo@stikom.edu

Abstract: *PT. Gresik Cipta Sejahtera (PT. GCS) is a company with a core business field of trade of fertilizers and chemicals in the environment PKG Group subsidiary. PT. GCS has implemented information technology such as enterprise accounting system (SAE), which has been operating for the last 1 year. As for problems that occur during the operation of SAE, namely: 1. Confidentiality error posting sales transactions that are not according to plan, 2. Integrity integrity of property, especially in IT and financial statements did not balance, and 3. Availability of information provision delay budgeting.*

To determine the level of security SAE ongoing, so do security audits SAE PT. GCS Based on ISO Standard 27002: 2005. The scope of the audit used are: 1. Clause 7 (Asset Management), 2. Clause 8 (Security Human Resources), 3. Clause 9 (Physical Security and Environment), and 4. Clause 11 (Access Control).

The value of the maturity level of security aspects confidentiality obtained was 2:53 while the security aspects of integrity and availability are included in the category of managed 2.78, which means most of the process is planned and implemented with limited documentation. The resulting recommendations are making policy and complements the information security procedures to reduce information security risks and improve information security SAE PT. GCS.
Keywords: Audit, *Information Security, ISO 27002:2005, level of maturity.*

PT. Gresik Cipta Sejahtera (PT. GCS) merupakan perusahaan dengan bisnis inti bidang perdagangan pupuk dan bahan kimia. PT. GCS merupakan anak perusahaan Petrokimia Gresik Group. PT. GCS didirikan berdasarkan Akta Pendirian No. 2 tanggal 3 April 1972 dengan Penetapan Menteri Kehakiman RI tertanggal 14 Juli 1972 No. J.A.5/149/16. PT. GCS merupakan hasil penggabungan dua perusahaan yaitu PT. Gresik Chemical and Supplies dengan PT. Petro Aneka Usaha berdasarkan Akte No. 402 tanggal 30 Nopember 1994.

PT. GCS memiliki kantor cabang di Medan, Makassar, Lampung, Riau, Sumatera Selatan, dan Jambi, PT. GCS berkantor pusat di Gedung Petrokimia Gresik Lantai 6, Jl. Jenderal Ahmad Yani - Gresik. Kantor cabang akan mengirimkan seluruh laporan berupa file *microsoft word* dan *microsoft excel* melalui *email* setiap satu minggu sekali ke kantor pusat, karena sistem di kantor cabang belum terkoneksi dengan sistem di kantor pusat.

PT. GCS telah mengimplementasikan teknologi informasi untuk menunjang proses bisnis berupa sistem akuntansi *enterprise* yang bertugas untuk mengelola akuntansi dan keuangan, distribusi (penjualan, pembelian, dan persediaan produk), dan aset. Sistem akuntansi *enterprise* menyediakan berbagai macam informasi penting, yaitu: informasi keuangan, aset, produk, jasa, penjualan, pembelian. Berbagai informasi yang di hasilkan sistem akuntansi *enterprise* ini berhubungan dengan beberapa bagian di PT. GCS, yaitu: bagian akuntansi dan keuangan, bagian penjualan, bagian pembelian, dan bagian TI.

Permasalahan yang terjadi adalah dari sisi (*Confidentiality*) kesalahan *posting* data transaksi penjualan yang tidak sesuai dengan perencanaan. Hal ini berdampak pada keterlambatan penyediaan informasi *budgeting*. Dari sisi (*Integrity*) keutuhan pencatatan aset khususnya di bidang TI dan laporan keuangan (tidak *balance*) yang disusun dari data persediaan, PPn masukan, hutang, piutang, PPn keluaran, dan penjualan. Dari sisi (*Availability*) keterlambatan penyediaan informasi *budgeting* yang disusun dari data *detail trial balance*, *summary trial balance*, laporan laba rugi, dan neraca. Dampak dari permasalahan ini adalah keterlambatan pihak manajemen dalam proses pengambilan keputusan dan terjadinya kesalahan

dalam penentuan kebijakan perencanaan anggaran bulanan dan tahunan PT. GCS yang menyebabkan penurunan kepercayaan *investor* dan *costumer* pada perusahaan.

PT. GCS tidak mengetahui sebab terjadinya masalah tersebut dan tingkat keamanan SAE, maka dari itu perlu dilakukan evaluasi keamanan SAE dengan cara melakukan audit keamanan SAE. Beberapa faktor pendukung pemilihan standar ISO 27002 sebagai acuan audit keamanan SAE yaitu: 1. ISO 27002 merupakan panduan praktis teknik keamanan informasi, 2. terdapat sertifikat SMKI yang telah diakui oleh internasional.

Penelitian ini diharapkan dapat mengukur tingkat keamanan SAE PT. GCS, sehingga dapat diketahui apakah SMKI yang sudah diterapkan sesuai dengan hasil yang diharapkan. Hasil penelitian dapat menjadi dasar untuk meningkatkan keamanan informasi SAE PT. GCS serta sebagai acuan untuk memperoleh ISMS *certification* dengan standar ISO 27002:2005.

METODOLOGI PENELITIAN

Gambar 1. Tahapan Audit Teknologi Informasi (Sumber: ISACA, 2010)

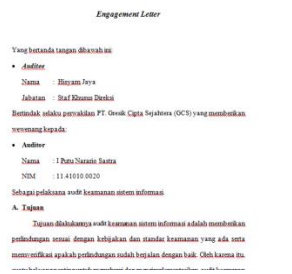
Dari 8 tahapan metode (ISACA, 2010), tahapan yang digunakan dalam Tugas Akhir ini adalah audit *charter*, *planning*, *performance of* audit *work*, dan *reporting* yang terbagi dalam 4 langkah:

1. Perencanaan Audit.
2. Persiapan Audit.
3. Pelaksanaan Audit.
4. Pelaporan Audit.

HASIL DAN PEMBAHASAN

Membuat *Engagement Letter*

Contoh *Engagement letter* pada Gambar 2 dibuat oleh auditor agar mendapat persetujuan mengenai kegiatan audit keamanan SAE, dan *auditee* dapat memberikan akses kepada auditor terhadap SAE dan lingkungannya. Isi dari *engagement leter* adalah keterangan nama auditor dan perwakilan *auditee*, tujuan audit keamanan SAE, keterangan tim auditor, ruang lingkup audit, wewenang kedua belah pihak, tanggung jawab kedua belah pihak, idependensi, obyektivitas, integritas, kerahasiaan, tabel kerja, dan penutup.



Engagement Letter

Yang bertanda tangan dibawah ini:

- *Auditee*

Nama : Hinyam Jaya

Jabatan : Staf Khusus Direksi

Bertindak selaku perwakilan PT. Gresik Cipta Sejahtera (GCS) yang memberikan wewenang kepada:

- Auditor

Nama : I Putu Narantu Sastra

NIM : 11.41010.0020

Sebagai pelaksana audit keamanan sistem informasi

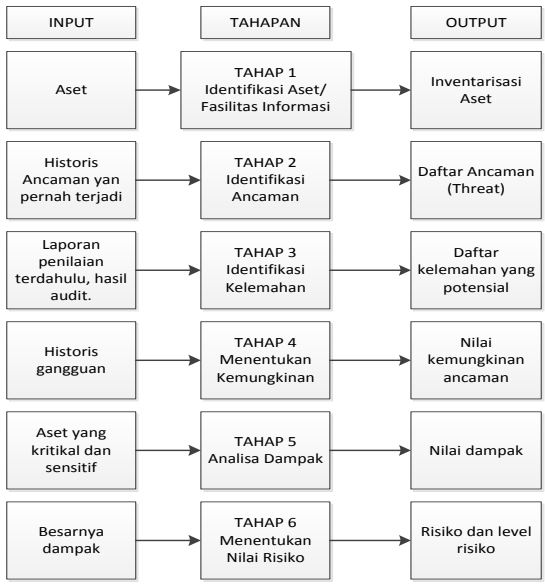
A. Tujuan

Tujuan dilaksanakanya audit keamanan sistem informasi adalah memberikan perlindungan sesuai dengan kebijakan dan standar keamanan yang ada serta memverifikasi apakah perlindungan sudah berjalan dengan baik. Oleh karena itu.

Gambar 2. *Engagement Letter*

Menentukan Tujuan, Ruang Lingkup, dan Risiko

1. Tujuan audit keamanan sistema akuntansi *enterprise* PT. GCS adalah audit substansi.
2. Sarno dan Iffano (2009) mengungkapkan hal-hal yang dibutuhkan dalam menentukan ruang lingkup SMKI adalah:
   a. Dokumen komitmen manajemen.
   b. Kondisi eksisting organisasi, antara lain: karakteristik proses bisnis organisasi, lokasi organisasi, aset-aset yang dimiliki, dan teknologi yang digunakan.
3. Setelah menentukan ruang lingkup, maka auditor akan melakukan penilaian risiko. Tahapan penilaian risiko dapat dilihat pada Gambar 3.



Gambar 3. Tahapan Penilaian Risiko (Sumber: Sarno dan Iffano, 2009)

Klausul ISO 27002:2005

Dari hasil pemetaan permasalahan yang terjadi dengan kontrol keamanan ISO 27002:2005 klausul-klausul tersebut dapat dikelompokkan menjadi 3 kelompok kontrol keamanan, yaitu manajemen/organisasi (*organizational*), teknikal (*technical*), dan operasional (*operational*) dapat dilihat pada Tabel 1. Dengan demikian, organisasi dapat memilih kontrol keamanan yang sesuai dengan kebutuhan organisasi.

Tabel 1. Kebutuhan Kontrol Keamanan

Kategori Kebutuhan	No. Klausul	Klausul Kontrol Keamanan
Manajemen atau Organisasi	5	*Security Policy*
	6	*Organization of Information Security*
	7	*Asset Manegement*
	15	*Compliance*
Teknikal	8	*Human Resources Security*
	9	*Physical and Environmental Security*
	11	*Access Control*
	12	*Information Systems Acquisition, Development and Maintenance*
Operasional	10	*Communication and Operation Management*
	13	*Information Security Incident Management*
	14	*Business Continuity Management*

(Sumber: Sarno dan Iffano, 2009)

Klausul yang digunakan dalam Tugas Akhir ini adalah klausul 7 (manajemen aset), klausul 8 (keamanan sumber daya manusia), klausul 9 (keamanan fisik dan lingkungan), dan klausul 11 (kontrol akses).

Pernyataan

Pernyataan yang telah dibuat berdasarkan kontrol keamanan yang terdapat pada klausul ISO 27002:2005. Tabel 2 merupakan contoh pernyataan klausul 9.

Tabel 2. Pernyataan

Audit Keamanan Sistem Informasi Klausul 9 (Keamanan Fisik dan Lingkungan)	Auditor: I Putu Narario Sastra *Auditee*: Pak Hisyam Tanggal: 20-10-2015 Tanda Tangan:	
Klausul 9.1 Wilayah Aman (*Secure Areas*)		
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)		
Kontrol : Pembatasan keamanan (dinding pengaman, kontrol kartu akses, penjaga) harus disediakan untuk melindungi wilayah dan perangkat pemrosesan informasi.		
No.	**PERNYATAAN**	
1.	Mempunyai parameter keamanan yang harus didefinisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi.	
2.	Dinding bangunan harus terbuat dari konstruksi yang kuat.	
3.	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.	
4.	Mempunyai ruang penerimaan tamu.	
5.	Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.	

Pembobotan

Dari hasil diskusi yang dilakukan oleh auditor dengan *auditee*, maka didapat hasil pembobotan pernyataan berdasarkan tingkat kepentingan pernyataan yang ada bagi perusahaan. Tabel 3 adalah contoh pembobotan pernyataan klausul 9.

Tabel 3. Pembobotan

Audit Keamanan Sistem Informasi Klausul 9 (Keamanan Fisik dan Lingkungan)	Auditor: I Putu Narario Sastra *Auditee*: Pak Hisyam Tanggal: 20-10-2015 Tanda Tangan:	
Klausul 9.1 Wilayah Aman (*Secure Areas*)		
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)		
Kontrol : Pembatasan keamanan (dinding pengaman, kontrol kartu akses, penjaga) harus disediakan untuk melindungi wilayah dan perangkat pemrosesan informasi.		
No.	**PERNYATAAN**	**Bobot**
1.	Mempunyai parameter keamanan yang harus didefinisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi.	0.3
2.	Dinding bangunan harus terbuat dari konstruksi yang kuat.	0.3
3.	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.	1
4.	Mempunyai ruang penerimaan tamu.	1

Pertanyaan

Pertanyaan dibuat untuk diajukan pada *auditee* saat pelaksanaan audit keamanan SAE. Pertanyaan mengacu pada pernyataan yang ada, dengan menggunakan metode 5W + 1H. Tabel 4 adalah contoh pertanyaan klausul 9.

Tabel 4. Pertanyaan

Audit Keamanan Sistem Informasi Klausul 9 (Keamanan Fisik dan Lingkungan)		Auditor : I Putu Narario S *Auditee* : Pak Hisyam Tanggal : 6-11-2015 Tanda Tangan :
Klausul 9.1 Wilayah Aman (*Secure Areas*)		
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)		
1	Mempunyai parameter keamanan yang harus di definisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi. P: Apakah perusahaan memiliki parameter keamanan yang telah di definisikan secara jelas terhadap ruang pemrosesan informasi (dinding, kartu akses, penjaga pintu)? J: P: Siapa yang bertugas menjaga pintu atau mengontrol ruang pemrosesan informasi? J: P: Apakah letak ruang pemrosesan informasi sudah sesuai dengan parameter keamanan yang ditetapkan perusahaan? J: P: Bagaimana pertimbangan pihak manajemen dalam penentuan parameter keamanan untuk ruang pemrosesan informasi? J:	

Wawancara dan Observasi

Wawancara dilakukan oleh auditor dengan kabag akuntansi dan keuangan dengan ruang lingkup klausul 7 (manajemen aset), pegawai SDM dengan ruang lingkup klausul 8 (keamanan SDM), dan staf khusus direksi yang bertanggung jawab terhadap SAE dengan ruang lingkup klausul 9 tentang keamanan fisik dan lingkungan, dan klausul 11 tentang kontrol akses. Wawancara mengacu pada pertanyaan yang telah dibuat, Tabel 5 merupakan contoh wawancara pada klausul 9.

Tabel 5. Wawancara

Audit Keamanan Sistem Informasi Klausul 9 (Keamanan Fisik dan Lingkungan)	Auditor : I Putu Narario S *Auditee* : Pak Hisyam Tanggal : 6-11-2015 Tanda Tangan :
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)	
1 Mempunyai parameter keamanan yang harus di definisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi.	
P: Apakah perusahaan memiliki parameter keamanan yang telah di definisikan secara jelas terhadap ruang pemrosesan informasi (dinding, kartu akses, penjaga pintu)? J: Perusahaan tidak memiliki definisi dari parameter keamanan untuk ruang pemrosesan informasi, parameter keamanan untuk ruang pemrosesan informasi, berupa dinding pembatas atau ruangan. P: Siapa yang bertugas menjaga pintu atau mengontrol ruang pemrosesan informasi? J: Yang bertugas menjaga atau mengontrol ruang pemrosesan informasi adalah Staf TI. P: Apakah letak ruang pemrosesan informasi sudah sesuai dengan parameter keamanan yang ditetapkan perusahaan? J: Menurut organisasi, letak ruang pemrosesan informasi sudah sesuai dengan parameter keamanan. P: Bagaimana pertimbangan pihak manajemen dalam penentuan parameter keamanan untuk ruang pemrosesan informasi? J: Pertimbangan pihak manajemen dalam penentuan parameter keamanan ruang pemrosesan informasi adalah keamanan peralatan, kemudahan operasional, terdapat pembatas atau ruangan pemrosesan informasi, pengaturan suhu udara yang tepat 23°C agar tidak cepat panas.	

Hasil Pemeriksaan Data, Bukti, dan Temuan

Auditor melakukan wawancara dan observasi untuk memperoleh bukti serta temuan terkait permasalahan yang terjadi. Contoh hasil pemeriksaan auditor klausul 9 ditunjukkan pada Tabel 6.

Tabel 6. Dokumen Pemeriksaan

Program Pemeriksaan Audit Keamanan Sistem Informasi Aspek : Klausul 7 (Manajemen Aset)	Pemeriksa : Pak Haryanto/Pak Erwin Auditor : I Putu Narario S *Auditee* : Pak Joko Tanggal : 29-10-2015 Tanda Tangan :
7.1 Tanggung Jawab Aset (*Responsibility for Assets*)	
7.1.1 Inventarisasi Aset (*Inventory of Assets*)	
No Pemeriksaan	Catatan Auditor
1. Identifikasi proses inventarisasi aset organisasi, dengan cara: 1. Wawancara mengenai proses inventarisasi aset organisasi. 2. Mendapatkan dokumentasi inventarisasi aset berupa dokumen daftar aktiva tetap dan foto laporan posisi aset pada sistem akuntansi *enterprise* (SAE).	Proses inventarisasi aset sudah dilakukan, tetapi pencatatan aset *software* tidak ada dan pencatatan aset *hardware* tidak lengkap. Pencatatan aset SAE tidak di masukkan ke dalam dokumen daftar aktiva tetap dan laporan posisi aset. Pencatatan *hardware* hanya ada PC, laptop, printer, pencatatan mengenai perangkat *server* tidak ada.
2. Identifikasi proses pemeliharaan terhadap aset organisasi, dengan cara: 1. Wawancara mengenai proses pemeliharaan terhadapaset organisasi. 2. Mendapatkan dokumen prosedur pemeliharaan.	Proses pemeliharaan terhadap aset organisasi sudah dilakukan rutin selama 1 tahun sekali untuk PC dan Laptop. Proses pemeliharaan terkait aset TI yang lain seperti perangkat *server* belum dilakukan dan tidak ada dokumen prosedur pemeliharaan untuk aset TI selain PC dan laptop.

Uji Kematangan

Uji kematangan menggunakan *Capability Maturity Model for Integration* (CMMI) to ISO 27002 pada Tabel 7 untuk mengetahui tingkat kematangan penerapan pengamanan. Berdasarkan hasil wawancara dari pengumpulan bukti dan temuan dengan *auditee*, maka diperoleh tingkat kematangan untuk masing-masing aspek keamanan informasi *confidentiality*, *integrity*, *availability* (CIA) dapat dilihat tabel 8. Tabel 9 adalah hasil perhitungan tingkat kematangan pada klausul 9, dan Gambar 6 merupakan representasi nilai tingkat kematangan. Dari hasil uji kematangan ini dapat diketahui keadaan keamanan SAE PT. GCS saat ini.

Tabel 7. CMMI to ISO 27002

Level	*Continous Representation Capability Levels*	*Staged Representation Maturity Levels*
0	***Incomplete***	
1	***Performed***	***Initial***
2	***Managed***	***Managed***
3	***Defined***	***Defined***
4		***Quantitatively Managed***
5		***Optimizing***

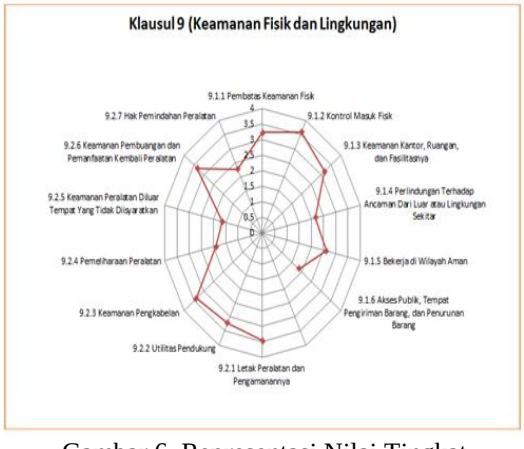
(Sumber: CMMI-DEV V1.3, 2010)

Tabel 8. Tingkat Kematangan

Klausul 9 (Keamanan Fisik dan Lingkungan)								
Klausul 9.1 Wilayah Aman (*Secure Areas*)								
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)								Nilai
No	Pernyataan	Bobot	0	1	2	3	4	5	
1.	Mempunyai parameter keamanan yang harus didefinisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi.	0.3	√						0
2.	Dinding bangunan harus terbuat dari konstruksi yang kuat.	0.3					√		4
3.	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.	1		√					1
4.	Mempunyai ruang penerimaan tamu.	1					√		4
5.	Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.	0.3			√				2
6.	Mempunyai pintu darurat yang selalu di kontrol.	0.6				√			3
7.	Pintu harus beroperasi dengan menggunakan kode darurat (kebakaran).	0.6				√			3
8.	Memiliki CCTV yang digunakan untuk memantau lingkungan kerja (monitoring).	1		√					1
9.	Ruangan pemrosesan informasi dikelola oleh organisasi.	1			√				2
10.	Ruangan pemrosesan inforamsi harus dipisahkan dari pihak ketiga.	1				√			3
Total Bobot		7.10	Total Nilai						23
Tingkat Kematangan									3.23

Tabel 9. Hasil Perhitungan Tingkat Kematangan Klausul 9

Tabel Penentuan Tingkat Kematangan Klausul 9 Keamanan Fisik dan Lingkungan				
No	Objektif Kontrol	Kontrol Keamanan	Tingkat Kematangan	Rata-Rata Tingkat Kematangan
1.	Klausul 9.1 Wilayah Aman (*Secure Areas*)	9.1.1 Pembatas Keamanan Fisik	3.23	2.78
		9.1.2 Kontrol Masuk Fisik	3.60	
		9.1.3 Keamanan Kantor, Ruangan, dan Fasilitasnya	3.17	
		9.1.4 Perlindungan Terhadap Ancaman Dari Luar atau Lingkungan Sekitar	2.18	
		9.1.5 Bekerja di Wilayah Aman	2.63	
		9.1.6 Akses Publik, Tempat Pengiriman Barang, dan Penurunan Barang	1.87	
2.	Klausul 9.2 Keamanan Peralatan (*Equipment Security*)	9.2.1 Letak Peralatan dan Pengamanannya	3.46	2.75
		9.2.2 Utilitas Pendukung	3.22	
		9.2.3 Keamanan Pengkabelan	3.38	
		9.2.4 Pemeliharaan Peralatan	1.90	
		9.2.5 Keamanan Peralatan Diluar Tempat Yang Tidak Diisyaratkan	1.66	
		9.2.6 Keamanan Pembuangan dan Pemanfaatan Kembali Peralatan	3.33	
		9.2.7 Hak Pemindahan Peralatan	2.28	
Tingkat Kematangan Klausul 9 (Keamanan Fisik dan Lingkungan)				2.76



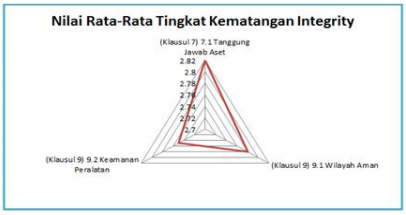
Gambar 6. Representasi Nilai Tingkat Kematangan Klausul 9

Dari proses perhitungan didapat nilai tingkat kematangan Klausul 9 (2.76) termasuk dalam

kategori *managed* yang berarti keamanan fisik dan lingkungan SAE PT. GCS masih dalam pengembangan dengan dokumentasi terbatas. Tabel 10 adalah hasil perhitungan tingkat kematangan aspek keamanan *integrity*, dan Gambar 7 merupakan hasil representasi tingkat kematangan *integrity*.

Tabel 10. Hasil Perhitungan Tingkat Kematangan *Integrity*

Klausul	Deskripsi	Tingkat Kematangan
Klausul 7)	7.1 Tanggung Jawab Aset	2.82
Klausul 9)	9.1 Wilayah Aman	2.78
Klausul 9)	9.2 Keamanan Peralatan	2.75
Nilai Rata-Rata Tingkat Kematangan (*Integrity*)		2.78



Gambar 7. Representasi Tingkat Kematangan *Integrity*

Nilai tingkat kematangan aspek keamanan *confidentiality* yang didapat adalah 2.53 sedangkan aspek keamanan *integrity* dan *availability* adalah 2.78 termasuk dalam kategori *managed* yang berarti sebagian besar proses sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas.

Temuan dan Rekomendasi

Dari hasil temuan yang didapat oleh auditor, penentuan nilai bobot kategori *medium* (0.6) dan *high* (1) yang sudah disepakati oleh auditor dan *auditee*, nilai tingkat kematangan yang dihasilkan, dipadukan dengan keterkaitan referensi antar klausul pada ISO 27002:2005, maka dibuatlah rekomendasi berdasarkan 3 kategori, yaitu: manajemen, teknikal, dan operasional mengacu pada ISO 27002:2005 untuk proses perbaikan keamanan sistem akuntansi *enterprise* PT. Gresik Cipta Sejahtera. Tabel 11 adalah contoh temuan dan rekomendasi klausul 9, dan Gambar 8 ruang pemrosesan informasi merupakan salah satu bukti foto pada klausul 9.

Tabel 11. Temuan dan Rekomendasi

Temuan Audit Keamanan Sistem Akuntansi *Enterprise*		Pemeriksa: I Putu Narario S Penyelia: Pak Haryanto Pak Erwin
Aspek : Klausul 9 Keamanan Fisik dan Lingkungan 9.1.1 Pembatas Keamanan Fisik		*Auditee*: Pak Hisyam Tanggal: 17-11-2015
No	Pernyataan	Temuan	Referensi, Risiko, dan Rekomendasi
3	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.	Perusahaan memiliki batasan akses ke ruang pemrosesan informasi berupa ruangan khusus untuk *server*. Ruang pemrosesan informasi masih dapat di akses oleh seluruh pegawai, karena di gabung oleh ruang foto *copy*.	Referensi: Pertanyaan 9.1.1 No. 3. Bukti: Lampiran 8 No. 23. Ref: ISO 27002 9.1.1 Pembatas Keamanan Fisik Risiko: - Pencemaran lingkungan dapat terjadi karena tidak disediakan tempat sampah di wilayah ruang pemrosesan informasi. - Akses ilegal oleh pegawai selain divisi TI dapat menyebabkan kerusakan pada *server* karena ruangan *server* digabung dengan ruang foto *copy* dan tidak dikunci pada jam kerja. Rekomendasi: a. Menyediakan tempat sampah disekitar ruang pemrosesan informasi agar tidak terjadi pencemaran lingkungan. b. Memisahkan ruang pemrosesan informasi dengan ruang foto *copy*, agar tidak semua pegawai dapat mengakses ruang *server* kecuali pegawai TI yang memiliki hak akses. c. Mengunci ruangan *server* pada jam kerja, dan kunci dipegang oleh pegawai TI yang memiliki hak akses ke ruangan *server*.

Gambar 8. Ruang Pemrosesan Informasi

Pelaporan Audit Keamanan SAE

Auditor wajib memberikan laporan audit keamanan SAE yang telah dilaksanakan pada *auditee*. Laporan audit hanya ditunjukkan pada pihak yang berhak saja, karena sifatnya rahasia. Keluaran dari tahap ini adalah Surat Pernyataan Pelaporan Audit dan *Exit Meeting*.

Kesimpulan

Berdasarkan Audit Keamanan Sistem Akuntansi *Enterprise* yang telah dilakukan:

1. Perencanaan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 dibuat berdasarkan langkah ISACA 2010, yaitu: *audit charter* dan *planning*.
   a. *Audit Charter* adalah langkah awal yang dilakukan dengan membuat *engagement letter*.
   b. *Planning* adalah langkah kedua yang dilakukan dengan menentukan tujuan, ruang lingkup audit meliputi dokumen gambaran umum perusahaan dan *sysflow* sistem akuntansi *enterprise*, melakukan penilaian risiko dengan

metode kuantitatif pendekatan matematis, melakukan pemetaan permasalahan yang terjadi dengan klausul kontrol keamanan ISO 27002:2005 sehingga dapat mempermudah organisasi dalam memilih kontrol keamanan yang akan digunakan untuk audit, dan membuat jadwal kerja audit.

2. Melaksanakan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 yang terdiri dari tahap perencanaan audit dan pelaksanaan audit.
   a. Tahap perencanaan audit dilakukan dengan cara membuat pernyataan berdasarkan standar ISO 27002:2005, melakukan pembobotan menggunakan rujukan (Niekerk dan Labuschagne dalam Yaner, 2006), dan membuat pertanyaan dengan menggunakan metode 5W+1H.
   b. Tahap pelaksanaan audit dilakukan dengan cara wawancara kepada *auditee* berdasarkan pertanyaan yang telah dibuat sebelumnya, melakukan pemeriksaan bukti dan temuan berdasarkan langkah ISACA 2010 *performance of audit work* sehingga menghasilkan catatan pemeriksaan auditor, melakukan uji kematangan dengan metode CMMI-DEV V1.3, menyusun temuan dan membuat rekomendasi, menyusun bukti audit berupa foto.
3. Penutup audit sesuai dengan tahapan ISACA 2010 *reporting* dilakukan dengan cara menyusun hasil Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 sehingga menghasilkan draf laporan audit, hasil audit juga dilengkapi dengan dokumen pengesahan dari pihak *auditee* berupa surat pernyataan pelaporan audit dan *exit meeting*.

Maka didapat kesimpulan berupa nilai tingkat kematangan dari aspek keamanan *confidentiality* adalah 2,53 aspek keamanan *integrity* dan *availability* adalah 2,78 termasuk dalam kategori *managed* yang berarti sebagian besar proses sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Rekomendasi yang dihasilkan adalah membuat kebijakan dan melengkapi prosedur keamanan informasi untuk menurunkan risiko-risiko keamanan informasi dan meningkatkan keamanan informasi SAE PT. GCS.

Saran

Saran yang diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. PT. Gresik Cipta Sejahtera dapat melakukan Audit Keamanan Sistem Akuntansi *Enterprise* secara berkala 6 bulan atau 1 tahun sekali agar keamanan sistem akuntansi *enterprise* tetap terkontrol. Audit dapat dilakukan oleh auditor internal maupun eksternal demi meningkatkan keamanan sistem akuntansi *enterprise*.
2. Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 dapat dikembangkan lagi pada penelitian serupa berikutnya dengan menggunakan klausul 5 Kebijakan Keamanan, klausul 6 Organisasi Keamanan Informasi, klausul 10 Komunikasi dan Manajemen Operasional, klausul 13 Manajemen Insiden Keamanan Informasi, dan klausul 15 Kesesuaian berdasarkan dari hasil pemetaan pada penelitian ini agar PT. GCS dapat mengetahui tingkat keamanan SAE lebih detil sesuai dengan permasalahan yang terjadi.

RUJUKAN

Asmuni, I. dan Firdaus, R. *Peranan Pengendalian Berbasis Audit Sistem Informasi Untuk Pengembangan Strategi Perusahaan Berbasis Komputer* (Suatu Bahasan Teoritis Atas Faktor Penentu Keberhasilan dan Penyimpangan Penerapan Sistem Informasi Dalam Suatu Organisasi Usaha), Yogyakarta: Seminar Nasional Aplikasi Teknologi Informasi, 2005.

CMMI-DEV, V1.3. 2010. *Improving processes for developing better products and services*. Software Engineering Institute, Carnegie Mellon University.

ISACA. 2010. *Guide to the Audit of IT Application*. Switzerland : Felice Lutz.

ISO/IEC 27002. 2005. *Information technology — Security techniques — Code of practice for information security management International*.ISO.

Sarno, R. dan Iffano, I. 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press.

Tanuwijaya, H. dan Sarno, R. 2010. *Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals*, International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

Yaner, Annisa Destiara. 2013. *Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Management (SIM-RS) Berdasarkan ISO 27002:2005 (Pada Rumah Sakit Haji Surabaya)*. Laporan Tugas Akhir: STIKOM Surabaya.