AUDIT KEAMANAN SISTEM AKUNTANSI *ENTERPRISE* PT. GRESIK CIPTA SEJAHTERA BERDASARKAN STANDAR ISO 27002:2005

TUGAS AKHIR

Program Studi

S1 Sistem Informasi

Oleh:

I PUTU NARARIO SASTRA

11.41010.0020

FAKULTAS TEKNOLOGI DAN INFORMATIKA
INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA
2016

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

AUDIT KEAMANAN SISTEM AKUNTANSI *ENTERPRISE* PT. GRESIK CIPTA SEJAHTERA BERDASARKAN STANDAR ISO 27002:2005

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk menyelesaikan

Program Sarjana Komputer

Oleh:

Nama : I Putu Narario Sastra

NIM : 11.41010.0020

Program : S1 (Strata Satu)

Jurusan : Sistem Informasi

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2016

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

TUGAS AKHIR

AUDIT KEAMANAN SISTEM AKUNTANSI *ENTERPRISE* PT. GRESIK CIPTA SEJAHTERA BERDASARKAN STANDAR ISO 27002:2005

Dipersiapkan dan disusun oleh

I Putu Narario Sastra

NIM : 11.41010.0020

Telah diperiksa, diuji dan disetujui oleh Dewan Penguji

Pada : Juni 2016

Susunan Dewan Penguji

Pembimbing

I. Dr. Haryanto Tanuwijaya, S.Kom., M.MT. _____

II. Erwin Sutomo, S.Kom., M.Eng. _____

Penguji

I. Tutut Wurijanto, M.Kom. _____

II. Yoppy Mirza Maulana, S.Kom., M.MT. _____

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana

Dr. Jusak
Dekan Fakultas Teknologi dan Informatika

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai Mahasiswa Institut Bisnis dan Informatika Stikom Surabaya, saya:

Nama : I Putu Narario Sastra

NIM : 11.41010.0020

Program Studi : S1 Sistem Informasi

Fakultas : Teknologi dan Informatika

Jenis Karya : Tugas Akhir

Judul Karya : **AUDIT KEAMANAN SISTEM AKUNTANSI *ENTERPRISE* PT. GRESIK CIPTA SEJAHTERA BERDASARKAN STANDAR ISO 27002:2005**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Institut Bisnis dan Informatika Stikom Surabaya Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalti Free Right)* atas seluruh isi atau sebagian karya ilmiah saya tersebut untuk disimpan, dialihmediakan, dan dikelola dalam bentuk pangkalan data (*database*) untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.
2. Karya tersebut adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya.
3. Apabila dikemudian hari ditemukan dan terbukti tindakan plagiat di karya ilmiah ini, maka saya bersedia untuk menerima pencabutan gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, Juni 2016

(I Putu Narario Sastra)
11.41010.0020

Hasil Tugas Akhir ini didekikasikan oleh penulis untuk kedua orang tua tercinta,

adek tercinta, dosen pembimbing,

staf PT. GCS, dan sahabat seperjuangan.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

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.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

ABSTRAK

PT. Gresik Cipta Sejahtera (PT. GCS) adalah perusahaan dengan bisnis inti bidang perdagangan pupuk dan bahan kimia dalam lingkungan anak perusahaan Petrokimia Gresik Group. PT. GCS telah mengimplementasikan teknologi informasi berupa sistem akuntansi *enterprise* (SAE) yang telah beroperasi selama 1 tahun terakhir. Adapun permasalahan yang terjadi selama pengoperasian SAE yaitu: 1. *Confidentiality* kesalahan *posting* transaksi penjualan yang tidak sesuai perencanaan, 2. *Integrity* keutuhan pencatatan aset khususnya di bidang TI dan laporan keuangan tidak *balance*, dan 3. *Availability* keterlambatan penyediaan informasi *budgeting*.

Untuk mengetahui tingkat keamanan SAE yang sedang berlangsung, maka dilakukan audit keamanan SAE PT. GCS Berdasarkan Standar ISO 27002:2005. Ruang lingkup audit yang digunakan yaitu: 1. Klausul 7 (Manajemen Aset), 2. Klausul 8 (Keamanan Sumber Daya Manusia), 3. Klausul 9 (Keamanan Fisik dan Lingkungan), dan 4. Klausul 11 (Kontrol Akses).

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. Rekomendasi yang dihasilkan adalah membuat kebijakan dan melengkapi prosedur keamanan informasi untuk menurunkan risiko-risiko keamanan informasi dan meningkatkan keamanan informasi SAE PT. GCS.

Kata Kunci: Audit, Keamanan Informasi, ISO 27002:2005, Tingkat Kematangan.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadapan Tuhan Yang Maha Esa karena atas bimbingan dan karunia-Nya sehingga penulis mampu menyelesaikan Tugas Akhir ini yang berjudul "Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005".

Dalam proses Tugas Akhir ini, banyak kesulitan yang dialami oleh penulis. Kesulitan itu timbul karena kemampuan dan pengalaman penulis yang terbatas. Akan tetapi berkat bantuan dan dorongan dari berbagai pihak, sehingga penulis dapat menyelesaikan Tugas Akhir ini. Oleh karena itu, penulis mengucapkan terima kasih yang sedalam-dalamnya kepada :

1. Papa, Mama, Dedek, dan Keluarga Besar yang selalu memberikan semangat dan memotivasi saya untuk menyelesaikan Tugas Akhir ini.
2. Bapak Dr. Haryanto Tanuwijaya, S.Kom., M.MT. dan Bapak Erwin Sutomo, S.Kom., M.Eng. selaku Dosen Pembimbing Tugas Akhir ini.
3. Bapak Tutut Wurijanto, M.Kom. dan Bapak Yoppy Mirza Maulana, S.Kom., M.MT. selaku dosen penguji Tugas Akhir ini.
4. Bapak Achmad Teguh Wibowo, S.Kom., M.T. selaku Dosen Wali terdahulu dan Bapak Dr. Drs. Antok Supriyanto, M.MT. selaku Dosen Wali yang sekarang.
5. Bapak Hisyam Jaya, Bapak Joko, Bapak Nanang, dan Bapak I.B.K. Bhayangkara selaku penyelia Tugas Akhir ini.
6. Bapak dan Ibu Dosen serta Staf STIKOM Surabaya.

7. Teman-teman sesama mahasiswa seperjuangan yang selalu memberikan semangat untuk menyelesaikan Tugas Akhir ini.

Demikian semoga perhatian dan petunjuknya dapat menjadi karma baik. Di samping itu penulis juga menyadari bahwa karya ini masih belum sempurna, penulis berharap semoga pembaca dapat memberikan saran demi perbaikan karya ini.

Surabaya, Juni 2016

Penulis

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

DAFTAR ISI

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

DAFTAR TABEL

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

DAFTAR GAMBAR

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

DAFTAR LAMPIRAN

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

BAB I

PENDAHULUAN

1.1 Latar Belakang

PT. Gresik Cipta Sejahtera (PT. GCS) adalah 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, *budgeting*. 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.

Adapun 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. Hal ini dapat menimbulkan risiko menurunnya tingkat kepercayaan *investor* dan *customer* pada perusahaan, dan dapat menyebabkan kerugian bagi perusahaan.

Selama ini PT. GCS belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut, oleh karena itu PT. GCS tidak mengetahui bagaimana tingkat keamanan sistem informasi yang dimilikinya. PT. GCS membutuhkan evaluasi keamanan sistem informasi yang dimilikinya. Evaluasi keamanan sistem informasi dapat dilakukan dengan audit keamanan sistem informasi (Asmuni dan Firdaus, 2005). Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), dan ketersediaan (*Availability*) dari informasi (ISO/IEC 27002, 2005). Agar audit keamanan sistem informasi dapat

berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya dan Sarno, 2010). Menurut (Sarno dan Iffano, 2009) tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi.

Standar ISO 27002 dipilih dengan pertimbangan bahwa standar ini berisi panduan praktis (*code of practice*) teknik keamanan informasi. Pertimbangan lainnya adalah ISO 27002 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional yang disebut *Information Security Management Sistem* (ISMS) *certification* (Sarno dan Iffano, 2009).

Dengan adanya penelitian tugas akhir tentang audit keamanan sistem akuntansi *enterprise* pada PT. GCS diharapkan dapat mengukur tingkat keamanan sistem informasi yang ada, sehingga akan menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sesuai dengan hasil yang diharapkan. Hasil penelitian ini diharapkan menjadi masukan yang dapat digunakan untuk meningkatkan keamanan informasi pada perusahaan serta menjadi acuan untuk mendapatkan ISMS *certification* dengan standar ISO 27002:2005.

1.2 Perumusan Masalah

1. Bagaimana membuat perencanaan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005.
2 Bagaimana melaksanakan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

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

1.3 Batasan Masalah

1. Sistem informasi yang di audit adalah Sistem Akuntansi *Enterprise*.
2. Audit hanya dilakukan pada kantor pusat PT. Gresik Cipta Sejahtera yang terletak di Gedung Petrokimia Gresik Lantai 6, Jl. Jenderal Ahmad Yani - Gresik.
3. Tahapan audit yang digunakan adalah tahapan ISACA 2010.
4. Tahapan audit yang tidak digunakan dari ISACA 2010 adalah *independence, professional ethics and standards*, *professional competence*, dan *follow-up activities*.
5. Periode data yang digunakan untuk Audit Keamanan Sistem Akuntansi *Enterprise* adalah tahun 2015.

1.4 Tujuan

1. Menghasilkan perencanaan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 yang terdiri dari membuat *engagement letter*, menentukan tujuan, ruang lingkup, dan risiko, membuat jadwal kerja audit.
2. Melaksanakan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 dengan menganalisa hasil wawancara berupa bukti, dan temuan-temuan audit sehingga dapat mengukur tingkat kematangan.
3. Menyusun hasil Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 dengan melakukan analisa dan

evaluasi dari bukti dan temuan yang ada sehingga didapat laporan hasil audit yang berupa temuan dan rekomendasi.

1.5 Sistematika Penulisan

Laporan Tugas Akhir ini ditulis dengan sistematika penulisan sebagai berikut:

BAB I: PENDAHULUAN

Pada bab ini membahas tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, dan sistematika penulisan buku Tugas Akhir ini.

BAB II: LANDASAN TEORI

Pada bab ini membahas tentang teori audit, audit sistem infromasi, keamanan informasi, sistem informasi, sistem informasi akuntansi, anggaran (*budget*), laporan keuangan, audit keamanan sistem informasi, manajemen aset, tahapan audit, standar sistem manajemen keamanan informasi, ISO 27002:2005, *maturity level*, dan lain-lain.

BAB III: METODE PENELITIAN

Pada bab ini membahas tentang langkah-langkah kegiatan metode penelitian Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 dimulai dari tahap perencanaan audit, persiapan audit, pelaksanaan audit, dan pelaporan audit.

BAB IV: HASIL DAN PEMBAHASAN

Pada bab ini aka dibahas tentang analisa dan evaluasi dari bukti, temuan dan rekomendasi yang didapat dari Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

BAB V: PENUTUP

Pada bab ini berisi tentang kesimpulan dari Tugas Akhir, dan saran sehubungan dengan adanya kemungkinan pengembangan dalam penelitian selanjutnya.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

BAB II

LANDASAN TEORI

2.1 Audit

Menurut (Canon, 2011) Audit dapat didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara objektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan Gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi.

2.2 Audit Sistem Informasi

Weber dalam Sarno (2009) mendefinisikan Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya yang efektif. Beberapa elemen utama tinjauan penting dalam Audit Sistem Informasi dapat diklasifikasikan sebagai berikut:

1. Tinjauan terkait fisik dan lingkungan, yakni: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, *temperature*, kontrol kelembaban, dan faktor lingkungan lain.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen *database*, seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud adalah bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan kemanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung ke dalam sistem, batasan tingkat keamanan, tinjauan terhadap *firewall*, daftar kontrol akses *router*, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur *backup* dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana atau kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verivikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang diterapkan.

2.3 Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya memastikan atau menjamin keberlangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*), dan

memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno dan Iffano, 2009). Contoh Kemanan Informasi menurut (Sarno dan Iffano, 2009) adalah:

1. *Physical Security* adalah Keamanan Informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security* adalah Keamanan Informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup '*Physical Security*'.
3. *Operation Security* adalah Keamanan Informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut agar beroperasi tanpa gangguan.
4. *Communications Security* adalah Keamanan Informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network Security* adalah Keamanan Informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya, dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

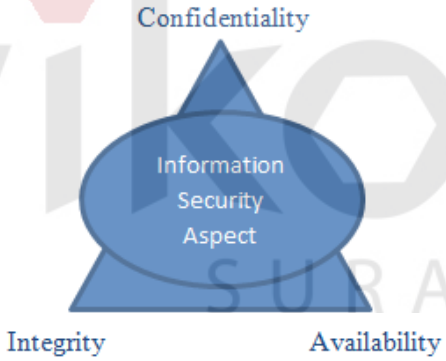
INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Aspek Keamanan Informasi meliputi tiga hal, yaitu: *Cofidentiality*, *Integrity*, dan *Availability* (CIA). Aspek tersebut dapat dilihat pada Gambar 2.1 yang lebih lanjut akan dijelaskan sebagai berikut.

a) *Cofidentiality*: Keamanan Informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses Informasi tertentu.

b) *Integrity*: Keamanan Informasi seharusnya menjamin kelengkapan Informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkan perubahan Informasi dari aslinya.

c) *Availability*: Keamanan Informasi seharusnya menjamin pengguna dapat mengakses Informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses Informasi.



Gambar 2.1 Aspek Keamanan Informasi
(Sumber: Sarno dan Iffano, 2009)

2.4 Sistem Informasi

Sistem Informasi (SI) adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar

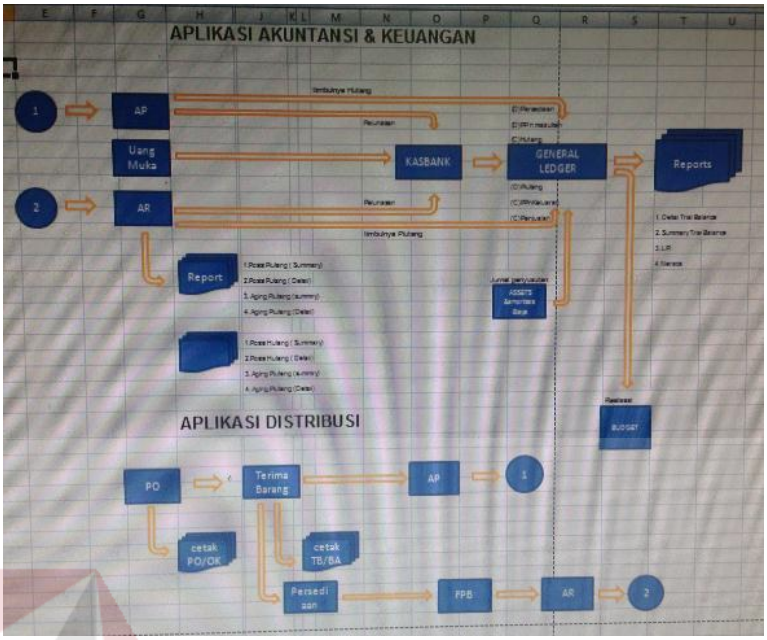
tertentu dengan laporan-laporan tertentu yang diperlukan (Leitch dan Davis dalam Jogiyanto 2005). Sedangkan definisi lain yaitu Sistem Informasi sebagai sebuah sistem yang menggunakan Teknologi Informasi (TI) untuk menangkap, mentransmisikan, menyimpan, mendapatkan, memanipulasi, atau menampilkan informasi yang dibutuhkan oleh satu atau lebih proses bisnis (Alter dalam Sarno, 2009). Agar dapat berdaya guna maka SI seharusnya merupakan rangkaian prosedur formal yang melakukan pengelompokkan data pemrosesan dan pendistribusian kepada pengguna (Hall dalam Sarno, 2009).

2.5 Sistem Informasi Akuntansi

Menurut (Krismiaji, 2005) Sistem Informasi Akuntansi adalah sebuah sistem yang memproses data dan transaksi guna menghasilkan informasi yang bermanfaat untuk merencanakan, mengendalikan, dan memproses bisnis.

Definisi lain menurut (Jogiyanto, 2005) Sistem Informasi Akuntansi adalah kumpulan kegiatan-kegiatan dari organisasi yang bertanggung jawab untuk menyediakan informasi keuangan dan informasi yang di dapat dari transaksi data untuk tujuan pelaporan internal kepada manajer untuk digunakan dalam pengendalian dan perencanaan sekarang dan operasi masa depan serta pelaporan eksternal kepada pemegang saham, pemerintah, dan pihak-pihak luar lainnya. Dibawah ini akan ditampilkan Gambar alur sistem akuntansi *enterprise* PT. GCS, Gambar 2.2.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA



Gambar 2.2 Alur Sistem Akuntansi *Enterprise*
(Sumber: PT. Gresik Cipta Sejahtera)

2.6 Anggaran (*Budget*)

Anggaran merupakan kata benda, yakni hasil yang diperoleh setelah menyelesaikan tugas perencanaan, sedangkan penganggaran (*budgeting*) merupakan suatu proses sejak tahap persiapan yang diperlukan sebelum dimulainya penyusunan rencana. Pengumpulan data dan informasi yang diperlukan, pembagian tugas perencanaan, penyusunan rencana, implementasi rencana, sampai pada tahap pengawasan dan evaluasi dari hasil pelaksanaan rencana tersebut (Adisaputro dan Asri, 2003).

Menurut (Adisaputro dan Asri, 2003) Anggaran (*budget*) merupakan rencana terinci yang disajikan secara kuantitatif yang menentukan bagaimana sumber daya manusia yang akan diperoleh dan digunakan selama periode waktu tertentu, anggaran seringkali digunakan sebagai alat untuk perencanaan, koordinasi, alokasi sumber

daya, dan juga digunakan untuk mengukur kinerja. Pada akhirnya digunakan untuk mengontrol dan mempengaruhi perilaku pihak-pihak yang terkait dengan penetapan dan pelaksanaan anggaran.

2.7 Laporan Keuangan

Menurut (Munawir, 2007) Laporan Keuangan merupakan alat yang sangat penting untuk memperoleh informasi sehubungan dengan posisi keuangan dan hasil-hasil yang telah dicapai oleh perusahaan yang bersangkutan.

Laporan keuangan dipersiapkan atau dibuat dengan maksud untuk memberikan Gambaran atau laporan kemajuan secara periodik yang dilakukan pihak manajemen yang bersangkutan. Laporan keuangan bersifat historis serta menyeluruh dan sebagai suatu program *report*.

2.8 Audit Keamanan Sistem Informasi

Menurut (Ahmad, 2012) Audit Keamanan Sistem Informasi adalah suatu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada, dan untuk memverifikasi apakah perlindungan yang ada berjalan dengan baik.

Adapun tujuan utama 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, suatu hal yang penting untuk memahami dan mengimplementasikan audit keamanan pada sistem informasi yang digunakan. Penerapan audit keamanan sistem informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non teknis.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

2.9 Jenis Audit

Menurut (Sarno dan Iffano, 2009) dalam melaksanakan audit SMKI ada dua jenis audit yang dapat dilakukan, yaitu: Audit Kepatutan dan Audit Substansi. Pelaksanaannya tergantung dengan kebutuhan dan tujuan audit itu sendiri (dapat dilakukan secara terpisah). Jenis audit SMKI dapat dilakukan dengan:

a. Audit Kepatutan (*Compliance* Audit)

   Audit kesesuaian adalah audit SMKI yang dilaksanakan untuk tujuan menegaskan apakah objektif kontrol, kontrol, dan prosedur memenuhi hal-hal berikut:

   1) Telah memenuhi persyaratan sebagaimana tertulis dalam manual SMKI.
   2) Telah efektif diimplementasikan dan di pelihara.
   3) Telah berjalan sesuai dengan yang diharapkan.

b. Audit Substansi (*Substantion* Audit)

   Audit substansi adalah audit SMKI yang dilaksanakan untuk tujuan menegaskan apakah hasil aktivitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang ditargetkan atau yang diharapkan.

2.10 Manajemen Aset

Menurut (Siregar, 2004) pengertian aset secara umum adalah barang (*thing*) atau suatu barang (*anything*) yang mempunyai nilai ekonomi (*economic value*), nilai komersial (*commercial value*) atau nilai tukar (*exchange value*) yang dimiliki oleh suatu badan usaha, instansi, individu (perorangan).

Aset tetap adalah aset berwujud yang mempunyai masa manfaat lebih dari dua belas bulan dalam kegiatan ekonomi perusahaan. Aset tetap diklasifikasikan berdasarkan kesamaan sifat atau fungsinya dalam aktivitas operasi seperti peralatan,

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

gedung bangunan, dan lain sebagainya. Aset tidak berwujud adalah jenis aset yang tidak memiliki wujud fisik, contohnya hak cipta, paten, merek dagang dan lain sebagainya.

2.11 Penilaian Risiko (*Risk Assessment*)

Sarno dan Iffano (2009) mengungkapkan penilaian risiko (*risk assessment*) adalah langkah atau tahap pertama dari proses manajemen risiko. Penilaian risiko bertujuan untuk mengetahui ancaman-ancaman dari luar yang berpotensi mengganggu Keamanan Informasi organisasi dan potensial kelemahan yang dimiliki oleh Informasi organisasi. Metode penilaian risiko terdiri dari 6 tahapan, yaitu:

1. Identifikasi Informasi.
2. Identifikasi Ancaman (*threat*).
3. Identifikasi Kelemahan (*vulnerability*).
4. Menentukan Kemungkinan Ancaman (*probability*).
5. Analisa Dampak (*impact analysis*).
6. Menentukan Nilai Risiko.

Menurut (Sarno dan Iffano, 2009) nilai risiko (*risk value*) adalah gambaran dari seberapa besar akibat yang akan diterima oleh organisasi jika ancaman (*threat*) yang menyebabkan kegagalan keamanan informasi terjadi. Dalam Tugas Akhir ini penilaian risiko menggunakan metode kuantitatif.

Metode kuantitatif adalah metode penilaian risiko dengan pendekatan matematis. Dengan metode ini nilai risiko dapat dihitung dengan menggunakan rumus berikut.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

a) Menghitung nilai aset berdasarkan aspek keamanan informasi, yaitu: kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Nilai aset dihitung dengan menggunakan persamaan matematis berikut:

Nilai Aset = NC + NI + NV ……(2.1)

Dimana:

NC = Nilai *Confidetiality* sesuai nilai yang dipilih tabel.

NI = Nilai *Integrity* sesuai nilai yang dipilih pada tabel.

NV = Nilai *Availability* sesuai nilai yang dipilih pada tabel.

b) Mengidentifikasi ancaman dan kelemahan yang dimiliki oleh aset dapat dilakukan dengan membuat tabel kemungkinan kejadian (*probability of occurrence*). Nilai rata-rata probabilitas dihasilkan dari klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut:

Low: Nilai rata-rata probabilitas 0,1 - 0,3.

Medium: Nilai rata-rata probabilitas 0,4 - 0,6.

High: Nilai rata-rata probabilitas 0,7 - 1,0.

Nilai ancaman dari suatu aset dapat dihitung dengan rumus:

NT = ∑PO / ∑Ancaman ……(2.2)

Dimana:

∑PO: Jumlah *probability of occurrence*.

∑Ancaman: Jumlah ancaman terhadap informasi.

c) Analisa dampak bisnis (*Business Impact Analysis*) dapat diistilahkan dengan BIA. Menganalisa dampak bisnis dapat dilakukan dengan cara membuat skala nilai BIA. Dampak bisnis dibagai dalam lima level penilaian, yaitu:

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

0 ≥ *Not Critical Impact* ≤ 20

20 > *Low Critical Impact* ≤ 40

40 > *Medium Critical Impact* ≤ 60

60 > *High Critical Impact* ≤ 80

80 > *Very High Critical Impact* ≤ 100

Mengidentifikasi level risiko dapat dilakukan dengan membuat tabel level risiko. Didalam tabel level risiko terdapat nilai ancaman yang dibagi dalam 3 level penilaian, yaitu:

0 ≥ *Low Probability* ≤ 0,1

0,1 > *Medium Probability* ≤ 0,5

0,5 > *High Probability* ≤ 1,0

d) Perhitungan nilai risiko dengan pendekatan matematis:

***Risk Value* = NA x BIA x NT** ……(2.3)

Dimana:

Nilai Aset: NA

Analisa Dampak Bisnis: BIA

Nilai Ancaman: NT

Menurut (Sarno dan Iffano, 2009) setelah menentukan metode penilaian risiko, maka organisasi harus menentukan bagaimana kriteria penerimaan risiko. Kriteria ini sebagai acuan tindakan apa yang akan dilakukan oleh organisasi dalam menerima risiko jika terjadi kegagalan Keamanan Informasi. Adapun kriteria penerimaan risiko dapat dikategorikan sebagai berikut.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

1. Risiko Diterima (*risk acceptance*)

   Organisasi menerima risiko yang terjadi dengan segala dampaknya dan proses bisnis organisasi berlangsung terus.

2. Risiko Direduksi (*risk reduction*)

   Organisasi menerima risiko yang terjadi direduksi dengan menggunakan Kontrol Keamanan sampai pada level yang dapat diterima oleh organisasi.

3. Risiko Dihindari atau Ditolak (*risk avoidance*)

   Organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul (seperti: mematikan komputer *server*, memutus koneksi jaringan, dan lain-lain).

4. Risiko Dialihkan Pada Pihak Ketiga (*risk transfer*)

   Organisasi menerima risiko dengan cara mengalihkan pada pihak ketiga untuk mendapat penggantian atau kompensasi dari pihak ketiga (seperti kepada perusahaan asuransi, vendor, dan lain-lain).

Metode untuk menentukan kriteria penerimaan risiko dapat menggunakan Tabel matrik 3x3 dapat dilihat pada Tabel 2.1.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 2.1 Kriteria Penerimaan Risiko

Probabilitas Ancaman (PA)	**Biaya Pemulihan (BP)**		
	Low	***Medium***	***High***
High	*Risk Acceptance*	*Risk Avoidance*	*Risk Transfer*
Medium	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
Low	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
	High	***Medium***	***Low***
	Biaya Transfer Risiko (BR)		

(Sumber: Sarno dan Iffano, 2009)

Kriteria penerimaan risiko pada Tabel 2.1 diatas menggunakan prinsip logika AND dapat dijelaskan sebagai berikut:

1. Jika salah satu nilai variabel ber logika *Low* maka risiko diterima dan sebaliknya jika salah satu nilai variabel berlogika *High* maka risiko ditolak.
2. Kriteria risiko diterima dapat dikembangkan dengan kriteria tambahan yaitu:
   a. Jika biaya pemulihan **lebih kecil** daripada biaya transfer risiko, maka risiko diterima dengan status *risk acceptance*.
   b. Jika biaya pemulihan **lebih besar** daripada biaya transfer risiko, maka risiko diterima dengan status *risk transfer*.
   c. Jika biaya pemulihan sama dengan biaya transfer risiko, maka risiko diterima dengan status *risk reduction*, yaitu risiko direduksi dengan menggunakan pengendalian Kontrol Keamanan sampai pada level yang dapat diterima oleh organisasi, kecuali jika probabilitas ancaman bernilai *HIGH* maka risiko ditolak.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

2.12 Kejahatan Komputer

Kejahatan komputer menurut (Sarno dan Iffano, 2009) adalah kejahatan yang dilakukan seseorang dengan menggunakan teknologi atau perangkat komputer beserta fasilitas pendukungnya. Hal tersebut juga dijelaskan oleh Thomas Porter dalam bukunya "*Electronic Data Processing* (EDP) *Control and Auditing*" (Porter, 1974) mendefinisikan mengenai: *computer abuse* (penyalahgunaan komputer), *computer crime* (kejahatan komputer), dan *computer related crime* (kejahatan yang berhubungan dengan komputer).

Computer abuse merupakan tindakan sengaja dengan melibatkan komputer yang melibatkan satu pelaku kejahatan atau lebih sehingga dapat memperoleh keuntungan dan kerugian bagi korban. *Computer crime* merupakan tindakan melanggar hukum yang membutuhkan banyak pengetahuan tentang komputer agar pelaksanaanya berjalan dengan baik. *Computer related crime* adalah kejahatan yang berkaitan dengan komputer yang tidak terbatas pada kejahatan bisnis kerah putih (*white collar crime*) atau ekonomi.

2.13 Tahapan Audit

Menurut (ISACA, 2010) terdapat delapan tahap yang dilakukan dalam proses audit sistem informasi (SI), yaitu: 1. *Audit Charter*, 2. *Idependence*, 3. *Professional Ethics and Standards*. 4. *Competence*, 5. *Planning*, 6. *Performance of Audit Work*, 7. *Reporting*, 8. *Follow-Up Activities.* Dibawah ini akan ditampilkan Gambar beserta penjelasan dari delapan tahapan audit, Gambar 2.3.

Gambar 2.3 Tahapan-tahapan Audit Teknologi Informasi
(Sumber: ISACA, 2010)

1. ***Audit Charter***

Sebelum melakukan kegiatan audit SI, seorang auditor harus membuat surat kesepakatan atau keterikatan dengan *client* yang berisi tentang tujuan, tanggung jawab, wewenang, dan akuntabilitas fungsi audit SI. *Audit Charter* adalah nama surat keterikatan untuk auditor internal, sedangkan untuk auditor eksternal biasa disebut dengan *engagement letter*. Surat keterikatan audit SI harus disepakati dan disetujui oleh pihak yang berwenang dalam organisasi.

2. ***Independence***

Dalam segala hal yang berkaitan dengan audit SI, auditor harus independen di daerah yang diaudit termasuk juga dalam hal bersikap dan berpenampilan. Didalam *audit charter* harus membahas independensi dan akuntabilitas dari fungsi audit.

3. ***Professional Ethics and Standards***

Kode Etik yang dikeluarkan oleh ISACA akan ditinjau dan diubah dari waktu ke waktu mengikuti kecenderungan yang muncul didalam profesi audit. Anggota ISACA

dan Auditor SI harus terus mengikuti dan mematuhi kode etik saat menjalankan tugas sebagai auditor. Angota ISACA dan Auditor SI harus berkomunikasi dengan tim mereka untuk memastikan kepatuhan kode etik. Auditor SI juga harus menangani semua permasalahan dengan tepat sehubungan dengan penerapan etika profesional atau standar audit SI.

4. *Professional Competence*

Auditor harus memiliki pengetahuan dan keterampilan dalam melakukan tugas audit SI. Kompetensi auditor SI harus dipertahankan dengan mengikuti pendidikan profesional berkelanjutan dan latihan yang tepat. Sebelum melaksanakan tugasnya, auditor SI harus memberikan jaminan mengenai keterampilan, pengetahuan, dan pengalaman yang relevan untuk tugas yang direncanakan, apabila tidak maka auditor SI harus mengundurkan diri dari tugasnya.

5. *Planning*

Auditor harus merencanakan cakupan pemeriksaan sistem informasi agar tujuan audit terpenuhi dan mematuhi hukum yang berlaku sesuai dengan standar audit profesional. Auditor SI harus mengembangkan dan mendokumentasikan pendekatan audit berbasis risiko. Perencanaan audit SI meliputi sifat dan tujuan, waktu, dan sumber daya yang diperlukan. Auditor juga harus memiliki pengetahuan mengenai sifat organisasi, lingkungan, dan risiko. Penilaian risiko juga harus dilakukan oleh auditor untuk memberikan keyakinan pada *auditee* mengenai kegiatan audit SI yang akan dilaksanakan.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

6. *Performance of Audit Work*

Auditee harus mengawasi auditor selama kegiatan audit berlangsung agar tujuan audit dapat terpenuhi. Audit harus memperoleh bukti yang cukup dan relevan, temuan dan kesimpulan audit harus didukung dengan analisis yang tepat dan interpretasi bukti audit SI. Dokumentasi proses audit harus menggambarkan pekerjaan audit yang dilakukan.

7. *Reporting*

Auditor SI harus memberikan laporan dalam bentuk yang tepat setelah selesainya audit. Laporan audit harus menyatakan waktu, ruang lingkup, tujuan pekerjaan audit yang telah dilakukan. Laporan audit juga harus berisi temuan, kesimpulan, dan rekomendasi yang diberikan oleh auditor. Auditor harus memberikan komentar dan melakukan diskusi dengan *auditee* mengenai bukti dan kelemahan yang ada setelah dilakukannya proses audit SI sebelum memberikan laporan akhir kepada *auditee*. Laporan audit akhir harus ditandatangani oleh pihak *auditee* sebagai bentuk pengesahan laporan sesuai dengan tanggal diserahkannya laporan audit SI tersebut pada *auditee*.

8. *Follow-Up Activities*

Setelah proses pelaporan temuan dan rekomendasi, auditor harus meminta hasil evaluasi informasi yang relevan untuk memastikan tindakan yang telah diambil sudah tepat. Proses tindak lanjut rekomendasi yang diberikan akan dilaksanakan oleh auditor SI internal dengan memperhitungkan pentingnya temuan dan dampak yang dilaporkan oleh auditor SI eksternal. Tindakan *auditee* dalam pelaksanaan rekomendasi diberikan atau diminta oleh auditor SI sebagai catatan respon.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

2.14 Standar Sistem Manajemen Keamanan Informasi

Sejak tahun 2005, *International Organization for Standardization* (ISO) atau organisasi Internasional untuk standarisasi telah mengembangkan sejumlah standar tentang *Information Security Management System* (ISMS). Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

a. ISO/IEC 27000: 2009 – *ISMS Overview and Vocabulary*

   Dokumen definisi-definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.

b. ISO/IEC 27001: 2005 – *ISMS Requirement*

   Berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

c. ISO/IEC 27002: 2005 – *Code of Practice for ISMS*

   Terkait dengan dokumen ISO 27001, namun dalam dokumen ini berisi panduan praktis (*code of practice*) teknik keamanan informasi.

d. ISO/IEC 27003: 2010 – *ISMS Implementation Guidance*

   Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

e. ISO/IEC 27004: 2009 – *ISMS Measuements*

   Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

f. ISO/IEC 27005: 2008 – *Information Security Risk Management*

   Dokumen panduan pelaksanaan manajemen risiko.

g. ISO/IEC 27006: 2007 – *ISMS Certification Body Requiements*

   Dokumen panduan untuk sertifikasi SMKI perusahaan.

h. ISO/IEC 27007 – *Guidelines for ISMS Auditing*

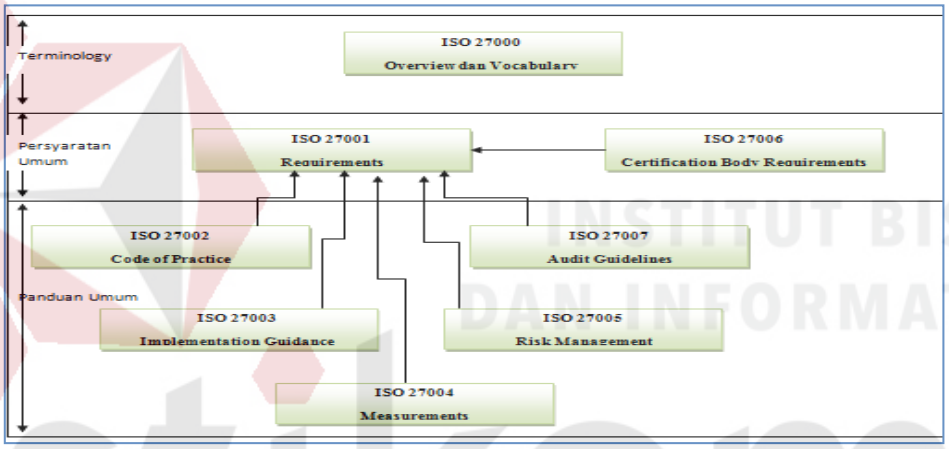
   Dokumen panduan audit SMKI perusahaan.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Adapun penjelasan dari standar ISMS tersebut dijelaskan sebagai berikut.

a. ISO/IEC 27000:2009 – *ISMS Overview and Vocabulary*

Standar ini dirilis tahun 2009, memuat prinsip-prinsip dasar *Information Security Management System*, definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang tahap pengembangan. Hubungan antar standar keluarga ISO 27000 dapat dilihat pada Gambar 2.4.



Gambar 2.4 Hubungan Antar Standar Keluarga SMKI
(Sumber: Direktorat Keamanan Informasi, 2011)

Dari standar seri ISO 27000 hingga September 2011 baru ISO/IEC 27001: 2005 yang telah diadopsi Badan Standardisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

b. ISO/IEC 27001:2005 – *ISMS Requirement*

ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini

bersifat independen terhadap produk teknologi masyarakat penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjauan ulang *(review)*, pemeliharaan dan peningkatan suatu SMKI. Model PLAN–DO–CHECK–ACT (PDCA) diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA (ISO/IEC 27002, 2005) *– Code of Practice for ISMS)*

c. ISO/IEC 27002: 2005 – *Code of Practice for ISMS*

ISO IEC 17799 tahun 2005, resmi dipublikasikan pada tanggal 15 Juni 2005. Pada tanggal 1 Juli 2007, nama itu secara resmi diubah menjadi ISO IEC 27002 tahun 2005. Konten tersebut masih persis sama. Standar ISO IEC 17799:2005 (sekarang dikenal sebagai ISO IEC 27002:2005) dikembangkan oleh IT *Security Subcommittee* (SC 27) dan *Technical Committee on Information Technology* (ISO/IEC JTC 1) (ISO 27002, 2005).

d. ISO/IEC 27003:2010 – *ISMS Implementation Guidance*

Tujuan dari ISO/IEC 27003 adalah untuk memberikan panduan bagi perancangan dan penerapan SMKI agar memenuhi persyaratan ISO 27001. Standar ini menjelaskan proses pembangunan SMKI meliputi pengarsipan, perancangan dan penyusunan atau pengembangan SMKI yang digambarkan sebagai suatu kegiatan proyek.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

e. ISO/IEC 27004:2009 – *ISMS Measuements*

Standar ini menyediakan penyusunan dan penggunaan teknik pengukuran untuk mengkaji efektivitas penerapan SMKI dan kontrol sebagaimana disyaratkan ISO/IEC 27001. Standar ini juga membantu organisasi dalam mengukur ketercapaian sasaran keamanan yang ditetapkan.

f. ISO/IEC 27005:2008 – *Information Security Risk Management*

Standar ini menyediakan panduan bagi kegiatan manajemen risiko keamanan informasi dalam suatu organisasi, khususnya dalam rangka mendukung persyaratan-persyaratan SMKI sebagaimana didefinisikan oleh ISO/IEC 27001. Standar ini diterbitkan pada bulan Juni 2008.

g. ISO/IEC 27006:2007–*ISMS Certification Body Requiements*

Standar ini menetapkan persyaratan dan memberikan panduan bagi organisasi yang memiliki kewenangan untuk melakukan audit dan sertifikasi SMKI. Standar ini utamanya dimaksudkan untuk mendukung porses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing.

h. ISO/IEC 27007–*Guidelines for ISMS Auditing*

Standar ini memaparkan penduan bagaimana melakukan audit SMKI perusahaan.

2.15 ISO 27002:2005

ISO 27002:2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya mencakup 12 kontrol area, 41 kontrol objektif, dan 133 kontrol sebagaimana ditetapkan dalam ISO/IEC 27001, dapat dilihat pada Tabel 2.2.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

ISO 27002:2005 tidak mengharuskan bentuk-bentuk kontrol yang tertentu menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya (Direktorat Keamanan Informasi, 2011).

Tabel 2.2 Ringkasan Jumlah Klausul Kontrol Keamanan, Obyektif Kontrol dan Kontrol pada ISO 27002:2005.

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
4	2	-
5	1	2
6	2	11
7	2	5
8	3	9
9	2	13
10	10	32
11	7	25
12	6	16
13	2	5
14	1	5
15	3	10
Jumlah: 12	Jumlah: 41	Jumlah:133

Dalam penelitian ini, audit keamanan sistem informasi akan difokuskan pada 4 klausul, yaitu klausul 7 tentang manajemen aset, klausul 8 tentang keamanan sumber daya manusia, klausul 9 tentang keamanan fisik dan lingkunagan, klausul 11 tentang kontrol akses yang sudah disesuaikan dengan kesepakatan auditor dan PT. GCS dalam *engagement letter* untuk detail struktur dokumen kontrol keamanan yang digunakan sebagai acuan audit dari ISO/IEC 27002:2005 dapat dilihat pada Tabel 2.3.

Tabel 2.3 Detail Struktur Kontrol Acuan Audit Keamanan Sistem Informasi ISO/IEC 27002:2005.

Klausul: 7 Manajemen Aset
Kategori Keamanan Utama: 7.1 Tanggung Jawab Aset Objektif Kontrol: Untuk memenuhi perlindungan dan pemeliharaan terhadap aset organisasi
Kontrol: 7.1.1 Inventarisasi Aset
Kontrol: 7.1.2 Kepemilikan Aset
Kontrol: 7.1.3 Penggunaan Aset yang Diterima
Kategori Keamanan Utama: 7.2 Klasifkasi Informasi Objektif Kontrol: Untuk memastikan bahwa setiap Informasi dalam organisasi mendapatkan keamanan yang memadai.
Kontrol: 7.2.1 Pedoman Klasifikasi
Kontrol: 7.2.2 Informasi Pelabelan dan Penanganan
Klausul: 8 Keamanan Sumber Daya Manusia
Kategori Keamanan Utama: 8.1 Sebelum Menjadi Pegawai Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami akan tanggung jawabnya dan bisa menjalankan aturan yang mereka dapatkan untuk meminimalkan risiko pencurian atau kesalahan dalam penggunaan fasilitas informasi.
Kontrol: 8.1.1 Peran dan tanggung Jawab
Kontrol: 8.1.2 Penyaringan
Kontrol: 8.1.3 Syarat dan Kondisi Kerja
Kategor i Keamanan Utama: 8.2 Selama Menjadi pegawai Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami Keamanan Informasi yang telah ditetapkan oleh organisasi demi mengurangi terjadinya kesalahan kerja *(human error)* dan risiko yang dihadapi oleh organisasi.
Kontrol: 8.2.1 Tanggung Jawab Manajemen
Kontrol: 8.2.2 Kesadaran Keamaan Informasi, Pendidikan dan Pelatihan
Kontrol: 8.2.3 Pemberhentian Tanggung Jawab
Kategori Keamanan Utama: 8.3 Pemberhentian dan Pemindahan Pegawai. Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga yang diberhentikan dipindah dilakukan sesuai dengan prosedur yang benar.
Kontrol: 8.3.1 Pemberhentian Taggung Jawab
Kontrol: 8.3.2 Pengembalian Aset
Kontrol: 8.3.3 Penghapusan Hak Akses

Tabel 2.3 Detail Struktur Kontrol Acuan Audit Keamanan Sistem Informasi ISO/IEC 27002:2005 (Lanjutan).

Klausul: 9 Keamanan Fisik dan Lingkungan
Kategori Keamanan Utama: 9.1 Daerah Aman Objektif Kontrol: Untuk mencegah akses fisik tanpa hak, kerusakan dan gangguan terhadap Informasi dan perangkatnya dalam organisasi.
Kontrol: 9.1.1 Keamanan Perimeter
Kontrol: 9.1.2 Kontrol Entri Fisik
Kontrol: 9.1.3 Keamanan Kantor, Ruang dan Fasilitasnya
Kontrol: 9.1.4 Perlidungan Terhadap Ancaman Dari Luar dan Lingkungan Sekitar
Kontrol; 9.1.5 Bekerja di Wilayah Aman
Kontrol: 9.1.6 Akses Publik, Tempat Pengiriman dan Penurunan Barang
Kategori Keamanan Utama: 9.2. Peralatan Keamanan. Objektif Kontrol: Untuk mencegah kehilangan, kerusakan, pencurian atau ketidaberesan aset dan gangguan tehadap aktivitas organisasi.
Kontrol: 9.2.1 Penempatan dan Perlindungan Peralatan
Kontrol: 9.2.2 Peralatan Pendukung
Kontrol: 9.2.3 Keamanan Kabel
Kontrol: 9.2.4 Pemeliharaan Peralatan
Kontrol: 9.2.5 Keamanan Peralatan Diluar Area
Kontrol: 9.2.6 Penggunaan Ulang Peralatan
Kontrol: 9.2.7 Pemindahan Peralatan
Klausul: 11 Kontrol Akses
Kategori Keamanan Utama: 11.1 Kebijakan Kontrol Akses Objektif Kontrol: Untuk megontrol akses informasi.
Kontrol: 11.1.1 Kebijakan Kontrol Akses
Kategori Keamanan Utama: 11.2 Manajemen Akses Uset Objektif Kontrol: Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak.
Kontrol: 11.2.1 Registrasi Pengguna
Kontrol: 11.2.2 Manajemen Hak Istimewa
Kontrol: 11.2.3 Manajemen *Password* User
Kategori Keamanan Utama: 11.2 Manajemen Akses user Objektif Kontrol: Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak
Kontrol: 11.2.4 Ulasan Hak Akses Pengguna

Tabel 2.3 Detail Struktur Kontrol Acuan Audit Keamanan Sistem Informasi ISO/IEC 27002:2005 (Lanjutan).

Kategori Keamanan Utama: 11.3 Tanggung Jawab Pengguna Objektif Kontrol: Untuk mencegah akses user tanpa hak atau pencurian Informasi dan fasilitas pemrosesan Informasi
Kontrol: 11.3.1 Penggunaan *Password*
Kontrol: 11.3.2 Peralatan Pengguna Yang Tidak Dijaga
Kontrol: 11.3.3 Kebijakan Kerapian Meja dan Penyaringan
Kategori Keamanan Utama: 11.4 Kebijakan Penggunaan Layanan Jaringan Objektif Kontrol: Untuk mencegah akses tanpa hak kedalam layanan jaringan.
Kontrol: 11.4.1 Kebijakan Penggunaan Layanan jaringan
Kontrol : 11.4.2 Otentikasi Pengguna Koneksi eksternal.
Kontrol: 11.4.3 Indikasi Peralatan Didalam Jaringan
Kontrol: 11.4.4 Diagnostik Jarak Jauh dan Perlindungan Port Konfigurasi
Kontrol: 11.4.5 Pemisahan jaringan
Kontrol: 11.4.6 Kontrol terhadap koneksi Jaringan
Kontrol: 11.4.7 Kontrol Terhadap Routing Jaringan
Kategori Keamanan Utama: 11.5 Kontrol Akses Sistem Operasi Objektif Kontrol: Untuk mencegah akses tanpa hak ke sistem operasi
Kontrol: 11.5.1 Prosedur log-on yang aman
Kontrol: 11.5.2 Identifkasi dan Otentikasi User
Kontrol: 11.5.3 Manajemen Password
Kontrol: 11.5.4 Sistem Peralatan Pengguna
Kontrol: 11.5.5 Sesi Time-Out
Kontrol: 11.5.6 Batasan Waktu Koneksi
Kategori Keamanan Utama: 11.6 Kontrol Akses Aplikasi Objektif Kontrol: Untuk mencegah akses tanpa hak terhadap Informasi didalam aplikasi.
Kontrol: 11.6.1 Pembatasan Akses Informasi
Kontrol: 11.6.2 Isolasi Sistem Yang Sensitif
Kategori Keamanan Utama: 11.7 Komputasi Bergerak dan Komunikasi Mobile Objektif Kontrol: Untuk memastikan Keamanan Informasi saat menggunakan fasilitas komputer bergerak atau bekerja dari lain tempat
Kontrol: 11.7.1 Komunikasi dan Terkomputerisasai yang bergerak
Kontrol: 11.7.2 Teleworking

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2.16 Tingkat Kematangan (CMMI) to ISO 27002.

Dimensi kematangan *Capability Maturity Model Integration* (CMMI) digunakan untuk kegiatan *benchmarking* dan penilaian, tingkat kematangan berlaku untuk pencapaian proses perbaikan organisasi (CMMI-DEV V1.3, 2010).

Tabel 2.4 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)

Tingkat kematangan organisasi pada Tabel 2.4 menyediakan cara untuk mengkarakterisasi kinerjanya. Pengalaman menunjukkan bahwa organisasi melakukan yang terbaik ketika mereka memfokuskan upaya perbaikan proses mereka pada sejumlah proses yang dikelola. Sebuah tingkat kematangan adalah dataran tinggi evolusi yang ditetapkan untuk perbaikan proses organisasi. Setiap tingkat kematangan organisasi sangat penting untuk mempersiapkan perpindahan ke tingkat kematangan berikutnya (CMMI-DEV V1.3, 2010).

1. Tingkat Kematangan Level 1: *Initial*

   Pada tingkat kematangan level 1, proses organisasi masih kacau. Organisasi tidak menyediakan lingkungan yang stabil untuk mendukung proses. Organisasi dapat sukses tergantung dari kompetensi dan orang-orang di dalam organisasi, bukan dari penggunaan proses. Pada level ini, organisasi ditandai dengan kecenderungan

untuk *overcommit*, meninggalkan proses mereka dalam waktu krisis, dan tidak dapat mengulangi keberhasilan mereka.

2. Tingkat Kematangan Level 2: *Managed*

   Pada tingkat kematangan level 2, telah dipastikan bahwa proses proyek sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Memperkerjakan sumber daya yang terampil untuk menghasilkan *output* yang dapat dikendalikan, melibatkan *stakeholder* terkait monitoring, pengendalian, peninjauan, dan proses evaluasi untuk kepatuhan terhadap deskripsi proses. Komitmen telah ditetapkan antar pemangku kepentingan dan direvisi sesuai dengan kebutuhan. Produk dan layanan pekerjaan ditentukan sesuai deskripsi proses, standar, dan prosedur mereka.

3. Tingkat Kematangan Level 3: *Defined*

   Pada tingkat kematangan level 3, proses sudah dipahami dengan baik, dijelaskan dalam standar, prosedur, alat, dan metode. Kumpulan proses organisasi merupakan dasar level 3 agar dapat ditingkatkan dari waktu ke waktu. Pada tingkatan level 2 deskripsi proses dan prosedur bisa sangat berbeda dengan level 3 yang lebih dijelaskan secara detil. Sebuah proses pada level 3 didefinisikan dengan jelas meliputi tujuan, masukan, kriteria, kegiatan, peran, langkah-langkah, verifikasi, dan hasil. Pada tingkat kematangan level 3, proses dikelola lebih proaktif menggunakan pemahaman tentang hubungan timbal balik dari kegiatan, langkah-langkah, produk kerja, dan layanannya.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

4. Tingkat Kematangan Level 4: *Quantitatively Managed*

   Pada tingkat kematangan level 4, organisasi dan proyek menerapkan tujuan kuantitatif untuk kualitas dan kinerja proses digunakan sebagai kriteria pengelolaan proyek. Tujuan kuantitatif didasarkan pada kebutuhan pelanggan, pengguna akhir, organisasi, dan pelaksana proses. Kualitas dan kinerja proses dipahami serta dikelola selama proyek berlangsung. Untuk subproses yang dipilih, langkah-langkah khusus dari kinerja proses dikumpulkan dan dianalisis secara statistik. Ketika memilih subproses untuk analisis, sangat penting untuk memahami hubungan antara subproses yang berbeda dan dampaknya terhadap pencapaian tujuan untuk kualitas dan kinerja proses. Pendekatan statistik membantu untuk memastikan bahwa pemantauan subproses menggunakan teknik kuantitatif statistik diterapkan agar memiliki nilai yang paling baik untuk bisnis. Perbedaan penting antara tingkat kematangan 3 dan 4 adalah prediktabilitas kinerja proses. Pada tingkat kematangan 4, kinerja proyek dan subproses yang dipilih dikendalikan menggunakan teknik kuantitatif statistik dan prediksi didasarkan pada sebagian data proses analisis statistik.

5. Tingkat Kematangan Level 5: *Optimizing*

   Pada tingkat kematangan level 5, sebuah organisasi terus-menerus meningkatkan proses yang didasarkan pada pemahaman kuantitatif tujuan bisnis dan kebutuhan kinerja. Organisasi menggunakan pendekatan kuantitatif untuk memahami variasi yang melekat dalam proses dan penyebab hasil proses. Tingkat kematangan level 5 berfokus pada kinerja proses terus ditingkatkan secara bertahap disertai dengan perbaikan teknologi. Kualitas dan kinerja organisasi terus direvisi mencerminkan

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

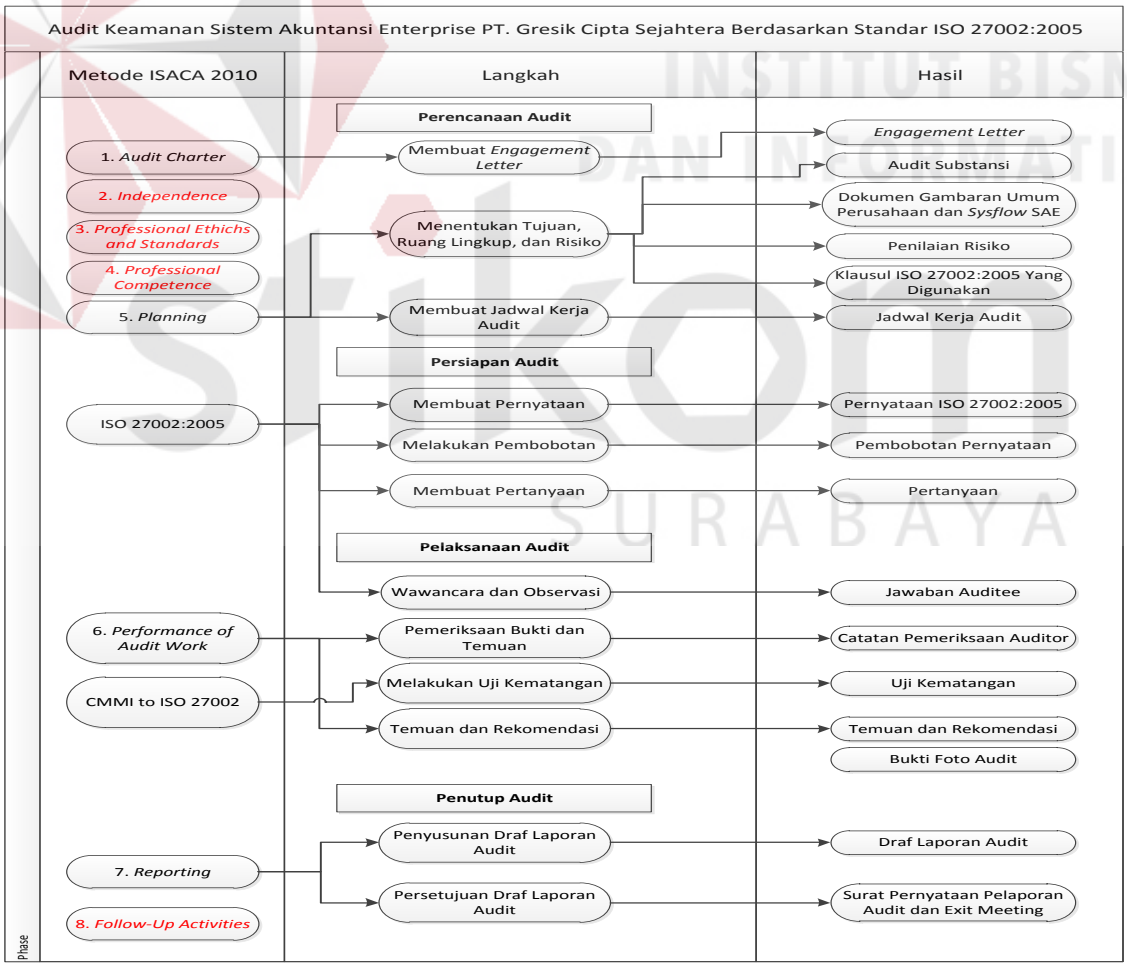
perubahan tujuan bisnis dan kinerja organisasi. Efek dari perbaikan proses diukur menggunakan teknik kuantitatif statistik dan dibandingkan dengan tujuan, kinerja, kualitas. Perbedaan penting antara tingkat kematangan 4 dan 5 adalah fokus pada pengelolaan dan meningkatkan kinerja organisasi. Pada tingkat kematangan 4, organisasi dan proyek fokus pada pemahaman dan mengendalikan kinerja di tingkat subproses dan menggunakan hasil untuk mengelola proyek. Pada tingkat kematangan 5, organisasi yang bersangkutan dengan kinerja organisasi secara keseluruhan menggunakan data yang dikumpulkan dari beberapa proyek. Analisis data mengidentifikasi kekurangan atau kesenjangan dalam kinerja. Kesenjangan ini digunakan untuk mendorong perbaikan proses organisasi yang menghasilkan peningkatan kinerja.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

BAB III

METODE PENELITIAN

Pada Bab III ini akan dilakukan pembahasan mengenai tahapan-tahapan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 yang akan dilaksanakan. Dibawah ini akan ditampilkan Gambar Langkah Audit Keamanan SAE, dapat dilihat pada Gambar 3.1. Langkah audit pada kolom Metode ISACA 2010 yang bertuliskan dengan huruf merah tidak digunakan dalam Tugas Akhir ini.



Gambar 3.1 Langkah Audit Keamanan Sistem Akuntansi *Enterprise*

3.1 Tahap Perencanaan Audit Sistem Akuntansi *Enterprise*

Pada tahap ini langkah-langkah yang dilakukan adalah: 1. Membuat *engagement letter*, 2. Menentukan Tujuan, Ruang Lingkup, dan Risiko, 3. Membuat Jadwal Kerja Audit. Tahapan ini akan menghasilkan *engagement letter*, tujuan audit, dokumen Gambaran umum PT. GCS, *sysflow* SAE, penilaian risiko, klausul yang akan digunakan untuk audit, dan jadwal kerja audit.

3.1.1 Membuat *Engagement Letter*

Sebelum melakukan audit, auditor harus membuat *engagement letter* atau surat perjanjian audit kepada *auditee*. *Engagement Letter* adalah surat perjanjian atau persetujuan antara auditor dengan *auditee* tentang pekerjaan audit yang akan dilaksanakan oleh auditor. Didalam *engagement letter* terdapat: Tujuan, Tim Auditor, Ruang Lingkup, Wewenang, Tanggung Jawab, Idependensi, Objektivitas, Integritas, Kerahasiaan, Tabel Kerja, dan Penutup.

3.1.2 Menentukan Tujuan, Ruang Lingkup, dan Risiko

1. Tujuan Audit Keamanan Sistem Akuntansi *Enteprise* PT. GCS

Tujuan dilakukannya audit keamanan sistem akuntansi *enterprise* PT. GCS adalah untuk mengukur tingkat keamanan sistem informasi yang ada, sehingga dapat menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sudah sesuai dengan yang diharapkan. Berdasarkan permasalahan yang ada berkaitan dengan aspek keamanan informasi (CIA) dan tujuan audit keamanan SAE, maka dilakukan audit substansi untuk menegaskan apakah hasil dari aktivitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang ditargetkan atau yang diharapkan.

2. Menentukan Ruang Lingkup

Menurut (Sarno dan Iffano, 2009) jika manajemen organisasi telah membuktikan komitmennya untuk menerapkan SMKI, kita dapat mulai merancang SMKI. Langkah pertama merencanakan SMKI, organisasi harus menentukan dahulu ruang lingkup implementasi SMKI. Hal-hal yang dibutuhkan dalam menentukan ruang lingkup SMKI adalah:

a. Dokumen komitmen manajemen (kebijakan, arahan atau tujuan keamanan informasi, aturan-aturan dan pernyataan dari pihak manajemen).
b. Kondisi eksisting organisasi, antara lain:
    1) Karakteristik proses bisnis yang dimiliki oleh organisasi.
    2) Lokasi organisasi dan seberapa besar organisasi yang dimiliki.
    3) Aset-aset yang dimiliki.
    4) Teknologi yang digunakan.

3. Penilaian Risiko

Setelah menentukan ruang lingkup, maka auditor akan melakukan penilaian risiko tahapan penilaian risiko dapat dilihat pada Gambar 3.2.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Gambar 3.2 Tahapan Penilaian Risiko
(Sumber: Sarno dan Iffano, 2009)

a. Identifikasi Aset

Tahap pertama dalam penilaian risiko adalah identifikasi aset dengan cara mengelompokkan aset dalam beberapa kategori. Menurut (ISO/IEC 27002, 2005) kategori aset antara lain berupa informasi, piranti lunak, fisik, layanan, orang atau aset tak terukur (*intangible*).

b. Identifikasi Ancaman

Sarno dan Iffano (2009) menyatakan Ancaman (*Threat*) adalah suatu potensi yang disebabkan oeh insiden yang tidak diinginkan yang mungkin

membahayakan proses bisnis organisasi. Tujuan mengidentifikasi ancaman adalah agar mengetahui ancaman yang mungkin terjadi dan membahayakan sistem dalam organisasi. Sumber ancaman dapat berasal dari alam, lingkungan, dan manusia. Contoh ancaman dapat dilihat pada Tabel 3.1.

Tabel 3.1 Contoh Ancaman

No	Sumber Ancaman	Jenis Ancaman
1.	Alam	Banjir, gempa bumi, angin puyuh, serangan petir.
2.	Lingkungan	Kegagalan sumber daya (*power failure*), polusi, bahan kimia berbahaya, kebocoran (cairan).
3.	Manusia - *Hacker, Cracker* - *Computer Criminal* - *Terorrist*	- *Hacking*, penyusupan ke sistem, akses ilegal. - Penyusupan ke sistem komputer, *criminal computer.* - *Black mail*, sistem penetrasi, virus.

(Sumber: Sarno dan Iffano, 2009)

c. Identifikasi Kelemahan

Vulnerability adalah kekurangan didalam prosedur keamanan informasi, perencanaan, implementasi dalam organisasi terhadap penjagaan informasi yang dimiliki, dimana kelemahan ini dapat menimbulkan ancaman (Sarno dan Iffano, 2009). Contoh kelemahan dapat dilihat pada Tabel 3.2.

Tabel 3.2 Contoh Kelemahan

Kelemahan (*Vulnerability*)	Sumber Ancaman	Aksi
Akses ID pegawai oleh rekan kerjanya.	Sesama pegawai	Akses ilegal
Penempatan ruang server yang digabungkan dengan ruang foto *copy*, sehingga dapat diakses seluruh pegawai.	Orang atau pegawai iseng	Server dapat mengalami kerusakan

d. Menentukan Kemungkinan Ancaman

Tujuan dari tahapan ini adalah untuk mengetahui kemungkinan ancaman yang akan timbul, baik ancaman dari alam, lingkungan, ataupun manusia. Untuk menentukan kemungkinan ancaman dilakukan dengan membuat Tabel kemungkinan ancaman yang terdiri dari: Jenis Ancaman, Detil Ancaman, Nilai Kemungkinan Ancaman (*Low* = Frekuensi Kejadian Rendah, *Medium* = Frekuensi Kejadian Sedang, *High* = Frekuensi Kejadian Tinggi) (Sarno dan Iffano, 2009).

e. Analisa Dampak

Analisa dampak adalah kegiatan untuk menentukan seberapa besar dampak risiko yang diakibatkan oleh ancaman atau kelemahan terhadap jalannya suatu proses bisnis organisasi, istilah analisa dampak bisnis dapat disingkat dengan BIA (*Business Impact Analysis*). Contoh nilai dampak dapat dilihat pada Tabel 3.3.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 3.3 Contoh Nilai Dampak

Risiko	Nilai BIA	Keterangan
Low	*Minor Critical*	Tidak mengganggu jalannya proses bisnis, nilai kerugian kecil.
Medium	*Critical*	Mengganggu jalannya proses bisnis, nilai kerugian besar.
High	*Mayor Critical*	Proses bisnis terhenti, nilai kerugian sangat besar.

(Sumber: Sarno dan Iffano, 2009)

f. Menentukan Nilai Risiko

Nilai risiko adalah Gambaran dari seberapa besar akibat yang diterima oleh organisasi apabila ancaman menyebabkan kegagalan keamanan informasi. Pada penelitian ini nilai risiko ditentukan dengan menggunakan metode kuantitatif dengan pendekatan matematis. Dengan metode ini nilai risiko dapat dihitung dengan rumus (2.3).

***Risk Value* = NA x BIA x NT**

Dimana:

Nilai Aset = NA

Analisa Dampak Bisnis = BIA

Nilai Ancaman = NT

g. Menentukan Klausul ISO 27002:2005

Organisasi (PT. GCS) dapat memahami risiko yang akan diterima dan menyediakan kebijakan organisasi yang paling aman serta menentukan kriteria untuk menerima risiko tersebut, yaitu apakah: menerima risiko apa adanya atau menerima risiko dengan melakukan pengelolaan risiko. 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 3.4. Dengan demikian, organisasi dapat memilih kontrol keamanan yang sesuai dengan kebutuhan organisasi.

Tabel 3.4 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)

3.1.3 Penyusunan Jadwal Kerja Audit

Audit *Working Plan* (AWP) atau bisa disebut dengan jadwal kerja audit merupakan dokumen yang dibuat oleh auditor TI dan digunakan untuk merencanakan

dan memantau pelaksanaan audit TI secara terperinci. Keluaran yang dihasilkan adalah jadwal kerja audit.

3.2 Tahap Persiapan Audit Sistem Akuntansi *Enterprise*

Pada tahap persiapan audit langkah-langkah yang akan dilakukan adalah membuat pernyataan berdasarkan standar ISO 27002:2005, melakukan pembobotan, dan membuat pertanyaan. Tahap persiapan audit akan menghasilkan pernyataan berdasarkan standar ISO 27002:2005, hasil pembobotan, dan pertanyaan yang akan diajukan untuk *auditee*

3.2.1 Membuat Pernyataan

Tahap selanjutnya adalah membuat pernyataan berdasarkan standar ISO 27002:2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang menjelaskan implementasi dan pengontrolan yang dilakukan, contoh pernyataan pada Klausul 7 Manajemen Aset dengan kontrol 7.1.1 (Inventarisasi Aset) dapat dilihat pada Tabel 3.5.

Tabel 3.5 Contoh Pernyataan Audit Klausul 7

Klausul: 7 Pengelolaan Aset	
Kontrol Obyektif: 7.1 Tanggung Jawab Aset	
Kontrol: 7.1.1 Inventarisasi Aset	
No	Pernyataan
1	Terdapat Inventarisasi aset organisasi organisasi.
2	Terdapat pemeliharaan terhadap aset organisasi.
3	Terdapat perlindungan aset organisasi.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

3.2.2 Melakukan Pembobotan

Pada setiap pernyataan harus memiliki nilai bobot masing-masing. Karena setiap pernyataan tidak bernilai sama dalam penerapannya untuk kontrol keamanan yang telah ditentukan. Metode ini menggunakan bobot pada penilaian risiko metode kualitatif, karena menurut (Sarno dan Iffano, 2009) risiko memiliki hubungan dengan keamanan informasi dan risiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi. Contoh tingkat pembobotan dapat dilihat pada Tabel 3.6.

Tabel 3.6 Tingkat Kepentingan dalam Pembobotan Peryataan

Bobot	Kriteria	Keterangan
Tinggi	0,70 - 1,00	Pernyataan tersebut dan mempunyai peranan sangat penting dalam proses sistem informasi
Cukup	0,40 - 0,69	Pernyataan tersebut dan mempunyai peranan cukup penting dalam proses sistem informasi
Rendah	0,00 - 0,39	Pernyataan tersebut dan mempunyai peranan kurang penting dalam proses sistem informasi

(Sumber: Niekerk dan Labuschagne dalam Yaner, 2006)

3.2.3 Membuat Pentanyaan

Pertanyaan dibuat berdasarkan pernyataan yang telah ditentukan sebelumnya. Satu pernyataan, bisa memiliki lebih dari satu pertanyaan, karena setiap pertanyaan harus mewakili pernyataan saat dilakukannya wawancara, observasi, dan identifikasi dokumen. Pertanyaan yang dibuat berkaitan dengan Klausul yang sudah ditetapkan. Contoh beberapa pertanyaan yang dihasilkan dari salah satu pernyataan Klausul 7 Manajemen Aset dapat dilihat pada Tabel 3.7.

Tabel 3.7 Contoh Pertanyaan Klausul 7

<table>
<tr><td colspan="2" rowspan="4">Audit Keamanan Sistem Informasi
Klausul 7
(Manajemen Aset)</td><td>Auditor : I Putu Narario S</td></tr>
<tr><td>Auditee : Pak Joko</td></tr>
<tr><td>Tanggal : 26-10-2015</td></tr>
<tr><td>Tanda Tangan :</td></tr>
<tr><td colspan="3">7.1 Tanggung Jawab Aset (Responsibility for Assets)</td></tr>
<tr><td colspan="3">7.1.1 Inventarisasi Aset (Inventory of Assets)</td></tr>
<tr><td>1</td><td colspan="2">Melakukan inventarisasi aset organisasi.</td></tr>
<tr><td></td><td colspan="2">P: Apakah proses inventarisasi aset organisasi sudah dilakukan? Apakah perusahaan memiliki dokumentasi inventarisasi aset?
J:
P: Siapakah yang melakukan dan mendokumentasikan proses inventarisasi aset pada perusahaan?
J:

P: Dimanakah proses inventarisasi aset organisasi dilakukan?
J:

P: Kapan inventarisasi aset pada organisasi dilakukan?
J:

P: Kapan dokumen inventarisasi aset pada organisasi dibuat?
J:

P: Bagaimana proses invetarisasi aset pada organisasi dilakukan?
J:

Bukti:</td></tr>
</table>

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

3.3 Tahap Pelaksanaan Audit Sistem Akuntansi *Enterprise*

Langkah-langkah yang akan dilakukan dalam pelaksanaan audit adalah melakukan wawancara dan observasi, proses pemeriksaan bukti dan temuan, melakukan uji kematangan, temuan dan rekomendasi. Pada tahap ini akan menghasilkan dokumen wawancara, bukti dan temuan, hasil nilai kematangan, dan rekomendasi.

3.3.1 Wawancara dan Observasi

Proses wawancara berdasarkan pertanyaan yang telah dibuat oleh auditor, wawancara dilakukan terhadap pihak-pihak yang terlibat dalam proses audit. Proses wawancara dilakukan pada 3 bagian, yaitu: bagian akuntansi dan keuangan, bagian sumber daya manusia (SDM), dan bagian TI. Keluaran yang dihasilkan pada tahap ini adalah dokumen wawancara. Contoh Tabel wawancara yang dihasilkan dari salah satu pernyataan Klausul 7 Manajemen Aset dapat dilihat pada Tabel 3.8.

Tabel 3.8 Contoh Wawancara Klausul 7

<table>
<tr><td colspan="2" rowspan="4">Audit Keamanan Sistem Informasi
Klausul 7
(Manajemen Aset)</td><td>Auditor : I Putu Narario S</td></tr>
<tr><td>Auditee : Pak Joko</td></tr>
<tr><td>Tanggal : 26-10-2015</td></tr>
<tr><td>Tanda Tangan :</td></tr>
<tr><td colspan="3">7.1 Tanggung Jawab Aset (Responsibility for Assets)</td></tr>
<tr><td colspan="3">7.1.1 Inventarisasi Aset (Inventory of Assets)</td></tr>
<tr><td>1</td><td colspan="2">Melakukan inventarisasi aset organisasi.</td></tr>
<tr><td></td><td colspan="2">P: Apakah proses inventarisasi aset organisasi sudah dilakukan? Apakah perusahaan memiliki dokumentasi inventarisasi aset?
J: Proses iventarisasi aset organisasi sudah dilakukan. Dokumentasi inventarisasi aset berupa dokumen daftar aktiva tetap dan laporan posisi aset.
P: Siapakah yang melakukan dan mendokumentasikan proses inventarisasi aset pada perusahaan?
J: Bagian sekretariat dan akuntan betugas untuk mencatat.
P: Dimanakah proses inventarisasi aset organisasi dilakukan?
J: Proses inventarisasi aset dilakukan di semua wilayah kantor pusat dan cabang (Gresik, Medan, Makasar, Lampung, Riau, Sumatera Selatan, dan Jambi).
P: Kapan inventarisasi aset pada organisasi dilakukan?
J: Waktu inventarisasi aset tidak dilakukan secara bersamaan, sesuai kebutuhan.
P: Kapan dokumen inventarisasi aset pada organisasi dibuat?
J: Dokumen inventarisasi aset dibuat pada 30 April 2013.
P: Bagaimana proses invetarisasi aset pada organisasi dilakukan?
J: Proses inventarisasi aset dilakukan mulai dari kantor pusat kemudian ke kantor cabang, dengan cara mencatat, memeriksa, dan mengidentifikasi aset.

Bukti: (Lampiran 8 No. 1) Dokumen Daftar Aktiva Tetap, (Lampiran 8 No. 2) Laporan Posisi Aset.</td></tr>
</table>

3.3.2 Pemeriksaan Bukti, dan Temuan

Pemeriksaan data dilakukan dengan cara wawancara dan observasi kepada *auditee* sesuai dengan ruang lingkup Sistem Akuntansi *Enterprise* dan Klausul yang sudah disepakati. Keluaran yang akan dihasilkan pada tahap ini adalah bukti dan temuan tentang permasalahan yang terjadi. Bukti dan temuan bisa berupa dokumen, foto, dan lain sebagainya. Contoh Tabel pemeriksaan Klausul 7 dapat dilihat pada Tabel 3.9.

Tabel 3.9 Contoh Pemeriksaan Klausul 7

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.

3.3.3 Uji Kematangan

Pada tahapan ini akan dilakukan uji kematangan untuk mengetahui tingkat kedewasaan atau *maturity level* berdasarkan metode CMMI to ISO 27002. Contoh Tabel tingkat kematangan Klausul 7 dapat dilihat pada Tabel 3.10. Perhitungan dapat dilakukan dengan beberapa tahapan:

a. Pada setiap pernyataan akan diberikan nilai bobot yang sesuai.
b. Dari hasil wawancara, temuan, dan bukti akan didapatkan nilai tingkat kematangan pada setiap pernyataan.
c. Bobot dan nilai pada setiap kontrol keamanan akan dijumlahkan, akan menghasilkan total bobot dan total nilai pada masing-masing kontrol keamanan.
d. Total nilai akan dibagi dengan total bobot, dan akan menghasilkan tingkat kematangan pada masing-masing kontrol keamanan.

Hasil nilai tingkat kematangan pada penelitian ini dikelompokkan menjadi 3 bagian berdasarkan 3 aspek keamanan informasi, yaitu: *Confidentiality*, *Integrity*, dan *Availability*.

Tabel 3.10 Contoh Tingkat Kematangan Klausul 7

Klausul 7 (Manajemen Aset)									
Klausul 7.1 Tanggung Jawab Aset (*Responsibility for Assets*)									
7.1.1 Inventarisasi Aset (*Inventory of Assets*)									Nilai
No	Pernyataan	Bobot	0	1	2	3	4	5	
1.	Melakukan inventarisasi aset organisasi.	1				√			3
2.	Melakukan pemeliharaan terhadap aset organisasi.	1				√			3
3.	Melakukan perlindungan aset organisasi.	0.6				√			3
Total Bobot		2.60	Total Nilai						9
Tingkat Kematangan									3.46

3.3.4 Temuan dan Rekomendasi

Pada proses penentuan temuan adanya ketidak efektifan suatu proses penerapan dan penggunaan sistem informasi, kelemahan dari prosedur pengendalian obyek audit, penyimpangan dan atau pelanggaran terhadap peraturan, standar praktik yang berlaku dan diketahui ditemukan oleh tim auditor TI berdasarkan hasil pemeriksaan dan evaluasi dari data dan bukti. Contoh temuan dan rekomendasi pada Klausul 7 Manajemen Aset dengan Kontrol 7.1.1 Inventarisasi Aset dapat dilihat pada Tabel 3.11.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 3.11 Contoh Temuan dan Rekomendasi Klausul 7

Temuan Audit Keamanan Sistem Akuntansi *Enterprise*			Pemeriksa: I Putu Narario S
			Penyelia: Pak Haryanto/Pak Erwin
Aspek : Klausul 7 Manajemen Aset **7.1.1 Inventarisasi Aset**			*Auditee*: Pak Joko
			Tanggal: 12-11-2015
No	Pernyataan	Temuan	Referensi, Risiko, dan Rekomendasi
1	Melakukan inventarisasi aset organisasi.	Nilai Bobot: 1 Nilai Kematangan: 3 ***Integrity*:** Pencatatan aset *software* SAE dan perangkat *server* tidak ada di dalam dokumen daftar aktiva tetap dan laporan posisi aset, pencatatan aset *hardware* hanya ada PC, laptop, printer.	Referensi: Pertanyaan 7.1.1 No. 1. Bukti: Lampiran 8 No. 1 dan 2. Ref: ISO 27002 7.1.1 Inventarisasi Aset Risiko: - Perusahaan dapat mengalami kerugian karena pengeluaran kas untuk pembelian aset dan tidak ada pencatatan yang jelas dan rinci. Rekomendasi: a. Mengidentifikasi seluruh aset dengan jelas beserta dokumen pentingnya. b. Dokumentasikan seluruh aset berdasarkan tingkat kepentingan dan nilai bisnisnya. c. Inventarisasi semua aset harus disusun dengan baik dan lengkap. d. Keterkaitan referensi Kepemilikan Aset (7.1.2) dan Klasifikasi Informasi (7.2).

3.4 Tahap Pelaporan Audit Sistem Akuntansi *Enterprise*

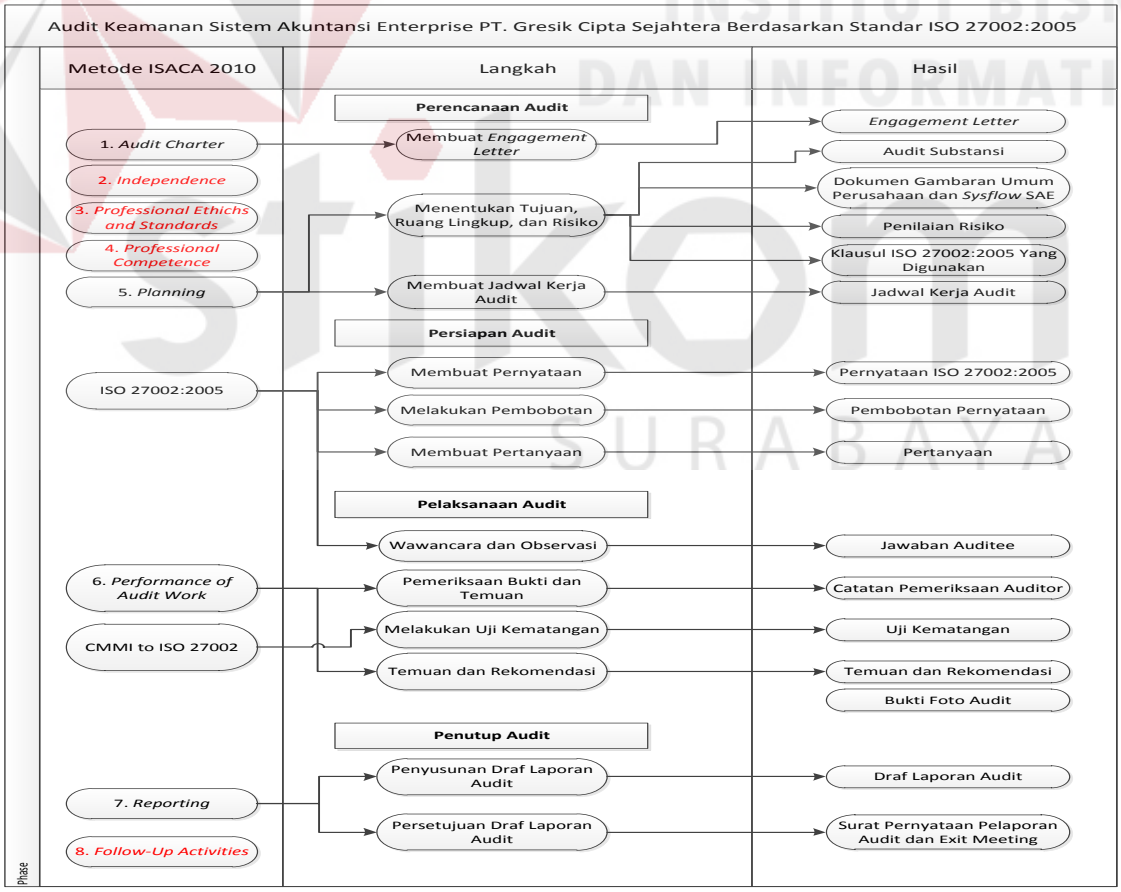
Pada tahapan ini auditor akan menyusun draf laporan Audit Keamanan Sistem Akuntansi *Enterprise* PT. Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002:2005 sebagai pertanggungjawaban atas audit yang telah dilaksanakan. Selanjutnya laporan audit akan ditunjukan pada pihak yang berwenang karena laporan audit bersifat rahasia. Tahap pelaporan audit dimulai dengan penyusunan draf laporan hasil audit, persetujuan draf laporan hasil audit, dan pelaporan hasil audit. Keluaran yang akan dihasilkan adalah surat pernyataan pelaporan audit dan *exit meeting*.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

BAB IV

HASIL DAN PEMBAHASAN

Pada Bab IV ini akan dilakukan pembahasan mengenai analisis hasil dan pembahasan dari tahap perencanaan audit keamanan sistem akuntansi *enterprise*, tahap persiapan, tahap pelaksanaan, dan tahap pelaporan audit keamanan sistem akuntansi *enterprise*. Dibawah ini akan ditampilkan Gambar Langkah Audit Keamanan SAE, dapat dilihat pada Gambar 4.1. Langkah audit pada kolom Metode ISACA 2010 yang bertuliskan dengan huruf merah tidak digunakan dalam Tugas Akhir ini.



Gambar 4.1 Langkah Audit Keamanan Sistem Akuntansi *Enterprise*

4.1 Hasil Perencanaan Audit Keamanan Sistem Akuntansi *Enterprise*

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Membuat *engagement letter*, 2. Menentukan Tujuan, Ruang Lingkup, dan Risiko, 3. Membuat Jadwal Kerja Audit. Tahapan ini akan menghasilkan *engagement letter*, pengetahuan tentang Gambaran umum perusahaan dan proses bisnis TI perusahaan, Klausul ISO 27002:2005 yang digunakan untuk audit, dan jadwal kerja audit.

4.1.1 *Engagement Letter*

Engagement letter adalah surat perjanjian atau persetujuan antara auditor dengan *auditee* tentang pekerjaan audit yang akan dilaksanakan oleh auditor. Contoh *engagement letter* dapat dilihat pada Gambar 4.2, dan lebih lengkapnya dapat dilihat pada Lampiran 1.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Engagement Letter

Yang bertanda tangan dibawah ini:

- ***Auditee***

  Nama : Hisyam Jaya

  Jabatan : Staf Khusus Direksi

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

- **Auditor**

  Nama : I Putu Narario Sastra

  NIM : 11.41010.0020

Sebagai pelaksana audit keamanan sistem informasi.

A. Tujuan

Tujuan dilakukannya 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, suatu hal yang penting untuk memahami dan mengimplementasikan audit keamanan

Gambar 4.2 *Engagement Letter*

4.1.2 Tujuan, Ruang Lingkup, dan Risiko

1. Tujuan Audit Keamanan Sistem Akuntansi *Enterprise* PT. GCS

Tujuan dilakukannya audit keamanan sistem akuntansi *enterprise* PT. GCS adalah untuk mengukur tingkat keamanan sistem informasi yang ada, sehingga dapat menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sudah sesuai dengan yang diharapkan. Berdasarkan permasalahan yang ada berkaitan dengan aspek keamanan informasi (CIA) dan tujuan audit keamanan SAE, maka dilakukan audit substansi untuk menegaskan apakah hasil dari aktivitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang ditargetkan atau yang diharapkan.

2. Menentukan Ruang Lingkup

PT. GCS berkomitmen untuk menjadi perusahaan perdagangan, pergudangan, angkutan, dan produsen saprotan, yang unggul dan handal serta mampu bersaing secara optimal.

SMKI PT. GCS diimplementasikan untuk ruang lingkup bisnis organisasi yaitu pada bagian: Keuangan dan Sistem TI internal PT. GCS yang digunakan adalah Sistem Akuntansi *Enterprise*.

A. Profil PT. Gresik Cipta Sejahtera

PT Gresik Cipta Sejahtera (PT GCS) adalah perusahaan dengan bisnis inti bidang perdagangan pupuk dan bahan kimia dalam lingkungan anak perusahaan Petrokimia Gresik Group yang sahamnya dimiliki oleh Yayasan Petrokimia Gresik (YPG) dan Koperasi Karyawan Keluarga Besar Petrokimia Gresik (K3PG).

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

PT GCS didirikan berdasarkan Akta Pendirian No.2 tanggal 3 April 1972 oleh Notaris Sugijanto, SH yang diperkuat dengan Penetapan Menteri Kehakiman RI tertanggal 14 Juli 1972 No. J.A.5/149/16.

PT GCS yang ada saat ini merupakan hasil penggabungan dua perusahaan yaitu PT Gresik Chemical and Supplies dengan PT Petro Aneka Usaha berdasarkan Akte No.402 tanggal 30 Nopember 1994 oleh Notaris Nurlaily Adam, SH.

Sejak mulai didirikan pada tanggal 3 April 1972, PT GCS telah mengalami beberapa kali perubahan nama, sebagai berikut :

- 3 April 1972-14 Juni 1972 : PT Petrokimia Trading Coy (PT Petrad)
- 15 Juni 1972-27 Januari 1998 : PT Gresik Chemical And Supplies (PT GCS)
- 28 Januari 1998- sekarang : PT Gresik Cipta Sejahtera (PT GCS)

Perubahan terakhir sesuai dengan Akte Perubahan tanggal 28 Januari 1998 yang dibuat oleh Notaris Ny. Hj. Netty Arni, SH yang berkedudukan di Gresik. Akte tersebut telah disahkan oleh Menteri Kehakiman Republik Indonesia dan telah diumumkan dalam Berita Negara Republik Indonesia tanggal 26 Pebruari 1998 Nomor C2-1220 HT.01.04.Th.98.

Sesuai Undang-Undang No. 3 Tahun 1982 tentang Wajib Lapor Daftar Perusahaan dan UU Republik Indonesia Nomor 40 Tahun 2007, PT GCS telah didaftarkan pada Dinas Koperasi Usaha Kecil Menengah Perindustrian dan Perdagangan Kabupaten Gresik dengan Nomor Tanda Daftar Perusahaan 13.02.1.51.00028.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Pada tanggal 19 September 2000 PT GCS telah memperoleh sertifikat ISO 9001 : 2000 dari SGS International Sertification Services Jakarta dengan Sertifikat nomor Q 18527 dan diperbarui dengan Sertifikat ISO 9001:2008 nomor ID03/00278 dengan tanggal berlaku 19 September 2012 sampai dengan 19 September 2015.

PT. GCS berkantor pusat di Gedung Petrokimia Gresik Lantai 6, Jl. Jenderal Ahmad Yani-Gresik, dan saat ini telah memiliki kantor cabang di Medan serta kantor perwakilan di Makassar, Lampung, Riau, Sumatera selatan, dan Jambi yang pada masa mendatang akan dikembangkan di daerah potensial lainnya (Sumatera Barat, Sulawesi Utara, Kalimantan Tengah, dan Maluku) serta sejumlah kantor pemasaran di Kabupaten wilayah pemasaran pupuk subsidi di Jawa Tengah, Jawa Timur, Sulawesi Selatan, Sulawesi Tengah, Sulawesi Tenggara, Sumatera Utara dan Lampung.

B. Visi dan Misi PT. Gresik Cipta Sejahtera

Visi : Menjadi perusahaan perdagangan, pergudangan, angkutan, dan produsen saprotan, yang unggul dan handal serta mampu bersaing secara optimal.

Misi :

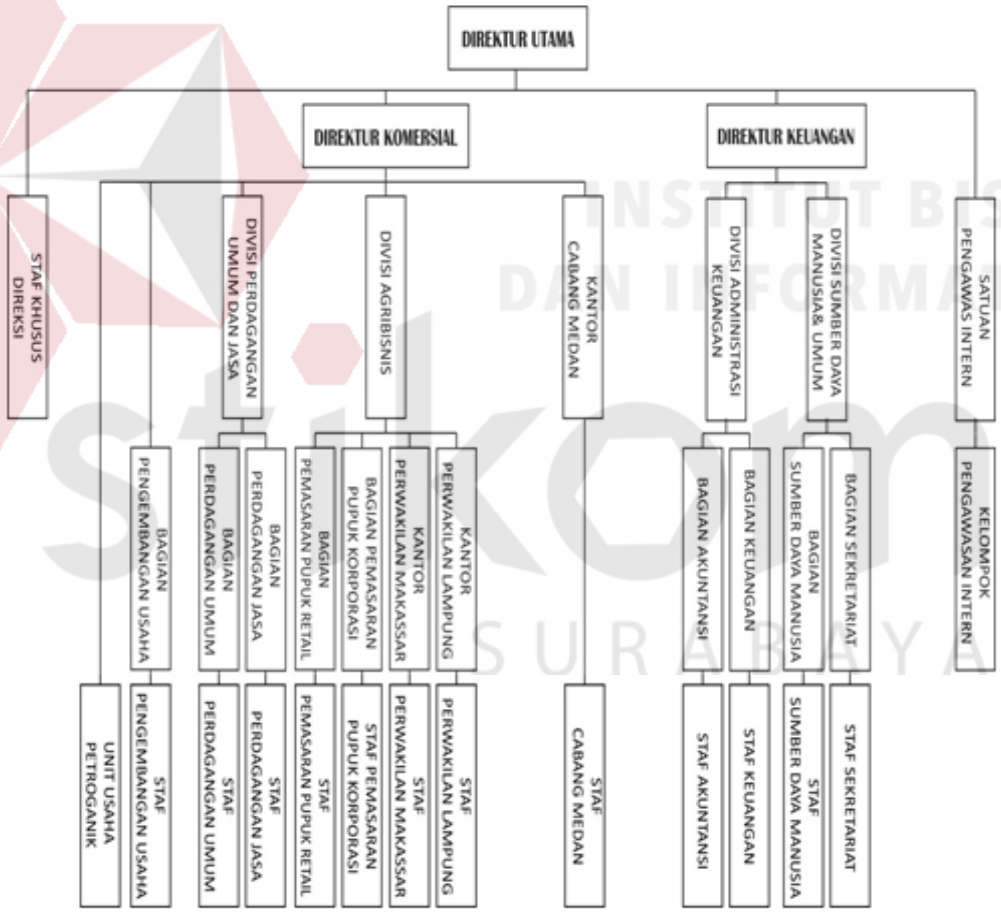
1) Menyediakan jasa pergudangan, pengangkutan dan melaksanakan perdagangan umum khususnya bahan kimia dan pupuk yang berkualitas dan bersaing.
2) Memberikan kepuasan pelanggan, menjaga komitmen dan kepercayaan pelanggan dengan pelayanan yang handal.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

3) Memberikan hasil yang terbaik kepada *Stakeholder* (pelanggan, pemegang saham, manajemen, karyawan, pemerintah dan lingkungan)
4) Berperan aktif dalam menunjang pelaksanaan program dan kebijaksanaan induk perusahaan.

C. Struktur Organisasi PT. Gresik Cipta Sejahtera

Struktur organisasi PT. Gresik Cipta Sejahtera (PT. GCS) dapat dilihat pada Gambar 4.3.



Gambar 4.3 Struktur Organisasi PT. GCS
(Sumber: PT. Gresik Cipta Sejahtera)

D. *Job Description* Pegawai PT. GCS

Uraian ringkas *job description* pegawai TI PT. GCS dapat dilihat pada Tabel 4.1, dan untuk lebih lengkapnya uraian pekerjaan pegawai TI dapat dilihat pada dokumen Lampiran 8 nomor 13, 14, dan 15.

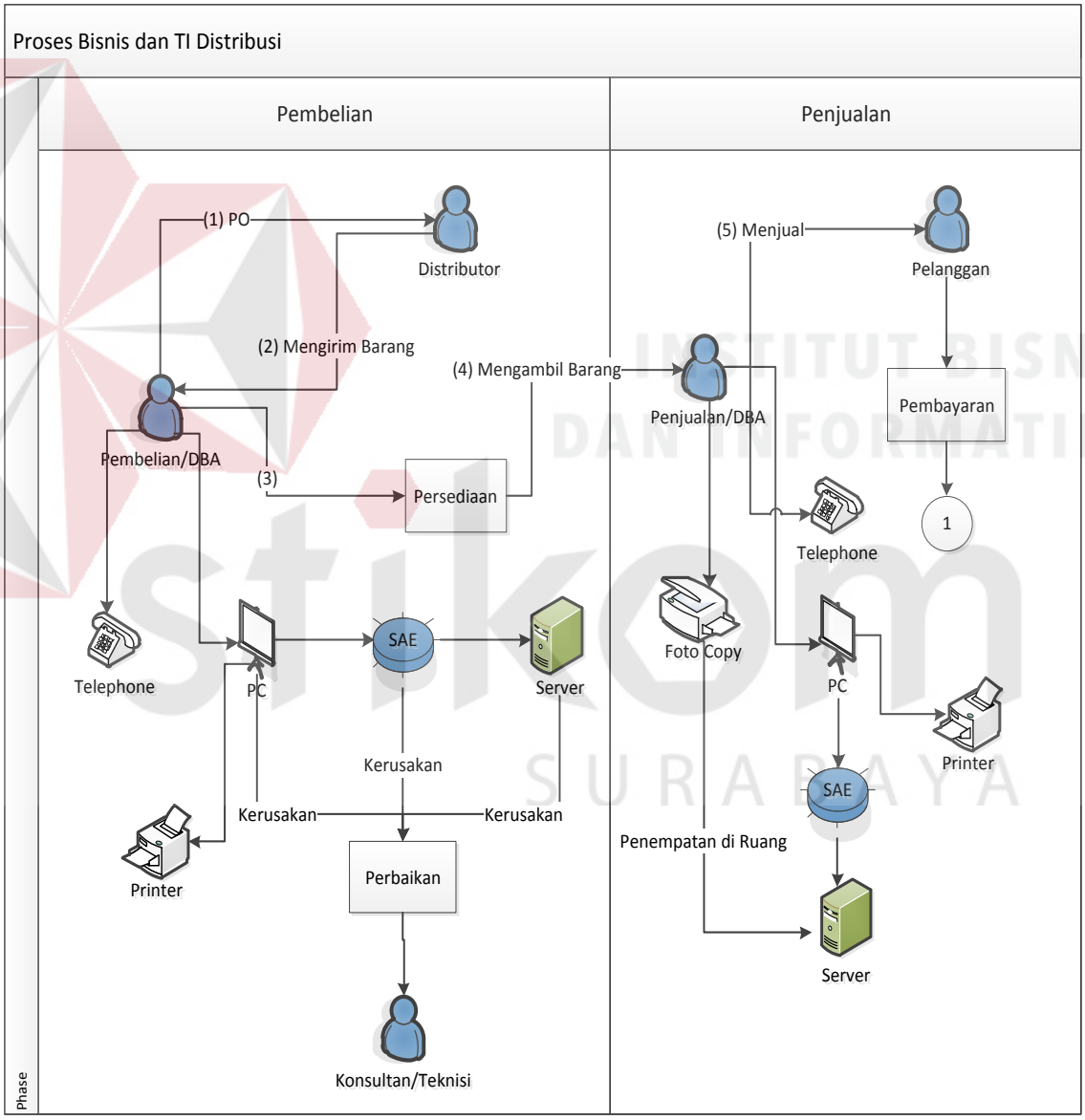
Tabel 4.1 *Job Description* Pegawai

No.	Jabatan	Uraian Ringkas Pekerjaan
1.	Staf Pemula Sistem Teknologi Informasi.	Bertanggung jawab atas jalannya seluruh sistem komputerisasi baik *hardware* maupun *software* termasuk didalamnya mengontrol seluruh kegiatan dan kinerja *server* berikut jaringannya serta menyelesaikan seluruh permasalahan yang timbul dengan cepat dan tepat agar sistem dapat berjalan kembali seperti semula di seluruh unit usaha yang terkait.
2.	Staf Muda Sistem Informasi Manajemen.	Membawahi seluruh unit kerja yang berada dibawah tugas, wewenang, dan tanggung jawabnya dalam rangka menyelenggarakan atau melaksanakan kegiatan sistem informasi manajemen sesuai dengan sistem dan prosedur, kebijakan perusahaan yang berlaku.
3.	Kepala Bagian Akuntansi	Bertanggung jawab atas terselenggaranya kegiatan pembuatan anggaran perusahaan dan pengendalian operasi, analisa dan peramalan keadaan perekonomian nasional dan internasional yang berhubungan dengan kegiatan perusahaan serta terselenggaranya kegiatan akuntansi perusahaan yang meliputi pencatatan, pemeliharaan, dan penyimpanan bukti-bukti akuntansi dan penyusunan, penyajian, dan penginterpretasi laporan-laporan termasuk pula analisanya.

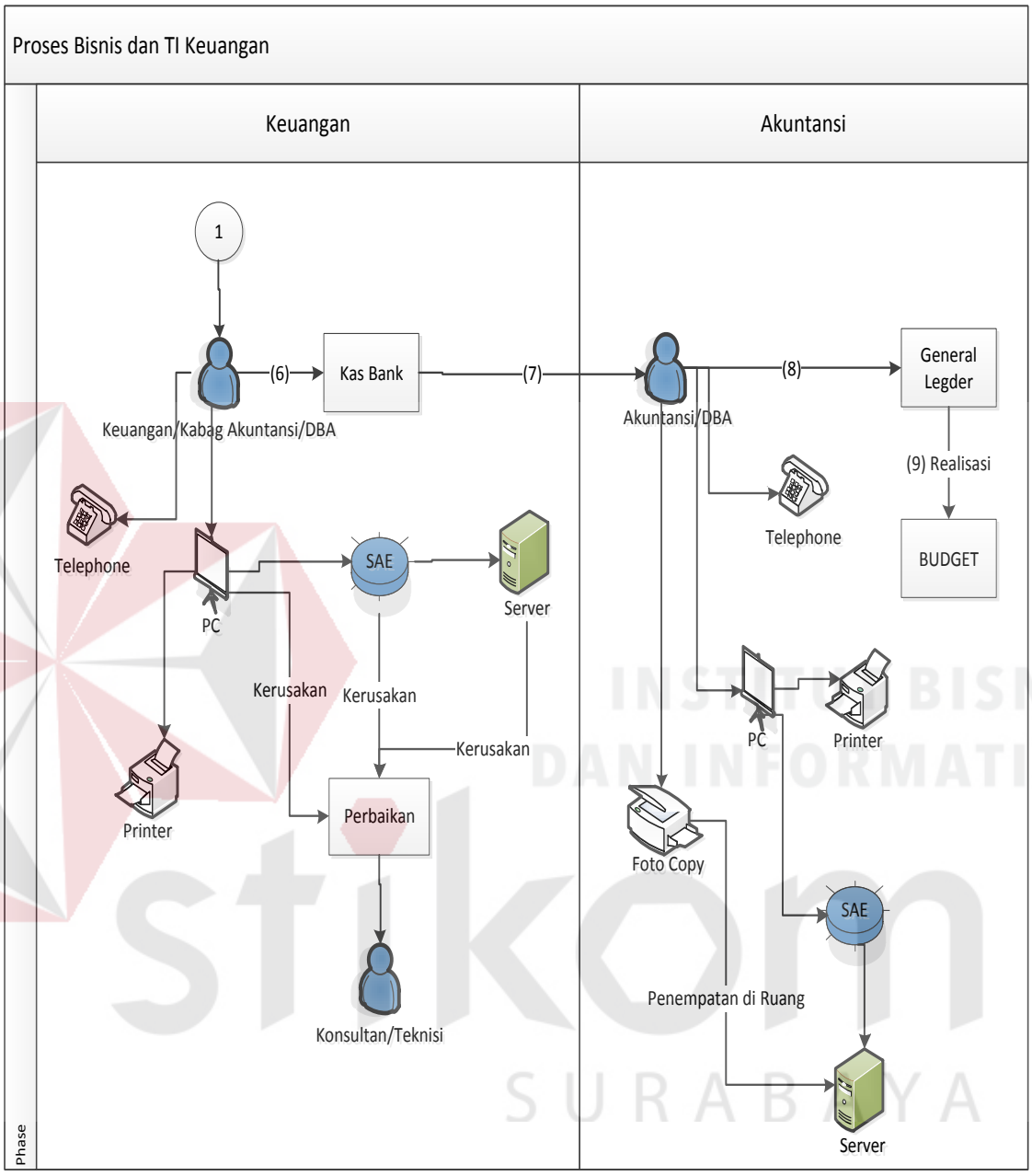
(Sumber: PT. Gresik Cipta Sejahtera)

E. Alur Proses Bisnis dan TI Distribusi dan Keuangan

Pada tahapan ini akan digambarkan alur proses bisnis dan TI PT. GCS yang didalamnya terdapat aktor atau SDM yang berperan, aset-aset perusahaan yang digunakan, dan proses bisnis yang berlangsung. Alur proses bisnis dan TI distribusi, keuangan dapat dilihat pada Gambar 4.4 dan 4.5.



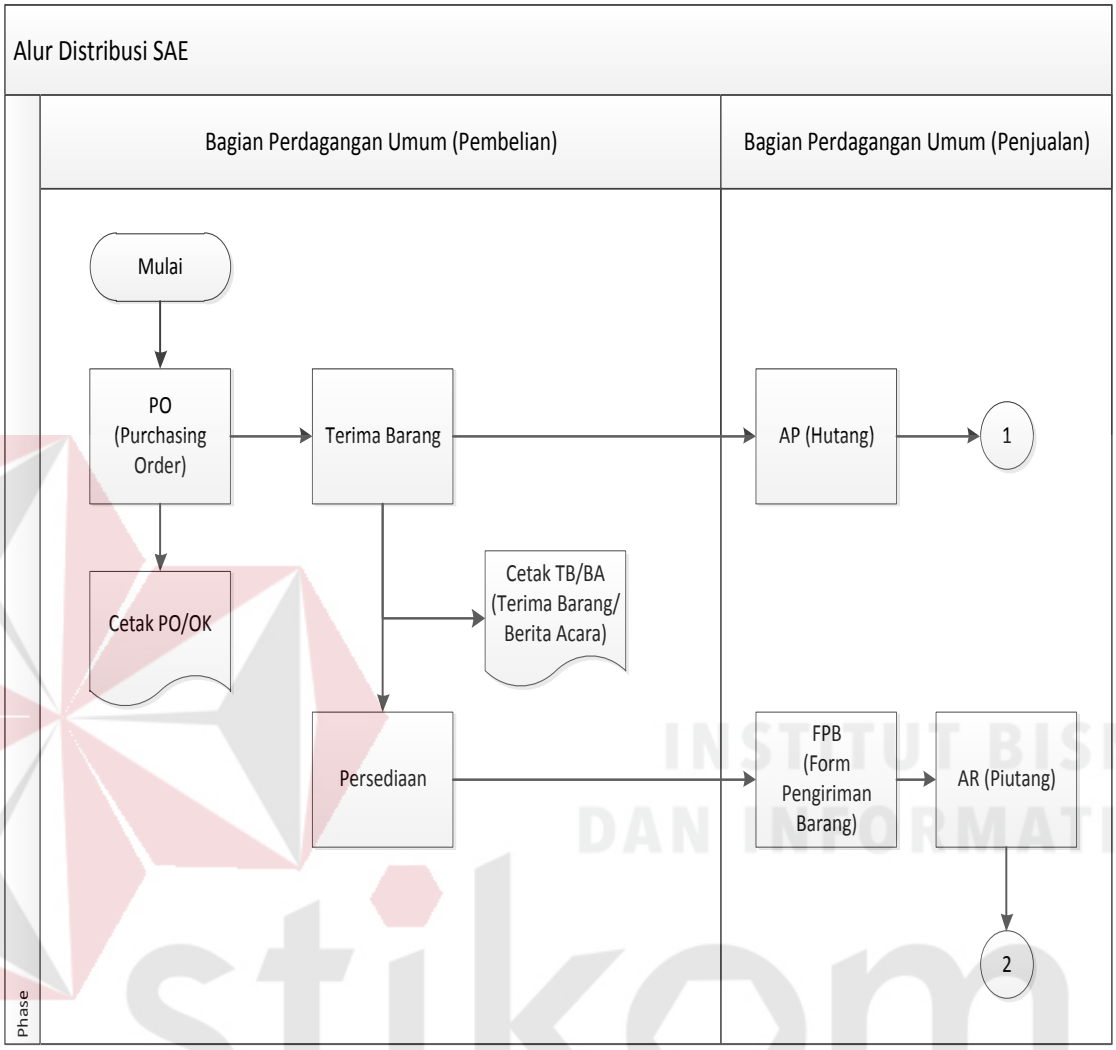
Gambar 4.4 Proses Bisnis dan TI Distribusi



Gambar 4.5 Proses Bisnis dan TI Keuangan

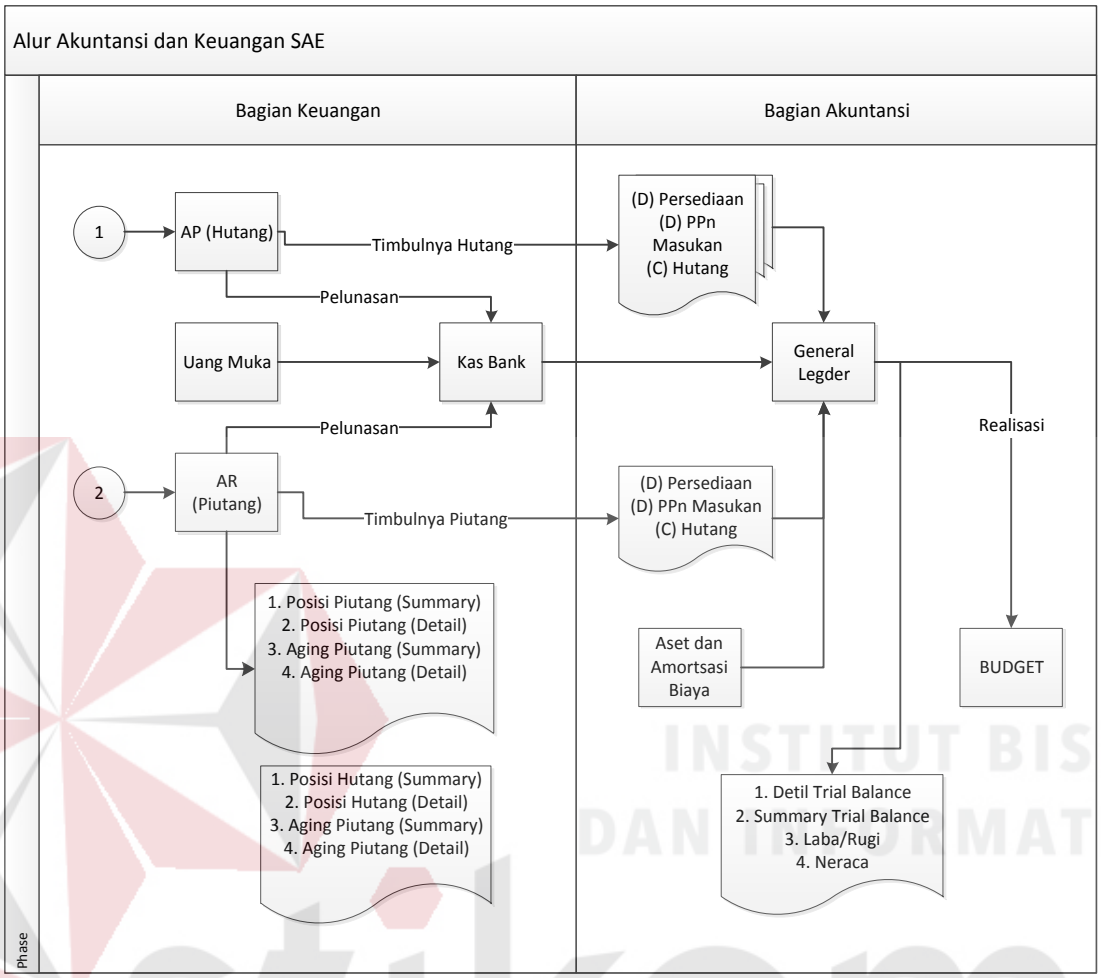
F. Alur Sistem Akuntansi *Enterprise*

Alur sistem akuntansi *enterprise* (SAE) dapat dilihat pada Gambar 4.6 dan 4.7.



Gambar 4.6 Alur Distribusi SAE
(Sumber: PT. Gresik Cipta Sejahtera)

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA



Gambar 4.7 Alur Akuntansi dan Keuangan SAE
(Sumber: PT. Gresik Cipta Sejahtera)

G. Penilaian Risiko

Setelah menentukan ruang lingkup proses bisnis dan TI PT. GCS, maka auditor akan melakukan penilaian risiko agar dapat menentukan klausul yang akan digunakan untuk kegiatan audit yang akan berlangsung, untuk lebih lengkapnya dapat dilihat pada Lampiran 3. Ada beberapa tahapan dalam penilaian risiko, yaitu:

1) Identifikasi Aset

Proses identifikasi aset dilakukan dengan cara membuat Tabel aset. Contoh Tabel aset dapat dilihat pada Tabel 4.2.

Tabel 4.2 Contoh Identifikasi Aset

Jenis Aset	Nama Aset
Dokumen	Laporan Keuangan
Software	Sistem Operasi (*Windows*) – (Sistem Akuntansi *Enterprise*)
Hardware	Server (SQL Server 2008)
	Personal Komputer (PC) Akuntansi dan Keuangan

Setelah membuat Tabel identifikasi aset maka akan dilakukan proses perhitungan nilai aset untuk mengetahui nilai informasi yang dimiliki oleh organisasi. Menghitung nilai aset berdasarkan aspek Keamanan Informasi, yaitu: *confidentiality*, *integrity*, dan *availability*. Contoh Tabel penilaian aset berdasarkan kriteria keamanan informasi dapat dilihat pada Tabel 4.3, 4.4, 4.5, dan untuk lebih lengkapnya dapat dilihat pada Lampiran 3.

Tabel 4.3 Penilaian Aset Kriteria *Confidentiality*

Kriteria *Confidentiality*	Nilai *Confidentiality* (NC)
Public	0
Internal Use Only	**1**
Private	2
Confidential	3
Secret	4

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.4 Penilaian Aset Kriteria *Integrity*

Kriteria *Integrity*	Nilai *Integrity* (NI)
No Impact	0
Minor Incident	**1**
General Disturbance	2
Mayor Disturbance	3
Unacceptable Damage	4

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.5 Penilaian Aset Kriteria *Availability*

Kriteria *Availability*	Nilai *Availability* (NV)
Low/No Availability	0
Office Hours Availability	**1**
Strong Availability	2
High Availability	3
Very High Availability	4

(Sumber: Sarno dan Iffano, 2009)

Dari ketiga Tabel tersebut, maka akan dilakukan pemilihan nilai aset dengan penulisan huruf tebal atau *bold*. Perhitungan nilai aset menggunakan persamaan matematis dengan rumus (2.1):

Nilai Aset = NC + NI + NV

Jenis Aset: Perangkat Keras

Nama Aset: Server

Nilai Aset:

Confidentiality: *Internal Use Only* (NC = 1)

Integrity: *Mayor Disturbance* (NI = 1)

Availability: *Strong Availability* (NV = 1)

NC + NI + NV = 1 + 1 + 1

Nilai Aset (Server) = 3

2) Identifikasi Ancaman dan Kelemahan

Proses identifikasi ancaman dan kelemahan dilakukan dengan cara membuat Tabel kemungkinan kejadian gangguan keamanan. Contoh Tabel kemungkinan gangguan keamanan dapat dilihat pada Tabel 4.6.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.6 Contoh Kemungkinan Gangguan Keamanan

Kejadian	Jenis	Probabilitas
Gangguan Sumber Daya	*Vulnerable*	*Low*
Gangguan Perangkat Keras	*Vulnerable*	*Medium*
Kebakaran	*Threat*	*Low*
Serangan Virus: *Trojan, Worm*, dll.	*Threat*	*High*
Penyusup atau *Hacker*	*Threat*	*Medium*
Kerusakan Data	*Vulnerable*	*Medium*
Kesalahan Pengiriman Data	*Vulnerable*	*Low*
Gangguan Petir	*Threat*	*Low*
Bencana Alam	*Threat*	*Low*
Akses Ilegal	*Threat*	*Medium*

(Sumber: Sarno dan Iffano, 2009)

Setelah mengidentifikasi ancaman dan kelemahan, maka auditor melakukan proses penilaian terhadap ancaman aset PT. GCS. Nilai probabilitas didapat dari hasil klasifikasi probabilitas. Rentang nilai probabilitas sebagai berikut:

(***Low*****:** Nilai probabilitas 0,1 – 0,3)

(***Medium*****:** Nilai probabilitas 0,4 – 0,6)

(***High*****:** Nilai probabilitas 0,7 – 1).

Contoh perhitungan nilai ancaman aset (Laporan Keuangan) PT. GCS dapat dilihat pada Tabel 4.7.

Tabel 4.7 Perhitungan Nilai Ancaman

Ancaman	Jenis	Probabilitas	Nilai Probabilitas
Gangguan Sumber Daya	*Vulnerable*	*Medium*	0.6
Gangguan Perangkat Keras	*Vulnerable*	*Low*	0.3
Virus: Trojan, Worm, dll.	*Threat*	*High*	0.7
Penyusup atau *Hacker*	*Threat*	*Low*	0.1
Kerusakan Data	*Vulnerable*	*Medium*	0.4
Akses Ilegal	*Threat*	*High*	0.7
Jumlah Ancaman = 6	**Jumlah Rata-Rata Probabilitas**		**2.8**

Dari hasil tersebut maka dapat dihitung nilai ancaman (NT) terhadap aset Laporan Keuangan PT. GCS dengan rumus (2.2):

NT (Server) = **∑PO / ∑Ancaman**

= 2.8 / 6 = 0.5

Definisi:

∑PO: Jumlah *Probability of Occurence*

∑Ancaman: Jumlah Ancaman Terhadap Informasi

3) Identifikasi Dampak (*Impact*) Kegagalan CIA

Pada langkah ini adalah mengidentifikasi dampak bisnis jika terjadi kegagalan terhadap aspek Keamanan Informasi (CIA). Contoh Tabel dampak bisnis jika terjadi kegagalan aspek Keamanan Informasi dapat dilihat pada Tabel 4.8.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.8 Dampak Bisnis

Kategori	Dampak		
	Low	*Medium*	*High*
***Confidentiality*:** Memastikan bahwa informasi hanya dapat diakses oleh orang yang memiliki hak akses.	Jika diakses tanpa ijin dapat menyebabkan kerugian terbatas pada organisasi dan pemilik informasi.	Jika diakses tanpa ijin dapat menyebabkan kerugian finansial, mengganggu proses bisnis, mengganggu reputasi organisasi.	Jika diakses tanpa ijin dapat menyebabkan kerugian finansial sangat besar, terhentinya proses bisnis, dan konsekuensi hukum.
Integrity: Menjaga bahwa informasi harus selalu akurat, valid dan utuh.	Merubah Informasi dengan tidak bertanggung jawab dapat menyebabkan kerugian terbatas pada organisasi dan pemilik informasi.	Merubah Informasi dengan tidak bertanggung jawab dapat menyebabkan kerugian finansial, mengganggu kelancaran proses bisnis, dan mengganggu reputasi organisasi.	Merubah Informasi dengan tidak bertanggung jawab dapat menyebabkan kerugian finansial sangat besar, terhentinya proses bisnis, dan konsekuensi hukum.
Availability: Memastikan bahwa informasi selalu tersedia jika dibutuhkan dan hanya bisa diakses oleh orang yang berwenang.	Gangguan terhadap akses Informasi dapat menyebabkan kerugian terbatas pada organisasi dan pemilik informasi.	Gangguan terhadap akses Informasi dapat menyebabkan kerugian finansial, mengganggu kelancaran proses bisnis, dan mengganggu reputasi organisasi.	Gangguan terhadap akses Informasi dapat menyebabkan kerugian finansial sangat besar, terhentinya proses bisnis, dan konsekuensi hukum.

(Sumber: Sarno dan Iffano, 2009)

4) Analisa Dampak Bisnis

Analisa dampak bisnis (*Business Impact Analysis*) dapat diistilahkan dengan BIA. BIA dapat menggambarkan ketahanan proses bisnis organisasi jika informasinya terganggu. Analisa dampak bisnis dilakukan dengan cara membuat skala nilai BIA yang dipilih dengan huruf tebal atau *bold* dapat dilihat pada Tabel 4.9, sedangkan contoh Tabel BIA untuk fasilitas informasi yang dimiliki PT. GCS dengan mengacu pada nilai skala yang ditandai dengan huruf tebal atau *bold* dapat dilihat pada Tabel 4.10.

Tabel 4.9 Contoh Skala Nilai BIA

Batas Toleransi Gangguan	**Keterangan**	**Nilai Skala**
< dari 1 minggu	*Not Critical*	0-20
1 hari s/d 2 hari	*Minor Critical*	21-40
< dari 1 hari	*Mayor Critical*	41-60
< dari 12 jam	*High Critical*	61-80
< dari 1 jam	***Very High Critical***	**81-100**

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.10 Contoh BIA Fasilitas Informasi

Fasilitas Informasi	**Dampak**	**Nilai BIA**
Informasi Keuangan	Pelaporan tertunda, kepercayaan *costumer* dan *investor* tertunda	25
Informasi *Budgeting*	Keterlambatan pengambilan keputusan, kesalahan penentuan kebijakan anggaran bulanan dan tahunan	55
SAE	Pekerjaan terhenti	50
PC	Pelaporan tertunda	22
Server	**Operasi terhenti**	**93**

5) Mengidentifikasi Level Risiko

Mengidentifikasi level risiko dapat dilakukan dengan cara membuat Tabel level risiko. Dengan Tabel level risiko kita dapat mengetahui gambaran seberapa besar risiko yang diterima organisasi jika terjadi kegagalan Keamanan Informasi. Contoh Tabel level risiko dapat dilihat pada Tabel 4.11. Didalam Tabel level risiko terdapat nilai probabilitas ancaman yang dibagi dalam 3 level penilaian, yaitu:

0 ≥ *Low Probability* ≤ 0,1

0,1 > *Medium Probability* ≤ 0,5

0,5 > *High Probability* ≤ 1,0

Sedangkan dampak bisnis dibagi dalam 5 level penilaian, yaitu:

0 ≥ *Not Critical Impact* ≤ 20

20 > *Low Critical Impact* ≤ 40

40 > *Medium Critical Impact* ≤ 60

60 > *High Critical Impact* ≤ 80

80 > *Very High Critical Impact* ≤ 100

Tabel 4.11 Level Risiko

Probabilitas Ancaman	**Dampak Bisnis (*Impact*)**				
	***Not Critical* (20)**	***Low Critical* (40)**	***Medium Critical* (60)**	***High Critical* (80)**	***Very High Critical* (100)**
***Low* (0,1)**	*Low* 20x0,1 = 2	*Low* 40x0,1 = 4	*Low* 60x0,1 = 6	*Low* 80x0,1 = 8	*Low* 100x0,1 = 10
***Medium* (0,5)**	*Low* 20x0,5 = 10	*Medium* 40x0,5 = 20	*Medium* 60x0,5 = 30	*Medium* 80x0,5 = 40	*Medium* 100x0,5 = 50
***High* (1,0)**	*Medium* 20x1,0 = 20	*Medium* 40x1,0 = 40	*High* 60x1,0 = 60	*High* 80x1,0 = 80	*High* 100x1,0 = 100

(Sumber: Sarno dan Iffano, 2009)

6) Menentukan Risiko Diterima atau Perlu Pengelolaan Risiko

Pada tahapan ini akan dilakukan penilaian risiko dengan menggunakan metode matematis berdasarkan hasil pada langkah-langkah sebelumnya, yaitu:

Nilai Aset: NA

Analisa Dampak Bisnis: BIA

Nilai Ancaman: NT

Nilai Risiko dapat dihitung dengan menggunakan rumus (2.3):

***Risk Value* = NA x BIA x NT**

Nama Aset: Server

Nilai Aset (NA) = 3

Nilai BIA = 10

Nilai Ancaman (NT) = 0.5

Nilai Risiko = 3 x 10 x 0,5 = 15

Level Risiko Server = *Medium Risk*

Dari hasil tersebut, nilai risiko aset server PT. GCS termasuk dalam kategori *medium risk* dan nilai ancaman (0,5) masuk dalam kategori *high*, maka risiko dihindari atau ditolak (*risk avoidance*) yang berarti organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul.

Tabel 4.12 Kriteria Penerimaan Risiko

No.	Nama Aset	PA	BP	BR	Nilai	Kriteria
1.	Informasi Keuangan	*High*	*Med*	*Med*	*Med*	*Risk Avoidance*
2.	Informasi *Budgeting*	*High*	*Med*	*Med*	*Med*	*Risk Avoidance*
3.	*Software* SAE	*Med*	*Med*	*Med*	*Med*	*Risk Reduction*
4.	*Hardware* PC	*Med*	*High*	*Low*	*Low*	*Risk Transfer*
5.	*Hardware Server*	*High*	*Med*	*Med*	*Med*	*Risk Avoidance*

7) Menentukan Klausul ISO 27002:2005

Pemetaan permasalahan yang terjadi dengan klausul kontrol keamanan ISO 27002:2005 digunakan untuk mempermudah organisasi dalam memilih kontrol keamanan yang sesuai kebutuhan organisasi dengan tiga kategori pengelompokkan kontrol keamanan, yaitu: manajemen, teknikal, dan operasional. Pemetaan antara permasalahan dan klausul dapat dilihat pada Tabel 4.13 hasil rangkuman dari Tabel

Kebutuhan Kontrol Keamanan dan Hubungan Klausul Kontrol Keamanan dengan aspek Keamanan Informasi sumber (Sarno dan Iffano, 2009).

Tabel 4.13 Pemetaan Permasalahan dan Klausul

Permasalahan	Klausul Kontrol Keamanan
***Confidentiality*:** Kesalahan *posting* data transaksi penjualan yang tidak sesuai dengan perencanaan	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 6 Organisasi Keamanan Informasi.
	Manajemen: Klausul 7 Manajemen Aset.
	Teknikal: Klausul 8 Keamanan Sumber Daya Manusia.
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Teknikal: Klausul 11 Kontrol Akses.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Operasional: Klausul 13 Manajemen Insiden Keamanan Informasi.
	Manajemen: Klausul 15 Kesesuaian
***Integrity*:** Keutuhan pencatatan aset khususnya di bidang TI dan laporan keuangan tidak *balance*.	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 7 Manajemen Aset.
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Operasional: Klausul 13 Manajemen Insiden Keamanan Informasi.
***Availability*:** Keterlambatan penyediaan informasi *budgeting*.	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 7 Manajemen Aset.
	Manajemen: Klausul 15 Kesesuaian
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Operasional: Klausul 13 Manajemen Insiden Keamanan Informasi.

Setelah melakukan pemetaan permasalahan dengan klausul ISO 27002:2005, maka auditor akan melakukan pemetaan antara permasalahan, proses, dan klausul yang akan digunakan untuk mengetahui kesesuaian klausul yang digunakan untuk audit dengan kebutuhan organisasi. Contoh pemetaan permasalahan dan proses dapat dilihat pada Tabel 4.14.

Tabel 4.14 Pemetaan Permasalahan dan Proses

Permasalahan	Proses	Klausul
***Confidentiality*:** Kesalahan *posting* data transaksi penjualan yang tidak sesuai dengan perencanaan.	Permasalahan *confidentiality* yang ada dapat terjadi pada divisi perdagangan umum dan jasa khususnya karyawan bagian penjualan pada saat memproses data transaksi penjualan pelanggan. Ancaman yang dimungkinkan terjadi adalah akses ilegal sesama karyawan dan kelemahan yang mungkin terjadi adalah kesalahan pengiriman data dikarenakan ketidaktahuan.	5, 6, 7, 8, 9, 10, 11, 13, dan 15.
***Integrity*:** Keutuhan pencatatan aset khususnya di bidang TI dan laporan keuangan tidak *balance*.	Permasalahan *integrity* yang ada dapat terjadi pada bagian keuangan dan akuntansi. Berawal dari bagian keuangan saat proses kas bank dan berlanjut pada bagian akuntansi saat proses pembuatan general ledger. Ancaman yang dimungkinan terjadi adalah akses ilegal sesama karyawan, penyusup internal (karyawan) maupun pihak ketiga, virus. Sedangkan kelemahan yang mungkin terjadi adalah kesalahan pengiriman data, kerusakan data, gangguan perangkat keras, dan gangguan sumber daya.	5, 7, 9, 10, dan 13.
***Availability*:** Keterlambatan penyediaan informasi *budgeting*.	Permasalahan *availability* yang ada dapat terjadi pada divisi keuangan khususnya pada bagian akuntansi. Berdasarkan permasalahan yang terjadi pada proses-proses sebelumnya, pihak akuntansi harus melakukan pengecekkan ulang yang akhirnya menyebabkan keterlambatan penyediaan informasi *budgeting*.	5, 7, 9, 10, 13 dan 15.

Dari hasil pemetaan permasalahaan dan proses bisnis dan TI yang ada, mayoritas memiliki dampak bisnis yang masuk dalam kategori *medium* terhadap aspek keamanan informasi (CIA):

1) *Confidentiality:* Jika diakses tanpa ijin dapat menyebabkan kerugian financial, mengganggu kelancaran proses bisnis, dan mengganggu citra atau reputasi organisasi.

2) *Integrity:* Merubah informasi dengan tidak bertanggung jawab dapat menyebabkan kerugian financial, mengganggu kelancaran proses bisnis, dan mengganggu citra atau reputasi organisasi.
3) *Availability:* Gangguan terhadap akses informasi dapat menyebabkan kerugian financial, mengganggu kelancaran proses bisnis, dan mengganggu citra atau reputasi organisasi.

Setelah melakukan proses pemetaan, maka hasil pemilihan klausul kontrol keamanan dengan aspek keamanan informasi dapat dilihat pada Tabel 4.15. Dari hasil pemetaan pada Tabel 4.14 ada beberapa klausul yang tidak digunakan dalam penelitian ini, yaitu: 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. Klausul-klausul yang tidak digunakan dalam penelitian ini dapat digunakan pada penelitian serupa berikutnya agar PT. GCS dapat mengetahui tingkat keamanan SAE lebih detil sesuai dengan permasalahan yang terjadi.

Tabel 4.15 Hubungan Klausul dengan Aspek Keamanan Informasi

ISO 27002			Aspek Keamanan Informasi		
No.	Klausul Kontrol Keamanan	Kategori Keamanan Utama	C	I	A
7	Manajemen Aset	Tanggung jawab terhadap aset	√	√	√
		Klasifikasi informasi	√		
8	Keamanan Sumber Daya Manusia	Keamanan SDM sebelum menjadi pegawai	√		
		Selama menjadi pegawai	√		
		Pemberhentian atau pemindahan pegawai	√		
9	Keamanan Fisik dan Lingkungan	Wilayah aman	√	√	√
		Keamanan peralatan	√	√	√

Tabel 4.15 Hubungan Klausul dengan Aspek Keamanan Informasi (Lanjutan)

ISO 27002			Aspek Keamanan Informasi		
No.	Klausul Kontrol Keamanan	Kategori Keamanan Utama	C	I	A
11	Kontrol Akses	Persyaratan bisnis untuk kontrol akses	√		
		Manajemen akses *user*	√		
		Tanggung jawab pengguna	√		
		Kontrol akses jaringan	√		
		Kontrol akses sistem operasi	√		
		Kontrol akses informasi dan aplikasi	√		
		Komputasi bergerak dan bekerja di tempat lain	√		

(Sumber: Sarno dan Iffano, 2009)

4.1.3 Jadwal Kerja Audit

Hasil dari penyusunan jadwal kerja berupa Tabel yang berisi tentang aktivitas selama kegiatan audit keamanan sistem akuntansi *enterprise* berlangsung. Jadwal kerja audit dapat dilihat pada Tabel 4.16.

Tabel 4.16 Jadwal Kerja Audit

No	KEGIATAN	September				Oktober				November				Desember				Januari				Februari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Membuat *Engagement Letter*																								
2	Identifikasi Proses Binis																								
3	Penentuan Tujuan, Ruang Lingkup, dan Risiko																								
4	Menentukan Klausul ISO 27002:2005																								
5	Penyusunan Jadwal Kerja dan Penyampaian Kebutuhan Data																								
6	Membuat Pernyataan																								
7	Membuat Pembobotan																								
8	Membuat Pertanyaan																								
9	Wawancara dan Observasi																								
	a. Klausul 7 (Manajemen Aset)																								
	b. Klausul 8 (Keamanan Sumber Daya Manusia)																								
	c. Klausul 9 (Keamanan Fisik dan Lingkungan)																								
	d. Klausul 11 (Kontrol Akses)																								
10	Pemeriksaan Data, Bukti, dan Temuan																								
11	Melakukan Uji Kematangan																								
12	Temuan dan Rekomendasi																								
13	Penyusunan Draf Laporan Audit																								
14	Persetujuan Draf Laporan Audit																								
15	Pelaporan Draf Audit																								
16	*Exit Meeting*																								

4.2 Hasil Persiapan Audit Keamanan Sistem Akuntansi *Enterprise*

Pada tahap persiapan audit ini langkah-langkah yang dilakukan adalah: 1. Membuat Pernyataan, 2. Membuat Pembobotan, 3. Membuat Pertanyaan. Hasil dari tahap ini adalah jadwal kerja audit, pernyataan, pembobotan, dan pertanyaan yang akan diajukan pada *auditee*.

4.2.1 Hasil Pernyataan

Penyataan dibuat berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang ada pada ISO 27002:2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang mendeskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Pernyataan juga dibuat untuk memudahkan auditor dalam membuat pertanyaan yang akan digunakan untuk wawancara audit keamanan SAE. Beberapa contoh pernyataan pada klausul 9 (keamanan fisik dan lingkungan) dengan objektif kontrol 9.1.1 (pembatas keamanan fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.17, dan untuk selengkapnya dapat dilihat pada Lampiran 4 Pernyataan dan Pembobotan.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.17 Pernyataan 9.1.1 Pembatas Keamanan Fisik

<table>
<tr><td colspan="2" rowspan="4">Audit Keamanan Sistem Informasi Klausul 9

(Keamanan Fisik dan Lingkungan)</td><td>Auditor: I Putu Narario Sastra</td></tr>
<tr><td>Auditee: Pak Hisyam</td></tr>
<tr><td>Tanggal: 20-10-2015</td></tr>
<tr><td>Tanda Tangan:</td></tr>
<tr><td colspan="3">Klausul 9.1 Wilayah Aman (Secure Areas)</td></tr>
<tr><td colspan="3">9.1.1 Pembatas Keamanan Fisik (Physical Security Parimeter)</td></tr>
<tr><td colspan="3">Kontrol : Pembatasan keamanan (dinding pengaman, kontrol kartu akses, penjaga) harus disediakan untuk melindungi wilayah dan perangkat pemrosesan informasi.</td></tr>
<tr><td>No.</td><td colspan="2">PERNYATAAN</td></tr>
<tr><td>1.</td><td colspan="2">Mempunyai parameter keamanan yang harus didefinisikan secara jelas (dinding, kartu akses, penjaga pintu) terhadap ruang pemrosesan informasi.</td></tr>
<tr><td>2.</td><td colspan="2">Dinding bangunan harus terbuat dari konstruksi yang kuat.</td></tr>
<tr><td>3.</td><td colspan="2">Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.</td></tr>
<tr><td>4.</td><td colspan="2">Mempunyai ruang penerimaan tamu.</td></tr>
<tr><td>5.</td><td colspan="2">Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.</td></tr>
<tr><td>6.</td><td colspan="2">Mempunyai pintu darurat yang selalu di kontrol.</td></tr>
<tr><td>7.</td><td colspan="2">Pintu harus beroperasi dengan menggunakan kode darurat (kebakaran).</td></tr>
</table>

4.2.2 Hasil Pembobotan

Setelah auditor membuat pernyataan, maka langkah selanjutnya adalah melakukan pembobotan pada setiap pernyataan. Hasil pembobotan dari pernyataan yang ada didapat dari diskusi dengan pihak *auditee* berdasarkan tingkat kepentingan pernyataan yang ada bagi perusahaan. Contoh hasil pembobotan pada klausul 9 (keamanan fisik dan lingkungan) dengan objektif kontrol 9.1.1 (pembatas keamanan

fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.18, dan untuk selengkapnya dapat dilihat pada Lampiran 4 Pernyataan dan Pembobotan.

Tabel 4.18 Pembobotan 9.1.1 Pembatas Keamanan Fisik

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
5.	Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.	0.3
6.	Mempunyai pintu darurat yang selalu di kontrol.	0.6
7.	Pintu harus beroperasi dengan menggunakan kode darurat (kebakaran).	0.6
8.	Memiliki CCTV yang digunakan untuk memantau lingkungan kerja (monitoring).	1
9.	Ruangan pemrosesan informasi dikelola oleh organisasi.	1
10.	Ruangan pemrosesan informasi harus dipisahkan dari pihak ketiga.	1

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

4.2.3 Hasil Pertanyaan

Setelah melakukan pembobotan, makan auditor akan membuat pertanyaan yang akan diajukan kepada *auditee* untuk pelaksanaan Audit Keamanan Sistem Akuntansi *Enterprise*. Pertanyaan yang dibuat oleh auditor mengacu pada pernyataan yang ada, satu pernyataan bisa memiliki lebih dari satu pertanyaan. Pertanyaan dibuat dengan acuan metode 5W + 1H. Contoh hasil pertanyaan pada klausul 9 (keamanan fisik dan lingkungan) dengan obyektif kontrol 9.1.1 (pembatas keamanan fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.19, dan untuk selengkapnya dapat dilihat pada Lampiran 5 Pertanyaan dan Jawaban.

Tabel 4.19 Pertanyaan 9.1.1 Pembatas Keamanan Fisik

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:	

Tabel 4.19 Pertanyaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
2	Dinding bangunan harus terbuat dari konstruksi yang kuat.
	P: Apakah semua dinding bangunan perusahaan sudah terbuat dari konstruksi yang kuat? J: P: Bahan apa yang digunakan untuk membuat dinding bangunan? J: P: Apakah ada pertimbangan dalam penggunaan bahan untuk membangun dinding bangunan? J: P: Apakah ada pertimbangan khusus dalam pembuatan dinding untuk suatu ruangan yang dianggap penting? J:
3	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.
	P: Apakah perusahaan memiliki peraturan mengenai batasan akses ke ruang pemrosesan informasi untuk mencegah akses ilegal serta pencemaran lingkungan? J: P: Siapa saja yang berhak mengakses ruang pemrosesan informasi? J: P: Batasan seperti apa yang digunakan untuk ruang pemrosesan informasi untuk mencegah terjadinya akses ilegal? J:
4	Mempunyai ruang penerimaan tamu.
	P: Apakah perusahaan memiliki ruang penerimaan tamu? J: P: Dimana letak ruang penerimaan tamu? J: P: Bagaimana penerapan dari kegunaan ruang penerimaan tamu tersebut? J:

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

Tabel 4.19 Pertanyaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
5	Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.
	P: Apakah perusahaan memiliki peraturan mengenai batasan akses ke tempat kerja untuk personil dengan otorisasi? J: P: Siapa yang bertugas mengontrol batasan akses ke tempat kerja? J: P: Kapan batasan itu mulai diberlakukan? Dan untuk siapa saja batasan itu digunakan? J: P: Bagaimana penerapan batasan akses menuju tempat kerja untuk personil dengan otorisasi? Bagaimana jika ada orang yang masuk tempat kerja tanpa otorisasi? J:
6	Mempunyai pintu darurat yang selalu di kontrol.
	P: Apakah perusahaan memiliki pintu darurat? J: P: Dimana letak pintu darurat tersebut? J: P: Siapakah yang bertugas mengontrol fungsi pintu darurat tersebut? J: P: Dalam kondisi apa pintu darurat itu digunakan? J:
7	Pintu harus beroperasi dengan menggunakan kode darurat (kebakaran).
	P: Apakah pintu darurat perusahaan dilengkapi dengan alaram kebakaran? J: P: Apakah ada alat pemadam kebakaran yang diletakkan di sekitar pintu darurat? J: P: Siapakah yang bertugas mengontrol kinerja alaram dan alat pemadam kebakaran? J: P: Kapan kode darurat dan alat pemadam kebakaran digunakan? J:

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.19 Pertanyaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
8	Memiliki CCTV yang digunakan untuk memantau lingkungan kerja (monitoring).
	P: Apakah perusahaan memiliki CCTV? J: P: Dimana saja CCTV diletakkan? J: P: Apakah penempatan CCTV sudah sesuai dengan kebutuhan? J: P: Siapa yang bertugas melakukan monitoring CCTV perusahaan? J:
9	Ruangan pemrosesan informasi dikelola oleh organisasi.
	P: Apakah ruang pemrosesan informasi di kelola sendiri oleh organisasi? J: P: Apakah ada peraturan bahwa ruang pemrosesan informasi harus dikelola oleh pegawai atau orang internal organisasi? J: P: Siapa saja yang bertugas mengelola ruang pemrosesan informasi? J: P: Bagaimana proses pengelolaan ruang pemrosesan informasi yang dilakukan oleh organisasi? J:
10	Ruangan pemrosesan inforamsi harus di pisahkan dari pihak ketiga.
	P: Apakah ruang pemrosesan informasi sudah dipisahkan dari pihak ketiga (tidak ada campur tangan pihak ketiga dalam hal pengelolaan, penggunaan, dan lain-lain)? J: P: Apakah ada peraturan bahwa ruang pemrosesan informasi harus dipisahkan dari pihak ketiga? J: P: Apakah tempat ruang pemrosesan informasi sudah jauh dari jangkauan pihak ketiga? J: P: Bagaimana tindakan pencegahan akses ruang pemrosesan informasi dari pihak ketiga? J:

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

4.3 Hasil Pelaksanaan Audit Keamanan Sistem Akuntansi *Enterprise*

Pada tahap pelaksanaan audit ini langkah-langkah yang dilakukan adalah: 1. Wawancara dan Observasi, 2. Pemeriksaan Data, Bukti, dan Temuan, 3. Melakukan Uji Kematangan, 4. Temuan dan Rekomendasi. Keluaran hasil pada tahapan ini adalah pertanyaan dan jawaban dari *auditee*, hasil pemeriksaan auditor, hasil uji kematangan, temuan dan rekomendasi, bukti foto audit yang dapat dilihat pada Lampiran 8.

4.3.1 Hasil Wawancara dan Observasi

Wawancara dilakukan oleh auditor berdasarkan pertanyaan yang telah dibuat sebelumnya. Wawancara dilakukan kepada pihak-pihak yang terlibat dalam proses Audit Keamanan Sistem Akuntansi *Enterprise*. Ada tiga pihak yang mewakili tiga bagian berbeda dalam proses audit, yaitu: Pak Joko adalah pihak yang bertanggung jawab pada bagian Akuntansi dan Keuangan, Pak Nanang adalah pihak yang bertanggung jawab pada bagian SDM, dan Pak Hisyam adalah pihak yang bertanggung jawab pada bagian TI. Contoh hasil wawancara dan observasi pada klausul 9 (keamanan fisik dan lingkungan) dengan obyektif kontrol 9.1.1 (pembatas keamanan fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.20, dan untuk selengkapnya dapat dilihat pada Lampiran 5 Pertanyaan dan Jawaban.

Tabel 4.20 Wawancara 9.1.1 Pembatas Keamanan Fisik

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^{o}C agar tidak cepat panas.
2	Dinding bangunan harus terbuat dari konstruksi yang kuat.
	P: Apakah semua dinding bangunan perusahaan sudah terbuat dari konstruksi yang kuat? J: Dinding bangunan perusahaan sudah terbuat dari konstruksi yang kuat. P: Bahan apa yang digunakan untuk membuat dinding bangunan? J: Bahan yang digunakan sewajarnya bangunan (batu bata, semen (cor), pasir, kayu, dan lain-lain). P: Apakah ada pertimbangan dalam penggunaan bahan untuk membangun dinding bangunan? J: Tidak ada pertimbangan dalam penggunaan bahan, sewajarnya saja. P: Apakah ada pertimbangan khusus dalam pembuatan dinding untuk suatu ruangan yang dianggap penting? J: Pertimbangan yang digunakan dari segi keamanan dan kekuatan bahan, agar tidak mudah rusak. Bukti: (Lampiran 8 No. 21) Foto Gedung, (Lampiran 8 No. 22) Foto Kantor.

Tabel 4.20 Wawancara 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
3	Memiliki batasan akses ke ruangan pemrosesan informasi untuk mencegah terjadinya akses ilegal serta pencemaran lingkungan.
	P: Apakah perusahaan memiliki peraturan mengenai batasan akses ke ruang pemrosesan informasi untuk mencegah akses ilegal serta pencemaran lingkungan? J: Batasan akses ke ruang pemrosesan informasi berdasarkan *job description* masing-masing pegawai. P: Siapa saja yang berhak mengakses ruang pemrosesan informasi? J: Yang berhak mengakses ruang pemrosesan informasi adalah divisi TI. P: Batasan seperti apa yang digunakan untuk ruang pemrosesan informasi untuk mencegah terjadinya akses ilegal? J: Batasan yang digunakan berupa pembuatan ruangan tersendiri untuk pemrosesan informasi, yang didalamnya terdapat pembatas ruangan lagi untuk *server* disertai dengan kunci ruangan. Bukti: (Lampiran 8 No. 23) Foto Ruang Pemrosesan Informasi.
4	Mempunyai ruang penerimaan tamu.
	P: Apakah perusahaan memiliki ruang penerimaan tamu? J: Perusahaan memiliki dua ruangan penerimaan tamu. P: Dimana letak ruang penerimaan tamu? J: Letak ruang penerimaan tamu disamping resepsionis, didekat pintu masuk kantor. P: Bagaimana penerapan dari kegunaan ruang penerimaan tamu tersebut? J: Penerapan ruang penerimaan tamu sudah sesuai dengan kegunaannya, hanya digunakan untuk menerima tamu atau tempat singgah tamu perusahaan dan karyawan. Bukti: (Lampiran 8 No. 24) Foto Ruang Penerimaan Tamu.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.20 Wawancara 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
5	Mempunyai batasan akses menuju tempat kerja untuk personil dengan otorisasi.
	P: Apakah perusahaan memiliki peraturan mengenai batasan akses ke tempat kerja untuk personil dengan otorisasi? J: Perusahaan belum memiliki peraturan tertulis mengenai batasan akses ke tempat kerja, akan tetapi sudah diterapkan oleh karyawan. P: Siapa yang bertugas mengontrol batasan akses ke tempat kerja? J: Yang bertugas mengontrol batasan akses ke tempat kerja adalah petugas resepsionis dan seluruh karyawan. P: Kapan batasan itu mulai diberlakukan? Dan untuk siapa saja batasan itu digunakan? J: Batasan akses ke tempat kerja mulai diberlakukan sejak berdirinya perusahaan 14 Juli 1972, berlaku untuk semua orang selain karyawan. P: Bagaimana penerapan batasan akses menuju tempat kerja untuk personil dengan otorisasi? Bagaimana jika ada orang yang masuk tempat kerja tanpa otorisasi? J: Batasan akses ke tempat kerja sudah diterapkan, apabila terdapat orang asing (selain karyawan) maka petugas resepsionis dan karyawan akan menanyakan keperluan orang tersebut, kemudian akan disuruh menunggu di ruang tamu sambil menunggu konfirmasi dari orang yang akan ditemui. Bukti: (Lampiran 8 No. 25) Foto Ruang Resepsionis.
6	Mempunyai pintu darurat yang selalu di kontrol.
	P: Apakah perusahaan memiliki pintu darurat? J: Perusahaan sudah memilik pintu darurat dan selalu dikontrol. P: Dimana letak pintu darurat tersebut? J: Pintu darurat berada di belakang kantor. P: Siapakah yang bertugas mengontrol fungsi pintu darurat tersebut? J: Yang bertugas mengontol pintu darurat adalah petugas umum. P: Dalam kondisi apa pintu darurat itu digunakan? J: Pintu darurat digunakan dalam kondisi yang mendesak, misalnya terjadi bencana seperti kebakaran, gempa bumi, dan lain-lain. Bukti: (Lampiran 8 No. 26) Foto Pintu Darurat.

Tabel 4.20 Wawancara 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
7	Pintu harus beroperasi dengan menggunakan kode darurat (kebakaran).
	P: Apakah pintu darurat perusahaan dilengkapi dengan alaram kebakaran? J: Pintu darurat perusahaan sudah dilengkapi dengan alaram kebakaran. P: Apakah ada alat pemadam kebakaran yang diletakkan di sekitar pintu darurat? J: Alat pemadam kebakaran sudah disediakan disektar pintu darurat tepatnya dibawah alaram kebakaran. P: Siapakah yang bertugas mengontrol kinerja alaram dan alat pemadam kebakaran? J: Yang bertugas mengontrol kinerja alaram kebakaran dan alat pemadam kebakaran adalah petugas umum. P: Kapan kode darurat dan alat pemadam kebakaran digunakan? J: Alaram kebakaran dan alat pemadam kebakaran digunakan jika terjadi kebakaran pada gedung atau lingkungan kerja. Bukti: (Lampiran 8 No. 26) Foto Pintu Darurat, (Lampiran 8 No. 27) Foto Alaram Kebakaran.
8	Memiliki CCTV yang digunakan untuk memantau lingkungan kerja (monitoring).
	P: Apakah perusahaan memiliki CCTV? J: Perusahaan sudah menggunakan CCTV. P: Dimana saja CCTV diletakkan? J: CCTV hanya diletakkan di pintu masuk kantor. P: Apakah penempatan CCTV sudah sesuai dengan kebutuhan? J: Penempatan CCTV sudah sesuai bagi organisasi, karena kantor hanya 1 wilayah, dan pihak manajemen hanya membutuhkan rekaman keluar dan masuknya orang saja. P: Siapa yang bertugas melakukan monitoring CCTV perusahaan? J: Yang bertugas melakukan monitoring CCTV adalah pegawai PT. Petrokimia Gresik. Bukti: (Lampiran 8 No. 28) Foto CCTV.

Tabel 4.20 Wawancara 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

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*)	
9	Ruangan pemrosesan informasi dikelola oleh organisasi.
	P: Apakah ruang pemrosesan informasi di kelola sendiri oleh organisasi? J: Ruang pemrosesan informasi di kelola sendiri oleh organisasi. P: Apakah ada peraturan bahwa ruang pemrosesan informasi harus dikelola oleh pegawai atau orang internal organisasi? J: Peraturan tentang pengelolaan ruang pemrosesan informasi terdapat pada *job description* pegawai. P: Siapa saja yang bertugas mengelola ruang pemrosesan informasi? J: Yang bertugas mengelola ruang pemrosesan informasi adalah staf TI. P: Bagaimana proses pengelolaan ruang pemrosesan informasi yang dilakukan oleh organisasi? J: Contoh proses pengelolaan ruang pemrosesan informasi yang dilakukan oleh organisasi adalah membersihkan ruangan, mengontrol suhu udara ruangan (AC), *backup* data dilakukan secara rutin 1 hari sekali.
10	Ruangan pemrosesan inforamsi harus di pisahkan dari pihak ketiga.
	P: Apakah ruang pemrosesan informasi sudah dipisahkan dari pihak ketiga (tidak ada campur tangan pihak ketiga dalam hal pengelolaan, penggunaan, dan lain-lain)? J: Campur tangan pihak ketiga terkait ruang pemrosesan informasi masih ada dalam hal pengelolaan (*maintenance*), dilakukan oleh teknisi dengan pengawasan pegawai yang bersangkutan, waktu *maintenance* sesuai dengan kebutuhan perusahaan. P: Apakah ada peraturan bahwa ruang pemrosesan informasi harus dipisahkan dari pihak ketiga? J: Tidak ada peraturan tertulis bahwa ruang pemrosesan informasi harus dipisahkan dari pihak ketiga. P: Apakah tempat ruang pemrosesan informasi sudah jauh dari jangkauan pihak ketiga? J: Tempat ruang pemrosesan informasi berada jauh dari jangkauan pihak ketiga. P: Bagaimana tindakan pencegahan akses ruang pemrosesan informasi dari pihak ketiga? J: Tindakan pencegahan yang dilakukan perusahaan untuk akses ruang pemrosesan informasi oleh pihak ketiga adalah tidak menggunakan tanda yang menarik perhatian, terdapat ruangan khusus disertai dengan pintu dan kunci

4.3.2 Hasil Pemeriksaan Data, Bukti, dan Temuan

Proses wawancara dan observasi dilakukan oleh auditor untuk mendapatkan bukti dan temuan mengenai fakta terkait permasalahan yang ada. Bukti berupa data, foto, atau dokumen. Contoh dokumen pemeriksaan pada klausul 9 (keamanan fisik dan lingkungan) dengan obyektif kontrol 9.1.1 (pembatas keamanan fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.21, dan untuk selengkapnya dapat dilihat pada Lampiran 6 Program Pemeriksaan Auditor.

Tabel 4.21 Dokumen Pemeriksaan 9.1.1 Pembatas Keamanan Fisik

<table>
<tr><td colspan="2" rowspan="5">Program Pemeriksaan

Audit Keamanan Sistem Informasi Aspek :

Klausul 9

(Keamanan Fisik dan Lingkungan)</td><td>Pemeriksa: Pak Haryanto/Pak Erwin</td></tr>
<tr><td>Auditor : I Putu Narario S</td></tr>
<tr><td>Auditee : Pak Hisyam</td></tr>
<tr><td>Tanggal: 9-11-2015</td></tr>
<tr><td>Tanda Tangan:</td></tr>
<tr><td colspan="3">Klausul 9.1 Wilayah Aman (Secure Areas)</td></tr>
<tr><td colspan="3">9.1.1 Pembatas Keamanan Fisik (Physical Security Parimeter)</td></tr>
<tr><td>No</td><td>Pemeriksaan</td><td>Catatan Auditor</td></tr>
<tr><td>1.</td><td>Identifikasi parameter keamanan yang di definisikan secara jelas untuk ruang pemrosesan informasi, dengan cara:

1. Survey.
2. Wawancara parameter keamanan untuk ruang pemrosesan informasi.</td><td>Perusahaan tidak memiliki definisi parameter keamanan untuk ruang pemrosesan informasi dengan jelas.</td></tr>
</table>

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.21 Dokumen Pemeriksaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

Program Pemeriksaan **Audit Keamanan Sistem Informasi Aspek :** **Klausul 9** **(Keamanan Fisik dan Lingkungan)**	Pemeriksa: Pak Haryanto/Pak Erwin
	Auditor : I Putu Narario S
	Auditee : Pak Hisyam
	Tanggal: 9-11-2015
	Tanda Tangan:

Klausul 9.1 Wilayah Aman (*Secure Areas*)		
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)		
No	Pemeriksaan	Catatan Auditor
2.	Cek dinding bangunan, dengan cara: 1. Survey. 2. Wawancara mengenai bahan pembuatan dinding bangunan. 3. Mendapatkan foto kantor dan gedung.	Dinding bangunan sudah di buat dari bahan konstruksi yang kuat.
3.	Identifikasi batasan akses ke ruang pemrosesan informasi, dengan cara: 1. Survey. 2. Wawancara mengenai batasan akses ke ruang pemrosesan informasi. 3. Mendapatkan foto ruang pemrosesan informasi.	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.
4.	Cek ruang penerimaan tamu, dengan cara: 1. Survey. 2. Mendapatkan foto ruang penerimaan tamu.	Perusahaan sudah memiliki 2 ruang penerimaan tamu.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.21 Dokumen Pemeriksaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

Program Pemeriksaan **Audit Keamanan Sistem Informasi Aspek :** **Klausul 9** **(Keamanan Fisik dan Lingkungan)**	Pemeriksa: Pak Haryanto/Pak Erwin
	Auditor : I Putu Narario S
	Auditee : Pak Hisyam
	Tanggal: 9-11-2015
	Tanda Tangan:

Klausul 9.1 Wilayah Aman (*Secure Areas*)

9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)

No	Pemeriksaan	Catatan Auditor
5.	Identifikasi batasan akses ke tempat kerja, dengan cara: 1. Survey. 2. Mendapatkan foto ruang resepsionis. 3. Wawancara mengenai batasan akses ke tempat kerja.	Perusahaan tidak memiliki peraturan atau teknologi mengenai batasan akses ke tempat kerja, namun sudah di kontrol oleh petugas resepsionis dan seluruh karyawan.
6.	Cek pintu darurat, dengan cara: 1. Survey. 2. Wawancara kegunaan pintu darurat. 3. Mendapatkan foto pintu darurat.	Perusahaan memiliki pintu darurat di belakang kantor, di gunakan untuk keadaan darurat seperti kebakaran. Kontrol pintu darurat tidak dilakukan secara rutin.
7.	Identifikasi pintu darurat disertai dengan kode darurat, dengan cara: 1. Survey. 2. Wawancara kegunaan kode darurat. 3. Mendapatkan foto pintu darurat dan kode darurat.	Pintu darurat perusahaan sudah di sertai dengan kode darurat (alaram kebakaran). Alaram kebakaran akan menyala apabila terjadi kebakaran di wilayah kantor.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.21 Dokumen Pemeriksaan 9.1.1 Pembatas Keamanan Fisik (Lanjutan)

Program Pemeriksaan **Audit Keamanan Sistem Informasi Aspek :** **Klausul 9** **(Keamanan Fisik dan Lingkungan)**	Pemeriksa: Pak Haryanto/Pak Erwin
	Auditor : I Putu Narario S
	Auditee : Pak Hisyam
	Tanggal: 9-11-2015
	Tanda Tangan:

Klausul 9.1 Wilayah Aman (*Secure Areas*)

9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)

No	Pemeriksaan	Catatan Auditor
8.	Identifikasi CCTV untuk memantau lingkungan kerja, dengan cara: 1. Survey. 2. Wawancara mengenai CCTV. 3. Mendapatkan foto CCTV.	Perusahaan memiliki CCTV, tetapi CCTV hanya ada di depan pintu masuk kantor, dan yang memonitoring CCTV bukan pegawai PT. GCS, melainkan pegawai PT. Petrokimia Gresik.
9.	Identifikasi proses pengelolaan ruang pemrosesan informasi, dengan cara: 1. Survey. 2. Wawancara mengenai proses pengelolaan ruang pemrosesan informasi.	Ruang pemrosesan informasi perusahaan tidak di kelola sendiri, melainkan masih ada campur tangan dari konsultan.
10.	Identifikasi penempatan ruang pemrosesan informasi yang terpisah dari pihak ketiga, dengan cara: 1. Survey. 2. Wawancara mengenai penempatan ruang pemrosesan informasi.	Ruang pemrosesan informasi sudah terpisah dari jangkauan pihak ketiga karena berada di belakang kantor, tetapi pihak ketiga (teknisi) masih dapat menjangkau apabila ada kerusakan dengan pengawasan pegawai.

4.3.3 Hasil Uji Kematangan

Uji kematangan yang dilakukan oleh auditor mengacu pada *Capability Maturity Model for Integration* (CMMI) to ISO 27002 untuk mengidentifikasi tingkat kematangan penerapan pengamanan, dapat dilihat pada Tabel 4.22. Berdasarkan hasil wawancara dan analisa dari pengumpulan bukti dengan *auditee*, maka diperoleh tingkat kematangan untuk masing-masing kontrol, dapat dilihat Tabel 4.23. Hasil perhitungan tingkat kematangan pada klausul 9 dapat dilihat pada Tabel 4.24, dan Gambar representasi nilai tingkat kematangan dapat dilihat pada Gambar 4.8.

Tabel 4.22 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)

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.23 Tingkat Kematangan 9.1.1 Pembatas Keamanan Fisik

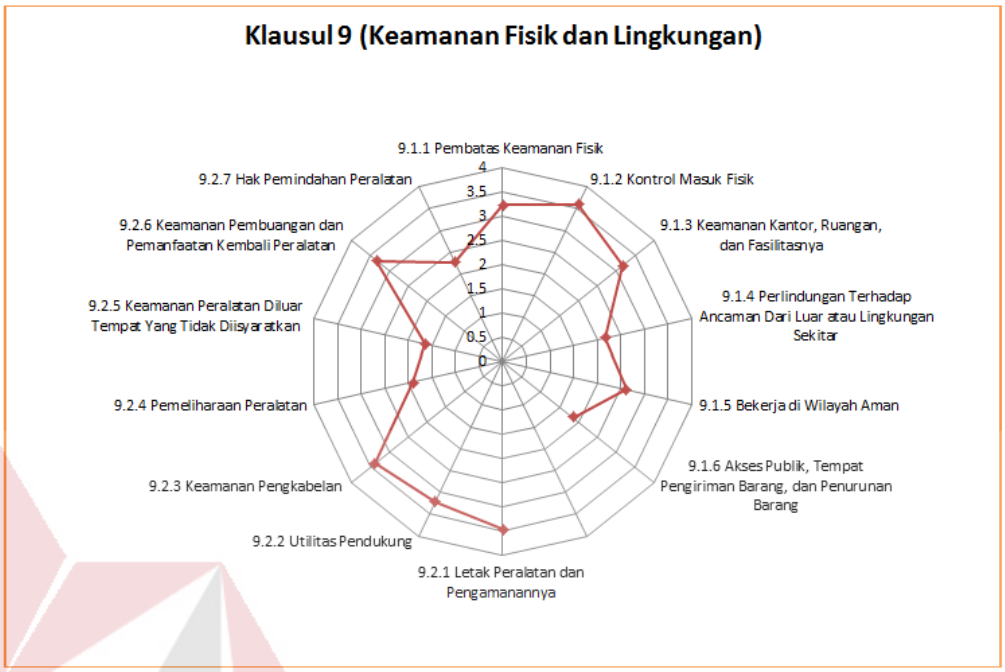
Klausul 9 (Keamanan Fisik dan Lingkungan)									
Klausul 9.1 Wilayah Aman (*Secure Areas*)									
9.1.1 Pembatas Keamanan Fisik (*Physical Security Parimeter*)									Nilai
No	Pernyataan	Bobot	0	1	2	3	4	5	
1.	Mempunyai parameter keamanan yang harus didefinisikan secara jelas (dinding, kartu akses, 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

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

Tabel 4.24 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

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA



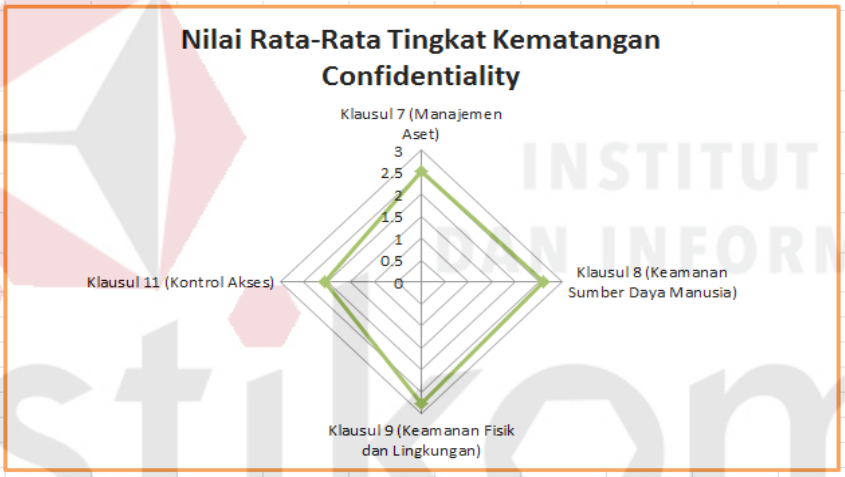
Gambar 4.8 Representasi Nilai Tingkat Kematangan Klausul 9

a. Hasil Tingkat Kematangan Klausul 9

Hasil dari proses perhitungan tingkat kematangan klausul 9 (keamanan fisik dan lingkungan) adalah 2.76 *managed*. Hasil tersebut menunjukkan bahwa keamanan fisik dan lingkungan sistem akuntansi *enterprise* PT. Gresik Cipta Sejahtera masih dalam tahap pengembangan dengan dokumentasi yang terbatas seperti kurangnya pendokumentasian prosedur, kebijakan, peraturan, dan sanksi yang diberikan untuk setiap pelanggaran yang dilakukan oleh pegawai berkaitan dengan keamanan sistem akuntansi *enterprise*. Hasil perhitungan tingkat kematangan *confidentiality* dapat dilihat pada Tabel 4.25, dan hasil representasi tingkat kematangan *confidentiality* dapat dilihat pada Gambar 4.9. Untuk lebih lengkapnya dapat dilihat pada Lampiran 7 uji kematangan.

Tabel 4.25 Hasil Perhitungan Tingkat Kematangan *Confidentiality*

Klausul	Deskripsi	Tingkat Kematangan
7	Manajemen Aset	2.52
8	Keamanan Sumber Daya Manusia	2.61
9	Keamanan Fisik dan Lingkungan	2.76
11	Kontrol Akses	2.05
Nilai Rata-Rata Tingkat Kematangan *Confidentiality*		**2.53**



Gambar 4.9 Representasi Tingkat Kematangan *Confidentiality*

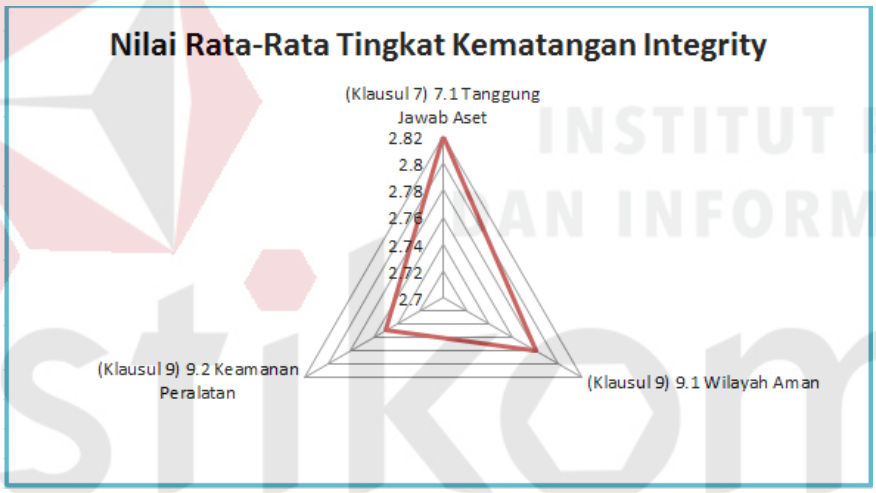
b. Hasil Tingkat Kematangan *Confidentiality*

Hasil dari proses perhitungan tingkat kematangan aspek keamanan *confidentiality* adalah 2.53 *managed*. Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan sistem akuntansi *enterprise* PT. Gresik Cipta Sejahtera sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Untuk lebih lengkapnya dapat dilihat pada Lampiran 7 uji kematangan. Pada Tabel 4.26

merupakan hasil perhitungan tingkat kematangan aspek keamanan *integrity*, hasil representasi tingkat kematangan *integrity* dapat dilihat pada Gambar 4.10.

Tabel 4.26 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* dan *Availability*)		2.78



Gambar 4.10 Representasi Tingkat Kematangan *Integrity*

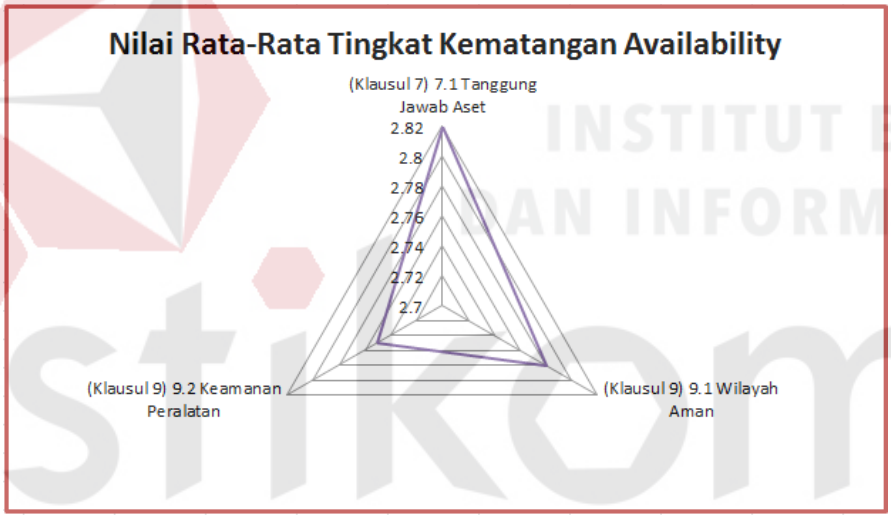
c. Hasil Tingkat Kematangan *Integrity*

Hasil dari proses perhitungan tingkat kematangan aspek keamanan *Integrity* adalah 2.78 *managed*. Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan sistem akuntansi *enterprise* PT. Gresik Cipta Sejahtera masih sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Untuk lebih lengkapnya dapat dilihat pada Lampiran 7 uji kematangan. Pada Tabel 4.27

merupakan hasil perhitungan tingkat kematangan aspek keamanan *availability*, hasil representasi tingkat kematangan *availability* dapat dilihat pada Gambar 4.11.

Tabel 4.27 Hasil Perhitungan Tingkat Kematangan *Availability*

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 (*Availability*)		2.78



Gambar 4.11 Representasi Tingkat Kematangan *Availability*

d. Hasil Tingkat Kematangan *Availability*

Hasil dari proses perhitungan tingkat kematangan aspek keamanan *Integrity* adalah 2.78 *managed*. Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan sistem akuntansi *enterprise* PT. Gresik Cipta Sejahtera masih sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Untuk lebih lengkapnya dapat dilihat pada Lampiran 7 uji kematangan.

4.3.4 Hasil 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. Contoh temuan dan rekomendasi pada klausul 9 (keamanan fisik dan lingkungan) dengan obyektif kontrol 9.1.1 (pembatas keamanan fisik (*physical security parimeter*)) dapat dilihat pada Tabel 4.28, dan untuk selengkapnya dapat dilihat pada Lampiran 8 Temuan dan Rekomendasi. Bukti foto dari rekomendasi 9.1.1 dengan pernyataan nomor 3 dapat dilihat pada Gambar 4.12 ruang pemrosesan informasi, dan untuk lebih lengkapnya dapat dilihat pada Lampiran 9 Bukti Foto.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

Tabel 4.28 Temuan dan Rekomendasi 9.1.1 Pembatas Keamanan Fisik

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.	Nilai Bobot: 1 Nilai Kematangan: 1 ***Confidentiality*:** 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: - 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. Pihak manajemen dapat mendefinisikan parameter keamanan untuk ruang pemrosesan informasi. b. Pihak manajemen harus membuat batasan akses menuju ruang pemrosesan informasi seperti (dinding pembatas, kunci ruangan atau kartu akses menuju ruang pemrosesan informasi, penempatan personil TI disekitar ruangan *server*). Hal ini untuk menghindari akses ilegal. c. Memisahkan ruang pemrosesan informasi dengan ruang foto *copy*, agar tidak semua pegawai dapat mengakses ruang *server* kecuali pegawai TI yang memiliki hak akses.

Gambar 4.12 Ruang Pemrosesan Informasi

4.4 Hasil Pelaporan Audit Keamanan Sistem Akuntansi *Enterprise*

Pada tahapan ini auditor memberikan laporan audit (*audit report*) sebagai pertanggung jawaban atas proses audit keamanan sistem akuntansi *enterprise* yang telah dilaksanakan. Laporan audit ditunjukkan kepada pihak yang berhak saja, karena laporan audit merupakan dokumen yang bersifat rahasia. Keluaran dari tahapan ini adalah Surat Pernyataan Pelaporan Audit dan *Exit Meeting* dapat dilihat pada Lampiran 10 Pelaporan Audit Keamanan SAE.

BAB V

PENUTUP

5.1 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.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

5.2 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.

INSTITUT BISNIS DAN INFORMATIKA stikom SURABAYA

DAFTAR PUSTAKA

Adisaputro, G. dan Asri, M. (2003). *Anggaran Perusahaan*. Buku 1. Penerbit BPFE Yogyakarta.

Ahmad, Amar. 2012. *Bakuan Audit Keamanan Informasi Kemenpora*. Republik Indonesia: Kementrian Pemuda dan Olahraga.

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.

Canon, D. (2011). *CISA (Certified Information System Auditor) Study Guide* (Vol. 3rd edition). Indriana Polis: Wiley Publising.

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

Direktorat Keamanan Informasi. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta: Kementrian Keamanan Informasi dan Informatika RI.

Ermana, Fine. 2011. *Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM : STIKOM Surabaya*. Laporan Tugas Akhir STIKOM Surabaya.

Halim, M. 2012. *Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 Pada PT. Aneka Jaya Baut Sejahtera (PT. AJBS).* Laporan Tugas Akhir: STIKOM Surabaya.

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.* Switzerland.

Jogiyanto, H, M. 2005. *Analisa dan Desain Sistem Informasi*. Yogyakarta: Andi Offset.

Krismiaji. 2005. *Sistem Informasi Akuntansi*. Yogyakarta: Unit Penerbit dan Percetakan Akademi Manajemen Perusahaan YKPN.

Munawir, S. 2007. *Analisa Laporan Keuangan*. Liberty, Yogyakarta.

Ningtyas, Hastin Istiqomah. 2012. *Audit Keamanan Sistem Informasi Manajemen Aset Berdasarkan Standar ISO 27002 (Studi Kasus PT. Varia Usaha Beton)*. STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.

Permata, Dian Ayu. 2015. *Audit Keamanan Sistem Informasi Pada Bagian Dekstop Management Berdasarkan Standar ISO 27002:2005 Di PT. Telkom Divre V Jatim.* STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.

Sarno, Riyanarto. 2009. *Audit Sitem & Teknologi Informasi*. Surabaya: ITS Press.

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

Siregar, Doli. 2004. *Manajemen Aset*. PT. Gramedia Pustaka Utama, Jakarta.

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.

Windriya, D. R. 2015. *Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Manajemen Rsud Bangil Berdasarkan ISO 27002*. STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.

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.

stikom SURABAYA