AUDIT SISTEM INFORMASI *CALL CENTER* PADA PT ARGA BANGUN BANGSA (ESQ LEAERSHIP CENTER) DENGAN MENGGUNAKAN *FRAMEWORK* COBIT

Siti Syaroh[a], Ditdit N Utama[b] dan Ellensyah Kurniawan[c]

[a]*Mahasiswa Fakultas Sains dan Teknologi*
Universitas Islam Negeri Syarif Hidayatullah Jakarta

[b]*Staff Pengajar Fakultas Sains dan Teknologi*
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Tel : (021) 7493606 Fax : (021) 7493315

[c]*Staff Pengajar Fakultas Sains dan Teknologi*
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Tel : (021) 7493606 Fax : (021) 7493315

ABSTRAK

Call center ESQ merupakan aplikasi berbasis web yang digunakan oleh tim telemarketing, tim telecorporate, finance, dan BM (Branch Manager) untuk menjalankan fungsi bisnis ESQ LC. Data sudah menjadi aset penting dalam perusahaan untuk mengantisipasi hal-hal yang tidak diinginkan berkaitan dengan penyalahgunaan data maka harus dilakukan audit. Pentingnya informasi, maka kebijakan tentang keamanan sistem merupakan salah satu aspek yang sangat penting dalam sebuah sistem informasi. Audit Sistem Informasi menjadi sebuah solusi untuk mengukur sejauh mana selama ini sistem call center melakukan proses DS5 dan DS11 agar ESQ LC dapat melakukan perbaikan-perbaikan. IT (Information Technology) Governance merupakan struktur hubungan dan proses untuk mengarahkan dan mengendalikan organisasi untuk mencapai tujuannya dengan menambahkan nilai ketika menyeimbangkan risiko dibandingkan dengan TI dan prosesnya. Kerangka kerja COBIT (Control Objective For Information and Related Technology) versi 4.1, dimana COBIT mempunyai tujuan untuk mengendalikan TI terkait dan merupakan suatu standar yang telah diakui cukup baik pada tingkat internasional. Dalam penelitian ini membahas 1 domain yaitu Deliver and Support dari 4 domain yang ada di COBIT dengan pembahasan dibatasi pada tingkat control process pengelolaan data (DS11) dan memastikan keamanan sistem (DS5) untuk management awareness dan maturity level. Hasil dari audit sistem informasi adalah tingkat kinerja proses DS5 (memastikan keamananan sistem) dan DS11 (pengelolaan data) adalah sedang. Maturiy Level DS5 dan DS11 saat ini (as is) ada pada level 3 kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari tapi kurang ada pengawasan untuk menjalankan itu semua. Dan (to be) yang diharapkan menunjukkan level 4 perusahaan memiliki indikator sebagai sasaran terhadap kinerja proses TI serta terdapat fasilitas untuk memonitor dan mengukur prosedur yang sudah berjalan. Rekomendasi ke level 4 IT Governance ini dibuat guna meningkatkan kinerja call center di ESQ LC. Usulan Performance Indicator dan Outcome Measure diharapkan dapat diterapkan agar proses TI tercapai sesuai dengan tujuan yang diharapkan dalam DS5 dan DS11.

Kata Kunci: Audit, *call center*, *IT Governance*, *Activities* dan IT Goals, COBIT.

1. PENDAHULUAN

Perkembangan teknologi yang semakin cepat telah membawa dunia memasuki era baru khususnya dibidang informasi dan bahkan lebih cepat dari yang pernah dibayangkan sebelumnya. Sistem Informasi merupakan aset bagi suatu perusahaan yang bila diterapkan dengan baik akan memberikan kelebihan untuk berkompetensi sekaligus meningkatkan kemungkinan bagi kesuksesan suatu usaha (Maniah dan Kridanto 2005).

PT. Arga Bangun Bangsa (ESQ LC) saat ini merupakan salah satu lembaga pelatihan sumber daya manusia terbesar di Indonesia. Dalam sebulan terselenggara rata-rata 100 even *training* di dalam maupun luar negeri, dan menghasilkan alumni sekitar 10.000-15.000 per bulan. Dalam hal sumber daya manusia, ESQ LC kini didukung lebih dari 500 orang karyawan.

Call center yang baik adalah *call center* yang mudah dihubungi, cepat, akurat, profesioanal dan mampu menangani pelanggan dengan baik. Data yang besar dibutuhkan pengelolaan yang baik agar mendapatkan output yang diharapkan. Memastikan keamanan sistem sangat penting untuk mengetahui kemungkinan penyalahgunaan aktivitas terkait dengan TI yang kritis di perusahaan. Untuk mengantisipasi dampak yang mungkin terjadi karena sistem tidak dapat diandalkan maka harus dilakukan audit terhadap sistem *call center*. Hasilnya dapat digunakan sebagai dasar untuk melakukan langkah-langkah luas untuk memecahkan masalah yang mungkin terjadi dimasa yang akan datang.

1.1 Rumusan Masalah

Berdasarkan latar belakang maka pokok masalah yang akan diteliti adalah:

1. Bagaimana cara melakukan audit sistem informasi untuk mengetahui tingkst kinerja *ensure system security* dan *manage data*?
2. Bagaimana caranya mengetahui maturity level untuk kondisi sistem call center saat ini (*as is*) dan kondisi yang diinginkan (*to be*) untuk proses *manage data* dan *ensure system security*?
3. Bagaimana caranya menentukan rekomendasi terhadap hasil audit yang telah dilakukan?

1.2 Batasan Masalah

Penelitian ini dibatasi pada audit sistem informasi hanya pada domain *deliver and support* untuk fokus are *manage data* (DS11) dan *ensure system security* (DS5) Sistem Informasi *Call Center* serta pembuatan rekomendasi untuk meningkatkan kinerja agar lebih baik dari sebelumnya menggunakan *framework Control Objective Framework Cobit* 4.1

1.3 Tujuan Penelitian

Didalam penelitian ini terdapat dua jenis tujuan, yaitu tujuan umum dan tujuan khusus. Tujuan umum penelitian ini adalah untuk menghasilkan audit terhadap penggunaan sistem informasi *call center* untuk *ensure system security* dan manage data pada PT. Arga Bangun Bangsa (*ESQ Leadership Center*). Sedangkan tujuan khusus dari penelitian ini adalah untuk menghasilkan:

1. Analisis audit sistem *call center* untuk *manage awareness*, *maturity level* proses teknologi informasi pada *manage data* dan *ensure security system call center.*
2. Pembuatan rekomendasi untuk mencapai *level* yang lebih baik dari hasil yang telah di audit.

1.4 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan dapat memberi manfaaat di antaranya:

1. Memberikan pengetahuan proses audit sistem informasi di bidang *call center.*
2. Memberikan pengetahuan tentang tentang menghitung nilai kinerja dan *maturity level* proses sebuah sistem.
3. Memberikan pengetahuan tahap-tahap melakukan audit sebuah sistem informasi.

2. LANDASAN TEORI

2.1 Pengertian Sistem Informasi

Menurut pendapat Jogiyanto (2001) bahwa sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan.

2.2 Pengertian Audit Sistem Informasi

Audit SI memberikan evaluasi yang bersifat independen atas kebijakan, prosedur, standar, pengukuran, dan praktik untuk menjaga/mencegah informasi yang bersifat elektronik dari kehilangan, kerusakan, penelusuran yang tidak disengaja dan sebagainya (NSAA & GAO, 2011). Audit SI secara umum mencakup hal-hal sebagai berikut: meninjau lingkungan dan fisik, administrasi sistem, software aplikasi, keamanan jaringan, kontinuitas bisnis, dan integritas data (Gondodiyoto & Hendarti, 2006).

2.2.1 Tujuan Audit SI

Tujuan audit sistem informasi untuk meninjau dan memberikan umpan balik, menjamin dan melakukan rekomendasi mengenai tiga hal sebagai berikut ketersediaan (*availability*), kerahasiaan (*Confidentiality*) dan integritas.

Detail tentang tujuan audit sistem informasi dijelaskan (Gondodiyoto & Hendarti, 2006) sebagai berikut:

1. Untuk mengidentifikasi sistem yang ada baik yang ada pada tiap divisi/unit/departemen maupun yang digunakan menyeluruh.
2. Untuk dapat lebih memahami seberapa besar sistem informasi mendukung kebutuhan strategis perusahaan, operasi perusahaan, mendukung kegiatan operasional departemen/unit/divisi, kelompok kerja maupun para petugas dalam melaksanakan kegiatannya.
3. Untuk mengetahui pada bidang atau area mana, fungsi, kegiatan atau *business process* yang didukung dengan sistem serta teknologi informasi yang ada.
4. Untuk menganalisis tingkat pentingnya data/informasi yang dihasilkan oleh sistem dalam rangka mendukung kebutuhan para pemakainya.
5. Untuk mengetahui keterkaitan antara sistem pengolahan dan transfer informasi.
6. Untuk mengidentifikasi apakan ada kesenjangan antara sistem dan kebutuhan.
7. Untuk membuat peta dari alur informasi yang ada.

2.3 Tata Kelola Teknologi Informasi

Menurut Surendro (2009) Tata kelola teknologi informasi adalah tanggungjawab Direksi dan Manajer eksekutif organisasi. Tata kelola teknologi informasi merupakan bagian terintegrasi dari pengelolaan perusahaan yang mencakup kepemimpinan, struktur data serta proses organisasi yang memastikan bahwa teknologi informasi perusahaan dapat dipergunakan untuk memepertahankan dan memperluas strategi dan tujuan organisasi.

a. Seluruh tujuan entitas telah ditentukan,
b. Metode untuk mencapai tujuan tersebut telah ditetapkan, dan
c. Tata cara pengawasan kinerja telah dijelaskan.

Inti dari tanggung jawab pengelolaan dalam menentukan strategi, menangani masalah, memberikan nilai dan mengukur kinerja adalah nilai *stakeholde*r, yang menentukan strategi perusahaan dan teknologi informasi. Berjalannya bisnis yang ada dan pengembangannya menjadi model-model bisnis baru tentu saja merupakan harapan pada stakeholder dan dapat dicapai dengan hanya dengan terbentuknya infrasrtuktur teknologi informasi perusahaan yang baik.

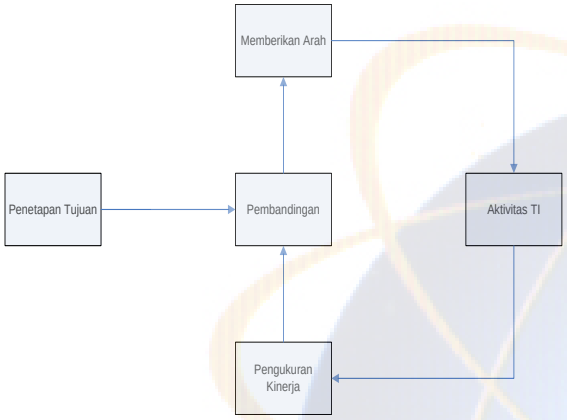
Tata kelola teknologi informasi adalah tanggung jawab dewan direksi dan eksekutif. Tata kelola teknologi informasi bukan suatu disiplin ilmu atau aktifitas yang terbatas, tapi lebih merupakan sebuah pengelolaan yang terintegrasi dengan pengelolaan perusahaan. Tata kelola teknologi informasi mencakup kepemimpinan dan struktur serta proses organisasi yang memastikan teknologi informasi berjalan dan memperluas strategi dan tujuan organisasi. Hal penting yang berpengaruh atas keberhasilan struktur dan proses tersebut adalah komunikasi yang efektif di antara semua pihak yang berdasar kepada hubungan yang konstruktif, pemahaman yang sama dan komitmen yang sama dalam segala hal.

Kegunaan tata kelola teknologi informasi adalah untuk mengatur penggunaan teknologi informasi, serta untuk memastikan kinerja teknologi informasi sesuai dengan tujuan berikut:

1. Keselarasan teknologi informasi dengan perusahaan dan realisasi keuntungan-keuntungan yang dijanjikan dari penerapan teknologi informasi.
2. Penggunaan teknologi informasi agar memungkinkan perusahaaan mengeksploitasi kesempatan yang ada, memaksimalkan apa yang sudah dimiliki saat ini dan memaksimalkan keuntungan.
3. Penanganan manajemen risiko yang terkait teknologi informasi secara tepat.

Tata kelola teknologi informasi seringkali berjalan dalam lapisan yang berbeda-beda antara lain *team-leader* memberikan laporan kepada eksekutif, dan eksekutif kepada direksi.

Laporan yang menandakan perbedaan tujuan akan selalu berisi rekomendasi untuk suatu tindakan yang harus dikuatkan oleh lapisan pengelola. Jelas sekali, pendekatan ini tidak akan efektif kecuali strategi dan tujuan pertama-tama harus sudah diturunkan dalam organisasi. Ilustrasi dalam gambar 2.1 memperlihatkan secara konseptual interaksi antara tujuan dan aktifitas teknologi informasi dan dapat diaplikasikan dalam lapisan yang berbeda-beda dalam perusahaan.



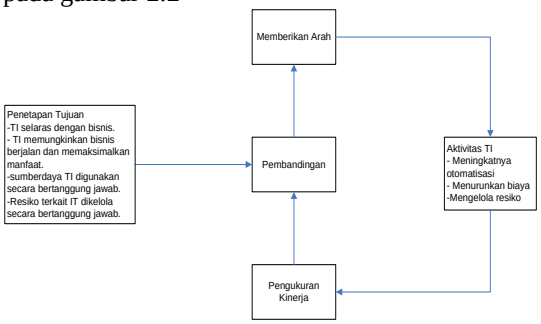
Gambar 2.1 Interaksi antara tujuan dan aktifitas teknologi informasi (ITTI, 2009)

Proses pengelolaan dimulai dengan menentukan tujuan dari teknologi informasi perusahaan, memberikan arahan awal. Setelah itu, suatu putaran/loop yang berkelanjutan dilakukan untuk mengukur kinerja, membandingkan tujuan dan akhirnya mengarahkan kembali aktifitas yang seharusnya dilakukan dan perubahan dari tujuan apabila diperlukan. Selama tujuannya adalah sebagian besar adalah tanggung jawab dewan direksi dan pengukuran kinerja manajemen. Ada suatu hal yang harus selalu dikembangkan sehingga tujuan-tujuan tersebut merupakan hal yang dapat dicapai dan pengukuran mempresentasikan tujuan secara tepat.

Dalam menanggapi arahan yang diterima, fungsi teknologi informasi harus fokus dalam:

1. Memberikan keuntungan dengan menambah otomatisasi dan membuat perusahaan menjadi lebih efektif, mengurangi biaya dan membuat keseluruhan perusahaan lebih efisien.
2. Menangani risiko (keamanan, kelayakan dan kesesuaian).

Dengan demikian kerangka kerja teknologi informasi dapat diselesaikan seperti yang terlihat pada gambar 2.2



Gambar 2.2 Kerangka Kerja Tata Kelola Teknologi Informasi (ITGI, 2003)

2.4 COBIT *Framework*

COBIT merupakan sekumpulan dokumentasi dan panduan yang mengarahkan pada *IT governance* yang membantu auditor, manajemen, dan pengguna (*user*) untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis. COBIT dikembangkan oleh *IT Governance Institute* (*ITGI*) yang merupakan bagian dari *Information Systems Audit and Control Association* (*ISACA*).

Adapun kerangka kerja COBIT secara keseluruhan terdiri atas arahan seperti:

a. *Control objectives*: terdiri atas 4 tujuan pengendalian tingkat tinggi yang tercermin dalam 4 domain Yang dapat dilihat pada gambar 2.3. Tiap-tiap kontrol mendukung standar informasi, yaitu standar kualitas (efektif dan efisien), standar keamanan (*confidentiality*, integritas, dan ketersediaan (*availability*)), dan *fiduciary requirement* (kepatuhan dan reliabilitas)
b. *Audit guidelines*: berisi 318 tujuan pengendalian bersifat rinci.
c. *Management guidelines*: berisi arahan, baik secara umum dan spesifik mengenai hal-hal yang menyangkut kebutuhan manajemen.

Dalam penulisan skripsi ini ada ada 2 kontrol utama yang menjadi fokus untuk melakukan audit sistem informasi yaitu DS5 dan DS11.

Penjelasan tiap-tiap kontrol sebagai berikut:

a. *DS5 Ensure System Security* (memastikan keamanan sistem)

Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI memerlukan proses manajemen keamanan. Proses ini meliputi penyusunan dan memelihara peranan-peranan keamanan (*security roles*) serta tanggung jawab, kebijakan, standar dan prosedur. Manajemen keamanan juga mencakup pengawasan keamanan dan ujicoba secara periodik, serta mengimplementasikan aksi perbaikan untuk kelemahan kekurangan atau insiden/bencana. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis terhadap kelemahan keamanan dan insiden.

DCO dapat dipandang sebagai suatu kontrol efektif untuk dapat mencapai tujuan, yang didefinisikan dalam COBIT 4.1. Adapun keberadaan (tingkat pemenuhannya) berkaitan langsung dengan upaya pengendalian terhadap kelemahan/kerentanan yang dapat memicu timbulnya ancaman yang berdampak serius pada pencapaian tujuan bisnis.

DS5 terdiri dari:

1. DS5.1 : Manajemen Keamanan TI (*Management of IT Security*)

Manajemen keamanan TI pada level organisasi yang tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis. Menerjemahkan bisnis, risiko dan kepatuhan (*compliance*) ke dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan.

2. DS5.2: Rencana Keamanan TI (*IT Security Plan*)
   Memastikan rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, *software* dan *hardware.* Mengkomunikasikan kebijakan dan prosedur keamanan kepada *stakeholder* dan *user*.
3. DS5.3 : Manajemen Identitas (*Identity Management*)
   Memastikan semua user (internal, eksternal dan temporer) dan aktivitas mereka dalam sistem TI (bisnis, aplikasi, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) secara unik teridentifikasi. Memudahkan user mengidentifikasi melalui mekanisme otentikasi. Mengkonfirmasi bahwa hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, dan kebutuhan kerja yang melekat pada identitas pengguna. Memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan. Memelihara identitas pengguna dan hak akses dalam repositori pusat. Melakukan langkah-langkah teknis yang menghemat biaya, mengukur prosedural dan menjaganya agar terus *update* dalam membuat identifikasi user, implementasi otentikasi dan memaksakan hak akses.
4. DS5.4: Manajemen Akun Pengguna (*User Account Management*)
   Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodifikasian dan penutupan akun pengguna serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna. Termasuk prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal dan eksternal, untuk normal dan kasus darurat. Hak dan kewajiban relatif terhadap akses ke sistem oraganisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis pengguna. Selanjutnya, melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung.
5. DS5.5: Uji Coba Keamanan, Penjagaan dan Pemantauan (*Security Testing, Surveillance and monitoring*)
   Menguji, menjaga dan memantau implementasi keamanan TI dalam langkah yang proaktif. Keamanan TI seharusnya ditinjau secara periodik untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara. *Logging* dan fungsi pemantauan keamanan TI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.
6. DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*)
   Mendefinisikan secara jelas dan mengkomuniksasikan karakteristik dari insiden keamanan yang potential sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah.
7. DS5.7: Proteksi Teknologi Keamanan (*Protection of Security Technology*)
   Membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.
8. DS5.8: Manajemen Kunci Kriptografi (*Cryptographic Key Management*)
   Menentukan bahwa kebijakan dan prosedur sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, *entry*, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.
9. DS5.9: Pencegahan *Software* Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)
   Memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama *patch* keamanan yang *up-to-date* dan pengendalian virus) diseluruh organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (seperti *virus*, *worm*, s*pyware* dan *spam*).
10. DS5.10 Keamanan Jaringan (*Network Security*)
    Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaring an, intruksi deteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.

11. DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*)
    Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan *non-repudiation*.

b. DS11 *Manage Data* (mengelola data)

Manajemen data yang efektif memerlukan identifikasi persyaratan data. proses pengolahan data juga mencakup pembentukan prosedur yang efektif untuk mengelola media libaray, backup dan pemulihan data, sertamedia pembuangan yang tepat. Pengelolaan data yang efektif membantu memastikan kualitas, ketepatan waktu dan ketersediaan data bisnis.

DS11 terdiri dari:

1. DS11.1: Persyaratan Bisnis untuk Manajemen Data (*Business Requirements for Data Management*)
   Melakukan verifikasi bahwa semua data yang diharapkan untuk pengolahan diterima dan diproses secara lengkap, akurat, tepat waktu serta seluruh output yang dikirim sesuai dengan kebutuhan bisnis, mendukung *restart* dan pengolahan kebutuhan.
2. DS11.2: Penyimpanan dan Pengaturan Retensi (*Storage and Retention Arrangements*)
   Menetapkan dan menerapkan prosedur untuk penyimpanan data secara efektif dan efisien, retensi serta pengarsipan untuk memenuhi tujuan bisnis, kebijakan keamanan organisai dan persyaratan peraturan.
3. DS11.3: Sistem Manajemen *Media Library (Media Libray Management system)*
   Menetapkan dan menerapkan prosedur untuk menjaga inventarisasi media penyimpanan dan pengarsipan kegunaan (*usability*) dan integritas.
4. DS11.4: Pembuangan (*Disposal*)
   Menetapkan dan menerapkan prosedur untuk memastikan bahwa persayaratan bisnis untuk perlindungan data sesnsitif dan software terpenuhi ketika data dan perangkat keras dibuang atau dialihkan.
5. DS11.5: *Backup* dan Pemulihan Sistem (*Backup and Restoration*)
   Menetapkan dan menerapkan prosedur untuk backup dan pemulihan sistem, aplikasi, data dan dokumentasi sesuai dengan kebutuhan bisnis dan rencana kesinambungan.
1. DS11.6: Persyaratan Keamanan untuk Manajemen Data (*Security Requirements for Data Management*)
   Menetapkan dan mengimplementasikan kebijakan dan prosedur untuk mengidentifikasi dan menerapkan persyaratan keamanan yang berlaku untuk penerimaan, pengolahan, penyimpanan dan output data untuk memenuhi tujuan bisnis, kebijakan keamanan organisasi dan peraturan.

2.5 *Call Center* ESQ

Call center merupakan aplikasi berbasis *web based* yang di gunakan oleh tim telemarketing, tim telecorporate, *finance*, dan BM.

1. Tim telemarketing menggunakan *call center* utuk *call* dan registrasi *customer* yang akan mengikuti training.
2. Tim telecorporate menggunakan *call center* untuk *registrasi customer* yang akan mengikuti *training*.
3. *Finance* untuk memvalidasi pembayaran *training*.
4. BM (*Branch Manager*) untuk monitoring jumlah peserta yg mengikuti *training* dan jumlah *call/day* yang di *call* oleh tim *telemarketing*.

Keuntungan menggunakan sistem *call center* diantaranya:

a. Bersifat *web based* seluruh kantor cabang dapat terintegrasi dalam hal melihat jumlah peserta *training.*
b. Data tersimpan lebih baik di server *call center* terhubung dengan media EMS (*Event Management System*).

3. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini di antaranya:

1. Metode Pengumpulan Data yang terdiri dari:

a. Studi Literatur Sejenis
   Mendapatkan gambaran yang menyeluruh tentang apa yang sudah dikerjakan orang lain dan bagaimana orang mengerjakannya, kemudian seberapa berbeda penelitian yang akan kita lakukan (Jogiyanto 2008).
b. Metode observasi
   Melalui pengamatan secara langsung atau observasi yang dilakukan di perusahaan guna mendapatkan data yang di maksud (Jogiyanto 2008).
c. Metode Wawancara
   Wawancara memungkinkan untuk mendapatkan data secara lebih mendalam karena bertatapan langsung dengan narasumber (Jogiyanto 2008).

2. Metode Audit SI

a. COBIT *Framework*

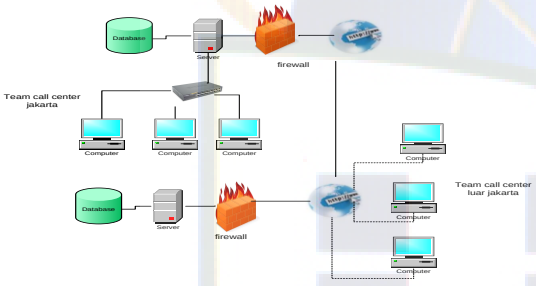
COBIT adalah *framework* yang dapat digunakan sebagai alat yang komprehensif untuk menciptakan dan mengefektifkan implementasi *IT Governance* pada suatu perusahaan (ITGI 2007).

b. Metode Kuisioner

Kumpulan pertanyaan dan pernyataan untuk responden dalam rangka pengumpulan data agar sesuai dengan tujuan penelitian (Surendro 2009).

4. ANALISIS DAN HASIL AUDIT

4.1. Arsitektur *Call Center*

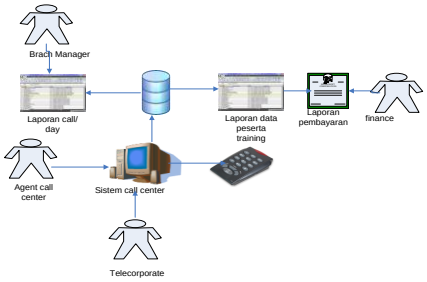


Gambar 4.1 Arsitektur *call center*

Call center merupakan aplikasi berbasis web yang di gunakan oleh tim telemarketing, tim telecorporate, finance, dan BM (*Branch Manager*) untuk menjalankan fungsi bisnis sesuai dengan tanggung jawabnya. 9 orang jumlah BM (*Branch Manager*). Jumlah telecorporate dan telemarketing ada 150 orang baik yang dipusat ataupun di cabang. Ada 12 *agent call center* yang melakukan *call/day*.

Ada 2 server yang digunakan untuk mengolah data lokal (jakarta) dan cabang (daerah). Server untuk mengolah data lokal terdapat di ESQ LC pondok pinang sedangkan server untuk menangani data daerah terdapat di gedung cyber yang terletak di Jl. Kuningan Barat No. 8 Jakarta Selatan. Jaringan yang digunakan adalah *Firstmedia*. Untuk kontrol akses keamanannya menggunakan *firewall*.

4.2 Proses Bisnis *Call center*



Gambar 4.2 Proses Bisnis *Call center*

Proses bisnis *call center* dimulai ketika agent *call center* melakukan *call* berdasarkan data pribadi, data alumni peserta *training*, data referensi dari alumni. *Telemarketing* sama dengan *agent call center* menggunakan *call center* untuk *call* dan registrasi peserta yang akan mengikuti *training*. *Telecorporate* menggunakan sistem *call center* untuk registrasi peserta *training*. *Finance* untuk memvalidasi pembayaran *training* dan BM (*Branch Manager*) untuk monitoring banyaknya peserta yang mengikuti *training* dan banyaknya jumlah *call/day* yang di *call* oleh tim *telemarketing*.

4.3 Analisis Audit

4.3.1 Analisis Identifikasi Responden

Dengan analisis identifikasi responden yang mengacu pada diagram RACI tersebut, maka sampling atau identifikasi responden diarahkan pada peran-peran yang terkait langsung dan representatif pada proses DS5 dan DS11. Sehingga diharapkan jawaban atas kuesioner mempunyai validitas yang memadai dan diharapkan dapat mewakili keadaan sesungguhnya dilapangan. Adapun jumlah responden yang teridentifikasi dalam pengisian kuesioner ini adalah sebanyak 10 responden untuk DS5 dan 6 responden untuk DS 11 seperti dirinci pada tabel 4.1 dan tabel 4.2.

Tabel 4.1 Identifikasi RACI Chart DS5

No	Fungsional struktur COBIT terkait		Fungsional struktur PT. ABB (ESQ LC)		Jumlah
1	Chief Exekutif Officer	CEO	President Director	TI	1
2	Chief Financial Officer	CFO	Finance and Administration Director	Non TI	1
3	Business Excecutive	BE	Business Unit Director	TI	1
4	Chief Information Officer	CIO	Business Unit Director	Non TI	1
5	Business Process Owner	BPO	Costomer Development Director	Non TI	1
6	Head Operation	HO	Information and Communication Dept Head	TI	1
			ICT Developer and Programer	TI	2
7	Chief architect	CA	Information and Communicatio	TI	1

			n Dept Head		
8	Head Development	HD	ICT Developer and Programer	TI	2
			Costumer Development Director	Non TI	1
9	Head IT administration	HITA	Information and Communication Dept Head	TI	1
10	Program Management Office	PMO	Head of President Director Office	Non TI	1
11	Compliance, Audit, Risk and security	CARS	Auditor Internal	Non TI	1

Tabel 4.2 Identifikasi RACI Chart DS11

No	**Fungsional struktur COBIT terkait**		**Fungsional struktur PT. ABB (ESQ LC)**		**Jumlah**
1	Chief Information Officer	CIO	Business Unit Director	TI	1
2	Business Process Owner	BPO	Costomer Development Director	Non TI	1
3	Chief architect	CA	Information and Communication Dept Head	TI	1
4	Head Operation	HO	Information and Communication Dept Head	TI	1
			ICT Developer and Programer	TI	1
5	Head Development	HD	ICT Developer and Programer	TI	2
			Costumer Developme nt Director	Non TI	1
6	Head IT administration	HIT A	Information and Communication Dept Head	TI	1
			ICT Developer and Programer	TI	2
7	Compliance, Audit, Risk and security	CARS	Auditor Internal	Non TI	1

4.3.2 Analisis Identifikasi Risiko

Tabel 4.3 Rekapitulasi jawaban responden kuesioner I *Management Awareness*

No	**Objek Pertanyaan**	**Distribusi Jawaban**		
		L (%)	**M (%)**	**H (%)**
1	Manajemen keamanan TI	0,00	61,54	38,46
2	Rencana Keamanan IT	0,00	69,23	30,77
3	Komunikasi kebijakan keamanan beserta investasi yang tepat (layanan, personel, *software* dan *hardware*)	7,70	69,23	23,08
4	Konfirmasi hak akses pengguna	7,70	61,54	30,77
5	Manajemen identitas	7,70	38,46	53,85
6	Manajemen akun pengguna	7,70	46,15	46,15
7	Pengujian keamananan, Pengawasan dan Pemantauan	15,38	30,77	53,85
8	Kebutuhan keamanan manajemen data	7,70	61,54	30,77
9	Perlindungan teknologi keamanan	15,38	61,54	23,08
10	Manajemen kunci *kryptografi*	0,00	61,54	38,46

11	*Software* untuk mendeteksi, koreksi program yang berbahaya	0,00	53,85	46,15
12	Keamanan jaringan	0,00	53,85	46,15
13	Pertukaran data sensitif	0,00	53,85	46,15
	Total	**5,77**	**55,77**	**38,46**

Secara umum rekapitulasi hasil kuesioner I *management awareness untuk* DS5 dapat ditarik suatu kecenderungan yang merefleksikan fakta di lapangan yaitu:

1. Sebagian besar responden, **55,77%** responden menyatakan pendapat, opini atau kesadarannya bahwa tingkat kinerja dalam memastikan keamanan sistem adalah **cukup** atau **sedang**.
2. Sebanyak **38,46%** responden mengemukakan pendapatnya bahwa kinerja dalam memastikan keamanan sistem adalah **baik**.
3. Hanya 5,77% responden yang menyatakan bahwa praktik dalam memastikan keamanan sistem **lemah**.

Tabel 4.4 Rekapitulasi jawaban responden kuesioner I *Management Awareness*

No	Objek Pertanyaan	Distribusi Jawaban		
		L (%)	M (%)	H (%)
1	Kebutuhan bisnis untuk manajemen data		25,00	75,00
2	Pengaturan penyimpanan		33,33	66,67
3	*Media library*		50,00	50,00
4	Penghapusan data/disposal		16,67	83,33
5	*Backup* dan *restore*		50,00	50,00
6	Kebutuhan keamanan manajemen data		41,67	58,33
7	Pengujian terhadap media *backup*	33,33	50,00	16,67
8	Kecepatan proses restorasi		50,00	50,00
9	Keberhasilan proses restorasi		83,33	16,67
10	Keamanan data sensitif setelah *disposal*	8,33	41,67	50,00
11	Penanganan insiden kapasitas penyimpanan		58,33	41,67
12	Keandalan sistem karena proses pemulihan		91,67	8,33
13	Kepuasan pengguna atas ketersediaan data		50,00	50,00
14	Kepatuhan pada aspek hukum/aturan	8,33	66,67	25,00
	Total	**3,57**	**50,60**	**45,83**

Tabel 4.5 Tingkat kinerja *detailed control objectives* (DCO) pada proses DS5

No	*Detailed Control Objectives*	Nilai Kinerja
1	Manajemen keamanan TI (DS5.1)	2,38
2	Rencana Keamanan IT (DS5.2)	2,31
3	Manajemen identitas (DS5.3)	2,62
4	Manajemen akun pengguna (DS5.4)	2,85
5	Pengujian keamananan, Pengawasan dan Pemantauan (DS5.5)	2,38
6	Kebutuhan keamanan manajemen data (DS5.6)	2,23
7	Perlindungan teknologi keamanan (DS5.7)	2,18
8	Manajemen kunci kryptografi (DS5.8)	2,38
9	*Software* untuk mendeteksi, koreksi program yang berbahaya (DS5.9)	2,46
10	Keamanan jaringan (DS5.10)	2,46
11	Pertukaran data sensitif (DS5.11)	2,46
	Rata-rata	**2,43**

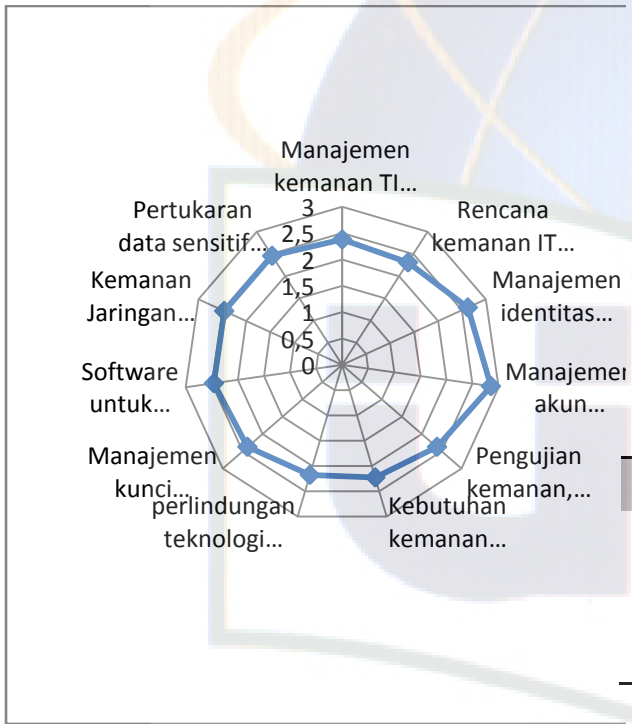
Tingkat pemenuhan DCO pada proses memastikan keamanan sistem mendekati tinggi dengan rata-rata nilai kinerja dalam proses pengelolaan data adalah sebesar 2,43 seperti dipresentasikan dalam diagram radar pada gambar 4.3 dan pemenuhan DCO pada proses DS11 secara kuantitatif yang dapat dilihat pada tabel 4.6.

Tabel 4.6 Tingkat kinerja *detailed control objectives* (DCO) pada proses DS11.

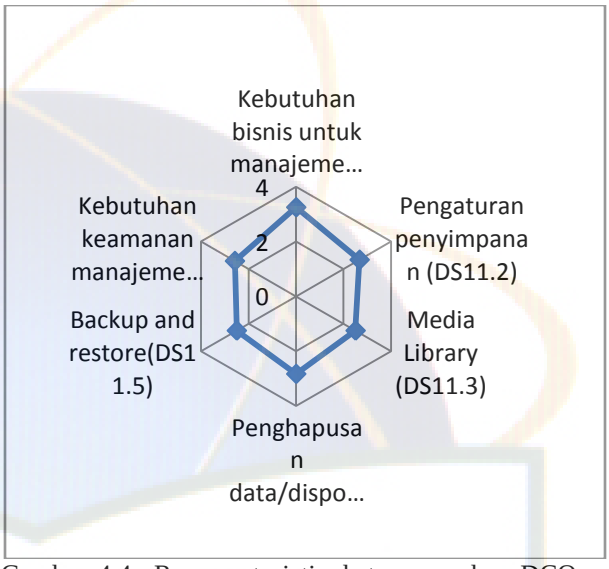
No	*Detailed Control Objectives*	Nilai Kinerja
1	Kebutuhan bisnis untuk manajemen data (DS11.1)	2,75
2	Pengaturan penyimpanan (DS11.2)	2,67
3	Media *Library* (DS11.3)	2,5
4	Penghapusan data/disposal (DS11.4)	2,83
5	*Backup* dan *Restore* (DS11.5)	2,5
6	Kebutuhan keamanan manajemen data (DS11.6)	2,58
	Rata-rata	**2,72**

Secara keseluruhan berdasarkan tabel 4.4 dapat ditarik suatu kesimpulan bahwa:

Tingkat pemenuhan DCO pada proses pengelolaan data cukup dan mendekati tinggi dengan rata-rata nilai kinerja dalam proses pengelolaan data adalah sebesar 2,72 seperti dipresentasikan dalam diagram radar pada gambar 4.3.



Gambar 4.3 Representasi tingkat pemenuhan DCO pada proses memastikan keamanan sistem



Gambar 4.4 Representasi tingkat pemenuhan DCO pada proses pengelolaan data

Tabel 4.7 Nilai dan tingkat kematangan proses DS5 kuesioner II *maturity level*

No	Atribut	Nilai Kematangan		Tingkat Kematangan	
		As is	*To be*	*As is*	*To be*
1	**AC**	3,05	3,23	3	3
2	**PSP**	3,15	4,00	3	4
3	**TA**	3,15	4,00	3	4
4	**SE**	3,37	3,62	3	4
5	**RA**	3,15	3,92	3	4
6	**GSM**	3,15	3,92	3	4
Rata-rata		3,17	3,77	3	4

Secara umum interpretasi terhadap hasil kuesioner adalah cukup atau sedang dalam proses pengelolaan data. Namun harus ditingkatkan lagi agar tidak menjadi suatu kerentanan (*vulnerability*) bagi munculnya ancaman (*threat*) yang sangat memungkinkan (*probability*) akan berdampak (*impact*) serius pada pencapaian kinerja bisnis perusahaan.

Beberapa ancaman (*threat*) yang mengancam keberadaan data sebagai aset perusahaan. Ancaman terhadap keberadaan data harus diwaspadai karena akan berdampak pada gangguan operasional maupun bisnis. Dampak yang ditimbulkan akibat bencana memerlukan waktu, tenaga dan biaya pemulihannya.

Nilai kematangan terhadap atribut kematangan pada tabel 4.12 dapat diperoleh informasi bahwa:

1. Tingkat kematangan yang diharapkan saat ini (*as is*) pada proses DS5 secara keseluruhan berada pada tingkat 3 terdefinisi atau *defined*.
2. Tingkat kematangan yang diharapkan (*to be*) pada proses DS 5 secara keseluruhan pada tingkat 4 terkelola atau *managed.*

Tabel 4.8 Nilai dan tingkat kematangan proses DS11 kuesioner II *maturity level*

No	Atribut	Nilai Kematangan		Tingkat Kematangan	
		As is	*To be*	*As is*	*To be*
1	**AC**	3,00	3,92	3	4
2	**PSP**	2,77	3,85	3	4
3	**TA**	3,15	4,00	3	4
4	**SE**	3,15	4,00	3	4
5	**RA**	3,10	4,00	3	4
6	**GSM**	3,00	3,92	3	4
Rata-rata		3,03	3,95	3	4

Nilai kematangan pengelolaan data terhadap atribut kematangan pada tabel, maka dapat diperoleh informasi bahwa:

1. Tingkat kematangan saat ini (*as is*), pada proses DS11 secara keseluruhan berada pada tingkat 3 atau terdefinisi proses pengelolaan datanya.
2. Tingkat kematangan yang diharapkan (*to be*), pada proses DS11, secara keseluruhan berada pada tingkat 4 atau terkelola/*managed.*

5. PENUTUP

5.1 Simpulan

Setelah melakukan audit sistem informasi *call center* maka dapat disimpulkan bahwa:

1. Hasil dari *Management Awareness* menunjukkan tingkat kinerja proses DS5 (memastikan keamananan sistem) dan DS11 (pengelolaan data) adalah sedang.
2. *Maturiy Level* DS5 dan DS11 saat ini (*as is*) ada pada level 3 yang artinya kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari namun namun kurang ada pengawasan untuk menjalankan prosedur sehingga memungkinkan terjadinya penyimpangan dan (*to be*) yang diharapkan menunjukkan level 4.
3. Rekomendasi berupa hal apa saja agar mampu meningkatkan nilai *maturity level* menjadi 4 untuk proses pengelolaan data dan memastikan keamanan sistem.
4. Rekomendasi berupa *performance indicators* dan *outcome measures* beserta targetnya agar proses pengelolaan data dan memastikan keamanan sistem sesuai dengan tujuan yang diinginkan oleh perusahaan.
5. Penerapan tekonologi informasi dengan menggunakan COBIT *Framework* dapat memberikan manfaat dalam arsitektur bisnis, arsitektur informasi, arsitektur teknologi dan arsitektur solusi sebagai pedoman untuk pengembangan sistem *call center* pada ESQ LC.

5.2 Saran

Adapun saran-saran bagi peneliti selanjutnya yang dapat dilakukan adalah:

1. Memberikan pemetaan secara menyeluruh terkait pengelolaan TI pada domain Deliver & Support tidak hanya untuk fokus area DS5 (memastikan keamanan sistem) da DS11 (pengelolaan data). Artinya, semua sasaran yang tidak terpenuhi dapat ditelusuri secara detil dan segera ditemukan penyebabnya untuk selanjutnya diputuskan apakah segera diperbaiki atau tidak.
2. Untuk peneliti selanjutnya sebaiknya dilakukan audit untuk semua domain dan semua fokus area agar diketahui proses IT yang dilakukan selama ini sudah mendukung tujuan perusahaan atau belum.
3. Menciptakan *tools* audit sendiri untuk mempermudah dalam melakukan audit sistem informasi.

6. Daftar Pustaka

Jogiyanto. 2008. Metodologi Penelitian Sistem Informasi. Yogyakarta: Penerbit ANDI.

[ITGI] Information Technologi Governance Institute 2007. COBIT 4.1 Edition: Audit Guidelines, IT Governance Institute. Illinois: ITGI.

Maniah & Surendro Kridanto. 2005. Usulan model audit sistem informasi studi kasus sistem informasi perawatan pesawat terbang.(SNATI 2005) Seminar Nasional Aplikasi Teknologi Informasi 2005. yogyakarta, 18 Juni 2005.

SURENDRO, K. (2009) Implementasi Tata Kelola Teknologi Informasi.

SKRIPSI

AUDIT SISTEM INFORMASI *CALL CENTER* PADA PT ARGA BANGUN BANGSA(ESQ LEADERSHIP CENTER) DENGAN MENGGUNAKAN FRAMEWORK COBIT

Dibuat Untuk Memenuhi Syarat
Dalam Menyelesaikan Studi Akhir
Program Strata Satu Program Studi Sistem Informasi
Universitas Islam Negeri Syarif Hidayatullah Jakarta

Disusun Oleh:

SITI SYAROH
NIM: 107093002922

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH

JAKARTA

2011 M/1432 H

PERNYATAAN

DENGAN INI SAYA MENYATAKAN BAHWA SKRIPSI INI BENAR-BENAR HASIL KARYA SAYA SENDIRI YANG BELUM PERNAH DIAJUKAN SEBAGI SKRIPSI ATAU KARYA ILMIAH PADA PERGURUAN TINGGI ATAUPUN LEMBAGA MANAPUN.

Jakarta, 1 Juli 2011

Siti Syaroh
107093002922

ABSTRAK

SITI SYAROH, Audit Sistem Informasi *Call Center* pada PT. Arga Bangun Bangsa (*ESQ Leadership Center)* dengan Menggunakan *Framework* COBIT di bawah bimbingan **DITDIT N UTAMA** dan **ELLENSYAH KURNIAWAN.**

Call center ESQ merupakan aplikasi berbasis web yang digunakan oleh tim telemarketing, tim telecorporate, *finance*, dan BM (*Branch Manager*) untuk menjalankan fungsi bisnis ESQ LC. Data sudah menjadi aset penting dalam perusahaan untuk mengantisipasi hal-hal yang tidak diinginkan berkaitan dengan penyalahgunaan data maka harus dilakukan audit. Pentingnya informasi, maka kebijakan tentang keamanan sistem merupakan salah satu aspek yang sangat penting dalam sebuah sistem informasi. Audit Sistem Informasi menjadi sebuah solusi untuk mengukur sejauh mana selama ini sistem *call center* melakukan proses DS5 dan DS11 agar ESQ LC dapat melakukan perbaikan-perbaikan. *IT (Information Technology) Governance* merupakan struktur hubungan dan proses untuk mengarahkan dan mengendalikan organisasi untuk mencapai tujuannya dengan menambahkan nilai ketika menyeimbangkan risiko dibandingkan dengan TI dan prosesnya. Kerangka kerja COBIT (*Control Objective For Information and Related Technology*) versi 4.1, dimana COBIT mempunyai tujuan untuk mengendalikan TI terkait dan merupakan suatu standar yang telah diakui cukup baik pada tingkat internasional. Dalam penelitian ini membahas 1 domain yaitu *Deliver and Support* dari 4 domain yang ada di COBIT dengan pembahasan dibatasi pada tingkat *control process* pengelolaan data (DS11) dan memastikan keamanan sistem (DS5) untuk *management awareness* dan *maturity level*. Hasil dari audit sistem informasi adalah tingkat kinerja proses DS5 (memastikan keamananan sistem) dan DS11 (pengelolaan data) adalah sedang. *Maturiy Level* DS5 dan DS11 saat ini (*as is*) ada pada *level* 3 kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari tapi kurang ada pengawasan untuk menjalankan itu semua. Dan (*to be*) yang diharapkan menunjukkan *level* 4 perusahaan memiliki indikator sebagai sasaran terhadap kinerja proses TI serta terdapat fasilitas untuk memonitor dan mengukur prosedur yang sudah berjalan. Rekomendasi ke level 4 *IT Governance* ini dibuat guna meningkatkan kinerja *call center* di ESQ LC. Usulan *Performance Indicator* dan *Outcome Measure* diharapkan dapat diterapkan agar proses TI tercapai sesuai dengan tujuan yang diharapkan dalam DS5 dan DS11.

Kata Kunci: Audit, *call center*, *IT Governance*, *Activities* dan IT Goals, COBIT.

V bab + xiii halaman + 108 halaman + 20 tabel + 21 gambar + 5 Lampiran
Pustaka Acuan (56, 2000 : 2010).

KATA PENGANTAR

Bismillaahirrohmaanir Rohiim

Puji dan syukur kehadirat Allah SWT, Tuhan Yang Maha Esa yang telah memberikan rahmat serta hidayah-Nya, sehingga penyusunan laporan skripsi ini dapat diselesaikan dengan baik. Shalawat serta salam semoga selalu tercurahkan kepada suri tauladan kita Rasulullah Muhammad SAW.

Penyusunan skripsi ini adalah salah satu syarat untuk memenuhi kelulusan pada Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta Program Reguler Program Studi Sistem Informasi. Dengan judul skripsi ini adalah " Audit Sistem Informasi *Call Center* pada PT. Arga Bangun Bangsa (*ESQ Leadership Center)* dengan Menggunakan *Framework* COBIT ".

Dalam penyusunan skripsi ini, telah banyak bimbingan dan bantuan yang didapatkan baik dari segi moral maupun segi material dari berbagai pihak. Oleh karena itu, pada kesempatan ini mengucapkan terima kasih kepada :

1. Bapak Dr. Ir. Syopiansyah Jaya Putra, M.Sis, selaku Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta.
2. Ibu Nur Aeni Hidayah, MMSI, selaku Ketua Program Studi Sistem Informasi Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta.
3. Bapak Ditdit N Utama, MMSI, M.Com, selaku Dosen Pembimbing I yang telah banyak membantu dalam penyelesaian skripsi.

4. Bapak Ellensyah Kurniawan, MTI, selaku Dosen Pembimbing II yang telah banyak membantu dalam penyelesaian skripsi.
5. Bapak Bayu Kelana, selaku ICT Head ESQ Leadership Center.
6. Bapak, mamah dan adikku tercinta terimakasih atas dukungannya baik moral maupun materil .
7. Surya Surahman, terima kasih atas pengertiannya selama ini.
8. Abangku terimakasih udah mau nganter-nganter nyari alamat.
9. Dosen-dosen walaupun bukan pembimbing secara langsung, terimakasih ilmu dan kesabarannya.
10. Sahabat-sahabat Mayang, Deti, Bernes, Erfat yang telah berpetualang denganku mengarungi indahnya dunia ini.
11. Sahabat-sahabat SIK Community, SIC 2007 kebersamaan dengan kalian adalah anugerah terindah dalam hidupku.

Penulis menyadari skripsi ini masih banyak kekurangan, oleh karena itu penulis mengharapkan kritik dan sarannya. Silahkan email ke sitisyaroh.si2007@gmail .com jika ada kritik dan saran yang ingin disampaikan. Akhir kata, dengan segala kerendahan hati penulis mengucapkan terima kasih yang tak terhingga kepada semua pihak yang telah membantu penyelesaian skripsi ini. Penulis juga berharap semoga skripsi ini bermanfaat bagi pembaca umumnya dan bagi penulis khususnya.

Wassalammualaikum Warohmatullaahi Wabarokatuh

Jakarta, 1 Juli 2011

Siti Syaroh
107093002922

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin cepat telah membawa dunia memasuki era baru khususnya dibidang informasi dan bahkan lebih cepat dari yang pernah dibayangkan sebelumnya. Sistem Informasi merupakan aset bagi suatu perusahaan yang bila diterapkan dengan baik akan memberikan kelebihan untuk berkompetensi sekaligus meningkatkan kemungkinan bagi kesuksesan suatu usaha (Maniah dan Kridanto 2005). Peranan sistem informasi pada setiap perusahaan berbeda-beda. Ada yang menjadikan sistem informasi hanya sebagai alat bantu untuk pencapaian tujuan organisasi, adapula perusahaan yang menjadikan sistem informasi sebagai sesuatu yang berfungsi secara strategis.

Untuk mengetahui apakah kinerja sistem informasi sesuai dengan perencanaan dan tujuan usaha yang dimilikinya maka harus dilakukan pengukuran. Hasil dari pengukuran digunakan oleh manajemen untuk melakukan perbaikan terhadap kinerja SI. Audit sistem informasi merupakan wujud dari pengukuran itu.

Penelitian di bidang Audit Sistem Informasi telah banyak dilakukan di antaranya oleh: Buddelmeijer *et al.* (2006) meneliti sistem audit privasi untuk *database* XML dan XPath *query* bahasa yang menggunakan konsep sebuah *query* audit untuk menggambarkan informasi rahasia. Radovonic *et al*. (2010) dengan judul *"IT audit in accordance with* COBIT *standard "* penelitian ini menggunakan *Framework* COBIT yang memberikan pedoman tentang apa yang dapat dilakukan

dalam suatu organisasi dalam hal kegiatan pengendalian, pengukuran dan dokumentasi proses dan operasi.

Cao and Yang (2010) meneliti integritas data pada perlindungan sistem informasi berdasarkan algoritma MD5. (Beidjilali, 2009) meneliti permasalahan yang berkaitan dengan teknologi informasi dan komunikasi dengan menggunakan analisis manajemen resiko, hasil dari penelitian itu adalah metode dan standar keamanan informasi yang digunakan di Eropa dan Amerika utara.

Penelitian lainnya dilakukan oleh Cao *et al.* (2009) tentang teori audit keamanan dan teknologi multi-agen agar dapat memenuhi persyaratan dari ISA. Chen *et al.* (2005) melakukan penelitian audit di bidang kesehatan untuk menilai kepatuhan terhadap kebijakan sebuah domain yang aman, mendeteksi contoh perilaku yang tidak patuh, dan untuk memfasilitasi deteksi penciptaan yang tidak tepat, akses, modifikasi dan penghapusan *Protected Health Information* (PHI).

Fe *et al*. (2007) melakukan audit sistem informasi *hot spot* di bidang keamananan jaringan, aplikasi pengenalan pola dan penggalian data. Hasil dari penelitian membuktikan promosi ketepatan kategorisasi teks. Geisler *et al*. (2003) menilai integritas informasi pada organisasi dalam bisnis, pemerintahan dan masyarakat yang bersangkutan.

Ada pula penelitian yang lain Guo *et al*. (2010) melakukan analisis komprehensif terhadap keamanan LAN berbasis Sistem Informasi Manajemen Pendidikan. Huang *et al.* (2000) menjelaskan bahwa penerapan teknologi informasi untuk pelatihan inspeksi, pengujian kontrol kualitas, audit dan control dll, dalam rangka meningkatkan proses pemeriksaan cacat dan meningkatkan hasil

fab. Sistem ini membantu TSMC untuk meningkatkan pengetahuan dan keterampilan instruktur dan insinyur.

Pada bidang keamanan sistem informasi Jang *et al*. (2009) menghasilkan sistem audit Usulan yang dapat membangun lingkungan komputasi aman di mana-mana. Huang *et al.* (2010) membahas pemodelan mekanisme transaksi dan pemulihan transaksi di *Next Generation Trading System* dari *Shanghai Stock Exchange.*

Penelitian lainnya dilakukan oleh Huang *et al.* (2009) melakukan penelitian untuk *Database Embedded* Aktif Berdasarkan Peraturan ECA dan Implementasi di *database SQLite* berdasarkan analisis teori basis data aktif. Ji (2009) memberikan analisis rinci tentang hubungan konduksi risiko proyek, pemasok jasa dan risiko *outsourcing*, risiko aplikasi dan risiko infrastruktur, risiko strategis sistem informasi, dan interaksi di antara berbagai risiko pada perusahaan manufaktur.

Kepatuhan terhadap hukum perlindungan data Johnson and Grandison (2007) membahas HDB sistem audit efisien melacak semua mengakses database dan memungkinkan auditor untuk merumuskan pertanyaan yang tepat audit untuk memonitor kepatuhan terhadap kebijakan privasi dan keamanan. Kurada (2010) Mengembangkan model keuangan praktis untuk mendefinisikan Teknologi Informasi dari pusat biaya menggunakan kerangka valIT dalam ISACA.

Li *et al.* (2010) memperkenalkan prosedur yang tersimpan, memicu untuk merancang suatu sistem *log* untuk menyimpan dan mengelola data spasial tiga dimensi. Li and Wang (2009) membangun aplikasi Ontologi Informasi

manajemen aset dengan menggunakan metodologi SWRL. Metodologi ini dapat membantu auditor untuk mengetahui status aset informasi baik setiap saat.

Liu *et al.*(2008) meneliti masalah kebocoran informasi didasarkan pada *isolasi-crypt* dan *log-audit* dengan metode ini mencegah informasi yang sensitif dari perusahaan yang bocor, sengaja atau tidak sengaja. Studi kasus Lo and Marchand (2004) meneliti audit sistem informasi meliputi masalah-masalah manajerial sensitif.

Penelitian audit sistem informasi lainnya pada bidang jaringan oleh Mahnic *et al.* (2001) manajemen router dengan metode COBIT. Mascher (2009) melakukan audit setelah pemilu untuk memeriksa pemilih interaksi informasi tambahan harus dikumpulkan untuk memungkinkan penyelidikan masalah faktor manusia sistem suara yang digunakan dalam pemilihan umum, sementara pada saat yang sama menjaga privasi pemilih.

Pada bidang perbankan Mielke *et al.* (2001) meneliti tentang pemantauan Kapasitor Bank menggunakan metode prototype dalam sistem pengembangannya dengan menggabungkan teknologi *surveilans* aplikasi-spesifik dan *off-the-rak* untuk pemantauan jarak jauh. Mrazik and Kollar (2008) meneliti perencanaan Sistem Informasi, kelanjutan audit. Dan perubahan aplikasi untuk memastikan aset terutama mengamankan sistem informasi dari penggunaan yang tidak sah yang sama untuk proses sistem informasi dengan data yang benar dengan ketersediaan tinggi tanpa kehilangan data.

Nianzu and Xiaoling (2009) Audit SI dilakukan untuk memprediksi penipuan data dari aplikasi yang berbeda lokasi. Auditor menggunakan *AFG*

untuk membantu pekerjaannya. Peto (2006) meneliti indeks komperhenship untuk penilaian resiko informasi dalam Audit Teknologi Informasi menggunakan metode COBIT.

Ramanathan *et al.* (2007) menjelaskan teknologi layanan audit yang termasuk dalam beberapa produk IBM untuk meningkatkan kemampuan pemeriksaan dan menjelaskan bagaimana hal ini jasa audit dapat digunakan untuk mendukung strategi kepatuhan perusahaan. Biffl *et al.* (2007) memperkenalkan pendekatan *Model Driven Architecture* (MDA) untuk membangun sistem yang menggambarkan secara eksplisit persyaratan mutu *stakeholder* pada *link* data yang dapat diandalkan antara sistem pendukung keputusan dan membuat versi sistem baru yang menerapkan persyaratan tersebut.

Zhang *et al.* (2009) meneliti strategi pencegahan kehilangan data kemudian menghasilkan sebuah usulan menggunakan enkripsi. Nicho and Cusack (2007) Meneliti tentang tata kelola teknologi informasi untuk mengukur kinerja atau efektivitas sistem informasi menggunakan metode COBIT dengan menerapkan model GQM. Tang and Xing. (2008) membangun teknik data mining berbasis *web* diterapkan untuk pengambilan keputusan perencanaan sumber daya hutan. Solusi ini menyediakan pengguna dengan modul otomatisasi kantor, modul pendukung keputusan, modul audit internal dan modul sistem integrator.

Zhao *et al.* (2007) meneliti sistem operasi yang aman dengan melakukan audit sistem informasi untuk memantau sistem, menerapkan kebijakan keamanan, dan membangun sistem deteksi gangguan. Xianlin and Genbao (2009) audit

kualitas digital berbasis *web* untuk manajemen mutu dan sistem jaminan dengan menggunakan model berpikir terintegrasi.

Zhang (2009) penelitian ini berorientasi pada permasalahan yang berhubungan informasi akuntansi di perusahaan Cina dan meminjam ide dari tata kelola teknologi informasi untuk menganalisis model ISCA. Penelitian ini membedakan antara pihak yang bertanggung jawab untuk audit sistem informasi dan menetapkan fokus kerja masing-masing. Masucci and Stinson (2001) meneliti penentuan biaya iklan untuk *server web* menggunakan skema matering.

Bottcher and Steinmetz (2006) meneliti sistem audit privasi untuk *database XML* dan XPath query bahasa yang menggunakan konsep sebuah *query* audit untuk menggambarkan informasi rahasia. Tadaaki (2008) meneliti tentang *software* yang dikembangkan oleh *NPA (National Police Agency)* untuk Tindakan terhadap kebocoran informasi dengan cara memanfaatkan enkripsi otomatis dan perangkat lunak kontrol akses.

Gotterbarn (2002) meneliti isu-isu profesional modul manajemen proyek, The *software development impact statement* (SoDIS) memfasilitasi proses identifikasi awal jenis tambahan risiko proyek dan membantu melakukan pertimbangan profesional pada tahap awal pengembangan perangkat lunak dan manajemen. Lee *et al*. (2008) melakukan penelitian pada masalah keamanan seperti arus keluar informasi pribadi, *hacking*, difusi virus. Kemudian mengusulkan sistem audit berbasis aturan yang menganalisis struktur kode target untuk memecahkan masalah, mendefinisikan sebagai aturan, mendeteksi kode berbahaya dan kerentanan perangkat lunak.

Li *et al*. (2003) melakukan analisis yang mendalam mengenai serangan dan pola penyalahgunaan dalam *file log*, kemudian mengajukan pendekatan menggunakan mesin dukungan vektor untuk deteksi anomali. Pendekatan satu-kelas berdasarkan SVM, dilatih dengan audit pengguna data log dari tahun 1999 DARPA. Mei and Huan (2008) Pemahaman dan evaluasi atas risiko kesalahan signifikan BPA audit dalam lingkungan pemrosesan informasi menggunakan SER untuk mengendalikan risiko audit CPA dan memperkenalkan metode kuantitatif untuk membantu auditor untuk menilai secara objektif.

Wang and Tsai (2009) melakukan perbandingan serta integrasi sistem pengendalian internal dari kedua ISO 9001 Manajemen Mutu dan ISO 27001 Manajemen Keamanan Informasi. Dengan cara mengeksplorasi kesamaan dari kedua sistem manajemen dan dilanjutkan untuk diintegrasikan ke dalam model manajemen yang efektif dengan mengadopsi metode hipotesis penelitian eksploratif. Soudain (2009) merancang sistem organisasi untuk mengurangi resiko yang didukung biaya keamanan, meningkatkan keamanan dan kepastian tingkat sistem dengan menggunakan FSDFD.

PT. Arga Bangun Bangsa (ESQ LC) saat ini merupakan salah satu lembaga pelatihan sumber daya manusia terbesar di Indonesia. Dalam sebulan terselenggara rata-rata 100 even *training* di dalam maupun luar negeri, dan menghasilkan alumni sekitar 10.000-15.000 per bulan. Dalam hal sumber daya manusia, ESQ LC kini didukung lebih dari 500 orang karyawan.

Jika awalnya ESQ LC hanya fokus pada pelaksanaan *training*, saat ini telah dibentuk divisi-divisi seperti: penerbitan, multimedia, retail, hingga ke *tours*

& *travel* untuk menunjang kegiatan ESQ LC. Selain itu, didirikan Forum Komunikasi Alumni (FKA) yang bertujuan untuk membina hubungan dan membangun sinergi di antara para alumni ESQ.

Call center yang baik adalah *call center* yang mudah dihubungi, cepat, akurat, profesioanal dan mampu menangani pelanggan dengan baik. Data yang besar dibutuhkan pengelolaan yang baik agar mendapatkan output yang diharapkan. Memastikan keamanan sistem sangat penting untuk mengetahui kemungkinan penyalahgunaan aktivitas terkait dengan TI yang kritis di perusahaan. Untuk mengantisipasi dampak yang mungkin terjadi karena sistem tidak dapat diandalkan maka harus dilakukan audit terhadap sistem *call center*. Hasilnya dapat digunakan sebagai dasar untuk melakukan langkah-langkah luas untuk memecahkan masalah yang mungkin terjadi dimasa yang akan datang.

COBIT adalah *framework* yang dapat digunakan sebagai alat yang komprehensif untuk menciptakan dan mengefektifkan implementasi *IT Governance* pada suatu perusahaan. Audit sistem informasi dapat dilakukan perusahaan untuk mengevaluasi/audit sistem yang telah ada jika terdapat kekurangan/kesalahan terhadap sistem yang ada. Dan COBIT *framework* digunakan untuk menyusun dan menerapkan model audit sistem informasi dengan tujuan memberikan masukan dan rekomendasi bagi perusahaan untuk perbaikan pengelolaan sistem informasi di masa mendatang (ITGI, 2007). Berdasarkan latar belakang di atas, skripsi dengan judul **"Audit Sistem Informasi *Call Center* pada PT. Arga Bangun Bangsa (*ESQ Leadership Center)***

dengan Menggunakan *Framework* COBIT " layak untuk dikembangkan**.**

1.2 Rumusan Masalah

Berdasarkan latar belakang maka pokok masalah yang akan diteliti adalah:

1. Bagaimana cara melakukan audit sistem informasi untuk mengetahui tingkat kinerja *ensure system security* dan *manage data*?
2. Bagaimana caranya mengetahui maturity level untuk kondisi sistem call center saat ini (*as is*) dan kondisi yang diinginkan (*to be*) untuk proses *manage data* dan *ensure system security*?
3. Bagaimana caranya menentukan rekomendasi terhadap hasil audit yang telah dilakukan?

1.3 Batasan Masalah

Penelitian ini dibatasi pada audit sistem informasi hanya pada domain *deliver and support* untuk fokus are *manage data* (DS11) dan *ensure system security* (DS5) Sistem Informasi *Call Center* serta pembuatan rekomendasi untuk meningkatkan kinerja agar lebih baik dari sebelumnya menggunakan *framework Control Objective Framework Cobit* 4.1. Pada penelitian ini tidak membahas domain plan and organize, acquired and implement dan monitor and evaluate.

1.4 Tujuan Penelitian

Didalam penelitian ini terdapat dua jenis tujuan, yaitu tujuan umum dan tujuan khusus. Tujuan umum penelitian ini adalah untuk menghasilkan audit terhadap penggunaan sistem informasi *call center* untuk *ensure system security* dan manage data pada PT. Arga Bangun Bangsa (*ESQ Leadership Center*). Sedangkan tujuan khusus dari penelitian ini adalah untuk menghasilkan:

1. Analisis audit sistem *call center* untuk *manage awareness, maturity level* proses teknologi informasi pada *manage data* dan *ensure security system call center*.
2. Pembuatan rekomendasi untuk mencapai *level* yang lebih baik dari hasil yang telah di audit.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan dapat memberi manfaaat di antaranya:

1. Memberikan pengetahuan proses audit sistem informasi di bidang *call center*.
2. Memberikan pengetahuan tentang tentang menghitung nilai kinerja dan *maturity level* proses sebuah sistem.
3. Memberikan pengetahuan tahap-tahap melakukan audit sebuah sistem informasi.

1.6 Metodologi Penelitian

Metode yang digunakan dalam penelitian ini di antaranya:

1. Metode Pengumpulan Data yang terdiri dari:

a. Studi Literatur Sejenis

Mendapatkan gambaran yang menyeluruh tentang apa yang sudah dikerjakan orang lain dan bagaimana orang mengerjakannya, kemudian seberapa berbeda penelitian yang akan kita lakukan (Jogiyanto 2008).

b. Metode observasi

Melalui pengamatan secara langsung atau observasi yang dilakukan di perusahaan guna mendapatkan data yang di maksud (Jogiyanto 2008).

c. Metode Wawancara

Wawancara memungkinkan untuk mendapatkan data secara lebih mendalam karena bertatapan langsung dengan narasumber (Jogiyanto 2008).

2. Metode Audit SI

a. COBIT *Framework*

COBIT adalah *framework* yang dapat digunakan sebagai alat yang komprehensif untuk menciptakan dan mengefektifkan implementasi *IT Governance* pada suatu perusahaan (ITGI 2007).

b. Metode Kuisioner

Kumpulan pertanyaan dan pernyataan untuk responden dalam rangka pengumpulan data agar sesuai dengan tujuan penelitian (Surendro 2009).

1.7 Sistematika Penulisan

Dalam penyusunan skripsi ini sistematika penulisan terdiri dari 5 (lima) bab, adapun uraian masing-masing bab tersebut adalah :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan dibahas mengenai dasar-dasar teori yang mendukung penulisan skripsi yaitu pengertian sistem, sistem informasi, audit sistem informasi, tata kelola teknologi informasi, framework COBIT dan *call center*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode pengumpulan data dan metode audit sistem informasi yang digunakan pada penelitian ini. Penjelasan yang terkait merupakan tahap dan kegiatan dalam penelitian skripsi.

BAB IV ANALISIS DAN PEM BAHASAN

Bab ini akan menguraikan sejarah singkat PT Arga Bangun Bangsa (ESQ LC) serta membahas analisis audit sistem informasi yang

telah dilakukan beserta pembuatan rekomendasi untuk kedepannya agar sistem menjadi lebih baik.

BAB V PENUTUP

Bab ini merupakan bab terakhir dari skripsi, yang terdiri dari kesimpulan dari apa yang telah diuraikan pada bab sebelumnya dan saran-saran yang *Insya Allah* bermanfaat untuk kemajuan perusahaan.

BAB II

LANDASAN TEORI

2.1 Konsep Dasar Sistem

Konsep dasar tentang sistem pertama kali dikemukakan oleh Ludwig von Bertalanffy dan William Ross Ashby pada tahun 1940-an. Konsep ini pada awalnya dikaji berdasarkan filosofi ilmu pengetahuan yang meliputi ilmu teknik, fisika, biologi, geografi, sosiologi, teori organisasi, manajemen, dan ekonomi. Saat ini, kajian tersebut disebut juga sebagai teori sistem.

2.1.1 Pengertian Sistem

Menurut Indrajit (2001). Sistem merupakan kumpulan dari komponen-komponen yang memiliki unsur keterkaitan antara satu dengan yang lainnya. Jogiyanto (2005), menjelaskan bahwa sistem adalah suatu kesatuan yang terdiri dari dua atau lebih komponen atau sub sistem yang berinteraksi untuk mencapai suatu tujuan tertentu.

McLeod (2001). Berpendapat bahwa sistem adalah "Sekelompok elemen yang terintegrasi dengan maksud yang sama untuk mencapai suatu tujuan". Dari beberapa definisi mengenai sistem, dapat diambil kesimpulan bahwa sistem adalah:

1. Sekumpulan komponen atau sekelompok elemen
2. Saling berhubungan satu dengan yang lainnya, dan
3. Bekerja sama (sinergi) untuk mencapai suatu tujuan.

a. Karakteristik Sistem

Menurut Jogiyanto (2001) suatu sistem mempunyai karakteristik atau sifat–sifat yang tertentu, yaitu mempunyai komponen-komponen *(components)*, batasan sistem *(boundary)*, lingkungan luar sistem *(environtment)*, antarmuka *(interface)*, masukan *(input)*, pengolah *(process)*, dan sasaran *(objectives)* atau tujuan *(goal)*.

1. Komponen sistem

   Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi, yang artinya saling bekerja dalam membentuk satu kesatuan. Komponen-komponen sistem atau elemen-elemen sistem dapat berupa subsistem atau bagian-bagian dari sistem.

2. Batasan sistem

   Batasan sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lainnya atau dengan lingkungan luarnya. Batasan sistem ini memungkinkan suatu sistem dipandang sebagai satu kesatuan. Batasan suatu sistem menunjukkan ruang lingkup dari sistem tersebut.

3. Lingkungan luar sistem

   Lingkungan luar sistem dari suatu sistem adalah apapun di luar batas dari sistem yang mempengaruhi operasi sistem. Lingkungan luar sistem dapat bersifat menguntungkan dan dapat juga bersifat merugikan sistem tersebut.

4. Penghubung sistem

   Penghubung merupakan media penghubung antara satu subsistem dengan susbsistem yang lainnya. Melalui penghubung ini memungkinkan sumber-

sumber daya mengalir dari satu subsistem ke subsistem yang lainnya. Keluaran dari satu subsistem akan menjadi masukan untuk subsistem lainnya dengan melalui penghubung.

5. Masukan sistem

   Masukan adalah energi yang dimasukkan ke dalam sistem. Masukan dapat berupa masukan perawatan *(maintenance input)* dan masukan sinyal *(signal input)*. Masukan perawatan adalah energi yang dimasukkan supaya sistem tersebut dapat beroperasi. Masukan sinyal adalah energi yang diproses untuk mendapatkan keluaran.

6. Keluaran sistem

   Keluaran adalah hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dari sisa pembuangan. Keluaran dapat merupakan masukan untuk subsistem yang lain atau kepada supra sistem.

7. Pengolah sistem

   Suatu sistem dapat mempunyai suatu bagian pengolah yang akan merubah masukan menjadi keluaran. Suatu sistem produksi akan mengolah masukan berupa bahan baku dan bahan-bahan yang lain menjadi keluaran berupa barang jadi.

8. Sasaran sistem

   Suatu sistem pasti mempunyai tujuan *(goal)* atau sasaran *(objective)*. Jika suatu sistem tidak mempunyai sasaran, maka operasi sistem tidak mempunyai

sasaran dari sistem sangat menentukan sekali masukan yang dibutuhkan sistem dan keluaran yang akan dihasilkan sistem.

2.1.2 Pengertian Informasi

Menurut Jogiyanto (2001). "Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya". Sumber dari informasi adalah data, yang merupakan kenyataan yang menggambarkan suatu kejadian dan kesatuan nyata. Data merupakan bentuk yang masih mentah dimana data yang masih mentah tersebut harus terlebih dahulu diolah untuk menjadi informasi yang lebih berguna.

Dari pendapat yang telah dikemukakan di atas, penulis dapat menarik kesimpulan bahwa dengan informasi adalah data yang diolah sehingga menjadi lebih berguna dan dapat digunakan sebagai pengambilan keputusan bagi penggunanya.

a. Kualitas Informasi

Berdasarkan pengertian informasi yang telah dikemukakan, agar informasi dapat menunjukkan nilai gunanya, menurut Jogiyanto (2001). informasi tersebut harus memiliki kualitas informasi seperti dibawah ini, yaitu

1. Akurat, berarti informasi harus bebas dari kesalahan-kesalahan yang jelas dalam mencerminkan maksudnya.
2. Tepat waktu, berarti informasi yang datang pada penerima tidak boleh terlambat. Karena keterlambatan penerimaan informasi akan mengurangi nilai

dari informasi tersebut atau bahkan dapat pula merugikan pihak yang memerlukan informasi tersebut.

3. Relevan, berarti informasi tersebut mempunyai manfaat untuk pemakainya dan benar-benar sesuai dengan yang dibutuhkan oleh si penerima informasi tersebut.

2.1.3 Pengertian Sistem Informasi

Menurut pendapat Jogiyanto (2001) bahwa sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan.

2.2 Pengertian Audit Sistem Informasi

Audit sistem informasi mulai banyak dilakukan di organisasi dan perusahaan karena ketergantungan perusahaan terhadap komputer untuk pemrosesan data, pemeliharaan dan pelaporan informasi semakin meningkat. Keandalan data dan sistem informasi menjadi perhatian utama auditor, termasuk kontrol internal dari sistem tersebut. Selain untuk mengurangi biaya, tujuannya untuk mengurangi risiko kerugian karena kesalahan, manipulasi, tindakan ilegal lainnya, serta insiden yang menyebabkan sistem menjadi tidak tersedia (*General Accounting Office*, 2009).

Audit SI memberikan evaluasi yang bersifat independen atas kebijakan, prosedur, standar, pengukuran, dan praktik untuk menjaga/mencegah informasi yang bersifat elektronik dari kehilangan, kerusakan, penelusuran yang tidak disengaja dan sebagainya (NSAA & GAO, 2011). Audit SI secara umum mencakup hal-hal sebagai berikut: meninjau lingkungan dan fisik, administrasi sistem, software aplikasi, keamanan jaringan, kontinuitas bisnis, dan integritas data (Gondodiyoto & Hendarti, 2006)

Audit SI sebagai proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem informasi dapat melindungi aset, teknologi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efisien (Sayana, 2002).

2.2.1 Tujuan

Tujuan audit sistem informasi untuk meninjau dan memberikan umpan balik, menjamin dan melakukan rekomendasi mengenai tiga hal sebagai berikut ketersediaan (*availability*), kerahasiaan (*Confidentiality*) dan integritas.

Detail tentang tujuan audit sistem informasi dijelaskan (Gondodiyoto & Hendarti, 2006) sebagai berikut:

1. Untuk mengidentifikasi sistem yang ada baik yang ada pada tiap divisi/unit/departemen maupun yang digunakan menyeluruh.
2. Untuk dapat lebih memahami seberapa besar sistem informasi mendukung kebutuhan strategis perusahaan, operasi perusahaan,

mendukung kegiatan operasional departemen/unit/divisi, kelompok kerja maupun para petugas dalam melaksanakan kegiatannya.

3. Untuk mengetahui pada bidang atau area mana, fungsi, kegiatan atau *business process* yang didukung dengan sistem serta teknologi informasi yang ada.
4. Untuk menganalisis tingkat pentingnya data/informasi yang dihasilkan oleh sistem dalam rangka mendukung kebutuhan para pemakainya.
5. Untuk mengetahui keterkaitan antara sistem pengolahan dan transfer informasi.
6. Untuk mengidentifikasi apakan ada kesenjangan antara sistem dan kebutuhan.
7. Untuk membuat peta dari alur informasi yang ada.

2.2.2 Tahapan Audit

Tahapan audit sistem informasi terdiri dari perencanaan audit, pengujian pengendalian, pengujian substantive, dan penyelesaian audit (Gondodiyoto & Hendarti, 2006). Sementara berdasarkan CISA Review Manual, 2009, ada beberapa langkah dalam perencanaan audit:

1. Memahami misi organisasi, sasaran, tujuan, dan proses-proses, termasuk informasi dan kebutuhan pengolahan, seperti ketersediaan, integritas, keamanan teknologi bisnis, serta kerahasiaan informasi.
2. Mengidentifikasi konten organisasi, seperti kebijakan, standar, panduan, prosedur dan struktur organisasi.

3. Menampilkan analisis risiko untuk membantu merancang rencana audit.
4. Meninjau kontrol internal berkaitan dengan teknologi informasi.
5. Merancang ruang lingkup dan sasaran audit.
6. Menyusun pendekatan audit berdasarkan strategi audit.
7. Menyediakan SDM untuk melakukan audit.
8. Menentukan kebutuhan logistik.

Sedangkan untuk mendapatkan gambaran tentang bisnis dan organisasi maka auditor sistem informasi perlu melakukan hal-hal sebagai berikut:

a. Melakukan tur fasilitas organisasi.
b. Membaca laporan tahunan, laporan analisis keuangan independen dan publik organisasi.
c. Meninjau strategi jangka panjang bisnis dan IT.
d. Melakukan wawancara ke narasumber utama untuk memahami isu bisnis.
e. Meninjau laporan audit sebelumnya atau laporan yang berkaitan dengan TI.
f. Mengidentifikasi regulasi dan spesifik yang diterapkan pada TI.
g. Mengidentifikasi fungsi TI atau yang berkaitan dengan di-*outsourced.*

2.3 Tata Kelola Teknologi Informasi (*IT Governance*)

Menurut Surendro (2009) Tata kelola teknologi informasi adalah tanggungjawab Direksi dan Manajer eksekutif organisasi. Tata kelola teknologi informasi merupakan bagian terintegrasi dari pengelolaan perusahaan yang mencakup kepemimpinan, struktur data serta proses organisasi yang memastikan

bahwa teknologi informasi perusahaan dapat dipergunakan untuk memepertahankan dan memperluas strategi dan tujuan organisasi.

a. Seluruh tujuan entitas telah ditentukan,

b. Metode untuk mencapai tujuan tersebut telah ditetapkan, dan

c. Tata cara pengawasan kinerja telah dijelaskan.

Inti dari tanggung jawab pengelolaan dalam menentukan strategi, menangani masalah, memberikan nilai dan mengukur kinerja adalah nilai *stakholde*r, yang menentukan strategi perusahaan dan teknologi informasi. Berjalannya bisnis yang ada dan pengembangannya menjadi model-model bisnis baru tentu saja merupakan harapan pada stakeholder dan dapat dicapai dengan hanya dengan terbentuknya infrasrtuktur teknologi informasi perusahaan yang baik.

Tata kelola teknologi informasi adalah tanggung jawab dewan direksi dan eksekutif. Tata kelola teknologi informasi bukan suatu disiplin ilmu atau aktifitas yang terbatas, tapi lebih merupakan sebuah pengelolaan yang terintegrasi dengan pengelolaan perusahaan. Tata kelola teknologi informasi mencakup kepemimpinan dan struktur serta proses organisasi yang memastikan teknologi informasi berjalan dan memperluas strategi dan tujuan organisasi. Hal penting yang berpengaruh atas keberhasilan struktur dan proses tersebut adalah komunikasi yang efektif di antara semua pihak yang berdasar kepada hubungan yang konstruktif, pemahaman yang sama dan komitmen yang sama dalam segala hal.

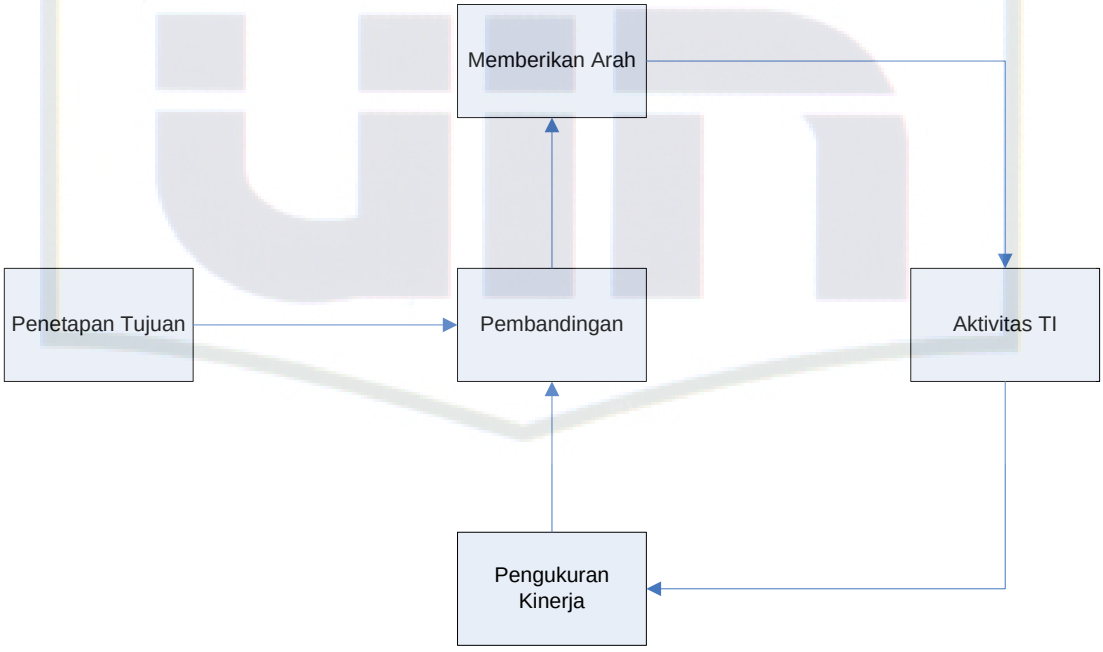
Tanggung jawab tata kelola teknologi informasi membentuk suatu bagian dari kerangka kerja yang lebih luas dari pengelolaan perusahaan dan sebaiknya diperlakukan seperti agenda strategi lainnya bagi dewan direksi. Dalam bentuk yang sederhana , untuk suatu sistem teknologi informasi yang sangat bergantung. Pengelolaan harus efektif, transparan dan akuntabel. Maksudnya, dewan direksi harus lebih memahami benar tanggung jawab manajemen dan pribadinya serta harus mempunyai suatu sistem untuk melaksanakan tanggung jawabnya tersebut. Tanggung jawab umumnya berhubungan dengan penyelarasan dan penggunaan teknologi informasi dalam seluruh aktifitas perusahaan. Manajemen risiko yang berhubungan dengan teknologi dan verifikasi nilai yang didapatkan dari penggunaan teknologi informasi dalam perusahaan.

Kegunaan tata kelola teknologi informasi adalah untuk mengatur penggunaan teknologi informasi, serta untuk memastikan kinerja teknologi informasi sesuai dengan tujuan berikut:

1. Keselarasan teknologi informasi dengan perusahaan dan realisasi keuntungan-keuntungan yang dijanjikan dari penerapan teknologi informasi.
2. Penggunaan teknologi informasi agar memungkinkan perusahaaan mengeksploitasi kesempatan yang ada, memaksimalkan apa yang sudah dimiliki saat ini dan memaksimalkan keuntungan.
3. Penanganan manajemen risiko yang terkait teknologi informasi secara tepat.

Tata kelola teknologi informasi seringkali berjalan dalam lapisan yang berbeda-beda antara lain *team-leader* memberikan laporan kepada eksekutif, dan eksekutif kepada direksi.

Laporan yang menandakan perbedaan tujuan akan selalu berisi rekomendasi untuk suatu tindakan yang harus dikuatkan oleh lapisan pengelola. Jelas sekali, pendekatan ini tidak akan efektif kecuali strategi dan tujuan pertama-tama harus sudah diturunkan dalam organisasi. Ilustrasi dalam gambar 2.1 memperlihatkan secara konseptual interaksi antara tujuan dan aktifitas teknologi informasi dan dapat diaplikasikan dalam lapisan yang berbeda-beda dalam perusahaan.



Gambar 2.1 Interaksi antara tujuan dan aktifitas teknologi informasi (ITTI, 2009)

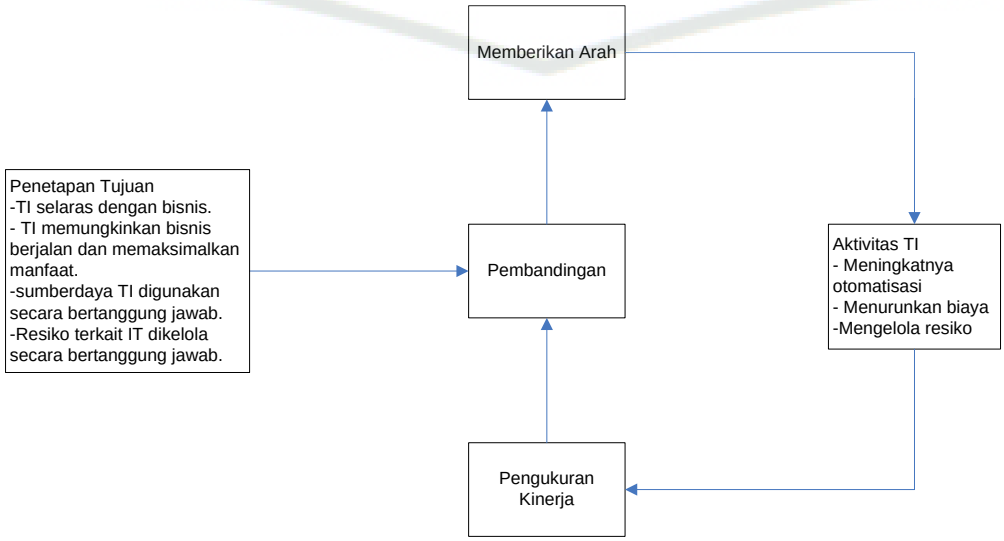
Proses pengelolaan dimulai dengan menentukan tujuan dari teknologi informasi perusahaan, memberikan arahan awal. Setelah itu, suatu putaran/loop yang berkelanjutan dilakukan untuk mengukur kinerja, membandingkan tujuan dan akhirnya mengarahkan kembali aktifitas yang seharusnya dilakukan dan perubahan dari tujuan apabila diperlukan. Selama tujuannya adalah sebagian besar

adalah tanggung jawab dewan direksi dan pengukuran kinerja manajemen. Ada suatu hal yang harus selalu dikembangkan sehingga tujuan-tujuan tersebut merupakan hal yang dapat dicapai dan pengukuran mempresentasikan tujuan secara tepat.

Dalam menanggapi arahan yang diterima, fungsi teknologi informasi harus fokus dalam:

1. Memberikan keuntungan dengan menambah otomatisasi dan membuat perusahaan menjadi lebih efektif, mengurangi biaya dan membuat keseluruhan perusahaan lebih efisien.
2. Menangani risiko (keamanan, kelayakan dan kesesuaian).

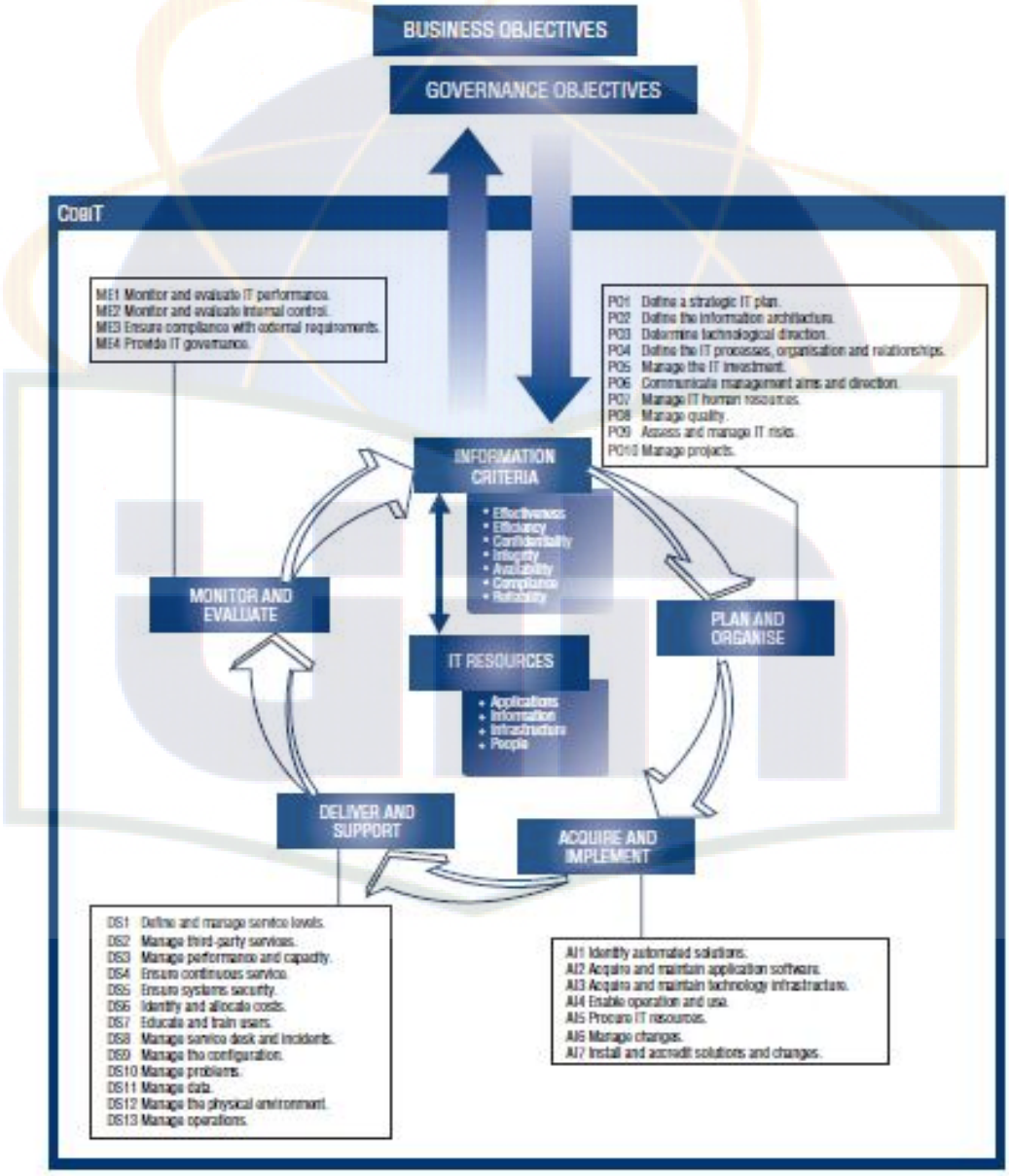
Dengan demikian kerangka kerja teknologi informasi dapat diselesaikan seperti yang terlihat pada gambar 2.2



Gambar 2.2 Kerangka Kerja Tata Kelola Teknologi Informasi (ITGI, 2003)

Kerangka kerja teknologi informasi yang digambarkan dengan diagram.

2.4 COBIT *Framework*



Gambar 2.3 *Cobit Framework*

Control Objectives for Information and Related Technology (COBIT) diperkenalkan pada tahun 1996 oleh *The Information System Audit and Control Assosiation*. Pada tahun 1998 *IT Governance Institute* (ITGI) berdiri dengan tujuan untuk memimpin riset pada area vital tata kelola teknologi informasi. Pada

tahun yang sama *The Information System Audit and Control Assosiation* dan ITGI melebur menjadi satu entitas dan mempublikasikan COBIT edisi ketiga pada tahun 2000 dan diikuti versi keempat pada tahun 2006.

Dalam situsnya, ITGI mengumumkan bahwa *framework* COBIT memudahkan *Chief Information Officer* (CIO) membantu stakeholder memahami proses teknologi informasi dan layanan, serta secara mudah berintegrasi dengan standar lain seperti ITIL, ISO 27002 dan COSO. Stakeholder juga dapat menggunakan COBIT sebagai *instrument* untuk mengelola informasi yang disediakan teknologi informasi untuk mendukung proses bisnis.

Menurut Campbell (2005) COBIT merupakan suatu cara untuk menerapkan *IT Governance*. COBIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat control objectives untuk bidang teknologi informasi, dirancang untuk memungkinkan tahapan bagi audit.

COBIT merupakan sekumpulan dokumentasi dan panduan yang mengarahkan pada *IT governance* yang membantu auditor, manajemen, dan pengguna (*user*) untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis. COBIT dikembangkan oleh *IT Governance Institute* (*ITGI*) yang merupakan bagian dari *Information Systems Audit and Control Association* (*ISACA*).

Adapun kerangka kerja COBIT secara keseluruhan terdiri atas arahan seperti:

a. *Control objectives*: terdiri atas 4 tujuan pengendalian tingkat tinggi yang tercermin dalam 4 domain Yang dapat dilihat pada gambar 2.3. Tiap-tiap kontrol mendukung standar informasi, yaitu standar kualitas (efektif dan efisien), standar keamanan (*confidentiality,* integritas, dan ketersediaan (*availability*)), dan *fiduciary requirement* (kepatuhan dan reliabilitas)
b. *Audit guidelines*: berisi 318 tujuan pengendalian bersifat rinci.
c. *Management guidelines*: berisi arahan, baik secara umum dan spesifik mengenai hal-hal yang menyangkut kebutuhan manajemen.

Dan dalam kerangka kerja COBIT juga memasukkan bagian-bagian seperti:

1. ***Maturity Models: untuk menilai tahap kematangan IT Governance dalam skala 0 – 5.***

Surendro (2009) Model kematangan untuk pengelolaan dan kontrol pada proses teknologi informasi didasarkan pada metode evaluasi organisasi, sehingga dapat mengevaluasi sendiri dari level tidak ada (0) hingga optimis (5). Pendekatan ini diperoleh dari model kematangan dari *Software Engineering Institute* yang mendefinisikannya untuk kapabilitas pengembangan perangkat lunak. Model kematangan dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. Model kematangan dirancang sebagai profil proses teknologi informasi, sehingga organisasi akan dapat mengenali sebagai deskripsi kemungkinan keadaan

sekarang dan mendatang. Penggunaan model kematangan yang dikembangkan untuk setiap 34 proses teknologi informasi, memungkinkan manajemen dapat mengidentifikasi:

a. Kinerja sesungguhnya perusahaan, di mana kondisi perusahaan sekarang.
b. Kondisi sekarang dari ndustri sebagai perbandingan.
c. Target peningkatan perusahaan, di mana kondisi yang diinginkan perusahaan.

Setiap 34 proses teknologi informasi mempunyai sebuah model kematangan yang telah didefinisikan dengan diberikan skala pengukuran bertingkat dari 0 (tidak ada) sampai 5 (*optimised*). Model kematangan yang dibangun berawal dari *generic qualitative model*, di mana prinsip dari atribut berikut ditambahkan dengan cara bertingkat:

1. Kepedulian dan komunikasi (*awareness and communication*).
2. Kebijakan, standar dan prosedur (*policies, standards and procedures*).
3. Perangkat bantu dan otomatisasi (*tools and automation*).
4. Ketrampilan dan keahlian (*skills and expertise*).
5. Pertanggungjawaban internal dan eksternal (*responsibility and acccountability*).
6. Penetapan tujuan dan pengukuran (*goal setting and measurement*).

Pendefinisian model kematangan suatu proses teknologi informasi

mengacu pada kerangka kerja COBIT secara umum adalah sebagai berikut:

Level 0: Tidak ada

1. Kondisi ini dimana perusahaan sama sekali belum melihat pentingnya teknologi informasi untuk dikelola secara baik oleh manajemen.

Level 1: Awal (*initial*)

1. Kondisi dimana perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.

Level 2: Berulang tapi intuitif (*Repeatable*)

1. Kondisi dimana perusahaan telah memiliki pola yang berulang kali dilakukan dalam melakukan manajemen aktivitas terkait dengan tata kelola teknologi informasi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidakkonsistenan.
2. Sudah mulai ada prosedur namun tidak seluruhnya terdokumentasi dan tidak seluruhnya disosialisasikan kepada pelaksana.
3. Belum ada pelatihan formal untuk mensosialisasikan prosedur tersebut.
4. Tanggung jawab pelaksanaan berada pada masing-masing individu.

Level 3: Proses terdefinisi (*defined*)

1. Kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
2. Tidak ada pengawasan untuk menjalankan prosedur, sehingga memungkinkan terjadinya banyak penyimpangan.

Level 4: Terkelola dan Terukur (*managed*)

1. Kondisi dimana perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses teknologi informasi.
2. Terdapat fasilitas untuk memonitor dan mengukur prosedur yang sudah berjalan, dapat mengambil tindakan jika terdapat proses yang diindikasikan tidak efektif.
3. Proses diperbaiki terus menerus dan dibandingkan dengan praktik-praktik terbaik.
4. Terdapat perangkat bantu dan otomatisasi untuk pengawasan proses.

Level 5: Optimis (*optimised*)

1. Kondisi di mana perusahaan dianggap telah mengimplementasikan tata kelola manajemen teknologi informasi yang mengacu pada praktik terbaik.
2. Proses telah mencapai level terbaik karena perbaikan yang terus menerus dan perbandingan dengan perusahaan lain.

3. Perangkat bantu otomatis digunakan untuk mendukung *workflow*, menambah efisiensi dan kualitas kinerja proses.
4. Memudahkan perusahaan untuk beradaptasi terhadap perubahan.

Beberapa tujuan pengukuran kematangan adalah untuk:

a. Menumbuhkan kepedulian (*awareness*).
b. Melakukan identifikasi kelemahan (*weakness*).
c. Melakukan identifikasi kebutuhan perbaikan (*improvement).*

Beberapa metode pendekatan yang umum dilakukan dalam melakukan penilaian kematangan di antaranya adalah:

a. Pendekatan multidisiplin kelompok orang yang mendiskusikan dan menghasilkan kesepakatan tingkat kematangan kondisi sekarang.
b. Dekomposisi deskripsi kematangan ke dalam beberapa pernyataan sehingga manajemen dapat memberikan tingkat persetujuannya.
c. Penggunaan matriks atribut kematangan sebagaimana didokumentasikan dalam COBIT's Management Guidelines dan memberikan nilai masing-masing atribut dari setiap proses.

2. ***Critical Success Factors* (*CSFs*): arahan implementasi bagi manajemen dalam melakukan pengendalian atas proses IT.**
3. ***Ooutcome Measure*: berisi mengenai arahan kinerja proses-proses IT sehubungan dengan kebutuhan bisnis.**
4. ***Performance Indicators*: kinerja proses-proses IT sehubungan dengan sasaran/tujuan proses (*process goals*).**

2.4.1 Fokus pada Bisnis

Surendro (2009) Orientasi pada bisnis menunjukkan bahwa COBIT dirancang untuk dapat digunakan oleh banyak pihak. Hal ini tidak tidak terbatas hanya bagi kalangan teknologi informasi, pengguna maupun auditor, tetapi lebih penting lagi adalah sebagai panduan yang komprehensif bagi manajemen dan dan pemilik bisnis proses. Kebutuhan bisnis tercermin dengan adanya kebutuhan informasi. Informasi itu sendiri perlu memenuhi kriteria kontrol tertentu guna mencapai tujuan bisnis. Kriteria kontrol untuk informasi sebagaimana dikemukakan COBIT adalah:

1. Efektifitas, terkait dengan informasi yang relevan dan berhubungan pada proses bisnis serta disampaikan juga secara tepat waktu, benar, konsisten dan mudah.
2. Efisiensi, terkait dengan ketentuan informasi melalui penggunaan sumberdaya secara optimal.
3. Kerahasiaan, terkait dengan pengamanan terhadap informasi yang sensitif dari pihak yang tidak berhak.
4. Integritas, terkait dengan keakuratan dan kelengkapan informasi serta validitasnya sesuai dengan nilai dan harapan bisnis.
5. Ketersediaan, terkait dengan ketersediaan informasi pada saat kapanpun diperlukan oleh proses bisnis.
6. Kepatuhan, terkait dengan kepatuhannya pada hukum, regulasi, maupun perjanjian perjanjian kontrak.
7. Keandalan, terkait dengan penyediaan informasi yang tepat bagi manajemen untuk mendukung operasional suatu entitas dan menjalankan tanggung jawab tatakelola.

Pencapaian kebutuhan bisnis, yang tercermin dengan adanya pemenuhan kebutuhan informasi, membutuhkan dukungan sumber daya teknologi informasi.

Sumberdaya teknologi informasi dalam COBIT, diidentifikasi dan didefinisikan sebagai berikut:

1. Aplikasi adalah sistem yang digunakan oleh para pemakai yang sudah diotomasikan dan prosedur manual yang digunakan untuk memproses informasi.
2. Informasi adalah data dalam semua bentuknya, dimasukkan, diproses dan dikeluarkan oleh sistem informasi dalam bentuk apa pun yang digunakan oleh bisnis.
3. Infrastruktur adalah teknologi dan fasilitas (*hardware, operating system, Database Management System*, jaringan, fasilitas yang memungkinkan pemrosesan aplikasi dan lain-lain).
4. Manusia adalah personil yang diperlukan untuk merencanakan, mengorganisir, mendapatkan, menerapkan, menyampaikan, mendukung, memonitor dan mengevaluasi informasi. Mereka bisa saja internal, direkrut dari luar (*outsource*), atau dikontrak ketika diperlukan.

2.4.2 Orientasi pada proses

Surendro (2009) Aktivitas teknologi informasi dalam COBIT didefinisikan kedalam model proses yang generik dan dikelompokkan dalam 4 (empat) domain: perencanaan dan Pengorganisasian (*Plan and Organize*), Pengadaan dan Implementasi (*Acquired and Implement*), Penyampain Layanan

dan Dukungan (*Deliver and Support*) dan Monitor dan Evaluasi (*Monitor and Evaluate*) dengan penjelasan sebagai berikut:

4 domain tersebut oleh Surendro (2009) disederhanakan sebagai berikut:

1. *Plan and Organize* (PO)

   Domain ini mencakup strategi, taktik dan perhatian pada identifikasi cara teknologi informasi dapat berkontribusi terbaik pada pencapaian objektif bisnis. Selanjutnya, realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda. Akhirnya suatu organisasi yang tepat seperti halnya infrastruktur teknologi harus diletakkan pada tempatnya. Fokus komponen yang ada pada domain Plan and Organize di antaranya:

   a. PO1 *Define a Strategic IT Plan* (Menenentukan Rencana Strategis TI)
   b. PO2 *Define the Information Architecture* (Menentukan Arsitektur Informasi)
   c. PO3 *Determine Technological Direction* (Menentukan Arah Teknologi)
   d. PO4 *Define the IT Processes, Organisation and Relationships* (Menentukan Hubungan Proses TI dan Organisasi)
   e. PO5 *Manage the IT Investment* (Mengelola Investasi TI)
   f. PO6 *Communicate Management Aims and Direction* (Mengkomunikasikan Arah dan Tujuan Manajemen)
   g. PO7 *Manage IT Human Resources* (Mengelola Sumber Daya Manusia TI)
   h. PO8 *Manage Quality* (Mengelola Kualitas)
   i. PO9 *Assess and Manage IT Risks* (Menilai dan Mengelola Risiko TI)
   j. PO10 *Manage Projects* (Mengelola Proyek)

2. *Acquired and Implement* (AI)

Guna merealisasikan strategi teknologi informasi, solusi teknologi informasi perlu diidentifikasi, dikembangkan atau diperoleh seperti halnya diimplementasikan dan diintegrasikan kedalam proses bisnis. Sebagai tambahan, perubahan dalam pemeliharaan sistem yang ada dicakup dalam domain ini untuk memastikan solusi berlangsung untuk memenuhi objektif bisnis. *Acquired and Implement* terdiri dari beberapa fokus area di antaranya:

a. *AI1 Identify Automated Solutions* (Identifikasi Solusi Otomatis)
b. AI2 *Acquire and Maintain Application Software* (Memperoleh dan Memelihara Aplikasi *Software*)
c. AI3 *Acquire and Maintain Technology Infrastructure* (Memperoleh dan Memelihara Infrastruktur Teknologi)
d. AI4 *Enable Operation and Use* (Mengaktifkan Operasi dan Penggunaan)
e. AI5 *Procure IT Resources* (Pengadaan Sumber Daya TI)
f. AI6 *Manage Changes* (Mengelola Perubahan)
g. AI7 *Install and Accredit Solutions and Changes* (Instal dan mengakreditasi Solusi dan Perubahan)

3. *Deliver and Support* (DS)

Domain ini dihubungkan dengan penyampaian sesungguhnya layanan yang diperlukan. Mencakup penyediaan layanan, manajemen keamanan dan kelangsungan, dukungan layanan pada pengguna, manajemen data dan fasilitas

operasional. Beberapa fokus komponen yang ada pada domain *Deliver and Support* di antaranya:

a. DS1 *Define and Manage Service Levels* (Menetapkan dan Mengelola Tingkat Layanan)
b. DS2 *Manage Third-party Services* (Mengelola Layanan Pihak Ketiga)
c. DS3 *Manage Performance and Capacity* (Mengelola Kinerja dan Kapasitas)
d. DS4 *Ensure Continuous Service* (Menjamin Layanan Berlanjut)
e. DS5 *Ensure Systems Security* (Memastikan Keamanan Sistem)
f. DS6 *Identify and Allocate Costs* (Mengidentifikasi dan Mengalokasikan Biaya)
g. DS7 *Educate and Train Users* (Mendidik dan Melatih Pengguna)
h. DS8 *Manage Service Desk and Incidents* (Mengelola Layanan *Service Desk* dan insiden)
i. DS9 *Manage the Configuration* (Mengelola Konfigurasi)
j. DS10 *Manage Problems* (Mengelola Masalah)
k. DS11 *Manage Data* (Mengelola Data)
l. DS12 *Manage the Physical Environment* (Mengelola Lingkungan Fisik)
m. DS13 *Manage Operations* (Mengelola Operasi)

4. *Monitor and Evaluate* (ME)

Semua proses teknologi informasi perlu secara rutin dinilai dari waktu ke waktu untuk kualitas dan pemenuhan dengan kebutuhan kontrol. Domain ini berkenaan dengan manajemen kinerja, pemantauan kontrol internal,

pemenuhan terkait dengan regulasi dan pelaksanaan tata kelola. Fokus komponen yang terdapat pada domain Monitor and Evaluate di antaranya:

a. ME1 *Monitor and Evaluate IT Performance* (Pemantauan dan Evaluasi Kinerja TI)
b. ME2 *Monitor and Evaluate Internal Control* (Pemantauan dan Evaluasi Pengendalian Internal)
c. ME3 *Ensure Compliance With External Requirements* (Memastikan Kepatuhan dengan Persyaratan Eksternal)
d. ME4 *Provide IT Governance* (Menyediakan Tata Kelola TI)

2.4.3 Berbasis Kontrol

Surendro (2009) kontrol/kendali dalam COBIT didefinisikan sebagai kebijakan, prosedur, praktik dan struktur organisasi yang dirancang untuk memberikan jaminan yang dapat diterima bahwa tujuan bisnis akan dicapai dan kejadian yang tidak diharapkan dapat dicegah, diketahui dan diperbaiki. Sedangkan tujuan kontrol teknologi informasi merupakan pernyataan mengenai maksud atau hasil yang diharapkan dengan menerapkan prosedur kontrol dalam aktivitas teknologi informasi tertentu. Tujuan kontrol dalam COBIT merupakan kebutuhan minimal untuk kontrol yang efektif dari setiap proses teknologi informasi.

Agar dapat mencapai tata kelola teknologi informasi yang efektif, kontrol perlu diimplementasikan dalam suatu kerangka kerja kontrol yang didefinisikan untuk semua proses teknologi informasi. Kerangka kerja kontrol dalam COBIT,

memberikan kaitan yang jelas diantara kebutuhan tata kelola teknologi informasi, proses teknologi informasi, karena tujuan kendali diorganisasikan menurut proses teknologi informasi. Setiap proses teknologi informasi yang terdapat dalam COBIT mempunyai tujuan kendali tingkat tinggi dan sejumlah tujuan kendali detail. Secara keseluruhan ini merupakan karakteristik proses yang dikelola dengan baik.

2.4.4 Dikendalikan oleh Pengukuran

Surendro (2009) Pemahaman terhadap status sistem teknologi informasi, diperlukan bagi organisasi agar dapat memutuskan tingkat manajemen dan kontrol yang harus diberikan. Dengan demikian organisasi perlu mengetahui apa yang harus diukur dan bagaimana pengukuran dilakukan, sehingga dapat diperoleh status tingkat kinerjanya. Selanjutnya pengetahuan ini akan membantu upaya peningkatan yang perlu dilakukan. Berkenaan dengan hal tersebut COBIT memberikan:

1. Model Kematangan, yang memungkinkan pembandingan/*benchmarking* dan identifikasi peningkatan kapabilitas yang perlu.
2. Tujuan dan Ukuran Kinerja untuk proses teknologi informasi, menunjukkan bagaimana proses memenuhi tujuan bisnis dan tujuan teknologi informasi dipakai untuk pengukuran kinerja.
3. Tujuan aktivitas untuk memungkinkan kinerja proses yang efektif.

2.4.5 Pengukuran Kinerja

Surendro (2009)Tujuan dan ukuran didefinisikan dalam COBIT pada tiga tingkat:

1. Tujuan dan ukuran teknologi informasi, yang mendefinisikan apa yang diharapkan bisnis dari teknologi informasi.
2. Tujuan dan ukuran proses, yang mendefinisikan proses apa yang harus diberikan untuk mendukung tujuan teknologi informasi.
3. Ukuran kinerja proses (untuk mengukur seberapa baik proses dilakukan untuk menunjukkan jika tujuan kemungkinan besar terpenuhi).

COBIT menggunakan 2 jenis ukuran yaitu indikator tujuan dan indikator kinerja. Indikator tujuan utama/ *Outcome Measures* mendefinisikan pengukuran yang menginformasikan kepada manajemen sesudah terjadinya fakta/aktivitas apakah suatu proses teknologi informasi telah mencapai kebutuhan misalnya:

a. Ketersediaan informasi yang diperlukan untuk mendukung kebutuhan bisnis.
b. Ketiadaan integritas dan risiko kerahasiaan.
c. Efisiensi biaya proses dan operasi.
d. Konfirmasi keandalan, efektifitas dan kepatuhan.

Indikator kinerja utama / *Performance Indicator* mendefinisikan pengukuran yang menentukan seberapa proses baik teknologi informasi dilakukan. Hal ini, mengindikasikan kemungkinan pencapaian tujuannya. *Performance Indicators* di merupakan indikator petunjuk. *Performance Indicators* mengukur tujuan aktivitas yang merupakan tindakan yang harus diambil pemilik proses yang efektif.

2.4.6 Fokus Area yang di Audit

Dalam penulisan skripsi ini ada ada 2 kontrol utama yang menjadi fokus untuk melakukan audit sistem informasi yaitu DS5 dan DS11.

Penjelasan tiap-tiap kontrol sebagai berikut:

a. *DS5 Ensure System Security* (memastikan keamanan sistem)

Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI memerlukan proses manajemen keamanan. Proses ini meliputi penyusunan dan memelihara peranan-peranan keamanan (*security roles*) serta tanggung jawab, kebijakan, standar dan prosedur. Manajemen keamanan juga mencakup pengawasan keamanan dan ujicoba secara periodik, serta mengimplementasikan aksi perbaikan untuk kelemahan kekurangan atau insiden/bencana. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis terhadap kelemahan keamanan dan insiden.

DS5 mengontrol proses untuk memastikan keamanan sistem. Tujuannya memelihara integritas informasi dan infrastruktur pemrosesan, serta meminimalkan dampak kelemahan keamanan dan insiden. Sasaran proses DS5 berfokus pada mendefinisikan kebijakan keamanan TI, rencana dan prosedur, serta pengawasan, deteksi, pelaporan dan mengatasi kelemahan keamanan dan insiden.

Keberhasilan pelaksanaan DS5 tercapai dengan pemahaman kebutuhan keamanan, kelemahan dan ancaman. Mengelola identitas user dan otorisasi dalam prosedur standar, ujicoba keamanan secara reguler. Hal ini terukur dengan jumlah

insiden yang merusak reputasi organisasi terhadap publik, jumlah sistem dimana kebutuhan keamanan tidak sesuai dan jumlah pelanggaran konflik tugas.

DCO dapat dipandang sebagai suatu kontrol efektif untuk dapat mencapai tujuan, yang didefinisikan dalam COBIT 4.1. Adapun keberadaan (tingkat pemenuhannya) berkaitan langsung dengan upaya pengendalian terhadap kelemahan/kerentanan yang dapat memicu timbulnya ancaman yang berdampak serius pada pencapaian tujuan bisnis.

DS5 terdiri dari:

1. DS5.1 : Manajemen Keamanan TI (*Management of IT Security*)

   Manajemen keamanan TI pada level organisasi yang tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis. Menerjemahkan bisnis, risiko dan kepatuhan (*compliance*) ke dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan.

2. DS5.2: Rencana Keamanan TI (*IT Security Plan*)

   Memastikan rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, *software* dan *hardware*. Mengkomunikasikan kebijakan dan prosedur keamanan kepada *stakeholder* dan *user*.

3. DS5.3 : Manajemen Identitas (*Identity Management*)

   Memastikan semua user (internal, eksternal dan temporer) dan aktivitas mereka dalam sistem TI (bisnis, aplikasi, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) secara unik teridentifikasi. Memudahkan

user mengidentifikasi melalui mekanisme otentikasi. Mengkonfirmasi bahwa hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, dan kebutuhan kerja yang melekat pada identitas pengguna. Memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan. Memelihara identitas pengguna dan hak akses dalam repositori pusat. Melakukan langkah-langkah teknis yang menghemat biaya, mengukur prosedural dan menjaganya agar terus *update* dalam membuat identifikasi user, implementasi otentikasi dan memaksakan hak akses.

4. DS5.4: Manajemen Akun Pengguna (*User Account Management*)

   Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodifikasian dan penutupan akun pengguna serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna. Termasuk prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal dan eksternal, untuk normal dan kasus darurat. Hak dan kewajiban relatif terhadap akses ke sistem oraganisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis pengguna. Selanjutnya, melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung.

5. DS5.5: Uji Coba Keamanan, Penjagaan dan Pemantauan (*Security Testing, Surveillance and monitoring*)

Menguji, menjaga dan memantau implementasi keamanan TI dalam langkah yang proaktif. Keamanan TI seharusnya ditinjau secara periodik untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara. *Logging* dan fungsi pemantauan keamanan TI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.

6. DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*)

   Mendefinisikan secara jelas dan mengkomuniksasikan karakteristik dari insiden keamanan yang potential sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah.

7. DS5.7: Proteksi Teknologi Keamanan (*Protection of Security Technology*)

   Membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.

8. DS5.8: Manajemen Kunci Kriptografi (*Cryptographic Key Management*)

   Menentukan bahwa kebijakan dan prosedur sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, *entry*, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.

9. DS5.9: Pencegahan *Software* Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)

   Memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama *patch* keamanan yang *up-to-date* dan pengendalian virus) diseluruh

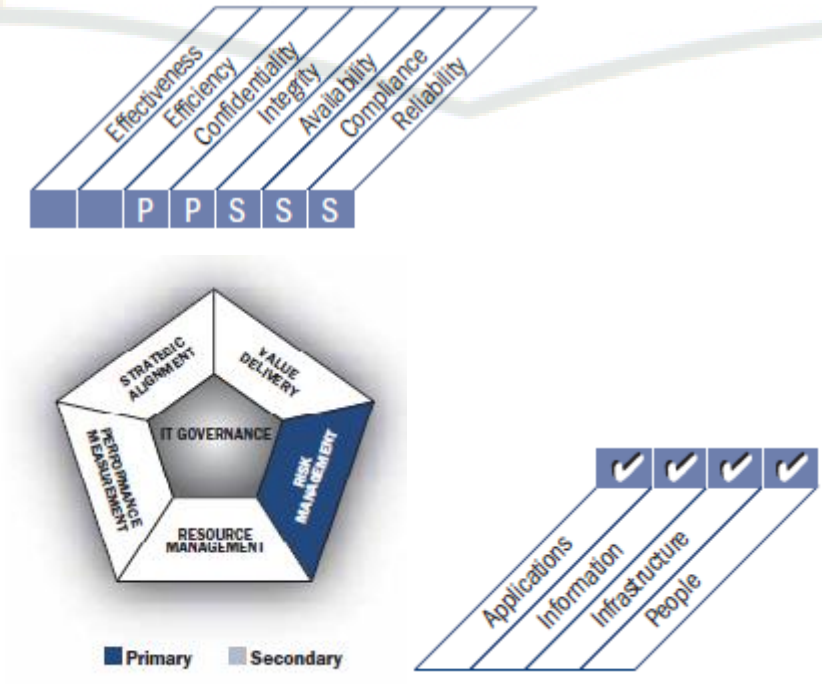
organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (seperti *virus*, *worm*, s*pyware* dan *spam*).

10. DS5.10 Keamanan Jaringan (*Network Security*)

    Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaringan, intruksi deteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.

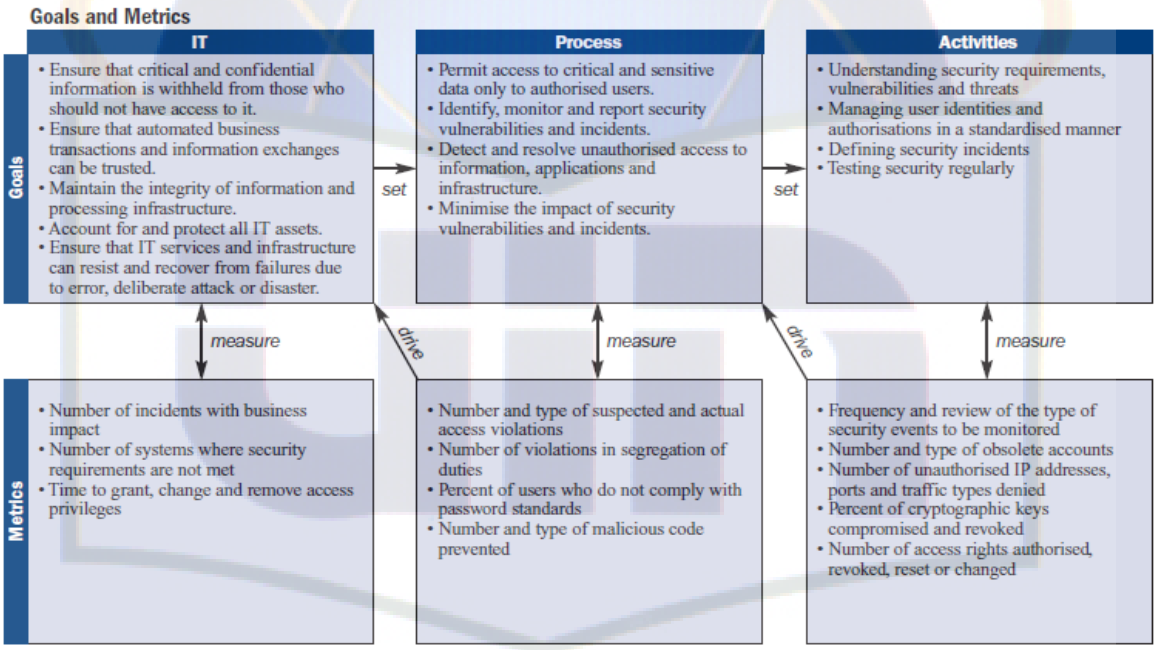
11. DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*)

    Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan *non-repudiation*.



Gambar 2.4 : Standar Informasi, jenis dan fokus area yang didukung DS5 (COBIT 4.1, IT *Governance Institute*, 2007)

Dengan menerapkan DS5 maka akan memelihara kerahasiaan dan integritas. Selain itu juga akan meningkatkan ketersediaan (*availability*), kepatuhan dan kepercayaan (*reliability*). DS5 berfokus pada aplikasi, informasi, infrastruktur dan SDM. Sasaran proses ini terutama mendukung *risk management.*



Gambar 2.5 : Sasaran Metrik DS5 (COBIT 4.1, *ITGI*, 2007)

Pada gambar 2.5 dijelaskan tujuan aktivitas dapat dipandang sebagai *Critical Success Factor* (CSF) yang meliputi tujuan berikut:

1. Memahami persyaratan keamanan kerentanan dan ancaman
2. Mengelola dan identitas pengguna otorisasi secara standar
3. Mendefinisikan insiden keamanan
4. Pengujian keamanan secara teratur

Untuk dapat menilai atau mengukur seberapa baik aktivitas di atas telah dilaksanakan, sebagai suatu bentuk transfaransi dalam pengawasan, maka didefinisikan *Performance Indicators*.

1. Frekuensi dan penelaahan terhadap jenis kejadian keamanan yang akan dipantau.
2. Jumlah dan jenis rekening usang.
3. Jumlah alamat IP yang tidak sah, pelabuhan dan jenis lalu lintas ditolak.
4. Persen kunci kriptografi dikompromikan dan dicabut.
5. Jumlah hak akses dasar, dicabut, reset atau diubah.

b. DS11 *Manage Data* (mengelola data)

Manajemen data yang efektif memerlukan identifikasi persyaratan data. proses pengolahan data juga mencakup pembentukan prosedur yang efektif untuk mengelola media libaray, backup dan pemulihan data, sertamedia pembuangan yang tepat. Pengelolaan data yang efektif membantu memastikan kualitas, ketepatan waktu dan ketersediaan data bisnis.

Proses TI kontrol dengan mengelola data yang membantu mengoptimalkan penggunaan informasi dan memastikan informasi tersdia seperti yang dibutuhkan. DS11 befokus pada pemeliharaan kelengkapan, keakuratan, ketersediaan dan perlindungan data. keberhasilan proses ini tercapai dengan melakukan *backup* daya dan ujicoba proses pemulihan, memelihara penyimpanan dan *onsite* dan *offsite* serta penghapusan data dan peralatan secara aman.

Proses ini diukur dengan tingkat kepuasan user dengan ketersediaan data (persen), tingkat pemulihan data yang berhasil (persen) dan jumlah insiden dimana data sensitif diambil setelah media dibuang.

DS11 terdiri dari:

1. DS11.1: Persyaratan Bisnis untuk Manajemen Data (*Business Requirements for Data Management*)

   Melakukan verifikasi bahwa semua data yang diharapkan untuk pengolahan diterima dan diproses secara lengkap, akurat, tepat waktu serta seluruh output yang dikirim sesuai dengan kebutuhan bisnis, mendukung *restart* dan pengolahan kebutuhan.

2. DS11.2: Penyimpanan dan Pengaturan Retensi (*Storage and Retention Arrangements*)

   Menetapkan dan menerapkan prosedur untuk penyimpanan data secara efektif dan efisien, retensi serta pengarsipan untuk memenuhi tujuan bisnis, kebijakan keamanan organisai dan persyaratan peraturan.

3. DS11.3: Sistem Manajemen *Media Library (Media Libray Management system)*

   Menetapkan dan menerapkan prosedur untuk menjaga inventarisasi media penyimpanan dan pengarsipan kegunaan (*usability*) dan integritas.

4. DS11.4: Pembuangan (*Disposal*)

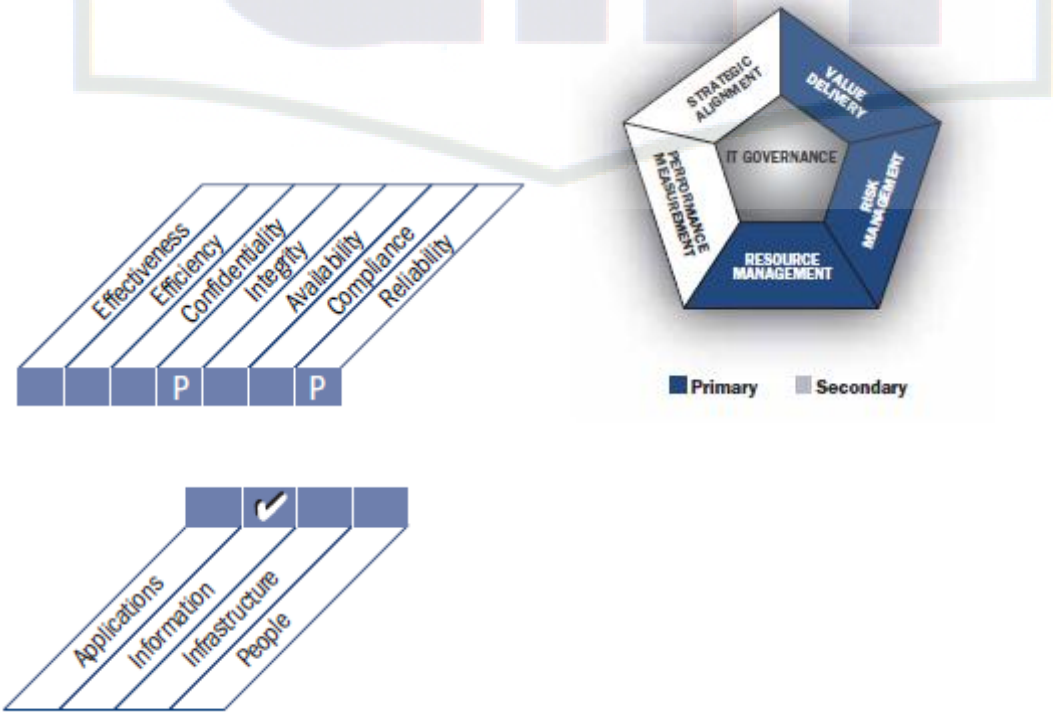
   Menetapkan dan menerapkan prosedur untuk memastikan bahwa persayaratan bisnis untuk perlindungan data sesnsitif dan software terpenuhi ketika data dan perangkat keras dibuang atau dialihkan.

5. DS11.5: *Backup* dan Pemulihan Sistem (*Backup and Restoration*)

   Menetapkan dan menerapkan prosedur untuk backup dan pemulihan sistem, aplikasi, data dan dokumentasi sesuai dengan kebutuhan bisnis dan rencana kesinambungan.

6. DS11.6: Persyaratan Keamanan untuk Manajemen Data (*Security Requirements for Data Management*)

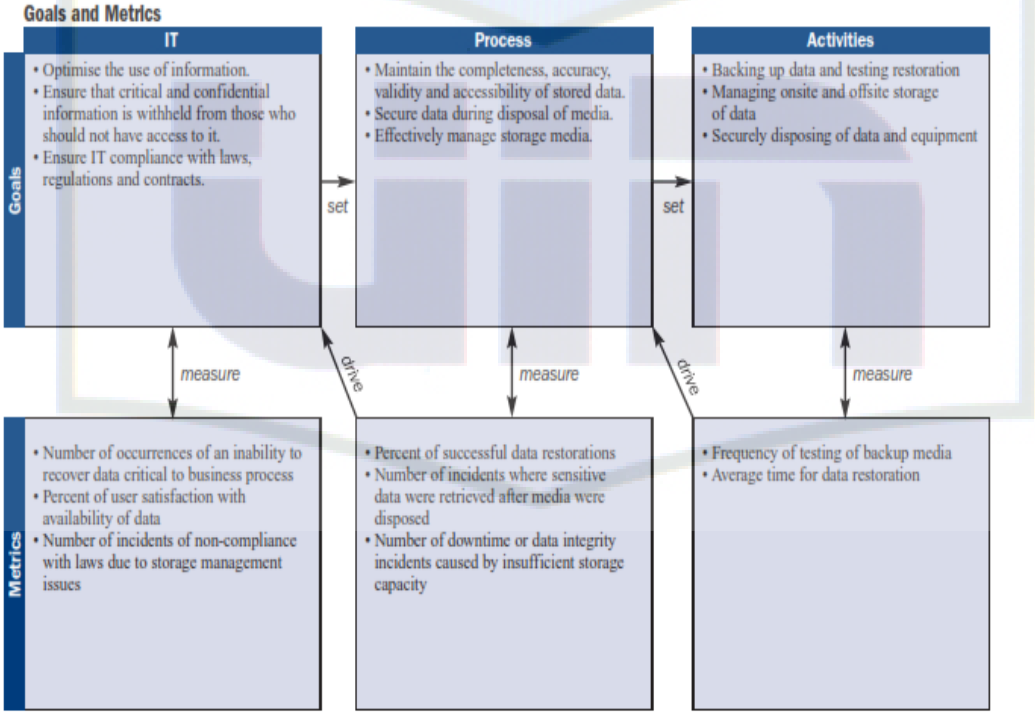
   Menetapkan dan mengimplementasikan kebijakan dan prosedur untuk mengidentifikasi dan menerapkan persyaratan keamanan yang berlaku untuk penerimaan, pengolahan, penyimpanan dan output data untuk memenuhi tujuan bisnis, kebijakan keamanan organisasi dan peraturan.



Gambar 2.6: Standar Informasi, jenis dan fokus area yang didukung DS10 (COBIT 4.1, ITGI, 2007)

Gambar 2.6 menjelaskan bahwa standar informasi *primary* itu *confidentiality* dan *realibility*. jenid fokus area yang didukung adalah *informations* dan berfokus pada *risk management, value delivery* dan *resource management*.

Dengan menerapkan DS11 maka akan memelihara integritas dan kepercayaan. DS11 berfokus pada informasi. Sasaran proses ini terutama mendukung *value delivery, resource management* dan *risk management.*



Gambar 2.7 : Sasaran Metrik DS10 (COBIT 4.1, ITGI, 2007)

Gambar di atas menjelaskan tujuan aktivitas dapat dipandang sebagai *Critical Success Factor* (CSF) yang meliputi tujuan berikut:

1. Melakukan *back-up* data dan menguji restorasi.
2. Mengelola penyimpanan data *onsite* dan *offsite*.
3. Melakukan penghapusan data dan peralatan secara aman.

Untuk dapat menilai atau mengukur seberapa baik aktivitas di atas telah dilaksanakan, sebagai suatu bentuk transfaransi dalam pengawasan, maka didefinisikan *Performance Indicators*:

1. *Frekuensi* terhadap pengujian *backup* media.
2. Waktu rata-rata untuk restorasi data.

2.5 Call Center ESQ

Call center merupakan aplikasi berbasis *web based* yang di gunakan oleh tim telemarketing, tim telecorporate, *finance*, dan BM.

1. Tim telemarketing menggunakan *call center* utuk *call* dan registrasi *customer* yang akan mengikuti training.
2. Tim telecorporate menggunakan *call center* untuk *registrasi customer* yang akan mengikuti *training*.
3. *Finance* untuk memvalidasi pembayaran *training*.
4. BM (*Branch Manager*) untuk monitoring jumlah peserta yg mengikuti *training* dan jumlah *call/day* yang di *call* oleh tim *telemarketing*.

Keuntungan menggunakan sistem *call center* diantaranya:

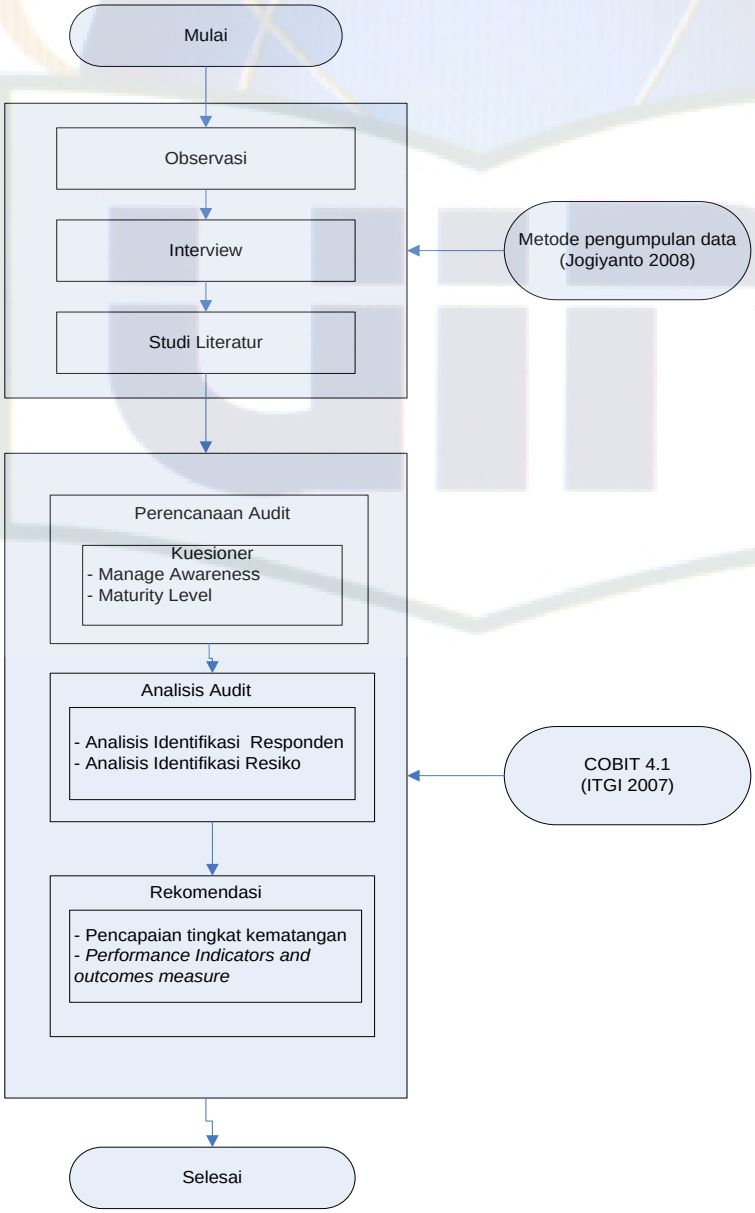
a. Bersifat *web based* seluruh kantor cabang dapat terintegrasi dalam hal melihat jumlah peserta *training.*
b. Data tersimpan lebih baik di server *call center* terhubung dengan media EMS (*Event Management System*).

BAB III

METODOLOGI PENELITIAN

3.1 Kerangka Berpikir Penelitian

Kerangka berpikir yang digunakan dalam penelitian ini adalah sebagai berikut:



Gambar 3.1 Kerangka Berpikir Penelitian

3.2 Metode Pengumpulan Data

Beberapa teknik pengumpulan data yang digunakan dalam penelitian ini di antaranya:

3.2.1 Metode Observasi

Melalui pengamatan secara langsung atau observasi yang dilakukan di perusahaan guna mendapatkan data yang dimaksud. Mengamati proses kerja *call center* dari mulai login ke sistem *call center* sebagai *agent*, melihat *reminder costumer* yang akan dihubungi, kemudian melakukan *out-going call*. *Call center* bisa juga dilakukan untuk *registrasi training* (pelatihan). Observasi dilakukan pada tanggal 24 Mei 20011 di Walroom Menara 165. (Lampiran 1)

3.2.2 Metode Wawancara

Wawancara dilakukan dengan Kepala ICT Bayu Kelana, Budi *agent call center* dan Ajeng Pranindya sebagai bisnis analis. Masing-masing diajukan beberapa pertanyaan untuk memperjelas area yang akan diaudit. Hasil wawancara tahap pertama diketahui tentang seputar proses bisnis call center yang digunakan oleh tim telemarketing, tim telecorporate, *finance dan branch mnager*. Untuk pengelolaan data sudah lengkap prosedur *restore* dan *backup*. Keamanan sistem menggunakan firewall. Mengetahui proses *call* pada sistem *call center* berbasis web. Bukti referensi yang terkait dengan hasil wawancara pun disamakan. Jika hasil wawancara dan bukti referensi tidak sesuai maka ditanyakan lagi wawancara kedua untuk validasi menentukan kebenaran. (Lampiran 5).

3.2.3 Studi Literatur Sejenis

Studi Literatur Sejenis dilakukan untuk menambah referensi teori-teori yang di perlukan dalam penelitian dengan cara membaca dan mempelajari literatur yang mendukung penelitian ini, pada penelitian ini menggunakan referensi beberapa jurnal, skripsi dan thesis yang membahas mengenai Audit sistem informasi, tata kelola teknologi informasi, COBIT dan *call center*. Beberapa referensi digunakan di antaranya thesis (Putra, 2002) berjudul "Penerapan Audit Sistem Informasi Untuk Mengevaluasi Sistem *Call Center* Studi Kasus PT. BCA Tbk " dan jurnal-jurnal yang telah disebutkan pada latar belakang.

3.2.4 *Framework* Audit Sistem Informasi

3.2.4.1 COBIT *Framework*

COBIT mengintegrasikan praktik-praktik yang baik mengelola teknologi informasi dan menyediakan kerangka kerja untuk tata kelola teknologi informasi yang dapat membantu pemahaman dan pengelolaan risiko serta memperoleh keuntungan terkait dengan teknologi informasi. Hanya pada domain *deliver and support* yang diteliti pada fokus area DS5 (*ensure security system*) dan DS11 (*Manage data*).

3.2.4.2 Metode Kuesioner

Kumpulan pertanyaan dibuat berdasarkan panduan dari buku "Implementasi Tata kelola Teknologi Informasi" dan COBIT 4.1. Penyebaran

kuesioner dilakukan pada 24 Mei 2011 sesuai dengan analisis responden RACI Chart.

3.2.4.2.1 Kuesioner I *Management Awareness*

Kuesioner ini dikembangkan untuk dapat mengidentifikasi beberapa ancaman dan kerentanan/kelemahan terhadap keberadaan data sebagai aset yang berharga bagi perusahaan. Serta untuk mengidentifikasi kelemahan keamanan sistem yang digunakan oleh perusahaan. Ancaman dan kerentanan tersebut merupakan potensi resiko yang mungkin terjadi pada proses pengelolaan data dan keamanan sistem yang bisa berdampak negatif bagi kelangsungan bisnis perusahaan.

Adapun tujuan secara lebih spesifik terhadap pengembangan survei kuesioner ini adalah untuk dapat memenuhi beberapa hal berikut ini:

1. Memberikan suatu justifikasi yang memadai dalam menetapkan ruang lingkup penelitian yang dilakukan pada proses memastikan keamanan sistem dan mengelola data .
2. Meningkatkan kepedulian (*awareness*) bagi manajemen perusahaan akan potensi resiko beserta implikasi yang akan terjadi bila proses pengelolaan data dan keamanan sistem tidak dilakukan secara efektif.
3. Memahami indikasi adanya kelemahan kontrol dan berbagai ancaman dalam proses pengelolaan data dan keamanan sistem beserta dampaknya.
4. Mengidentifikasi langkah-langkah perbaikan yang diperlukan dalam pengembangan solusi, sehubungan dengan kelemahan kontrol yang ditemukan.

5. Memberikan gambaran tentang strategi untuk dapat mengurangi secara efektif dampak negatif secara tepat.

Objek pertanyaan dalam kuesioner ini, pada prinsipnya dirancang sedemikian rupa sehingga dapat mengakomodasikan beberapa hal yaitu:

1. Tingkat pemenuhan terhadap keseluruhan *detailed control objectives* (DCO).
2. Pencapaian terhadap beberapa indikator kinerja (*Performance Indicators*) maupun indikator tujuan (*Outcome Measures*).

DCO dapat dipandang sebagai suatu kontrol efektif untuk dapat mencapai tujuan, yang didefinisikan dalam COBIT 4.1. Adapun keberadaan (tingkat pemenuhannya) berkaitan langsung dengan upaya pengendalian terhadap kelemahan/kerentanan yang dapat memicu timbulnya ancaman yang berdampak serius pada pencapaian tujuan bisnis. Dengan pertimbangan tersebut maka objek pertanyaan DCO mendapat penekanan untuk selanjutnya dilakukan analisis. Adapun DCO dalam proses DS5 dan DS11 pada COBIT 4.1 yang dirujuk sebagai objek pertanyaan dalam kuesioner ini telah dijelaskan dalam BAB II penelitian ini:

Pengisian kuesioner dilakukan secara mandiri (*self-assessment*) berdasarkan pengetahuan, kesadaran maupun opini dari para responden, menyangkut sejauhmana tingkat pemenuhan kinerja maupun pencapaian yang telah dilakukan. Jawaban pertanyaan menggunakan model pilihan ganda, responden dapat menentukan jawaban dengan memilih salah satu pilihan tingkat kinerja yang dianggap mewakili kondisi yang sesungguhnya, yaitu:

1. **H** untuk kinerja yang dianggap baik.

2. **M** untuk kinerja yang dianggap sedang atau cukup.
3. **L** untuk kinerja yang dianggap kurang atau buruk.

Sedangkan pada kolom komentar, responden dapat memberikan jawaban bebas yang diharapkan dapat diperoleh gambaran mengenai tingkat kemungkinan risiko serta juga akibat/dampak negatif yang dapat terjadi, jika tingkat pemenuhan atas objek pertanyaannya rendah.

3.2.4.2.2 Kuesioner II *Maturity Level*

Kuesioner ini dikembangkan untuk dapat menilai dan mengukur tingkat kematangan untuk memastikan keamanan sistem (DS5) dan proses pengelolaan data (DS11) baik untuk kondisi yang saat ini (*as is*) maupun untuk kondisi yang diharapkan (*to be*). Dengan mengetahui tingkat kematangan tersebut maka beberapa hal yang merupakan tujuan spesifik diharapkan dapat dilakukan, antara lain:

1. Melakukan identifikasi prioritas perbaikan secara komprehensif berdasarkan atribut kematangan yang diperhatikan dalam tahap pengembangan solusi.
2. Melakukan identifikasi kelemahan terkait dengan tingkat atribut kematangan.
3. Menumbuhkan kepedulian terhadap risiko dalam proses pengelolaan data dan memastikan keamanan sistem.

Mempertimbangkan penekanan tujuan pengukuran di atas adalah dalam rangka untuk melakukan identifikasi perbaikan yang dilakukan secara komprehensif maka pada penelitian ini digunakan metode pendekatan yang menilai dan mengukur setiap atribut kematangan dari suatu proses. Berdasarkan

penilaian masing-masing atribut baik yang mencerminkan kondisi *as is* maupun *to be*, akan didapatkan informasi dan interpretasi untuk setiap atribut. Dengan cara penyajian secara bersama-sama antara *as is* dan *to be* akan memudahkan untuk melihat secara jelas adanya kesenjangan (*gap*) yang dapat diinterpretasikan sebagai kelemahan dan peluang dari setiap atribut.

Mengacu pada COBIT 4.1 maka penilaian dan pengukuran tingkat kematangan proses untuk memastikan keamanan sistem dan pengelolaan data dilakukan dengan mempertimbangkan 6 (enam) atribut model kematangan yang meliputi:

1. Kepedulian dan komunikasi (*awareness and communication/AC*).
2. Kebijakan, standar dan prosedur (*policies, standards and procedures/ PSP*).
3. Perangkat bantu dan otomatisasi (*tools and automations/TA*).
4. Keterampilan dan keahlian (*skills and expertise/SE*).
5. Pertanggungjawaban internal dan eksternal (*responsibility and accountability/RA*).
6. Penetapan tujuan dan pengukuran (*goal setting and measurement/GSM*).

Pengembangan objek pertanyaan maupun pilihan jawaban dalam kuesioner ini, dilakukan dengan melakukan beberapa tahapan penting berikut:

a. Dekomposisi deskripsi dari setiap tingkat kematangan pada DS5 dan DS11, ke dalam beberapa pertanyaan dengan merealisasikan dengan atribut kematangan pada tabel 3.1 dan Tabel 3.2
b. Melengkapi hasil langkah (1), dengan melakukan penelaahan lebih lanjut untuk dapat mendefinisikan suatu pernyataan kematangan sedemikian rupa

sehingga dapat mempresentasikan keseluruhan atribut pada semua tingkat kematangan.

c. Menuangkan hasil langkah (2) kedalam sel-sel dalam matriks atribut kematangan.

d. Mentranslasikan hasil langkah (3) kedalam bentuk pertanyaan dan pilihan jawaban kuesioner.

Tabel 3.1 berikut ini adalah menjelaskan deskripsi model kematangan dalam pernyataan proses DS5.

Tabel 3.1 Deskripsi model kematangan ke dalam pernyataan proses DS5

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
1	*0 Non-Existent*	- Organisasi mengetahui kebutuhan akan keamanan TI. - Tanggung jawab dan akuntabilitas dilakukan untuk memastikan keamanan. - Ukuran untuk mendukung manajemen keamanan TI diimplementasikan. - Adanya pelaporan keamanan TI dan proses tanggapan untuk pelanggaran keamanan TI. - Apakah kekurangan akan proses administrasi keamanan sistem diketahui.
2.	*1 initial/Ad Hoc*	- Organisasi mengetahui kebutuhan keamanan TI. - Kesadaran akan kebutuhan untuk keamanan tergantung pada masing-masing individu. - Keamanan TI dilaksanakan berdasarkan reaksi atas permasalahan. - Keamanan TI terukur. - Pelanggaran keamanan TI yang terdeteksi menyebabkan saling melempar tanggung jawab karena tidak jelasnya pelimpahan pelaksana. - Tanggapan terhadap pelanggaran TI dapat diprediksi.
3	2 *Repeatable but intuitive*	- Tanggung jawab dan akuntabilitas akan keamanan TI ditugaskan kepada seorang koordinator keamanan TI, walaupun kewenangan pengelolaan koordinator tersebut dibatasi.

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
		- Kesadaran akan kebutuhan keamanan dipecah-pecah dan dibatasi. - Analisis terhadap hasil informasi yang relevan terhadap keamanan yang dihasilkan oleh sistem. - Layanan dari pihak ketiga memenuhi kebutuhan keamanan organisasi. - Kecukupan peralatan dan keahlian dalam pengembangan kebijakan keamanan. - Pelaporan keamanan TI yang lengkap, berhubungan dan terarah. - *Training* keamanan telah tersedia tetapi - pelaksanaannya tergantung pada masing-masing orang. Keamanan TI dilihat sebagai sebuah tanggung jawab dari pihak TI dan pihak bisnis melihat bahwa keamanan TI sebagai bagian dari areanya.
4	3 *Defined Process*	- Kesadaran akan keamanan telah ada dan dipromosikan oleh manajemen. - Prosedur keamanan TI telah didefinisikan dan sejalan dengan kebijakan keamanan TI. - Tanggung jawab keamanan TI telah ditugaskan dan dimengerti dan dijalankan secara konsisten. - Sebuah rencana dan solusi keamanan TI ada karena adanya analisis risiko. - Pelaporan keamanan mencakup fokus bisnis yang jelas. - Testing keamanan ad hoc (misal testing penyusupan) telah dilakukan. - *Training* keamanan telah tersedia untuk TI dan bisnis tetapi hanya dijadwalkan dan diatur secara informal.
5	4 *Managed and measurable*	- Tanggung jawab untuk keamanan TI telah ditugaskan secara jelas, teratur dan dijalankan. - Analisis risiko dan dampak keamanan TI dilakukan secara konsisten. - Kebijakan dan praktik dari keamanan dilengkapi dengan *baseline* keamanan tertentu. - Pengungkapan metode untuk mempromosikan kesadaran akan keamanan dianggap penting. - Identifikasi pengguna, otentifikasi dan otorisasi terstandar.

		- Sertifikasi keamanan disarankan untuk staf yang bertanggung jawab untuk audit dan manajemen keamanan.

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
		- *Testing* keamanan dipenuhi menggunakan standar dan proses yang formal menuju peningkatan tingkat keamanan. - Proses keamanan TI dikoordinasikan dengan seluruh fungsi keamanan organisasi. - Pelaporan keamanan TI dikaitkan dengan tujuan bisnis. - Pelatihan keamanan TI dilakukan baik dalam lingkup TI maupun bisnis. - Pelatihan keamanan TI direncanakan dan diatur agar mampu menanggapi kebutuhan bisnis dan profil risiko keamanan yang telah terdefinisi. - Tujuan dan metrik untuk manajemen keamanan telah didefinisikan tetapi belum diukur.
6	5 *Optimised*	- Keamanan TI adalah tanggung jawab bersama pihak manajemen bisnis dan manajemen TI dan terintegrasi dengan tujuan bisnis keamanan perusahaan. - Kebutuhan keamanan TI didefinisikan dengan jelas, dioptimasi dan dimasukkan dalam rencana keamanan yang telah disetujui. - Pengguna dan pelanggan makin akuntabel dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi pada saat tahap desain. - Insiden keamanan ditangani dengan menanggapi prosedur insiden yang formal yang didukung oleh *tool* yang terotomatisasi. - Penilaian keamanan periodik dilaksanakan untuk mengetahui efektivitas implementasi dari rencana keamanan. - Informasi akan ancaman dan kerentanan secara sistematis dikumpulkan dan dianalisis - Kontrol yang cukup untuk mengurangi resiko telah dikomunikasikan dan diimplementasikan. - *Testing* keamanan, *root cause anlysis* akan risiko, digunakan untuk peningkatan proses

		secara berkelanjutan. - Proses keamanan dan teknologi terintegrasi diseluruh lini perusahaan.
6	5 *Optimised*	- Metrik untuk menajemen keamanan diukur, dikumpulkan dan dikomunikasikan. - Manajemen menggunakan hasil ukuran metrik untuk menyesuaikan rencana keamanan dalam proses peningkatan yang berkelanjutan.

Tabel 3.2 Deskripsi model kematangan ke dalam pernyataan proses DS11

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
1	*1 Non-Existent*	- Data belum diakui sebagai aset dan sumber daya perusahaan. - Tidak ada kepemilikan data atau siapa yang bertanggung jawab dalam pengelolaan data. - Kualitas dan keamanan dapat dikatakan buruk atau tidak ada.
2	2 *Initial/Ad Hoc*	- Organisasi menyadari/mengetahui adanya kebutuhan manajemen data yang akurat. - Menggunakan pendekatan yang *adhoc* untuk menangani kebutuhan keamanan pada manajemen data, belum menggunakan prosedur pendekatan formal, namun pengaturan dalam *backup* atau restorasi dan pengaturan penghapusan telah dilakukan. - Belum ada pelatihan khusus untuk manajemen data. - Tanggung jawab manajemen data tidak jelas.
3	2 *Repeatable but intuitive*	- Adanya kesadaran akan kebutuhan manajemen data. - Kepemilikan data secara umum telah diterapkan. - Kebutuhan keamanan pada manajemen data telah didokumentasikan masih secara perorangan.

		- Aktivitas pengawasan terhadap manajemen data telah dilakukan terutama pada aktivitas penting seperti *backup*, restorasi dan penghapusan.

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
		- Penanggung jawab atas manajemen data secara informal telah ditetapkan.
4	3 *Defined Process*	- Kebutuhan manajemen data untuk teknologi informasi dan organisasi secara keseluruhan telah dipahami dan diterima. - Tanggung jawab dan kepemilikan data telah ditetapkan dan permasalahan integritas dan keamanan data dikendalikan oleh pihak yang bertanggung jawab. - Prosedur manajemen data diformalkan - Digunakan beberapa *tools* untuk keperluan *backup*/restorasi serta penghapusan peralatan/media. - Pengawasan terhadap manajemen data telah diakukan dan telah didefinisikan pengukuran kinerja dasar. - Pelatihan bagi staf manajemen data mulai dilakukan. -
5	4 *Manage and Measurable*	- Kebutuhan bagi manajemen data dipahami dan tindakan yang diperlukan sudah diterima di organisasi. - Tanggung jawab kepemilikan dan manajemen data didefinisikan secara jelas, ditetapkan dan dikomunikasikan dalam organisasi. - Prosedur-prosedur telah diformalkan dan dikenal secara luas serta dilakkan *sharing* terhadap *knowledge.* - Penggunaan *tools* terkini telah mulai dimanfaatkan. - Indikator pencapaian tujuan dan kinerja telah disepakati pengguna dan dimonitor dengan proses yang telah didefinisikan - Pelatihan formal terhadap staf manajemen data telah dilakukan.
6	5 *Optimised*	- Kebutuhan manajemen data dan

		pemahamannya atas langkah yang diperlukan telah dipahami dan diterima di organisasi.

No	Tingkat Kematangan	Deskripsi Pernyataan Kematangan
		- Keperluan dan kebutuhan kedepan senantiasa digali secara proaktif. Peluang bagi perbaikan dan penyempurnaan terus digali. - Tanggung jawab kepemilikan data dan manajemen data ditetapkan secara jelas, diketahui secara luas di organisasi serta di diperbaharui secara periodik. - Prosedur diformalkan dan disosialisasikan serta *sharing knowledge* menjadi praktik yang harus dilakukan. - Perangkat bantu yang canggih digunakan dengan otomasi manajemen data maksimal. - Indikator pencapaian tujuan dan kinerja telah disepakati oleh pengguna, dikaitkan dengan tujuan bisnis dan secara konsisten dimonitor menggunakan proses yang telah didefinisikan. Pelatihan untuk staf manajemen data telah dilembagakan.

Dengan mengacu pada tabel 3.1 dan tabel 3.2 tersebut, pertanyaan maupun pilihan jawaban dalam kuesioner ini dikembangkan. Untuk mempermudah responden dalam menjawab maka kuesioner ini didisain dalam format pilihan ganda yang terdiri dari 12 pertanyaan. Pertanyaan-pertanyaan dikelompokan menurut atribut kematangan (6 kelompok pertanyaan) dan pada tiap kelompok pertanyaan akan melibatkan 2 (dua) pertanyaan yang masing-masing berorientasi pada kondisi saat ini dan kondisi yang diharapkan. Masing-

masing pertanyaan mempunyai 6 (enam) pilihan jawaban yang merepresentasikan tingkat kematangan suatu atribut dalam proses DS5 dan DS11.

Seperti pada kuesioner sebelumnya, pada kuesioner ini responden pun memberikan salah satu jawaban secara mandiri (*self assessment)* yang dianggap paling bisa mewakili kondisi kematangan baik saat ini maupun yang diharapkan terkait dengan atribut kematangan tertentu dalam proses memastikan keamanan sistem dan proses pengelolaan data. Dengan mengetahui posisi kematangan saat ini dan yang diharapkan, selanjutnya akan dilakukan analisis dan kajian yang diharapkan dapat menjadi dasar dalam pendefinisian solusi yang diusulkan dalam rangka perbaikan yang diperlukan dalam proses memastikan keamanan sistem dan pengelolahan data untuk *call center* di ESQ LC.

BAB IV

ANALISIS DAN PEMBAHASAN

4.1 Gambaran Umum Objek Penelitian

4.1.2 Sejarah PT. Arga Bangun Bangsa (*ESQ Leadership Center*)

PT Arga Bangun Bangsa (ESQ LC) adalah lembaga *training* sumber daya manusia yang bertujuan membentuk karakter melalui penggabungan 3 potensi manusia yaitu kecerdasan intelektual, emosional, dan spiritual. Selama ini, ketiga potensi tersebut terpisah dan tidak didayagunakan secara optimum untuk membangun sumber daya manusia. Akibatnya, terjadi krisis moral dan *split personality* yang berdampak pada turunnya kinerja. Lebih buruk lagi, mereka menjadi manusia yang kehilangan makna hidup serta jati dirinya.

Training ESQ adalah solusi untuk menjawab permasalahan tersebut dengan menggunakan metode spiritual *engineering* yang komprehensif serta berkelanjutan. Melalui *training* ESQ, ketiga potensi manusia digabungkan dan dibangkitkan sehingga terbentuk karakter yang tangguh, kompetensi secara total dan peningkatan produktivitas sekaligus melahirkan kehidupan yang bahagia dan penuh makna .

Setelah 10 tahun berdiri, sejak 16 Mei 2000, ESQ LC telah menjadi salah satu lembaga pelatihan sumber daya manusia terbesar di Indonesia. Setiap bulan terselenggara rata-rata 100 *even training* di dalam maupun luar negeri, dan menghasilkan alumni per bulan rata-rata 10.000-15.000 orang. Sampai dengan saat ini, telah terselenggara lebih dari 5.000 *training* (data per Nopember 2010)

dengan total alumni lebih dari 1 juta orang (data per Nopember 2010). Untuk melaksanakan itu semua, ESQ LC saat ini didukung lebih dari 500 orang karyawan.

Sejak tahun 2006, mulai diselenggarakan *training* di luar negeri seperti Malaysia, Brunei, Singapura, Belanda, Amerika Serikat, dan Australia. Tahun 2009, beberapa negara lainnya seperti Jepang, Dubai, Mesir pun menunggu untuk terselenggaranya *training* ESQ. Khusus di Malaysia, sejak bulan April 2007 secara resmi dibuka cabang ESQ di Malaysia.

Training ESQ bukan hanya ditujukan bagi kalangan dewasa namun juga bagi mahasiswa, remaja dan anak-anak, sebagai generasi penerus masa depan yang harus diselamatkan. Menyadari akan tanggung jawab sosialnya, ESQ LC bekerjasama dengan Forum Komunikasi Alumni ESQ telah melaksanakan berbagai program bagi masyarakat dan salah satu diantaranya adalah training cuma-cuma bagi 95.981 (data per Mei 2010) guru di seluruh Indonesia. Tujuannya, agar para guru memiliki kecerdasan emosional dan spiritual disamping kecerdasan intelektual dan membangun ketiga kecerdasan tersebut pada para siswa. Program tersebut akan terus digulirkan hingga target minimum 1 juta orang guru tercapai pada tahun 2020.

Gambar 4.1 Logo ESQ *Leadership Center*

4.1.2 Visi, Misi & Nilai

4.1.2.1 Visi

Visi dari ESQ LC adalah:

"Terciptanya Peradaban Emas melalui The ESQWay 165".

4.1.2.2 Misi

Misi dari ESQ LC adalah:

"Menyebarkan dan menjadikan The ESQWay 165 sebagai jalan hidup terbaik di muka bumi".

4.1.2.3 Nilai

7 BUDI UTAMA

Jujur

Tanggung jawab

Visioner

Disiplin

Kerjasama

Adil

Peduli

4.1.3 Struktur Organisasi

Gambar 4.2 Struktur Organisasi ESQ *Leadership Center*. (Lampiran 2)

4.2 Perencanaan Audit

Berdasarkan hasil pengumpulan data, rencana audit yang akan dilakukan pada domain *deliver and support* dari *framework* COBIT pada DS5 dan DS11 untuk mengetahui apakah sistem keamanan sudah diterapkan sesuai dengan prosedur yang ada dan pada pengelolaan data untuk mengetahui apakah data yang masuk, diolah dengan benar dan menghasilkan *output* yang diinginkan.

Data dalam jumlah yang besar diperlukan pengelolaan yang benar agar menghasilkan *output* yang diinginkan dan menguntungkan bagi perusahaan ataupun orang-orang yang terlibat di area itu sendiri. Karena bagaimana pun informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa sudah berada di sebuah *"information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi. Keamanan sistem merupakan salah satu aspek yang penting dari sebuah sistem informasi. Untuk mengetahui keamanan sistem yang ada sudah melindungi sistem secara aman atau belum maka dilakukan audit.

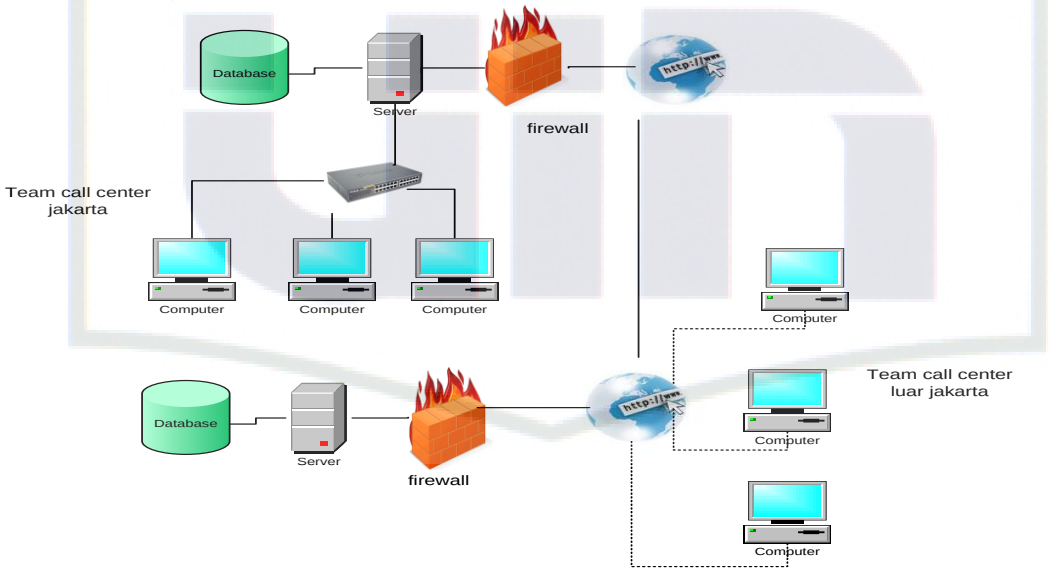
4.2.1 Sistem *Call Center*

Untuk mengetahui objek yang akan diaudit yaitu *call center*, maka diperlukan pengetahuan mengenai proses bisnis dan arsitektur *call center* itu sendiri. Dengan mengetahui sistem *call center* secara keseluruhan maka dapat diketahui bagian mana saja yang mendapat perhatian karena sifatnya yang kritis

dan juga bisa diketahui apakah secara sistem, arsitektur tersebut sudah dapat memenuhi *level* objektif yang diinginkan.

Proses bisnis akan memperlihatkan prosedur-prosedur yang dilakukan dalam sitem *call center*. Sehingga dengan mengatahui proses bisnisnya dapat diketahui prosedur yang dilakukan sudah benar atau belum benar.

4.2.2 Arsitektur *Call Center*

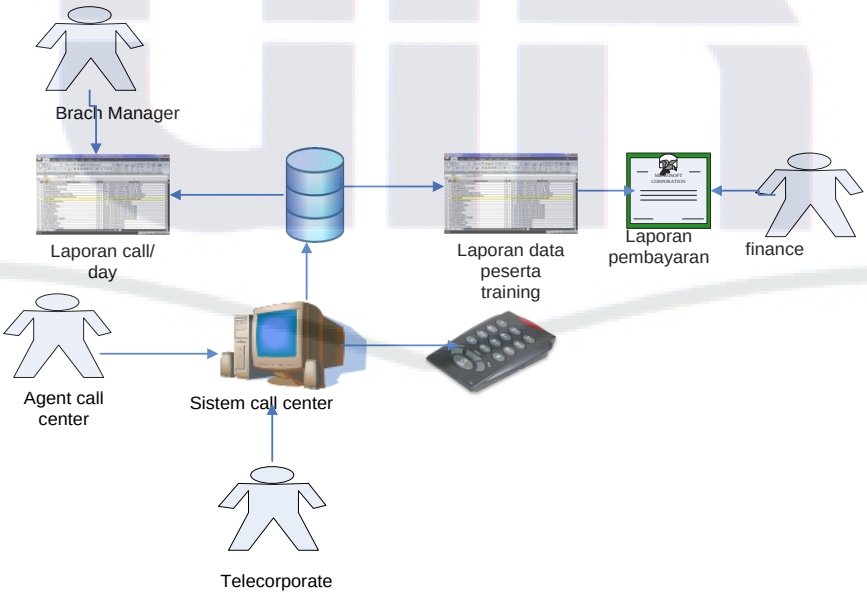


Gambar 4.3 Arsitektur *call center*

Call center merupakan aplikasi berbasis web yang di gunakan oleh tim telemarketing, tim telecorporate, finance, dan BM (*Branch Manager*) untuk menjalankan fungsi bisnis sesuai dengan tanggung jawabnya. 9 orang jumlah BM (*Branch Manager*). Jumlah telecorporate dan telemarketing ada 150 orang baik yang dipusat ataupun di cabang. Ada 12 *agent call center* yang melakukan *call/day.*

Ada 2 server yang digunakan untuk mengolah data lokal (jakarta) dan cabang (daerah). Server untuk mengolah data lokal terdapat di ESQ LC pondok pinang sedangkan server untuk menangani data daerah terdapat di gedung cyber yang terletak di Jl. Kuningan Barat No. 8 Jakarta Selatan. Jaringan yang digunakan adalah *Firstmedia*. Untuk kontrol akses keamanannya menggunakan *firewall*.

4.2.3 Proses Bisnis *Call center*



Gambar 4.4 Proses Bisnis *Call center*

Proses bisnis *call center* dimulai ketika agent *call center* melakukan *call* berdasarkan data pribadi, data alumni peserta *training*, data referensi dari alumni. *Telemarketing* sama dengan *agent call center* menggunakan *call center* untuk *call* dan registrasi peserta yang akan mengikuti *training*. *Telecorporate* menggunakan

sistem *call center* untuk registrasi peserta *training*. *Finance* untuk memvalidasi pembayaran *training* dan BM (*Branch Manager*) untuk monitoring banyaknya peserta yang mengikuti *training* dan banyaknya jumlah *call/day* yang di *call* oleh tim *telemarketing*.

4.3 Analisis Audit

4.3.1 Analisis Identifikasi Responden

Analisis identifikasi responden dilakukan dengan secara konsisten mengacu pada diagram Responsible, Accountable, Consulted and/or Informed (RACI) seperti didefinisikan pada COBIT 4.1 khususnya pada proses DS5 dan DS11. Peran-peran yang didefinisikan pada diagram RACI, sebagai pemangku utama (*key stakeholder*) yang terkait secara langsung pada proses DS5 dan DS11 tersebut, selanjutnya diinterpretasikan (dipetakan) pada fungsional struktur di PT. Arga Bangun Bangsa (ESQ *Leadership Center*) seperti diperlihatkan pada tabel 4.1 dan tabel 4.2 yang melibatkan fungsi teknologi informasi maupun teknologi informasi.

Dengan analisis identifikasi responden yang mengacu pada diagram RACI tersebut, maka sampling atau identifikasi responden diarahkan pada peran-peran yang terkait langsung dan representatif pada proses DS5 dan DS11. Sehingga diharapkan jawaban atas kuesioner mempunyai validitas yang memadai dan diharapkan dapat mewakili keadaan sesungguhnya dilapangan. Adapun jumlah responden yang teridentifikasi dalam pengisian kuesioner ini adalah

sebanyak 10 responden untuk DS5 dan 6 responden untuk DS 11 seperti dirinci pada tabel 4.1 dan tabel 4.2.

Tabel 4.1 Identifikasi RACI Chart DS5

No	Fungsional struktur COBIT terkait		Fungsional struktur PT. ABB (ESQ LC)		Jumlah
1	Chief Exekutif Officer	CEO	President Director	TI	1
2	Chief Financial Officer	CFO	Finance and Administration Director	Non TI	1
3	Business Excecutive	BE	Business Unit Director	TI	1
4	Chief Information Officer	CIO	Business Unit Director	Non TI	1
5	Business Process Owner	BPO	Costomer Development Director	Non TI	1
6	Head Operation	HO	Information and Communication Dept Head	TI	1
			ICT Developer and Programer	TI	2
7	Compliance, Audit, Risk and security	CARS	Auditor Internal	Non TI	1

Tabel 4.2 Identifikasi RACI Chart DS11

No	Fungsional struktur COBIT terkait		Fungsional struktur PT. ABB (ESQ LC)		Jumlah
1	Chief Information Officer	CIO	Business Unit Director	TI	1
2	Business Process Owner	BPO	Costomer Development Director	Non TI	1
3	Head Operation	HO	Information and Communication Dept Head	TI	1
			ICT Developer and Programer	TI	1
4	Head Development	HD	ICT Developer and Programer	TI	2
			Costumer Development Director	Non TI	1
5	Compliance, Audit, Risk and security	CARS	Auditor Internal	Non TI	1

4.3.2 Analisis Identifikasi Risiko

Analisis identifikasi resiko terhadap pengumpulan data hasil kuesioner I *Management Awareness* untuk memastikan keamanan sistem (DS5) dan pengelolaan data (DS11). Dari pelaksanaan kuesioner, diperoleh jawaban sebanyak 13 kuesioner yang telah didistribusikan kepada para responden yaitu *ICT Head*, *agent call center* dan *business analyst* untuk mengetahui pemenuhan kinerja, maupun pencapaian yang sekarang berlangsung diperusahaan PT. Arga Bangun Bangsa (ESQ LC) terhadap beberapa objek pertanyaan, baik pemenuhan DCO maupun indikator yang terkait pada proses pengelolaan data secara umum

pada *call center*. Analisis identifikasi resiko terhadap pengumpulan data hasil kuesioner I *Management Awareness* untuk memastikan keamanan sistem (DS5). Untuk menghitung persentase distribusi jawaban menggunakan perhitungan di bawah ini untuk setiap pertanyaan:

$$\mathbf{MA=\ \frac{Jumlah\ nilai\ kinerja\ (jnk\ terdiri\ dari\ L,M,H)}{Jumlah\ responden(jr)}\ x\ 100\%}$$

Keterangan:

MA = hasil untuk setiap pertanyaan

Jnk = jumlah nilai kinerja semua responden pada tiap pertanyaan terdiri dari L,M,H

Jr = jumlah responden yang mengisi kuesioner *Management awareness*

Tabel 4.3 merupakan rekapitulasi jawaban responden kuesioner I *Management Awareness* untuk DS5.

Tabel 4.3 Rekapitulasi jawaban responden kuesioner I *Management Awareness*

No	Objek Pertanyaan	Distribusi Jawaban		
		L (%)	M (%)	H (%)
1	Manajemen keamanan TI	0,00	61,54	38,46
2	Rencana Keamanan IT	0,00	69,23	30,77
3	Komunikasi kebijakan keamanan beserta investasi yang tepat (layanan, personel, *software* dan *hardware*)	7,70	69,23	23,08
4	Konfirmasi hak akses pengguna	7,70	61,54	30,77
5	Manajemen identitas	7,70	38,46	53,85
6	Manajemen akun pengguna	7,70	46,15	46,15
7	Pengujian keamananan, Pengawasan dan Pemantauan	15,38	30,77	53,85
8	Kebutuhan keamanan manajemen data	7,70	61,54	30,77
9	Perlindungan teknologi keamanan	15,38	61,54	23,08
10	Manajemen kunci *kryptografi*	0,00	61,54	38,46
11	*Software* untuk mendeteksi, koreksi program yang berbahaya	0,00	53,85	46,15
12	Keamanan jaringan	0,00	53,85	46,15
13	Pertukaran data sensitif	0,00	53,85	46,15
	Total	**5,77**	**55,77**	**38,46**

Secara umum rekapitulasi hasil kuesioner I *management awareness untuk* DS5 dapat ditarik suatu kecenderungan yang merefleksikan fakta di lapangan yaitu:

1. Sebagian besar responden, **55,77%** responden menyatakan pendapat, opini atau kesadarannya bahwa tingkat kinerja dalam memastikan keamanan sistem adalah **cukup** atau **sedang**.
2. Sebanyak **38,46%** responden mengemukakan pendapatnya bahwa kinerja dalam memastikan keamanan sistem adalah **baik**.

3. Hanya 5,77% responden yang menyatakan bahwa praktik dalam memastikan keamanan sistem **lemah**.

Analisis identifikasi resiko terhadap pengumpulan data hasil kuesioner I *Management Awareness* untuk proses pengelolaan data (DS11).

Tabel 4.4 merupakan rekapitulasi jawaban responden kuesioner I *Management Awareness* untuk DS11.

Tabel 4.4 Rekapitulasi jawaban responden kuesioner I *Management Awareness*

No	Objek Pertanyaan	Distribusi Jawaban		
		L (%)	M (%)	H (%)
1	Kebutuhan bisnis untuk manajemen data		25,00	75,00
2	Pengaturan penyimpanan		33,33	66,67
3	*Media library*		50,00	50,00
4	Penghapusan data/disposal		16,67	83,33
5	*Backup* dan *restore*		50,00	50,00
6	Kebutuhan keamanan manajemen data		41,67	58,33
7	Pengujian terhadap media *backup*	33,33	50,00	16,67
8	Kecepatan proses restorasi		50,00	50,00
9	Keberhasilan proses restorasi		83,33	16,67
10	Keamanan data sensitif setelah *disposal*	8,33	41,67	50,00
11	Penanganan insiden kapasitas penyimpanan		58,33	41,67
12	Keandalan sistem karena proses pemulihan		91,67	8,33
13	Kepuasan pengguna atas ketersediaan data		50,00	50,00
14	Kepatuhan pada aspek hukum/aturan	8,33	66,67	25,00
	Total	**3,57**	**50,60**	**45,83**

Secara umum rekapitulasi hasil kuesioner *management awareness* untuk DS11 terlihat pada tabel 4.4 dapat ditarik suatu kecenderungan yang merefleksikan fakta di lapangan yaitu bahwa:

1. Sebagian besar responden, **50,60%** responden menyatakan pendapat, opini atau kesadarannya bahwa tingkat kinerja dalam proses pengelolaan data adalah **cukup** atau **sedang**.
2. Sebanyak **45,83%** responden mengemukakan pendapatnya bahwa kinerja proses pengelolaan data adalah sudah **baik**.
3. Hanya **3,57%** responden yang menyatakan bahwa praktik pengelolaan data **rendah** atau **kurang baik**.

Deskripsi hasil kajian tentang kinerja proses DS5 dan DS11, khususnya pada pemenuhan kriteria-kriteria dalam proses DS5 dan DS11 yang tertuang dalam DCO, maka dilakukan pemetaan terhadap jawaban kuesioner I dengan nilai kinerja yang mereflesikan secara kuantitatif tingkat kinerjanya, seperti terlihat pada tabel 4.5.

Tabel 4.5 Pemetaan jawaban kuesioner I dan nilai/tingkat kinerja *detailed control objective* (DCO) pada proses DS5 dan DS11.

No	Jawaban	Nilai Kinerja	Tingkat Kinerja
1	L *(low)*	1,00	Kurang
2	M(*midle*)	2,00	Sedang
3	H(*high*)	3,00	Baik

Dengan merujuk dari tabel 4.5 dapat diperoleh nilai kinerja terhadap pemenuhan DCO pada proses DS5 secara kuantitatif yang dapat dilihat pada tabel 4.6.

Nk DCO n=(MAL x nk)+(MAM x nk)+MAH x nk)

Keterangan:

Nk DCO n = nilai kinerja untuk setiap DCO

Nk = nilai kinerja yang telah ditentukan pada tabel 4.3

MAL = merujuk dari hasil *management awareness* untuk kondisi kurang

MAM = merujuk dari hasil *management awareness* untuk kondisi sedang

MAH = merujuk dari hasil *management awareness* untuk kondisi Baik

Tabel 4.6 Tingkat kinerja *detailed control objectives* (DCO) pada proses DS5

No	*Detailed Control Objectives*	Nilai Kinerja
1	Manajemen keamanan TI (DS5.1)	2,38
2	Rencana Keamanan IT (DS5.2)	2,31
3	Manajemen identitas (DS5.3)	2,62
4	Manajemen akun pengguna (DS5.4)	2,85
5	Pengujian keamananan, Pengawasan dan Pemantauan (DS5.5)	2,38
6	Kebutuhan keamanan manajemen data (DS5.6)	2,23
7	Perlindungan teknologi keamanan (DS5.7)	2,18
8	Manajemen kunci kryptografi (DS5.8)	2,38
9	*Software* untuk mendeteksi, koreksi program yang berbahaya (DS5.9)	2,46
10	Keamanan jaringan (DS5.10)	2,46
11	Pertukaran data sensitif (DS5.11)	2,46
	Rata-rata	**2,43**

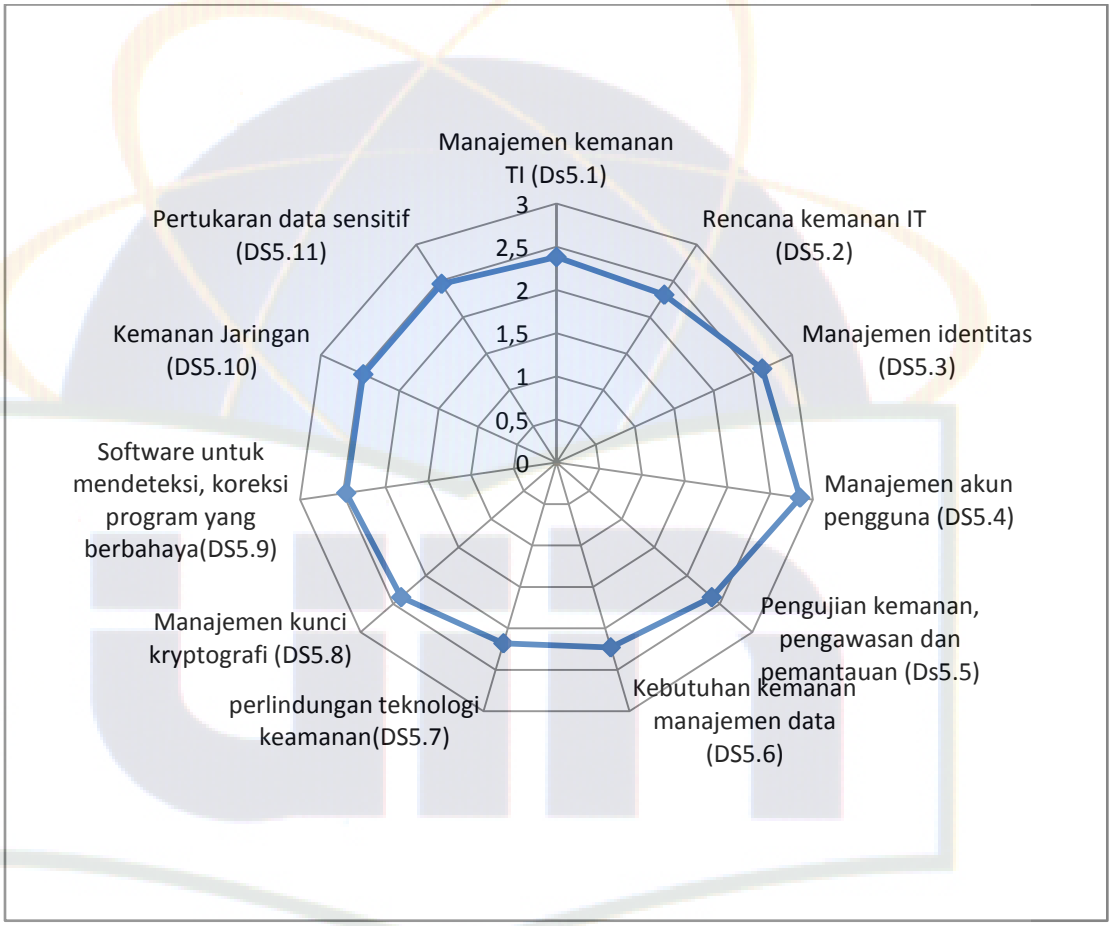
Tingkat pemenuhan DCO pada proses memastikan keamanan sistem mendekati tinggi dengan rata-rata nilai kinerja dalam proses pengelolaan data adalah sebesar 2,43 seperti dipresentasikan dalam diagram radar pada gambar 4.7 Dengan merujuk dari tabel 4.5 dapat diperoleh nilai kinerja terhadap pemenuhan DCO pada proses DS11 secara kuantitatif yang dapat dilihat pada tabel 4.7.

Tabel 4.7 Tingkat kinerja *detailed control objectives* (DCO) pada proses DS11.

No	*Detailed Control Objectives*	Nilai Kinerja
1	Kebutuhan bisnis untuk manajemen data (DS11.1)	2,75
2	Pengaturan penyimpanan (DS11.2)	2,67
3	Media *Library* (DS11.3)	2,5
4	Penghapusan data/disposal (DS11.4)	2,83
5	*Backup* dan *Restore* (DS11.5)	2,5
6	Kebutuhan keamanan manajemen data (DS11.6)	2,58
	Rata-rata	**2,72**

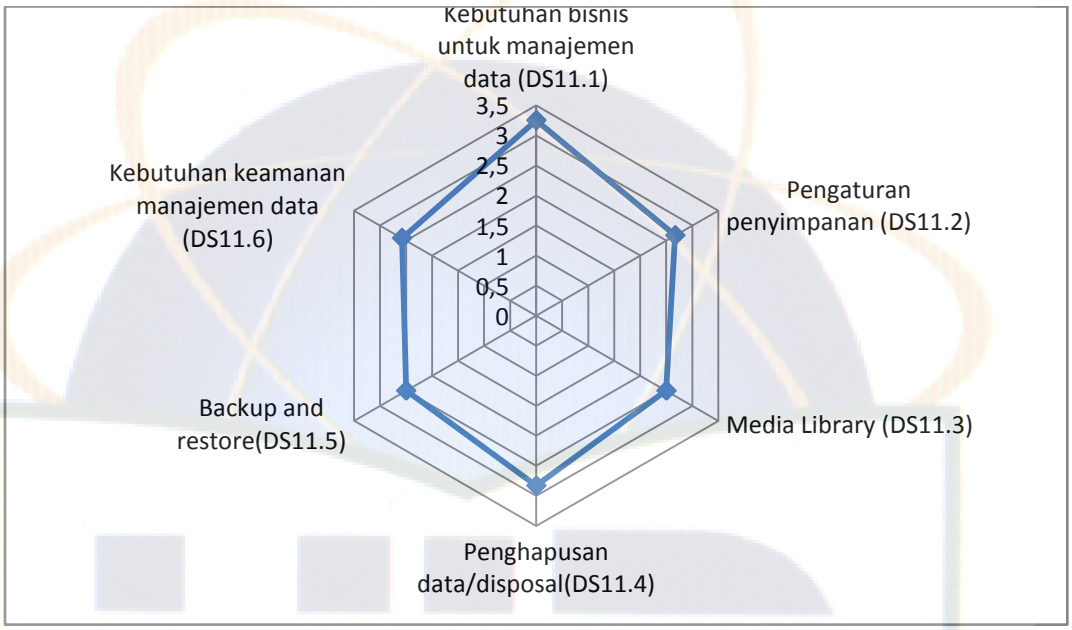
Secara keseluruhan berdasarkan tabel 4.4 dapat ditarik suatu kesimpulan bahwa:

Tingkat pemenuhan DCO pada proses pengelolaan data cukup dan mendekati tinggi dengan rata-rata nilai kinerja dalam proses pengelolaan data adalah sebesar 2,72 seperti dipresentasikan dalam diagram radar pada gambar 4.5.



Gambar 4.5 Representasi tingkat pemenuhan DCO pada proses memastikan keamanan sistem

Secara keseluruhan interpretasi terhadap hasil kuesioner adalah cukup atau sedang dalam proses memastikan keamanan sistem. Ancaman yang kemungkinan berdampak pada keamanan sistem masih bisa ditangani dengan baik. Namun harus ditingkatkan lagi agar tidak menjadi suatu kerentanan (*vulnerability*) bagi munculnya ancaman (*threat*) yang sangat memungkinkan (*probability*) akan berdampak (*impact*) serius pada pencapaian kinerja bisnis perusahaan.



Gambar 4.6 Representasi tingkat pemenuhan DCO pada proses pengelolaan data

Secara umum interpretasi terhadap hasil kuesioner adalah cukup atau sedang dalam proses pengelolaan data. Namun harus ditingkatkan lagi agar tidak menjadi suatu kerentanan (*vulnerability*) bagi munculnya ancaman (*threat*) yang sangat memungkinkan (*probability*) akan berdampak (*impact*) serius pada pencapaian kinerja bisnis perusahaan.

Beberapa ancaman (*threat*) yang mengancam keberadaan data sebagai aset perusahaan. Ancaman terhadap keberadaan data harus diwaspadai karena akan berdampak pada gangguan operasional maupun bisnis. Dampak yang ditimbulkan akibat bencana memerlukan waktu, tenaga dan biaya pemulihannya.

Tabel 4.8 Identifikasi ancaman terhadap keberadaan data

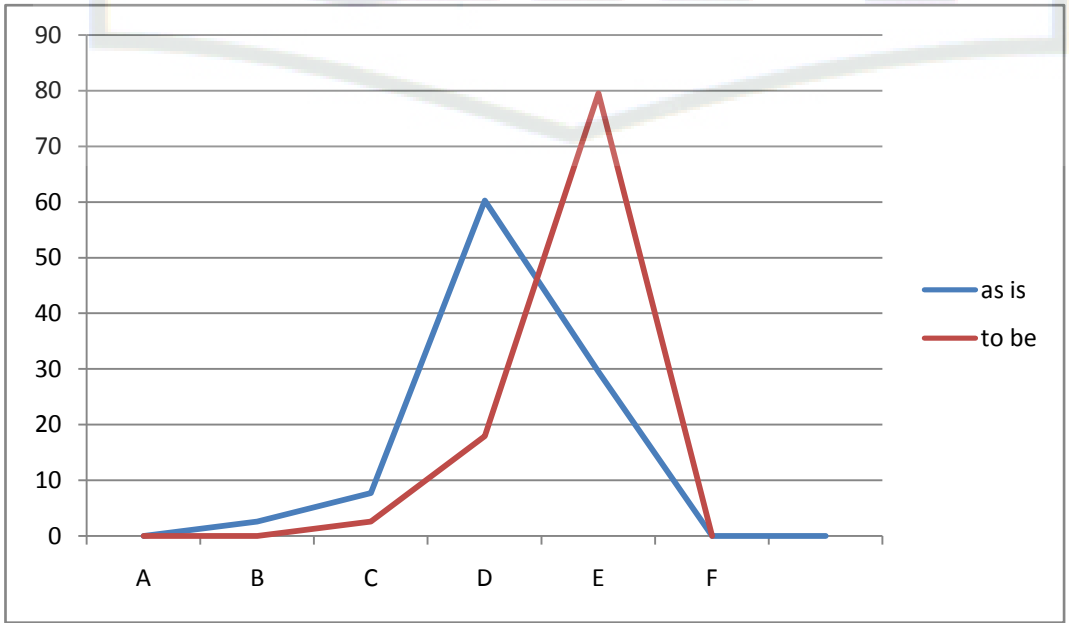
No	Ancaman	Dampak Umum
1.	Bencana Alam Banjir, kebakaran, gempa bumi, petir dan lain-lain.	Membahayakan proses bisnis. Proses bisnis dapat terhenti.
2.	Gangguan yang disengaja Kerusakan, perusakan, pencurian, sabotase, terorisme.	Membahayakan proses bisnis menggangu.
3.	Gangguan utilitas umum Listrik padam, gangguan telekomunikasi	Proses bisnis berjalan dalam kondisi dan perangkat darurat Menggangu
4.	Kerusakan peralatan dan sistem Sistem perangkat lunak, *hardware*, jaringan komputer, gangguan hubung singkat (internal power).	Proses bisnis terhenti Membahayakan proses bisnis Mengganggu
5.	Gangguan keamanan TI Serangan hacker, virus komputer, pencurian data.	Membahayakan proses bisnis Proses bisnis berjalan bukan dalam kondisi normal.
6.	Gangguan lainnya Kerusakan tempat, moral pegawai	Proses bisnis berjalan bukan dalam kondisi normal Membahayakan proses bisnis

4.3.3 Penilaian Tingkat Kematangan

Pelaksanaan kuesioner II *maturity level*, diperoleh jawaban atas kuesioner yang didistribusikan kepada para responden yang sama yaitu *ICT Head, agent call center* dan *business analyst*. Dari hasil jawaban responden tersebut maka dibuatlah suatu rekapitulasi pada tabel dan dinyatakan dalam grafik pada gambar yang secara garis besar dapat memberikan gambaran kecenderungan tingkat kematangan atas beberapa atribut, pada proses pengelolaan data di PT Arga Bangun Bangsa (ESQ LC).

Tabel 4.9 Rekapitulasi distribusi jawaban kuesioner II *Maturity Level* DS5

No	Atribut	Status	Distribusi Jawaban					
			A (%)	B (%)	C (%)	D (%)	E (%)	F (%)
1	AC	As is	0,00	15,38	7,70	23,08	53,85	0,00
		To be	0,00	0,00	15,38	46,15	38,46	0,00
2	PSP	As is	0,00	0,00	30,77	23,08	46,15	0,00
		To be	0,00	0,00	0,00	0,00	100	0,00
3	TA	As is	0,00	0,00	7,70	84,62	7,70	0,00
		To be	0,00	0,00	0,00	7,70	92,30	0,00
4	SE	As is	0,00	0,00	0,00	61,54	38,46	0,00
		To be	0,00	0,00	0,00	38,46	61,54	0,00
5	RA	As is	0,00	0,00	0,00	84,62	15,38	0,00
		To be	0,00	0,00	0,00	7,70	92,30	0,00
6	GSM	As is	0,00	0,00	0,00	84,62	15,38	0,00
		To be	0,00	0,00	0,00	7,70	92,30	0,00
As is			0,00	2,56	7,69	60,26	29,49	0,00
To be			0,00	0,00	2,56	17,95	79,49	0,00



Gambar 4.7 Representasi distribusi jawaban kuesioner II *maturity level* DS5

Secara umum dari rekapitulasi hasil kuesioner II *Maturity Level* pada tabel 4.9 dapat diperoleh suatu kecenderungan fakta di lapangan tentang tingkat

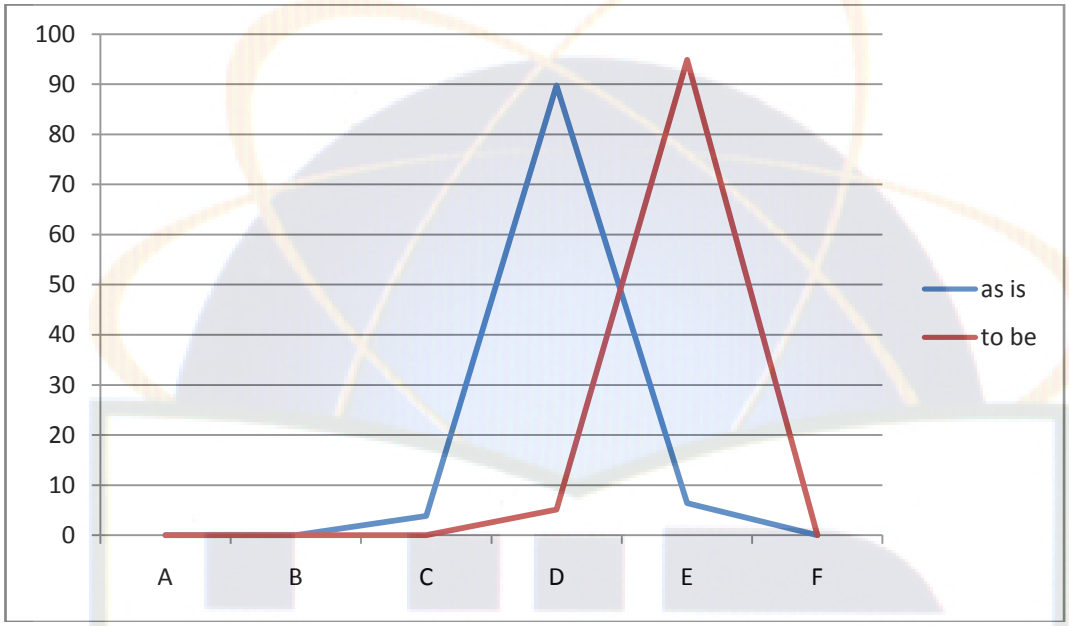
kematangan proses untuk memastikan keamanan sistem baik yang saat ini (*as is*) maupun yang diharapkan (*to be*) sebagai berikut:

1. Sebagian besar responden 60,26% memberikan jawaban "d" atas pertanyaan yang berorientasi masa kini (*as is*).
2. Pada jawaban pertanyaan yang berorientasi masa depan (*to be*) sebagian besar responden 79,49 memberikan jawaban "e".

Adanya pola kecenderungan tersebut ditunjukkan secara lebih jelas pada Gambar 4.6 dimana posisi puncak *as is* melebihi "d" mendekati "e", dan posisi puncak *to be* lebih dekat pada jawaban "e".

Tabel 4.10 Rekapitulasi distribusi jawaban kuesioner II *Maturity Level* DS11

No	**Atribut**	**Status**	**Distribusi Jawaban**					
			A (%)	**B (%)**	**C (%)**	**D (%)**	**E (%)**	**F (%)**
1	AC	As is	0,00	0,00	0,00	100	0,00	0,00
		To be	0,00	0,00	0,00	7.69	92,31	0,00
2	PSP	As is	0,00	0,00	23,08	76,92	0,00	0,00
		To be	0,00	0,00	0,00	15,38	84,62	0,00
3	TA	As is	0,00	0,00	0,00	84,62	15,38	0,00
		To be	0,00	0,00	0,00	0,00	100	0,00
4	SE	As is	0,00	0,00	0,00	84,62	15,38	0,00
		To be	0,00	0,00	0,00	0,00	100	0,00
5	RA	As is	0,00	0,00	0,00	92,31	7,69	0,00
		To be	0,00	0,00	0,00	0,00	100	0,00
6	GSM	As is	0,00	0,00	0,00	100	0,00	0,00
		To be	0,00	0,00	0,00	7,69	92,31	0,00
As is			0,00	0,00	3,85	89,74	6,41	0,00
To be			0,00	0,00	0,00	5,13	94,87	0,00



Gambar 4.8 Representasi distribusi jawaban kuesioner II *maturity level* DS11

Secara umum dari rekapitulasi hasil kuesioner II *Maturity Level* pada tabel 4.10 dapat diperoleh suatu kecenderungan fakta di lapangan tentang tingkat kematangan proses pengelolaan data baik yang saat ini (*as is*) maupun yang diharapkan (*to be*) sebagai berikut:

1. Sebagian besar responden 89,74% memberikan jawaban "d" atas pertanyaan yang berorientasi masa kini (*as is*).
2. Pada jawaban pertanyaan yang berorientasi masa depan (*to be*) sebagian besar responden 94,87 memberikan jawaban "e".

Adanya pola kecenderungan tersebut ditunjukkan secara lebih jelas pada gambar 4.7 posisi puncak responden memberikan jawaban untuk pertanyaan *as is* yaitu "d" yang mendekati "e" dan menajawab "e" untuk kondisi *to be*.

Untuk dapat mendeskripsikan secara jelas hasil analisis dan kajian tentang tingkat kematangan pada masing-masing atribut yang berkontribusi secara langsung pada tingkat kematangan untuk proses memastikan keamanan sistem dan pengelolaan data secara keseluruhan. Dengan mengacu pada model kematangan COBIT tiap pilihan jawaban kuesioner dapat dipetakan seperti terlihat pada tabel 4.11.

Tabel 4.11 Pemetaan jawaban dan nilai/tingkat kematangan

No	Jawaban	Nilai Kematangan	Tingkat Kematangan
1	A	0,00	0 *Non-existent*
2	B	1,00	1 *Initial/Ad Hoc*
3	C	2,00	2 *Repeatable but intuitive*
4	D	3,00	3 *Defined Process*
5	E	4,00	4 *Manage and measurable*
6	F	5,00	5 *Optimised*

Tabel 4.12 Nilai dan tingkat kematangan proses DS5 kuesioner II *maturity level*

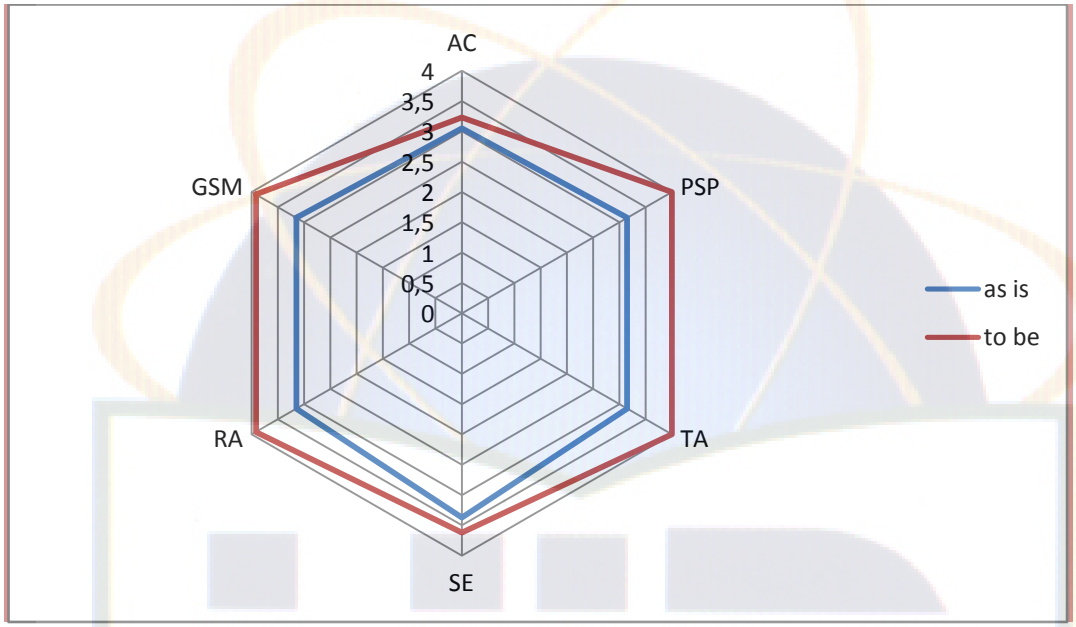
No	Atribut	Nilai Kematangan		Tingkat Kematangan	
		As is	***To be***	***As is***	***To be***
1	**AC**	3,05	3,23	3	3
2	**PSP**	3,15	4,00	3	4
3	**TA**	3,15	4,00	3	4
4	**SE**	3,37	3,62	3	4
5	**RA**	3,15	3,92	3	4
6	**GSM**	3,15	3,92	3	4
Rata-rata		3,17	3,77	3	4

Menurut (Surendro, 2009) pembedaan istilah antara nilai kematangan dan tingkat kematangan. Nilai kematangan bisa bernilai tidak bulat (bilangan pecahan) yang merepresentasikan proses pencapaian menuju suatu tingkat kematangan tertentu. Sedangkan tingkat kematangan lebih menunjukkan tahapan atau kelas yang dicapai dalam proses kematangan yang dinyatakan dalam bilangan bulat.

Keterkaitan antara model kematangan dan beberapa atribut kematangan pada proses memastikan keamanan sistem dan mengacu pada tabel 4.11. Nilai kematangan terhadap atribut kematangan pada tabel 4.12 dapat diperoleh informasi bahwa:

1. Tingkat kematangan saat ini (*as is*) pada proses DS5 secara keseluruhan berada pada tingkat 3 terdefinisi atau *defined.*
2. Tingkat kematangan yang diharapkan (*to be*) pada proses DS 5 secara keseluruhan pada tingkat 4 terkelola atau *managed.*

Kedua kondisi kematangan tersebut untuk masing-masing atribut kematangan secara lebih jelas direpresentasikan pada gambar tersebut terlihat posisi nyata nilai kematangan rata-rata (*as is*) atau (*to be*) untuk tiap atribut kematangan tersebut secara tepat diharapkan akan diperoleh gambaran tentang skala prioritas dan besarnya usaha sebagai suatu prasyarat yang penting dan perlu bagi setiap atribut untuk melakukan perbaikan.



Gambar 4.9 Representasi nilai kematangan pada proses DS5 untuk status kematangan saat ini (*as is*) dan yang akan datang (*to be*).

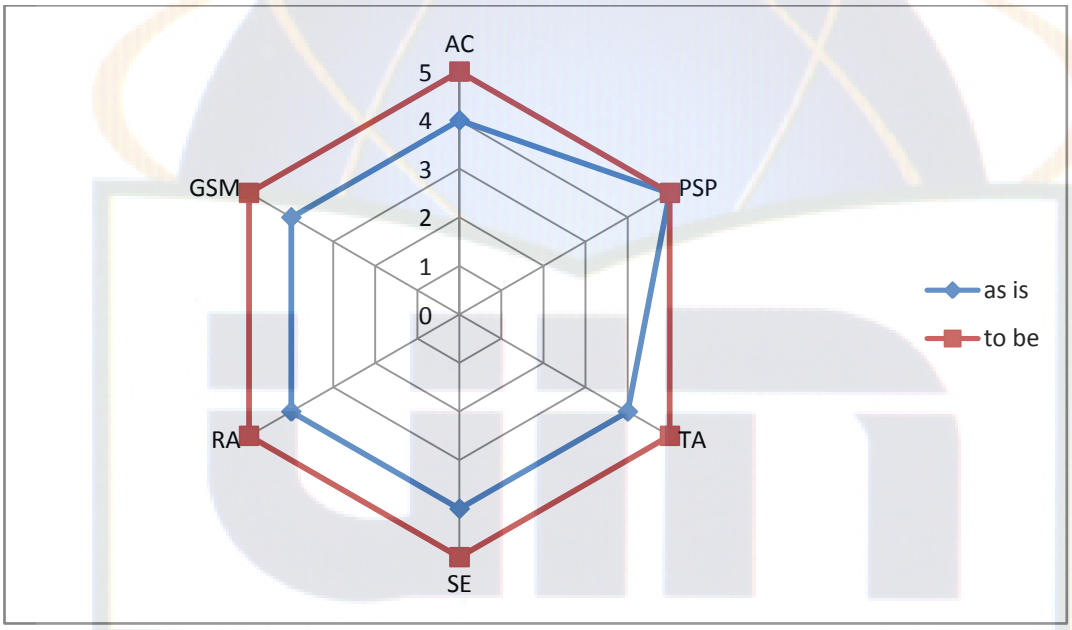
Tabel 4.13 Nilai dan tingkat kematangan proses DS11 kuesioner II *maturity level*

No	Atribut	Nilai Kematangan		Tingkat Kematangan	
		As is	***To be***	***As is***	***To be***
1	**AC**	3,00	3,92	3	4
2	**PSP**	2,77	3,85	3	4
3	**TA**	3,15	4,00	3	4
4	**SE**	3,15	4,00	3	4
5	**RA**	3,10	4,00	3	4
6	**GSM**	3,00	3,92	3	4
Rata-rata		3,03	3,95	3	4

Nilai kematangan pengelolaan data terhadap atribut kematangan pada tabel, maka dapat diperoleh informasi bahwa:

1. Tingkat kematangan saat ini (*as is*), pada proses DS11 secara keseluruhan berada pada tingkat 3 atau terdefinisi proses pengelolaan datanya.

2. Tingkat kematangan yang diharapkan (*to be*), pada proses DS11, secara keseluruhan berada pada tingkat 4 atau terkelola/*managed*.



Gambar 4.10 representasi nilai kematangan pada proses DS11 untuk status kematangan saat ini (*as is*) dan yang akan datang (*to be*).

Untuk dapat melihat skala prioritas pada besarnya upaya dalam melakukan perbaikan berikutnya, maka berdasarkan nilai-nilai kematangan *as is* masing-masing atribut untuk DS 5 dan DS11 diurutkan sesuai prioritas pada tabel. 4.14. dan tabel 4.15.

Tabel 4.14 Penetapan skala prioritas atribut kematangan untuk perbaikan DS5

Prioritas		Atribut Kematangan	Tingkat Kematangan	
			As is	*To be*
I	SE	*Skills and Expertise*	3	4
II	GSM	*Goal Setting and Measurement*	3	4
III	RA	*Responsibility and Accounttability*	3	4
IV	AC	*Awareness and Communication*	3	4
V	TA	*Tools and Automation*	3	4
VI	PSP	*Policy, Standard and Procedure*	3	4

Tabel 4.15 Penetapan skala prioritas atribut kematangan untuk perbaikan DS11

Prioritas		Atribut Kematangan	Tingkat Kematangan	
			As is	*To be*
I	SE	*Skills and Expertise*	3	4
II	GSM	*Goal Setting and Measurement*	3	4
III	RA	*Responsibility and Accounttability*	3	4
IV	AC	*Awarness and Communication*	3	4
V	TA	*Tools and Automation*	3	4
VI	PSP	*Policy, Standard and Procedure*	3	4

4.4 Rekomendasi

Proses memastikan keamanan sistem dan pengelolaan data yang dilakukan ditujukan untuk dapat memenuhi kebutuhan bisnis yaitu untuk mengoptimalkan penggunaan informasi dan dapat memastikan bahwa informasi yang diperlukan tersedia. Dalam rangka memenuhi kebutuhan bisnis tersebut secara lebih efektif maka proses memastikan keamanan sistem dan pengelolaan data harus dilakukan tata kelola sedemikian rupa sehingga dapat memenuhi proses pematangan seperti yang diharapkan.

Hasil yang diperoleh dari tahapan analisis yang telah dilakukan yang menjadi pertimbangan utama dalam mendefinisikan rekomendasi, untuk dapat memberikan suatu usulan tindakan perbaikan yang diperlukan. Beberapa hal penting dalam analisis yang dapat diperoleh adalah:

1. Pada analisis identifikasi risiko telah diperoleh adanya kepedulian tentang dampak negatif sebagai suatu risiko bila proses DS5 dan DS11 tidak dilakukan tata kelola secara efektif dan juga diidentifikasi adanya kelemahan kontrol terutama dalam pemenuhan DCO pada DS5 dan DS11.
2. Pada penilaian tingkat kematangan telah diperoleh tingkat kematangan yang saat ini *(as is)* maupun yang diharapkan *(to be)* serta ditetapkannya strategi pencapaian kematangan yang diperlukan, yang dipandang efektif dalam rangka proses pematangan yang diharapkan.

Dengan proses perbaikan secara bertahap sesuai dengan prioritas, maka proses pembelajaran menuju pematangan proses DS11 dalam organisasi dapat berlangsung secara efektif. Mengacu pada strategi pencapaian kematangan yang

telah didefinisikan sebelumnya, maka usulan tindakan perbaikan dilakukan menuju pencapian tingkat kematangan 4, yaitu:

Pada kelompok pencapaian tingkat kematangan 3, proses pematangan tumbuh dari 3 menuju 4. Melibatkan atribut secara berturut turut meliputi SE, GSM, RA dan TA. Penekanan pada kelompok pencapaian ini adalah konsistensi menjalankan semua kebijakan yang telah ditetapkan dan terus meng-*update skills* serta teknologi sesuai dengan kebutuhan serta perkembangan jaman. Di bawah ini adalah tabel beberapa tindakan dalam kelompok pencapaian tingkat kematangan 4 beserta grafik RACI mengidentifikasi siapa yang bertanggung jawab (R), akuntabel (A), dikonsultasikan (C) dan Informasi (I) dalam perbaikan setiap atribut dapat dilihat pada tabel 4.16.

Tabel 4.16 Tindakan perbaikan dalam kelompok pencapaian tingkat kematangan 4 untuk proses DS11

No	Atribut	Tindakan Perbaikan	CIO	BPO	HO	HD	CARS
1.	SE	- Melakukan *update* secara rutin kebutuhan kompetensi dalam pengelolaan data untuk mendapatkan keahlian dan sertifikasi. - Menjalankan pelatihan formal dan *knowledge sharing* bagi staf pengelolaan data yang dialakukan sesuai dengan rencana hal: - Pemahaman pada hal-hal yang berkaitan dengan pengelolaan data. - Penerapan prosedur. - Penggunaan perangkat bantu. - Melakukan evaluasi terhadap efektivitas rencana pelatihan.	A	C	R	-	C
2	GSM	- Melakukan kesepakatan dengan pengguna layanan teknologi informasi atas indikator pencapaian sasaran dan kinerja yang berkaitan dengan kebutuhan bisnis. - Menjalankan pengawasan dengan menggunakan proses yang terdefinisi. - Melakukan perbaikan secara berkelanjutan pada proses pengelolaan data.	A	C	R	-	C
3	RA	- Menumbuhkan budaya memberikan penghargaan bagi pengamban peran yang berprestasi sebagai upaya memotivasi.	A	I	C	-	C

Pendefinisian usulan tindakan perbaikan pada DS5 dengan mempertimbangkan strategi pencapaian kematangan yang telah didefinisikan pada tahapan sebelumnya. Pendefinisian di sini adalah berupa tindakan apa yang perlu dilakukan pada setiap atribut kematangan yang diarahkan pada pada pencapaian proses pematangan yang diharapkan.

Dengan proses perbaikan secara bertahap sesuai dengan prioritas, maka proses pembelajaran menuju pematangan proses DS5 dalam organisasi dapat berlangsung secara efektif. Mengacu pada strategi pencapaian kematangan yang telah didefinisikan sebelumnya, maka usulan tindakan perbaikan pencapian tingkat kematangan 4.

Pada kelompok pencapaian tingkat kematangan 3, proses pematangan tumbuh dari 3 menuju 4. Melibatkan atribut secara berturut turut meliputi SE, PSP, GSM, RA, AC dan TA. Penekanan pada kelompok pencapaian ini adalah konsistensi menjalankan semua kebijakan yang telah ditetapkan dan terus mengupdate skills serta teknologi sesuai dengan kebutuhan serta perkembangan jaman. Di bawah ini adalah tabel beberapa tindakan dalam kelompok pencapaian tingkat kematangan 4 beserta grafik RACI mengidentifikasi siapa yang bertanggung jawab (R), akuntabel (A), dikonsultasikan (C) dan Informasi (I) dalam perbaikan setiap atribut dapat dilihat pada tabel 4.17.

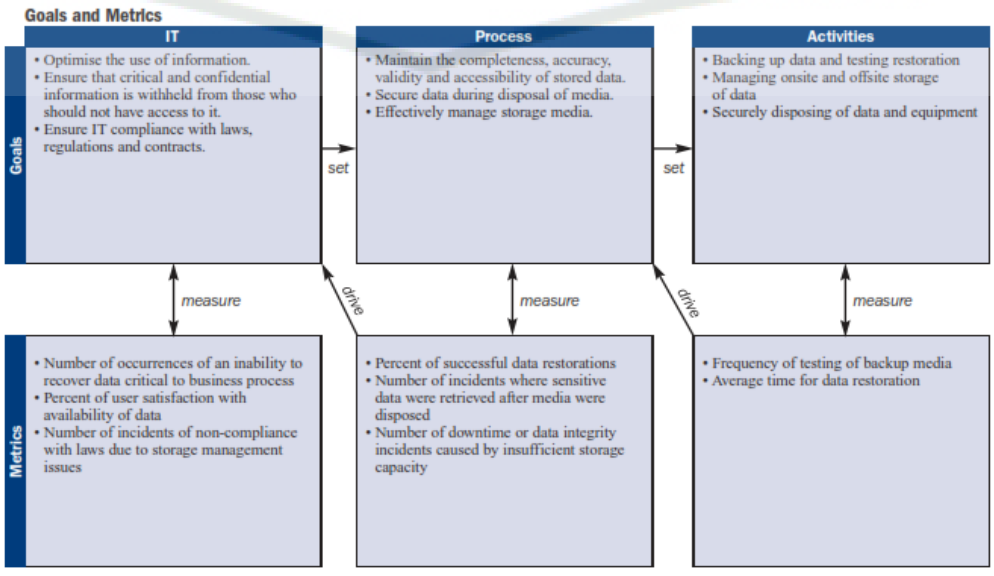
Tabel 4.17 Tindakan perbaikan dalam kelompok pencapaian tingkat kematangan 4 untuk proses DS5

No	Atribut	Tindakan Perbaikan	CEO	CFO	BE	CIO	BPO	HO	CARS
1.	SE	– Sertifikasi keamanan disarankan untuk staf yang bertanggung jawab untuk audit dan manajemen keamanan. – Training keamanan TI dilakukan baik dalam lingkup TI maupun bisnis. – Training keamanan TI direncanakan dan diatur agar mampu merespons kebutuhan bisnis dan profil resiko keamanan yang telah terdefinisi.	I	C	C	A	C	C	R
2	PSP	– Kebijakan dan praktik dari keamanan dilengkapi dengan baseline keamanan tertentu. – Proses keamanan TI dikoordinasikan dengan seluruh fungsi keamanan organisasi. – Pelaporan keamanan TI dikaitkan dengan tujuan bisnis	–	–	–	A	C	R	C

No	Atribut	Tindakan Perbaikan	CEO	CFO	BE	CIO	BPO	HO	CARS
3	GSM	– Identifikasi pengguna otentifikasi dan otorisasi terstandar – Tujuan dan metrik untuk manajemen keamanan telah didefinisikan tetapi belum diukur	–	–	I	A	C	R	C
4	RA	Tanggung jawab keamanan TI telah ditugaskan secara jelas, teratur dan dijalankan				A	I	R	R
5	AC	Analisis resiko dan dampak keamanan TI dilakukan secara konsisten. Pengungkapan metode untuk untuk mempromosikan kesadaran akan keamanan dianggap penting	I	C	C	A	C	C	R
6	TA	Testing keamanan dipenuhi menggunakan standar dan proses yang formal menuju peningkatan tingkat keamanan		I		A	I	C	R

4.4.1 Rekomendasi *Performance Indicators* dan *Outcome Measures*

Sebagai tindak lanjut dari rekomendasi perbaikan, maka pada tahap awal evaluasi terhadap proses perbaikan perlu dilakukan suatu pengawasan dalam bentuk penilaian atau pengukuran. Evaluasi ini diperlukan untuk mengetahui kemajuan yang terjadi sehingga tindakan yang diperlukan dapat diambil yang mengarah pada pencapaian tujuan yang diinginkan. Penilaian atau pengukuran dilakukan baik pada proses pelaksanaannya maupun pencapaiannya. Untuk itu perlu didefinisikan beberapa indikator pegukuran yaitu *performance indicators* dan *Outcome Measures*. Dimana *Outcome Measures* dapat diuraikan lagi dalam *Process performance indicators* maupun *Outcome Measures* yang berkaitan dengan proses memastikan keamanan sistem dan proses pengelolaan data secara transparan dapat dinilai efektivitas perbaikan yang telah dilakukan.



Gambar 4.11 Indikator pengukuran dalam evaluasi perbaikan proses DS11

Performance indicators merupakan kegiatan penting dalam proses DS11, yang bersifat krisis terhadap keberhasilan bagi tercapainya tujuan teknologi

informasi. Tujuan aktivitas dapat dipandang sebagai *Critical Success Factor* (CSF) dari proses DS11 yang meliputu keagiatan berikut:

1. Melakukan *backup* data dan menguji restorasi.
2. Mengelola penyimpanan data *onsite* dan *offsite.*
3. Melakukan penghapusan data dan peralatan secara aman.

Untuk dapat menilai atau mengukur seberapa baik aktifitas di atas telah dilaksanakan, sebagai suatu bentuk transfaransi dalam pengawasan, maka didefinisikan *Performance indicators*:

1. Frekuensi terhadap pengujian backup media.
2. Waktu rata-rata untuk restorasi data.

Hasil penilaian/pengukuran *performance indicators* akan menunjang/mengendalikan keberhasilan tujuan proses, yaitu:

1. Memelihara kelengkapan, akurasi, validitas, aksesibilitas data yang disimpan.
2. Mengamankan data selama penghapusan.
3. Mengelola media penyimpanan secara efektif.

Untuk dapat menilai/mengukur keberhasilan tujuan proses diperlukan indikator pengukuran *Outcome Measures* yang didefinisikan sebagai berikut:

1. Presentase restorasi data yang berhasil.
2. Jumlah insiden di mana data sensitif dapat ditarik lagi setelah media dihapus.
3. Jumlah *down time* atau insiden integritas data yang disebabkan kapasitas penyimpanan yang tidak mencukupi.

Hasil penilaian/pengukuran *Outcome Measures* akan menunjang/mengendalikan keberhasilan dalam pencapaian tujuan teknologi informasi, yaitu:

1. Mengoptimalkan penggunaan informasi.
2. Memastikan informasi yang kritikal dan konfidensial dari pihak yang tidak berhak.
3. Memastikan kepatuhan teknologi informasi pada hukum dan regulasi.

Untuk dapat menilai/mengukur keberhasilan dalam tujuan teknologi informasi diperlukan indikator pengukuran ITGI, yaitu:

1. Kejadian ketidakmampuan untuk memulihkan data kritis untuk proses bisnis.
2. Kepuasan pengguna terhadap ketersediaan data.
3. Insiden ketidakpatuhan pada hukum diakibatkan permasalahan manajemen penyimpanan.

Untuk melakukan pengawasan pada proses pengelolaan data, maka perlu dilakukan pengukuran secara berkelanjutan terhadap indikator yang telah ditetapkan dalam performance indicators dan *Outcome Measures*, dan membandingkan realisasi hasil pengukuran dengan suatu target tingkat kinerja. Penentuan besaran target tingkat kinerja dibuat untuk tiap indikator (*performance indicators* dan *Outcome Measures*), dilakukan dengan mempertimbangkan beberapa hal yang dipandang perlu untuk diperhatikan sebagai suatu justifikasi dalam penetapannya. Adapun nilai besaran target kinerja yang telah ditetapkan secara periodik dapat dan perlu dievaluasi disesuaikan dengan kebutuhan perusahaan. Terkait dengan realisasi hasil pengukuran yang tidak memenuhi

target tingkat kinerja, akan segera dilakukan langkah-langkah perbaikan dan penyempurnaan yang diperlukan.

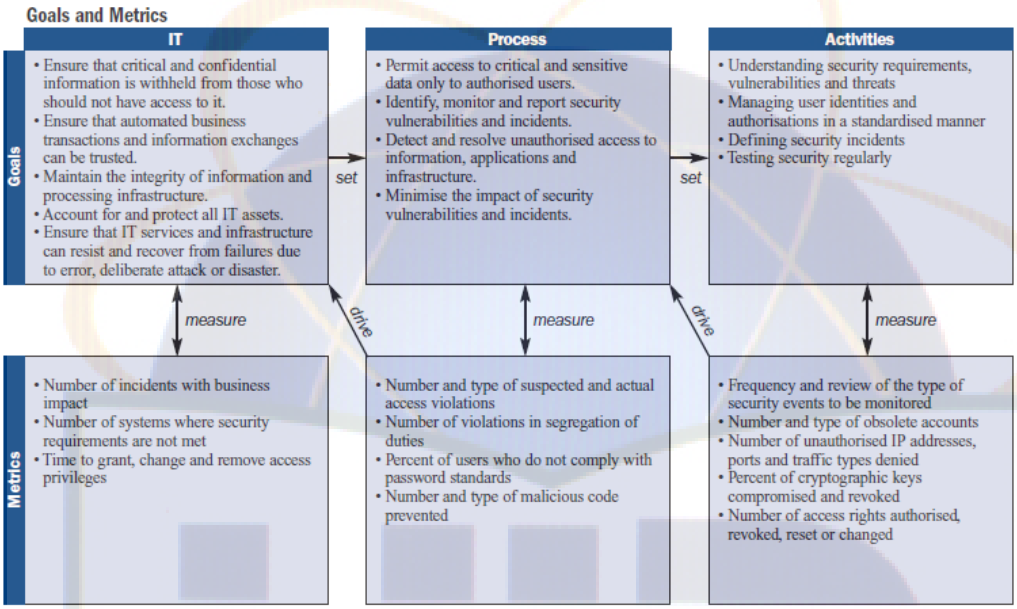
Tabel indikator dan target tingkat kinerja dibuat berdasarkan *performance indicators* dan *outcome measures* yang sudah digunakan beserta usulan terhadap target tingkat kinerja yang diharapkan akan tercapai sebagai indikasi keberhasilan pada pencapaian tujuan dalam rangkaian proses pengelolaan data.

Tabel 4.18 indikator dan target tingkat kinerja DS11 yang digunakan

No	Indikator	Satuan	Target
	Performance Indicators		
1.	Frekuensi terhadap pengujian *backup* media	Kali/hari	1
2.	Waktu rata-rata untuk restorasi data	Jam	3
	Outcome Measures		
3.	Persentase restorasi data yang berhasil	%	100
4.	Jumlah insiden di mana data sensitif dapat di tarik lagi setelah media dihapus	Kali	0
5.	Jumlah *down time* atau insiden integritas data yang disebabkan kapasitas penyimpanan yang tidak mencukupi	Kali	0

Tabel 4.19 Usulan indikator dan target tingkat kinerja DS11

No	Indikator	Satuan	Target
	Performance Indicators		
1.	Frekuensi terhadap pengujian *backup* media	Kali/hari	1
2.	Waktu rata-rata untuk restorasi data	Jam	1
	Outcome Measures		
3.	Persentase restorasi data yang berhasil	%	100
4.	Jumlah insiden di mana data sensitif dapat di tarik lagi setelah media dihapus	Kali	0
5.	Jumlah *down time* atau insiden integritas data yang disebabkan kapasitas penyimpanan yang tidak mencukupi	Kali	0



Gambar 4.12 Indikator pengukuran dalam evaluasi perbaikan proses DS5

Performance indicators merupakan kegiatan penting dalam proses DS5, yang bersifat krisis terhadap keberhasilan bagi tercapainya tujuan teknologi informasi. Tujuan aktivitas dapat dipandang sebagai *Critical Success Factor* (CSF) dari proses DS5 yang meliputi kegiatan berikut:

1. Memahami persyaratan keamanan, kerentanan dan ancaman.
2. Mengelola dan identitas pengguna otorisasi secara standar.
3. Mendefinisikan insiden keamanan.
4. Pengujian keamanan secara teratur.

Untuk dapat menilai atau mengukur seberapa baik aktifitas di atas telah dilaksanakan, sebagai suatu bentuk transfaransi dalam pengawasan, maka didefinisikan *Performance indicators*:

1. Frekuensi dan penelaahan terhadap jeniskejadian keamanan yang akan dipantau.
2. Jumlah dan jenis rekening usang
3. Jumlah alamat IP yang tidak sah, pelabuhan dan jenis lalu lintas ditolak.
4. Persen kunci kriptografi dikompromikan dan dicabut.
5. Jumlah hak akses dasar, dicabut, reset atau diubah.

Hasil penilaian/pengukuran *performance indicators* akan menunjang/mengendalikan keberhasilan tujuan proses, yaitu:

1. Ijin akses untuk data sensitif dan kritis hanya untuk pengguna yang berwenang.
2. Mengidentifikasi, memantau, melaporkan kerentanan keamanan dan insiden.
3. Mendeteksi, menyelesaikan akses tidak sah ke informasi, aplikasi dan infrastruktur.
4. Meminimalkan dampak keamanan kerentanan dan insiden.

Untuk dapat menilai/mengukur keberhasilan tujuan proses diperlukan indikator *Outcome Measures* yang didefinisikan sebagai berikut:

1. Jumlah aktual jenis yang dicurigai dan akses pelanggaran.
2. Jumlah pelanggaran dalam pemisahan tugas.
3. Persentase pengguna yang tidak sesuai dengan sandi standar.
4. Jumlah dan jenis kode berbahaya dicegah.

Hasil penilaian/pengukuran *Outcome Measures* akan menunjang/mengendalikan keberhasilan dalam pencapaian tujuan teknologi informasi, yaitu:

1. Pastikan bahwa kritis dan rahasia informasi tidak diberikan dari mereka yang tidak harus memiliki akses untuk itu.
2. Pastikan bahwa otomatis bisnis transaksi dan pertukaran informasi dapat dipercaya.
3. Menjaga integritas informasi dan pengolahan infrastruktur.
4. Rekening untuk dan melindungi semua aset TI.
5. Memastikan bahwa pelayanan dan infrastruktur TI dapat menolak dan pulih dari kegagalan karena kesalahan, serangan sengaja atau bencana.

Untuk dapat menilai/mengukur keberhasilan dalam tujuan teknologi informasi diperlukan indikator pengukuran ITGI, yaitu:

1. Jumlah insiden dengan dampak bisnis
2. Jumlah sistem di mana keamanan persyaratan yang tidak terpenuhi.
3. Waktu untuk hibah, mengubah dan menghapus akses hak istimewa.

Untuk melakukan pengawasan pada proses memastikan keamanan sistem, maka perlu dilakukan pengukuran secara berkelanjutan terhadap indikator yang telah ditetapkan dalam *Performance indicators* dan *Outcome Measures*, dan membandingkan realisasi hasil pengukuran dengan suatu target tingkat kinerja. Penentuan besaran target tingkat kinerja dibuat untuk tiap indikator (Performance indicators dan *Outcome Measures*), dilakukan dengan mempertimbangkan beberapa hal yang dipandang perlu untuk diperhatikan sebagai suatu justifikasi dalam penetapannya. Adapun nilai besaran target kinerja yang telah ditetapkan secara periodik dapat dan perlu dievaluasi disesuaikan dengan kebutuhan perusahaan. Terkait dengan realisasi hasil pengukuran yang tidak memenuhi

target tingkat kinerja, akan segera dilakukan langkah-langkah perbaikan dan penyempurnaan yang diperlukan.

Tabel indikator dan target tingkat kinerja dibuat berdasarkan *performance indicators* dan *outcome measures* yang sudah digunakan beserta usulan terhadap target tingkat kinerja yang diharapkan akan tercapai sebagai indikasi keberhasilan pada pencapaian tujuan dalam rangkaian proses memastikan keamanan sistem.

Tabel 4.20 indikator dan target tingkat kinerja DS5 yang telah ada

No	Indikator	Satuan	Target
	Performance Indicators		
1.	Frekuensi dan penelaahan terhadap jenis kejadian keamanan yang akan dipantau.	Kali/hari	1
2.	Jumlah dan jenis rekening usang.	Jumlah/hari	Untuk account email dan aplikasi, jika ada 1.pemberitahuan pengurangan pegawai dari HRD 2. pemberitahuan dari manajemen user
3.	Jumlah alamat IP yang tidak sah, pelabuhan dan jenis lalu lintas ditolak.	Jumlah/hari	0
4.	Persen kunci kriftografi dikompromikan dan dicabut.	%	0
5.	Jumlah hak akses dasar, dicabut atau diubah.	Kali	Jika ada permintaan dari manajemen user
	Outcome Measures		
6.	Jumlah aktual jenis yang dicurigai dan akses pelanggaran.	Jumlah/hari	0
7.	Jumlah pelanggaran dalam pemisahan tugas	Jumlah/bulan	5
8.	Persentase pengguna yang tidak sesuai dengan sandi standar.	%	0
9.	Jumlah dan jenis kode berbahaya dicegah.	Jumlah/hari	20

Tabel 4.21 Usulan indikator dan target tingkat kinerja DS5

No	Indikator	Satuan	Target
	Performance Indicators		
1.	Frekuensi dan penelaahan terhadap jenis kejadian keamanan yang akan dipantau.	Kali/hari	1
2.	Jumlah dan jenis rekening usang.	Jumlah/hari	Untuk account email dan aplikasi, jika ada 1.pemberitahuan pengurangan pegawai dari HRD 2. pemberitahuan dari manajemen user
3.	Jumlah alamat IP yang tidak sah, pelabuhan dan jenis lalu lintas ditolak.	Jumlah/hari	0
4.	Persen kunci kriftografi dikompromikan dan dicabut.	%	10
5.	Jumlah hak akses dasar, dicabut atau diubah.	Kali	Jika ada permintaan dari manajemen user
	Outcome Measures		
6.	Jumlah aktual jenis yang dicurigai dan akses pelanggaran.	Jumlah/hari	0
7.	Jumlah pelanggaran dalam pemisahan tugas	Jumlah/bulan	5
8.	Persentase pengguna yang tidak sesuai dengan sandi standar.	%	0
9.	Jumlah dan jenis kode berbahaya dicegah.	Jumlah/hari	10

BAB V

PENUTUP

5.1 Simpulan

Setelah melakukan audit sistem informasi *call center* maka dapat disimpulkan bahwa:

1. Hasil dari *Management Awareness* menunjukkan tingkat kinerja proses DS5 (memastikan keamananan sistem) dan DS11 (pengelolaan data) adalah sedang.
2. *Maturiy Level* DS5 dan DS11 saat ini (*as is*) ada pada level 3 yang artinya kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari namun namun kurang ada pengawasan untuk menjalankan prosedur sehingga memungkinkan terjadinya penyimpangan dan (*to be*) yang diharapkan menunjukkan level 4.
3. Rekomendasi berupa hal apa saja agar mampu meningkatkan nilai *maturity level* menjadi 4 untuk proses pengelolaan data dan memastikan keamanan sistem.
4. Rekomendasi berupa *performance indicators* dan *outcome measures* beserta targetnya agar proses pengelolaan data dan memastikan keamanan sistem sesuai dengan tujuan yang diinginkan oleh perusahaan.
5. Penerapan tekonologi informasi dengan menggunakan COBIT *Framework* dapat memberikan manfaat dalam arsitektur bisnis, arsitektur informasi,

arsitektur teknologi dan arsitektur solusi sebagai pedoman untuk pengembangan sistem *call center* pada ESQ LC.

5.2 Saran

Adapun saran-saran bagi peneliti selanjutnya yang dapat dilakukan adalah:

1. Memberikan pemetaan secara menyeluruh terkait pengelolaan TI pada domain Deliver & Support tidak hanya untuk fokus area DS5 (memastikan keamanan sistem) da DS11 (pengelolaan data). Artinya, semua sasaran yang tidak terpenuhi dapat ditelusuri secara detil dan segera ditemukan penyebabnya untuk selanjutnya diputuskan apakah segera diperbaiki atau tidak.
2. Untuk peneliti selanjutnya sebaiknya dilakukan audit untuk semua domain dan semua fokus area agar diketahui proses IT yang dilakukan selama ini sudah mendukung tujuan perusahaan atau belum.
3. Menciptakan *tools* audit sendiri untuk mempermudah dalam melakukan audit sistem informasi.

Daftar Pustaka

BEIDJILALI, T. (2009) Methods and safety standards of systems. *Proc. Canadian Conf. Electrical and Computer Engineering CCECE '09.*

BIFFL, S., MORDINYI, R. & SCHATTEN, A. (2007) A Model-Driven Architecture Approach Using Explicit Stakeholder Quality Requirement Models for Building Dependable Information Systems. *Proc. Fifth Int. Workshop Software Quality WoSQ'07: ICSE Workshops 2007.*

BOTTCHER, S. & STEINMETZ, R. (2006) Finding the Leak: A Privacy Audit System for Sensitive XML Databases. *Proc. 22nd Int Data Engineering Workshops Conf.*

BUDDELMEIJER, C. I., HABRAKEN, J. B. A., ADAMS, R. & PIEK, J. J. (2006) A fast and simple CCU complication risk registration module for the Local Cardiology Information System (LCIS). *Proc. Computers in Cardiology.*

CAMPBELL & L, P. (2005) *A COBIT Primier,* USA, Sandia National Laboratories.

CAO, D. & YANG, B. Design and implementation for MD5-based data integrity checking system. *Proc. 2nd IEEE Int Information Management and Engineering (ICIME) Conf.*

CAO, X., YANG, L., WAN, L., LI, J., CHEN, X. & WANG, X. (2009) Research on network audit system based on multi-agents. *Proc. IEEE Int. Conf. Communications Technology and Applications ICCTA '09.*

GEISLER, E., PRABHAKER, P. & NAYAR, M. (2003) Information integrity: an emerging field and the state of knowledge. *Proc. Technology Management for Reshaping the World. Portland Int. Conf. Management of Engineering and Technology PICMET '03.*

GONDODIYOTI S & H, H. (2006) *Audit Sistem Informasi,* Jakarta, Mitra Wacana Media.

GOTTERBARN, D. (2002) Introducing professional issues into project management modules. *Proc. 32nd Annual Frontiers in Education FIE 2002.*

GUO F & H, S. (2010) On Designing the Security System for LAN-Based Educational Management Information System. *Proc. 2nd Int e-Business and Information System Security (EBISS) Conf.*

HM, J. (2001) *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis,* Yogyakarta, ANDI.

HM, J. (2008) *Metodologi Penelitian Sistem Informasi,* Yogyakarta, ANDI.

HUANG K, CHEN P, CHEN Y, SONG W & X, C. (2009) The Research for Embedded Active Database Based on ECA Rule and Implementation in SQLite Database. *Proc. First Int Database Technology and Applications Workshop.*

HUANG, S. H., LEE, L. Y., LOU, C. C. & LING, K. R. (2000) Visual inspection management system. *Proc. Ninth Int. Symp. Semiconductor Manufacturing ISSM 2000.*

HUANG, Y., HUANG, J., WANG, B., WU, J. & BAI, S. Transactional recovery mechanism in stock trading system. *Proc. 2nd Int Computer Engineering and Technology (ICCET) Conf.*

HUNG, M.-H., HO, R.-W. & CHENG, F.-T. (2004) An e-Diagnostics framework with security considerations for semiconductor factories. *Proc. Semiconductor Manufacturing Technology Workshop.*

INDRAJIT & EKO, R. (2001) *Sistem Informasi dan Teknologi Informasi*, Jakarta, Gramedia.

JANG, C., KIM, J., JANG, H., PARK, S., JANG, B., KIM, B. & CHOI, E. (2009) Rule-based auditing system for software security assurance. *Proc. First Int. Conf. Ubiquitous and Future Networks ICUFN 2009.*

JI, Z. (2009) An empirical study on the risk framework based on the enterprise information system. *Proc. Int. Conf. Future BioMedical Information Engineering FBIE 2009.*

JOHNSON, C. M. & GRANDISON, T. W. A. (2007) Compliance with data protection laws using Hippocratic Database active enforcement and auditing. *IBM Systems Journal*, 46**,** 255-264.

KURADA, N. Developing a practical financial model to redefine Information Technology from a cost centre to a benefit enabling centre. *Proc. IEEE/IFIP Network Operations and Management Symp. Workshops (NOMS Wksps).*

LEE, M., CHO, S., CHANG, H., JO, J., JUNG, H. & CHOI, E. (2008) Auditing System Using Rule-Based Reasoning in Ubiquitous Computing. *Proc. Int. Conf. Computational Sciences and Its Applications ICCSA '08.*

LI, J., LI, X., LIU, G. & HE, Z. Log management approach in three-dimensional spatial data management system. *Proc. 18th Int Geoinformatics Conf.*

LI, K.-L., HUANG, H.-K., TIAN, S.-F. & XU, W. (2003) Improving one-class SVM for anomaly detection. *Proc. Int Machine Learning and Cybernetics Conf.*

LI, S.-H. & WANG, K.-C. (2009) Applications of Ontology in Management of Information Asset. *Proc. Fifth Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP '09.*

LIU, S., ZHANG, Z., CUI, Y. & LINTAO, W. (2008) A new information leakage defendable model. *Proc. 9th Int. Conf. Computer-Aided Industrial Design and Conceptual Design CAID/CD 2008.*

LO, E. C. & MARCHAND, M. (2004) Security audit: a case study [information systems]. *Proc. Canadian Conf. Electrical and Computer Engineering.*

MANIAH & KRIDANTO, S. (2005) Usulan model audit sistem informasi studi kasus sistem informasi perawatan pesawat terbang. *(SNATI 2005) Seminar Nasional Aplikasi Teknologi Informasi 2005*.

MASCHER, A. L., COTTON, P. T. & JONES, D. W. (2009) Improving Voting System Event Logs. *Proc. First Int Requirements Engineering for e-Voting Systems (RE-VOTE) Workshop.*

MASSAWE, L. V., AGHDASI, F. & KINYUA, J. (2009) The Development of a Multi-Agent Based Middleware for RFID Asset Management System Using the PASSI Methodology. *Proc. Sixth Int. Conf. Information Technology: New Generations ITNG '09.*

MASUCCI, B. & STINSON, D. R. (2001) Efficient metering schemes with pricing. *#IEEE_J_IT#,* 47**,** 2835-2844.

MEI, L. Y. & HUAN, J. Z. (2008) Comprehension and evaluation on significant error risk of CPA audit in the information-processing environment. *Proc. Conf. Int Management Science and Engineering ICMSE 2008. 15th Annual.*

MIELKE, A. M., BOYLE, C. M., BUENAFE, C. A., DREICER, J. S., GATTIKER, J. R., MARTINEZ, B. J. & SMITH, D. A. (2001) Continuous monitoring of a capacitor bank. *IEEE Instrumentation & Measurement Magazine,* 4**,** 14-19.

MORSELLI, R., BHATTACHARJEE, B., KATZ, J. & MARSH, M. (2007) Exploiting approximate transitivity of trust. *Proc. Fourth Int. Conf. Broadband Communications, Networks and Systems BROADNETS 2007.*

MRAZIK, I. F. & KOLLAR, D. I. J. (2008) Information system security assessment. *Proc. 6th Int. Symp. Applied Machine Intelligence and Informatics SAMI 2008.*

NIANZU, L. & XIAOLING, W. (2009) Research on the Audit Fraud Grid. *Proc. Int. Symp. Computer Network and Multimedia Technology CNMT 2009.*

NICHO, M. & CUSACK, B. (2007) A Metrics Generation Model for Measuring the Control Objectives of Information Systems Audit. *Proc. 40th Annual Hawaii Int. Conf. System Sciences HICSS 2007.*

PETO, D. (2006) Generalized risk assessment index for information systems auditing. *Proc. 28th Int Information Technology Interfaces Conf.*

PINGPING, Z., SHIGUANG, J. & WEIHE, C. (2008) A Location-Based Secure Spatial Audit Policy Model. *Proc. Int Computer Science and Software Engineering Conf.*

R, M. J. (2001) *Management Information System,* New Jersey, Prentice Hall International Inc.

RADOVANOVIC, D., RADOJEVIC, T., LUCIC, D. & SARAC, M. IT audit in accordance with Cobit standard. *Proc. 33rd Int MIPRO Convention.*

RAMANATHAN, J., COHEN, R. J., PLASSMANN, E. & RAMAMOORTHY, K. (2007) Role of an auditing and reporting service in compliance management. *IBM Systems Journal,* 46**,** 305-318.

SEKHAR, A. N., RAJAN, K. S. & JAIN, A. (2008) Spatial informatics and Geographical Information Systems: Tools to transform Electric Power and Energy Systems. *Proc. TENCON 2008 - 2008 IEEE Region 10 Conf.*

SINDHU, S. S. S., GEETHA, S., SIVANATH, S. S. & KANNAN, A. (2006) A Neuro-genetic ensemble Short Term Forecasting Framework for Anomaly Intrusion Prediction. *Proc. Int. Conf. Advanced Computing and Communications ADCOM 2006.*

SOUDAIN, N., RAGGAD, B. G. & ZOUARI, B. (2009) A formal design of secure information systems by using a Formal Secure Data Flow Diagram

(FSDFD). *Proc. Fourth Int Risks and Security of Internet and Systems (CRiSIS) Conf.*

SUN, J. & ZHANG, Y. Railway passenger dynamic E-business based on Web services and RFID. *Proc. IEEE Int Wireless Communications, Networking and Information Security (WCNIS) Conf.*

SURENDRO, K. (2009) Implementasi Tata Kelola Teknologi Informasi.

TADAAKI, Y. (2008) Measures against police information leakage utilizing automatic encryption and access control software. *Proc. 42nd Annual IEEE Int. Carnahan Conf. Security Technology ICCST 2008.*

TANG, H. & XING, L.-N. (2008) A Web-Based Data Mining System for Forest Resource Planning System. *Proc. Fifth Int. Conf. Fuzzy Systems and Knowledge Discovery FSKD '08.*

WANG, C.-H. & TSAI, D.-R. (2009) Integrated installing ISO 9000 and ISO 27000 management systems on an organization. *Proc. 43rd Annual 2009 Int Security Technology Carnahan Conf.*

WEBER, R. (1999) *Information System Control and Audit*, Prentice Hall.

XIANLIN, R. & GENBAO, Z. (2009) Study on and Development of the Information System for Digital Quality Audit and Control. *Proc. Int. Conf. E-Business and Information System Security EBISS '09.*

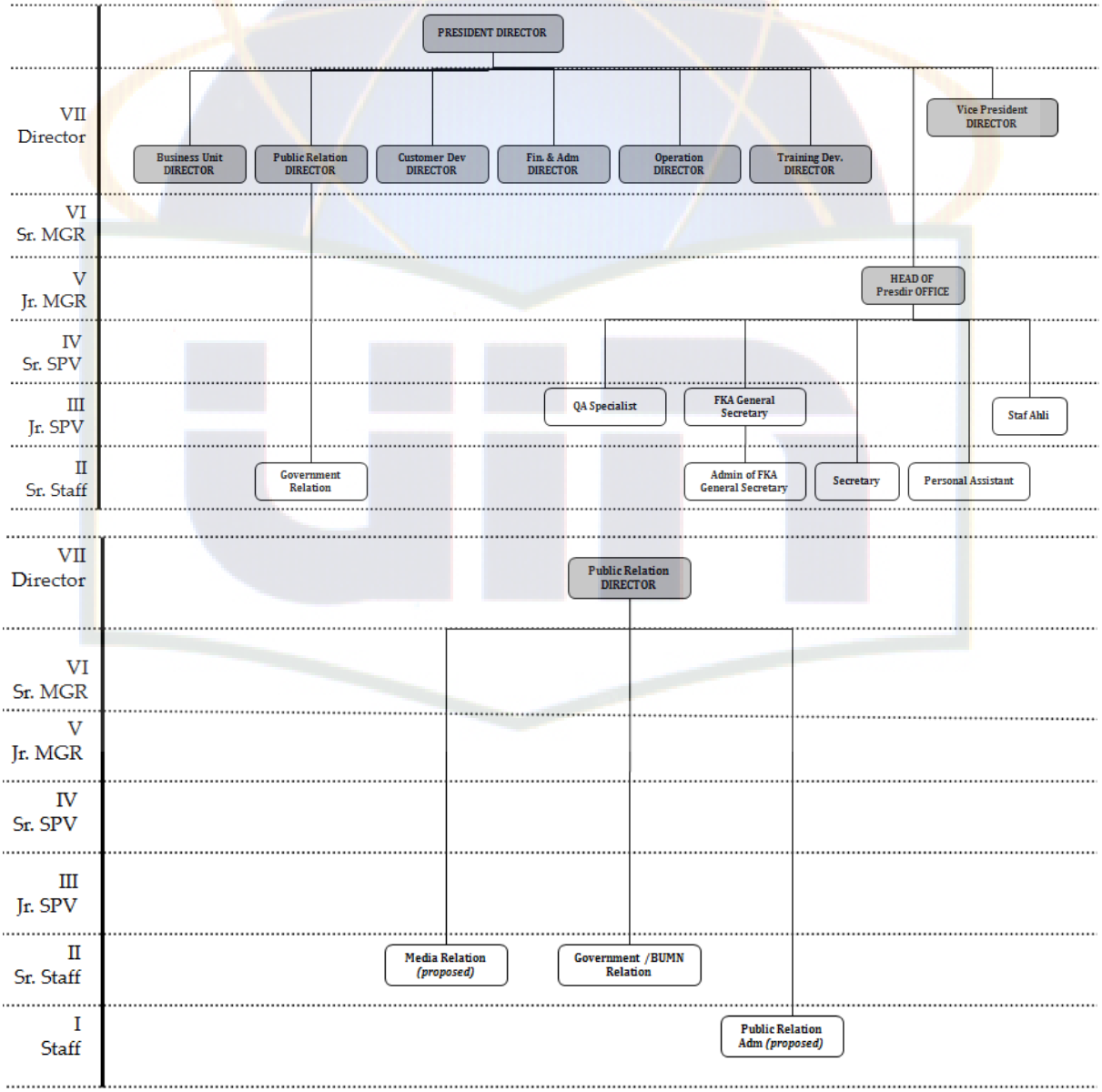
ZHANG, C. (2009) Thinking on ISCA Model from IT Goverance Perspective. *Proc. Asia-Pacific Conf. Information Processing APCIP 2009.*

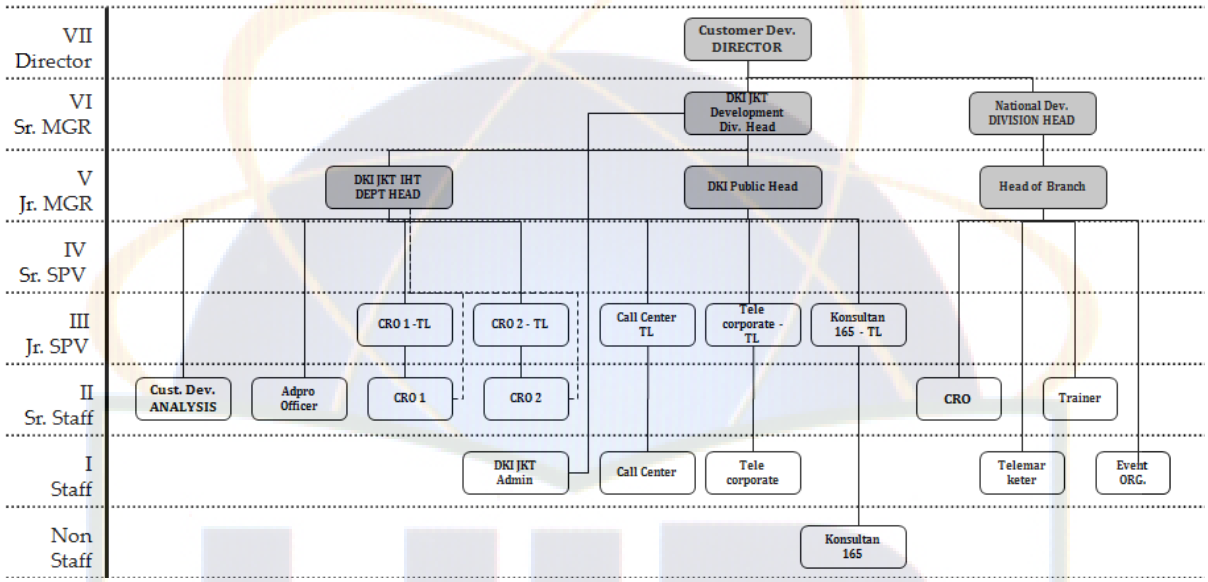
ZHANG, X., LIU, F., CHEN, T. & LI, H. (2009) Research and Application of the Transparent Data Encpryption in Intranet Data Leakage Prevention. *Proc. Int. Conf. Computational Intelligence and Security CIS '09.*

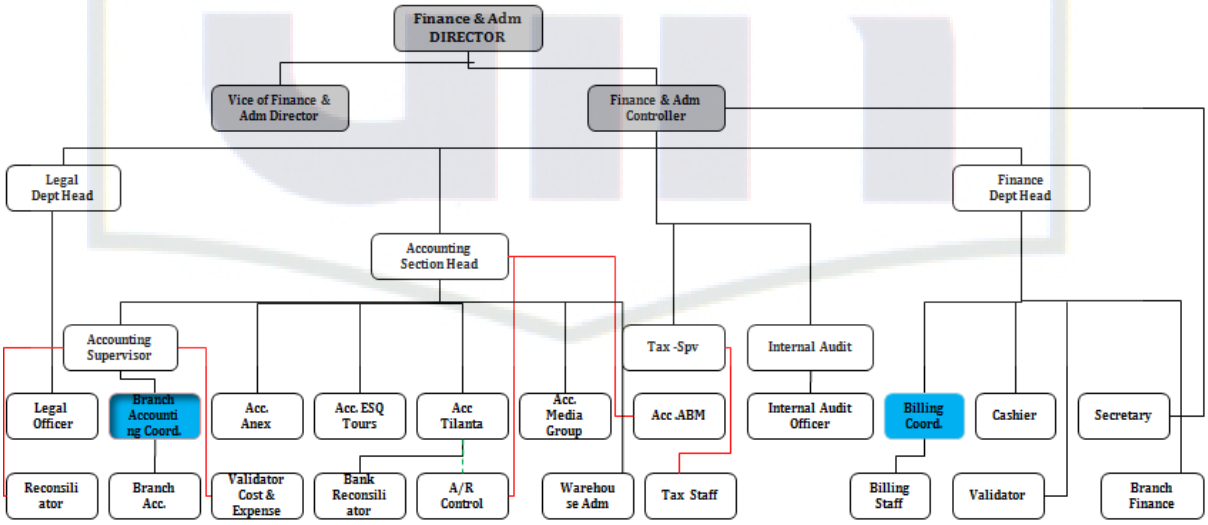
ZHAO, K., LI, Q., KANG, J., JIANG, D. & HU, L. (2007) Design and Implementation of Secure Auditing System in Linux Kernel. *Proc. IEEE Int Anti-counterfeiting, Security, Identification Workshop.*

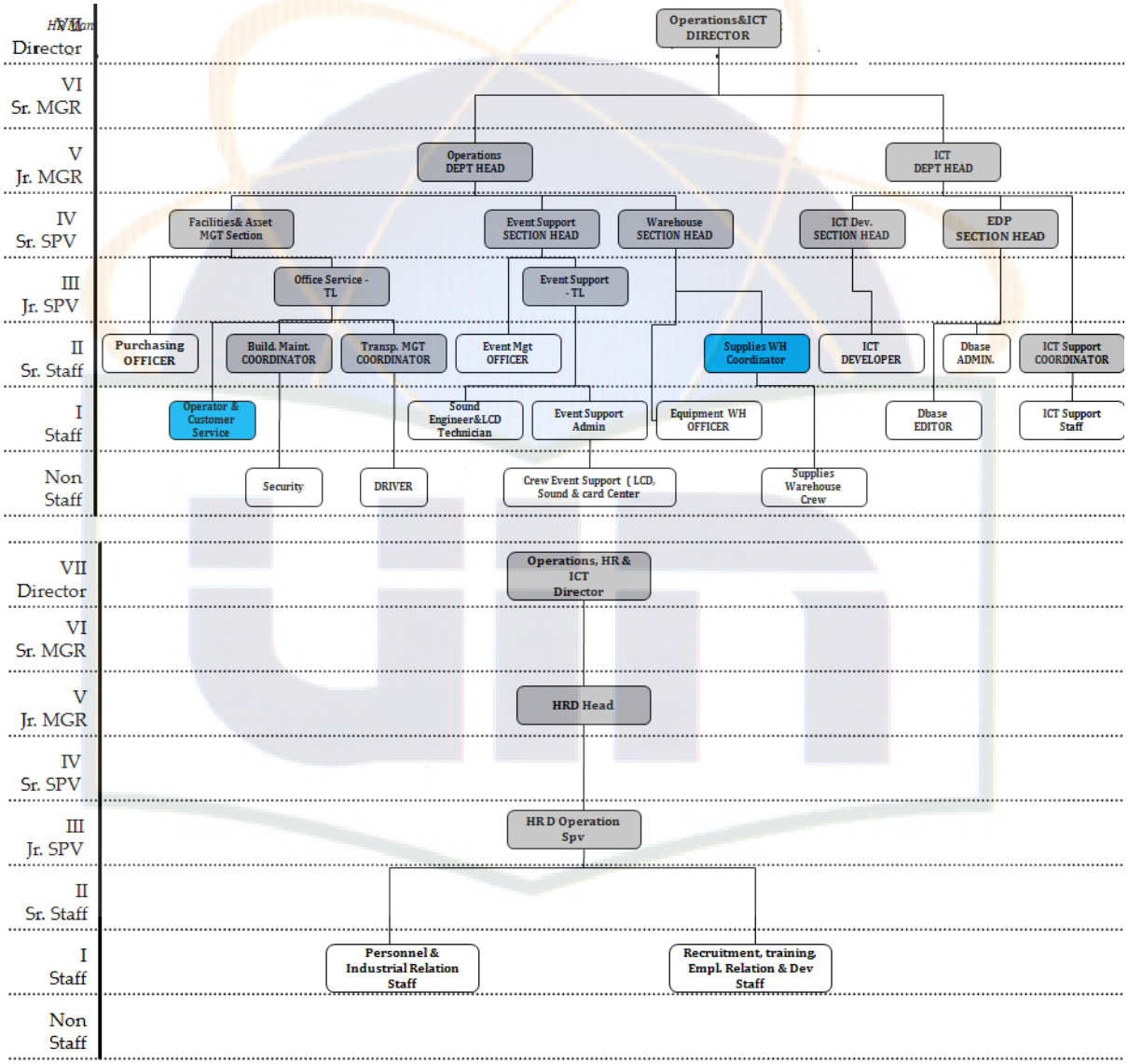
ZHONGHUA, D. & YING, W. Overcoming Disadvantages by Making Full Use of Extrinsic Objects: Advancing Information Resource Construction by ISA. *Proc. Third Int Intelligent Information Technology and Security Informatics (IITSI) Symp.*

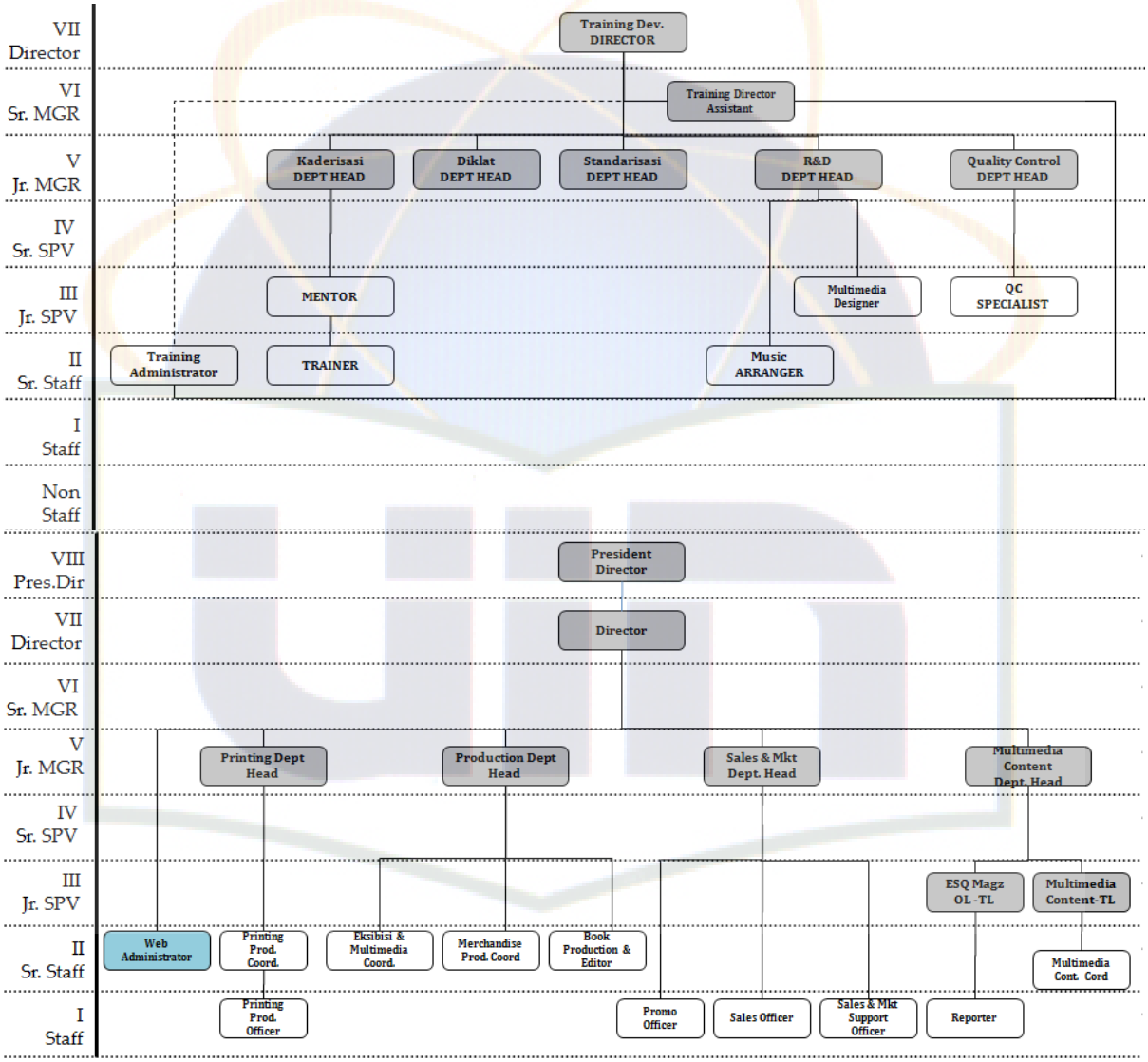
STRUKTUR ORGANISASI PT. ARGA BANGUN BANGSA (ESQ LC)

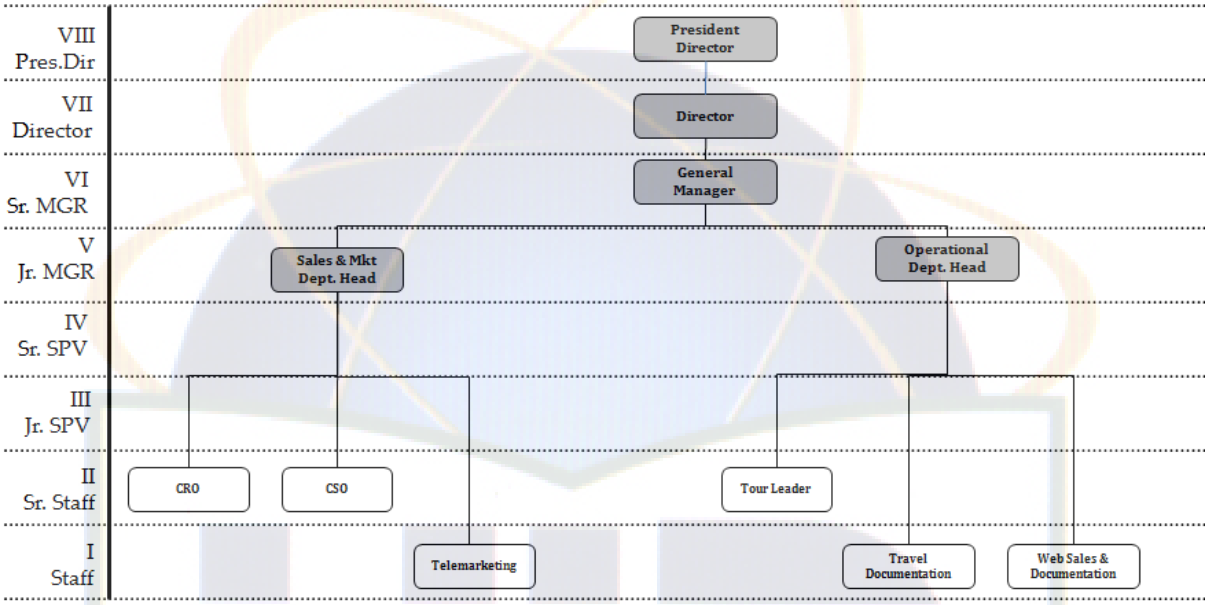



VII Director
VI Sr. MGR
V Jr. MGR
IV Sr. SPV
III Jr. SPV
II Sr. Staff
I Staff
Non Staff
Customer Dev. DIRECTOR
DKI JKT Development Div. Head
National Dev. DIVISION HEAD
DKI JKT IHT DEPT HEAD
DKI Public Head
Head of Branch
CRO 1 -TL
CRO 2 - TL
Call Center TL
Tele corporate - TL
Konsultan 165 - TL
Cust. Dev. ANALYSIS
Adpro Officer
CRO 1
CRO 2
CRO
Trainer
DKI JKT Admin
Call Center
Tele corporate
Telemar keter
Event ORG.
Konsultan 165


Finance & Adm DIRECTOR
Vice of Finance & Adm Director
Finance & Adm Controller
Legal Dept Head
Finance Dept Head
Accounting Section Head
Accounting Supervisor
Tax -Spv
Internal Audit
Legal Officer
Branch Accounti ng Coord.
Acc. Anex
Acc. ESQ Tours
Acc Tilanta
Acc. Media Group
Acc .ABM
Internal Audit Officer
Billing Coord.
Cashier
Secretary
Reconsili ator
Branch Acc.
Validator Cost & Expense
Bank Reconsili ator
A/R Control
Warehou se Adm
Tax Staff
Billing Staff
Validator
Branch Finance


VII Director
VI Sr. MGR
V Jr. MGR
IV Sr. SPV
III Jr. SPV
II Sr. Staff
I Staff
Non Staff
Operations&ICT DIRECTOR
Operations DEPT HEAD
ICT DEPT HEAD
Facilities& Asset MGT Section
Event Support SECTION HEAD
Warehouse SECTION HEAD
ICT Dev. SECTION HEAD
EDP SECTION HEAD
Office Service - TL
Event Support - TL
Purchasing OFFICER
Build. Maint. COORDINATOR
Transp. MGT COORDINATOR
Event Mgt OFFICER
Supplies WH Coordinator
ICT DEVELOPER
Dbase ADMIN.
ICT Support COORDINATOR
Operator & Customer Service
Sound Engineer&LCD Technician
Event Support Admin
Equipment WH OFFICER
Dbase EDITOR
ICT Support Staff
Security
DRIVER
Crew Event Support (LCD, Sound & card Center
Supplies Warehouse Crew
VII Director
VI Sr. MGR
V Jr. MGR
IV Sr. SPV
III Jr. SPV
II Sr. Staff
I Staff
Non Staff
Operations, HR & ICT Director
HRD Head
HR D Operation Spv
Personnel & Industrial Relation Staff
Recruitment, training, Empl. Relation & Dev Staff


VII Director
VI Sr. MGR
V Jr. MGR
IV Sr. SPV
III Jr. SPV
II Sr. Staff
I Staff
Non Staff
Training Dev. DIRECTOR
Training Director Assistant
Kaderisasi DEPT HEAD
Diklat DEPT HEAD
Standarisasi DEPT HEAD
R&D DEPT HEAD
Quality Control DEPT HEAD
MENTOR
Multimedia Designer
QC SPECIALIST
Training Administrator
TRAINER
Music ARRANGER
VIII Pres.Dir
VII Director
VI Sr. MGR
V Jr. MGR
IV Sr. SPV
III Jr. SPV
II Sr. Staff
I Staff
President Director
Director
Printing Dept Head
Production Dept Head
Sales & Mkt Dept. Head
Multimedia Content Dept. Head
ESQ Magz OL-TL
Multimedia Content-TL
Web Administrator
Printing Prod. Coord.
Eksibisi & Multimedia Coord.
Merchandise Prod. Coord
Book Production & Editor
Multimedia Cont. Cord
Printing Prod. Officer
Promo Officer
Sales Officer
Sales & Mkt Support Officer
Reporter


VIII
Pres.Dir
VII
Director
VI
Sr. MGR
V
Jr. MGR
IV
Sr. SPV
III
Jr. SPV
II
Sr. Staff
I
Staff
President Director
Director
General Manager
Sales & Mkt Dept. Head
Operational Dept. Head
CRO
CSO
Telemarketing
Tour Leader
Travel Documentation
Web Sales & Documentation

Kuesioner I
Analisis Tata kelola Teknologi Informasi Pada *Ensure System Security Call Center* di PT Arga Bangun Bangsa (ESQ LC)

Kuesioner ini merupakan bagian dari penelitian Skripsi mahasiswa program studi Sistem Informasi UIN Syarif Hidayatullah Jakarta, yang bertujuan untuk memperoleh data ataupun opini dari karyawan Perusahaan PT Arga Bangun Bangsa sebagai pihak yang terkait dalam pengelolaan TI khususnya pada penjaminan keamanan sistem call informasi center.
Kuesioner I *Management Awarness* ini dikembangkan untuk mengetahui tingkat pemenuhan terhadap *Detailed Control Objective* (DCO) dan pencapaian indikator kinerja dalam proses menjamin keamanan sistem. Adapun DCO tersebut meliputi penyusunan dan memelihara peranan-peranan keamanan (security roles) serta tanggung jawab, kebijakan, standar dan prosedur. Manajemen keamanan juga mencakup pengawasan keamanan dan ujicoba secara periodik, serta mengimplementasikan aksi perbaikan untuk kelemahan kekurangan atau insiden/bencana. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis terhadap kelemahan keamanan dan insiden.
Kuesioner ini didisain dalam format campuran pilihan ganda dan essay, yang terdiri dari 13 pertanyaan. Pada kolom "Tingkat Kinerja", responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili kondisi yang sebenarnya di lapangan dengan memberikan tanda (v) pada tempat yang tersedia, dimana kolom L menyatakan tingkat kinerja "Kurang", kolom M menyatakan tingkat kinerja "Sedang", dan kolom H menyatakan tingkat kinerja "Baik". Sedangkan pada kolom "komentar", responden dapat memberikan jawaban bebas dalam bentuk essay yang mendukung tingkat kinerja.
Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan pilihan maupun opininya sebagai jawaban atas pertanyaan-pertanyaan yang diberikan dalam kuesioner ini untuk kemudian dapat diolah dalam penelitian skripsi ini.

Nama Responden		Kode :
Jabatan Responden		
Unit/Bidang/Subbid		

No	Pertanyaan	Tingkat Kinerja			Komentar
		L	M	H	
1	Bagaimana Manajemen keamanan TI pada level organisasi yang tertinggi Menerjemahkan bisnis, risiko dan kepatuhan (*compliance*) ke dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan?				
2	Bagaimana rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, *software* dan *hardware*?				
3	Bagaimana mengkomunikasikan kebijakan dan prosedur keamanan kepada *stakeholder*				

	dan *user* ?				
4	Bagaimana konfirmasi hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, kebutuhan kerja yang melekat pada identitas pengguna serta memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan ?				
5	Bagaimana prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua *user* termasuk administrator, *user* internal dan eksternal, untuk normal dan kasus darurat hak dan kewajiban terhadap akses ke sistem oraganisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis *user*?				
6	Bagaimana melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung?				
7	Bagaimana menguji dan memantau implementasi keamanan TI dalam langkah yang proaktif ?				
8	Bagaimana mendefinisikan secara jelas dan mengkomuniksasikan karakteristik dari insiden keamanan yang potential sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah?				
9	Bagaimana membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentaasi keamanan yang tidak perlu ?				
10	Bagaimana penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah?				
11	Bagaimana memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama *patch* keamanan yang *up-to-date* dan pengendalian virus) diseluruh organisasi untuk melindungi sistem				

	informasi dan teknologi dari *malware* (aeperti *virus*, *worm*, s*pyware* dan *spam*)?				
12	Bagaimana teknik dan prosedur keamanan manajemen yang terkait (misalnya, firewall, peralatan keamanan, segmentasi jaringan, intrusi deteksi) untuk mengotorisasi akses dan kontrol arus informasi dari dan ke jaringan?				
13	Bagaimana Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan *non-repudiation* ?				

Kuesioner II
Analisis Tata Kelola Teknologi Informasi Ensure System Security pada PT. Arga Bangun Bangsa (ESQLC)
Maturity Level

Kuesioner ini merupakan bagian dari penelitian Skripsi mahasiswa program studi Sistem Informasi UIN Syarif Hidayatullah Jakarta, yang bertujuan untuk memperoleh data ataupun opini dari karyawan Perusahaan PT Arga Bangun Bangsa sebagai pihak yang terkait dalam pengelolaan TI khususnya pada proses memastikan keamanan sistem.

Kuesioner II Pengukuran Tingkat Kematangan ini dikembangkan untuk mengetahui tingkat kematangan pada proses pengelolaan data baik untuk kondisi yang saat ini, maupun untuk kondisi yang diharapkan, yang selanjutnya dapat dijadikan dasar yang cukup untuk identifikasi prioritas penigkatan (*improvement*) pada proses pengelolaan data. Adapun pendekatan dalam pengukuran tingkat kematangan ini dilakukan dengan mempertimbangkan kematangan 6 (enam) atribut kematangan yang didefinisikan dalam COBIT 4.1, meliputi: *awareness and communication*, *policies standars and procedures*, *tools and automation*, *skills and expertise*, *responsibilities* dan *goal and measurement.*

Untuk mempermudah responden dalam menjawab, maka kuesioner ini didisain dalam format pilihan ganda, yang terrdiri dari 12 pertanyaan. Petanyaan-pertanyaan dikelommenurut atribut kematangan, dan pada tiap kelompok pertanyaan akan melibatkan dua (dua) pertanyaan yang masing-masing mewakili kondisi kekinian dan kondisi yang diharapkan. Masing-masing pertanyaan mempunyai 6 (enam) pilihan jawaban yang meunjukkan tingkat kematangan terhadap atribut tertentu pada proses pengelolaan data. pilihan-pilihan jawaban tersebut dari a sampai f secara berturut-turut mempresentasikan tingkat kematangan yang semakin meningkat terhadap suatu atribut pada proses *Ensure system security*.

Pada kolom "jawaban", responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili kondisi kematangan baik yang saat ini maupun yang diharapkan, terkait dengan atribut kematangan tertentu dalam proses pengelolaan data dengan memberikan tanda (v) pada tempat yang tersedia. Dengan mengetahui posisi kematangan saat ini dan yang diharapkan, selanjutnya akan dilakukan analisis yang diharapkan dapat menjadi dasar dalam pendefinisian rancagan solusi untuk perbaikan dalam proses *ensure system security*.

Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan jawaban atas pertanyaan-pertanyaan yang diberikan dalam kuesioner ini untuk kemudian dapat diolah untuk penelitian skripsi ini.

I	AWARENESS AND COMMUNICATION	
Nama Responden		Kode :
Jabatan Responden		
Unit/Bidang/Subbid		

	Berikut pilihan jawaban untuk pertanyaan kuesioner no 1 dan 2 (a) Organisasi tidak menyadari kebutuhan untuk keamanan IT. Tanggung jawab dan akuntabilitas tidak ditugaskan untuk menjamin keamanan. (b) Organisasi mulai menyadari adanya kebutuhan keamananan IT pada *Call Center*. keamanan ditujukan secara reaktif. Keamanan TI tidak diukur. Terdeteksi TI pelanggaran keamanan memanggil jari-menunjuk tanggapan, karena tanggung jawab tidak jelas. (c) Adanya kesadaran akan kebutuhan keamanan sistem untuk segera ditindaklanjuti. Diselenggarakan semacam forum untuk dapat mengkomunikasikan permasalahan terkait dengan keamanan sistem pada *Call Center*. (d) Adanya pemahaman akan kebutuhan keamanan sistem *call center*. kebutuhan tersebut telah dipahami dan diterima diperusahaan secara keseluruhan. Adanya semacam surat edaran dari manajemen atas untuk dapat melakukan langkah-langkah efektif untuk melakukan proses keamanan TI pada *call center*. (e) Kebutuhan bagi manajemen keamanan sistem secara utuh telah dipahami dan tindakan yang diperlukan sudah diterima secara luas di organisasi. Secara berkala diadakan forum internal perusahaan untuk dapat mencari solusi bersama atas permasalahan yang timbul dalam keamanan sistem pada *call center*. (f) Kebutuhan manajemen keamanan sistem dan pemahamannya atas langkah yang diperlukan telah dipahami dan diterima di organisasi. Keperluan dan kebutuhan kedepan	

	senantiasa digali secara proaktif. Mengikuti forum berskala nasional maupun internasional untuk dapat melihat kecenderungan kedepan terkait dengan permasalahan dalam keamanan sistem pada *call center* yang juga merupakan peluang pengembangan kedepan.						
No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
1.	Sejauhmana tingkat kesadaran pihak manajemen sampai saat ini terkait dengan keamanan TI pada *call center*?						
2.	Apa harapan di masa yang akan datang terkait dengan kesadaran akan kebutuhan keamanan call center?						

II	POLICIES, STANDARDS AND PROCEDURES	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 3 dan 4 (a) Tidak ada prosedur untuk mengangani keamanan sistem *call center*. (b) Menggunakan pendekatan ad hoc untuk menangani kebutuhan keamanan pada manajemen keamanan sistem, namun pemahaman informal tentang prosedur sudah ada. (c) Tanggung jawab dan akuntabilitas untuk keamanan TI yang ditugaskan ke koordinator TI keamanan, meskipun kewenangan manajemen dari koordinator terbatas. (d) Keamanan kesadaran ada dan dipromosikan oleh manajemen. TI prosedur keamanan didefinisikan dan selaras dengan kebijakan keamanan TI. Tanggung jawab untuk keamanan TI ditugaskan dan dipahami, tetapi tidak konsisten. Rencana keamanan TI dan keamanan solusi ada sebagai penggerak dengan analisis risiko. (e) Tanggung jawab untuk keamanan TI jelas ditetapkan, dikelola dan ditegakkan. Keamanan TI risiko dan analisis dampak secara konsisten dilakukan. Kebijakan keamanan dan prosedur yang dilengkapi dengan baseline keamanan tertentu. (f) Prosedur keamanan TI pada *call center* adalah tanggung jawab bersama bisnis dan manajemen TI	

	dan terintegrasi dengan tujuan bisnis keamanan perusahaan. IT persyaratan keamanan secara jelas didefinisikan, dioptimalkan dan termasuk dalam rencana keamanan disetujui.						
No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
3.	Sejauhmana tingkat penerapan prosedur telah dilakukan dalam keamanan sistem pada *call center*?						
4.	Apa harapan di masa yang akan datang terkait dengan penerapan prosedur dalam keamanan sistem pada *call center*?						

III	TOOLS AND AUTOMATION	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 5 dan 6 (a) Tidak adanya *tools* apapun untuk mendukung proses dalam keamanan IT pada *call center*. (b) Beberapa *tools* mungkin telah ada, karena memang sudah tersedia (bawaan) dalam tools perangkat standar. Belum ada rencana menggunakan software khusus keamanan IT untuk *call center*. (c) Telah digunakannya tools untuk membantu proses keamanan IT sebagai solusi yang dikembangkan atas inisiatif perorangan berdasarkan pengalaman/keahliaannya dan dibantu oleh vendor. (d) Adanya rencana penggunaan *tools* standar untuk melakukan otomasi dalam keamanan IT, namun masih belum terintegrasi. (e) Penggunaan tools terkini telah mulai dimanfaatkan sesuai rencana standarisasi penggunaan tools. Beberapa tools telah terintegrasi dengan tools yang lainnya. *Tools* tersebut digunakan untuk mengotomasikan keamanan sistem. (f) *Tools* yang canggih digunakan dengan otomasi manajemen keamanan sistem secara maksimal dan terintegrasi dengan tools lain yang terkait. *Tools* digunakan untuk mendukung upaya perbaikan proses yang secara otomatis mampu mendeteksi kelemahan kontrol yang terjadi.	
No	Pertanyaan	Jawaban

		a	b	c	d	e	f
5.	Sejauhmana penggunaan tools dalam mengotomasikan proses-proses terkait dengan keamanan sistem pada *call center*?						
6.	Apa harapan di masa yang akan datang terkait dengan pengguna tools dalam mengotomasikan keamanan sistem pada *call center*?						

IV	SKILLS AND EXPERTISE	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 7 dan 8 (a) Tidak ada pelatihan keamanan IT untuk *call center*. (b) Belum ada dalam perencanaan adanya pelatihan untuk keamanan IT dan belum ada pelatihan formal dilakukan. (c) Kebutuhan *skills* minimal telah diidentifikasi untuk menangani permasalahan kritis keamanan IT pada *call center*. Pelatihan dilakukan masih secara informal inisiatif individu. (d) Kebutuhan skills keamanan IT telah diidentifikasi dan didokumentasikan secara lengkap. Perencanaan pelatihan formal telah dikembangkan. Pelatihan formal bagi bagi staf mulai dilakukan, walau masih didasarkan inisiatif perorangan. (e) Kebutuhan *skilss* secara rutin di *update* untuk keamanan sistem guna mendapatkan keahlian dan sertifikasi. Pelatihan formal terhadap staf terkait manajemen keamanan sistem telah dilakukan sesuai dengan rencana dan *knowledge sharing* dilakukan. Dilakukan evaluasi terhadap efektivitas rencana pelatihan. (f) Perusahaan secara formal memberikan kesempatan pada staf untuk mengembangkan skill secara berkelenjutan. Pelatihan dan pembelajaran mendukung praktek terbaik eksternal serta telah menggunakan konsep dan teknik terkini. Pelatihan untuk staff keamanan sistem telah dilembagakan. *Knowledge sharing* menjadi budaya perusahaan. Ahli	

	dari luar dimanfaatkan sebagai konsultan yang mampu memberikan panduan.						
No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
7.	Sejauhmana tingkat kesadaran pengembangan keterampilan dan keahlian sumberdaya manusia dalam bentuk pelatihan untuk keamanan sistem pada *call center*?						
8.	Apa harapan di masa yang akan datang terkait dengan pengembangan keterampilan dan keahlian sumberdaya manusia dalam bentuk pelatihan dilakukan guna mendukung proses keamanan sistem pada *call center*?						

V	RESPONSIBILITIES AND ACCOUNTTABILITIES	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 9 dan 10 (a) Tidak ada yang bertanggungjawab pada keamanan sistem *call center*. (b) Tanggungjawab manajemen keamanan sistem masih tidak jelas dan belum didefinisikan. Tanggung jawab dilakukan secara reaktif dan atas dasar inisiatif perorangan. (c) Peran dan tanggungjawab atas manajemen keamanan sistem secara informal tidak diterapkan oleh perorangan. Bila terjadi permasalahan terkait dengan manajemen keamanan sistem, tidak jelas siapa yang harus bertanggung jawab sehingga muncul kecenderungan budaya menyalahkan. (d) Peran dan tanggungjawab manajemen keamanan sistem telah ditetapkan serta permasalahan integritas dan keamanan data dikendalikan oleh pihak yang bertanggungjawab. Namun pemilik proses dalam menjalankan perannya. (e) Peran dan tanggungjawab pada manajemen keamanan sistem didefinisikan secara jelas, ditetapkan dan didokumentasikan dalam organisasi. Hal demikian mendukung pemilik proses dalam menjalankan perannya dengan baik. Ada budaya untuk memberikan penghargaan sebagai upaya memotivasi peran ini.	

	(f) Tanggungjawab keamanan IT ditetapkan secara jelas, diketahui secara luas di organisasi serta di-update secara periodik. Pemilik proses diberdayakan sehingga dapat membuat keputusan dan melakukan tindakan yang diperlukan.						
No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
9.	Sejauhmana penetapan tanggungjawab dan dalam keamanan IT diperusahaan untuk *call center*?						
10.	Apa harapan di masa yang akan datang terkait dengan penetapan tanggungjawab keamanan sistem?						

VI	GOAL SETTING AND MEASUREMENT	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 11 dan 12 (a) Kebutuhan akan kualitas dan keamanan IT belum ada. (b) Tujuan keamanan sistem belum jelas dan belum ada pengukuran. (c) Aktivitas pengawasan terhadap manajemen keamanan sistem mulai dilakukan walaupun masih belum secara konsisten terutama pada aktivitas penting seperti Jumlah hak akses dasar, dicabut, reset atau diubah. (d) Beberapa tujuan dan pengukuran dalam keamanan IT telah ditetapkan, walaupun belum dikomunikasikan. Ada kaitan yang jelas dengan tujuan bisnis. Pengukuran proses mulai dilakukan walaupun masih belum konsisten. Frekuensi dan penelaahan terhadap jenis kejadian keamanan yang akan dipantau. Pengawasan terhadap proses manajemen keamanan telah dilakukan. (e) Indikator pencapain tujuan dan kinerja telah disepakati pengguna dan dimonitor dengan proses yang telah didefinisikan serta dikaitkan dengan tujuan bisnis dan rencana strategi TI. Telah diterapkan "ISO27k" (ISO/IEC 27000-series). dalam menilai kinerja keamanan sistem. Perbaikan secara berkelanjutan pada proses	

	keamanan IT dilakukan. (f) Indicator pencapaian tujuan dan kinerja telah disepakati oleh pengguna, dikaitkan dengan tujuan bisnis dan secara konsisten dimonitor menggunakan proses yang telah didefinisikan. Mengintegrasikan sistem pengukuran kinerja proses keamanan sistem yang mengaitkan kinerja TI dan tujuan bisnis dengan menerapkan "ISO27k" (ISO/IEC 27000-series).						
No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
11.	Sejauhmana telah dilakukan pengawasan dan pengukuran atas kinerja keamanan sistem dilakukan?						
12.	Apa harapan di masa yang akan datang terkait dengan pengawasan dan pengukuran atas kinerja keamanan sistem?						

Kuisioner I
Analisis Tata kelola Teknologi Informasi Pada *Ensure System Security Call Center* di PT Arga Bangun Bangsa (ESQ LC)
Ensure System Security

Kuisioner ini merupakan bagian dari penelitian Skripsi mahasiswa program studi Sistem Informasi UIN Syarif Hidayatullah Jakarta, yang bertujuan untuk memperoleh data ataupun opini dari karyawan Perusahaan PT Arga Bangun Bangsa sebagai pihak yang terkait dalam pengelolaan TI khususnya pada penjaminan keamanan sistem call informasi center.

Kuisioner I *Management Awarness* ini dikembangkan untuk mengetahui tingkat pemenuhan terhadap *Detailed Control Objective* (DCO) dan pencapaian indikator kinerja dalam proses menjamin kemanan sistem. Adapun DCO tersebut meliputi penyusunan dan memelihara peranan-peranan keamanan (security roles) serta tanggung jawab, kebijakan, standar dan prosedur. Manajemen keamanan juga mencakup pengawasan keamanan dan ujicoba secara periodik, serta mengimplementasikan aksi perbaikan untuk kelemahan kekurangan atau insiden/bencana. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis terhadap kelemahan keamanan dan insiden.

Kuisioner ini didisain dalam format campuran pilihan ganda dan essay, yang terdiri dari 14 pertanyaan. Pada kolom "Tingkat Kinerja", responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili kondisi yang sebenarnya di lapangan dengan memberikan tanda (v) pada tempat yang tersedia, dimana kolom L menyatakan tingkat kinerja "Kurang", kolom M menyatakan tingkat kinerja "Sedang", dan kolom H menyatakan tingkat kinerja "Baik". Sedangkan pada kolom "komentar", responden dapat memberikan jawaban bebas dalam bentuk essay yang mendukung tingkat kinerja.

Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan pilihan maupun opininya sebagai jawaban atas pertanyaan-pertanyaan yang diberikan dalam kuesioner ini untuk kemudian dapat diolah dalam penelitian skripsi ini.

Nama Responden		Kode :
Jabatan Responden		
Unit/Bidang/Subbid		

No	Pertanyaan	Tingkat Kinerja			Komentar
		L	M	H	
1	Bagaimana Manajemen kemanan TI pada level organisasi yang tertinggi Menerjemahkan bisnis, risiko dan kepatuhan (*compliance*) ke dalam rencana kemanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan?				

2	Bagaimana rencana diimplementasikan dalam prosedur dan kebijakan kemanan bersama-sama investasi yang tepat dalam layanan, personel, *software* dan *hardware*?				
3	Bagaimana mengkomunikasikan kebijakan dan prosedur kemanan kepada *stakeholder* dan *user* ?				
4	Bagaimana konfirmasi hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, kebutuhan kerja yang melekat pada identitas pengguna serta memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan ?				
5	Bagaimana memelihara identitas pengguna dan hak akses dalam repositori pusat. menjaganya agar terus update dalam membuat identifikasi user, implementasi otentikasi dan memaksakan hak akses ?				
6	Bagaimana menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodifikasian dan penutupan akun user serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun *user* ?				
7	Bagaimana prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua *user* termasuk administrator, *user* internal dan eksternal, untuk normal dan kasus darurat ?				
8	Bagaimana hak dan kewajiban terhadap akses ke sistem oraganisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis *user* ?				
9	Bagaimana melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung?				
10	Bagaimana menguji dan memantau implementasi keamanan TI dalam langkah yang proaktif ?				

11	Bagaimana kemanan TI ditinjau secara periodik untuk memastikan landasan kemanan informasi organisasi yang disetujui dan dipelihara?				
12	Bagaimana mendefinisikan secara jelas dan mengkomuniksasikan karakteristik dari insiden keamanan yang potential sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah?				
13	Bagaimana membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentaasi keamana yang tidak perlu ?				
14	Bagaimana penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah?				
15	Bagaimana memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama *patch* keamanan yang *up-to-date* dan pengendalian virus) diseluruh organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (aeperti *virus*, *worm*, s*pyware* dan *spam*)?				
16	Bagaimana Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan *non-repudiation* ?				

Kuisioner II
Analisis Tata Kelola Teknologi Informasi Ensure System Security pada PT. Arga Bangun Bangsa
(ESQ LC)
Maturity Level

Kuisioner ini merupakan bagian dari penelitian Skripsi mahasiswa program studi Sistem Informasi UIN Syarif Hidayatullah Jakarta, yang bertujuan untuk memperoleh data ataupun opini dari karyawan Perusahaan PT Arga Bangun Bangsa sebagai pihak yang terkait dalam pengelolaan TI khususnya pada proses pengelolaan data.

Kuisioner II Pengukuran Tingkat Kematangan ini dikembangkan untuk mengetahui tingkat kematangan pada proses pengelolaan data baik untuk kondisi yang saat ini, maupun untuk kondisi yang diharapkan, yang selanjutnya dapat dijadikan dasar yang cukup untuk identifikasi prioritas penigkatan (*improvement*) pada proses pengelolaan data. Adapun pendekatan dalam pengukuran tingkat kematangan ini dilakukan dengan mempertimbangkan kematangan 6 (enam) atribut kematangan yang didefinisikan dalam COBIT 4.1, meliputi: awareness and communication, policies standars and procedures, tools and automation, skills and expertise, responsibilities dan goal and measurement.

Untuk mempermudah responden dalam menjawab, maka kuisioner ini didisain dalam format pilihan ganda, yang terrdiri dari 12 pertanyaan. Petanyaan-pertanyaan dikelommenurut atribut kematangan, dan pada tiap kelompok pertanyaan akan melibatkan dua (dua) pertanyaan yang masing-masing mewakili kondisi kekinian dan kondisi yang diharapkan. Masing-masing pertanyaan mempunyai 6 (enam) pilihan jawaban yang meunjukkan tingkat kematangan terhadap atribut tertentu pada proses pengelolaan data. pilihan-pilihan jawaban tersebut dari a sampai f secara berturut-turut mempresentasikan tingkat kematangan yang semakin meningkat terhadap suatu atribut pada proses *Ensure system security*.

Pada kolom "jawaban", responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili kondisi kematangan baik yang saat ini maupun yang diharapkan, terkait dengan atribut kematangan tertentu dalam proses pengelolaan data dengan memberikan tanda (v) pada tempat yang tersedia. Dengan mengetahui posisi kematangan saat ini danyang diharapkan, selanjutnya akan dilakukan analisis yang diharapkan dapat menjadi dasar dalam pendefinisian rancagan solusi untuk perbaikan dalam proses pengelolaan data.

Untuk kebutuhan di atas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan jwaban atas pertanyaan-pertanyaan yang diberikan dalam kuesioner ini untuk kemudian dapat diolah untuk penelitian skripsi ini.

Nama Responden		Kode :
Jabatan Responden		
Unit/Bidang/Subbid		

I	AWARENESS AND COMMUNICATION	
	Berikut pilihan jawaban untuk pertanyaan kuesioner no 1 dan 2 (a) Organisasi tidak menyadari kebutuhan untuk keamanan IT. Tanggung jawab dan akuntabilitas tidak ditugaskan untuk menjamin keamanan. (b) Organisasi mulai menyadari adanya kebutuhan kemananan IT pada *Call*	

	Center. keamanan ditujukan secara reaktif. Keamanan TI tidak diukur. Terdeteksi TI pelanggaran keamanan memanggil jari-menunjuk tanggapan, karena tanggung jawab tidak jelas. (c) Adanya kesadaran akan kebutuhan kemanan sistem untuk segera ditindaklanjuti. Diselenggarakan semacam forum untuk dapat mengkomunikasikan permasalahan terkait dengan keamanan sistem pada *Call Center*. (d) Adanya pemahaman akan kebutuhan kemanan sistem *call center*. kebutuhan tersebut telah dipahami dan diterima diperusahaan secara keseluruhan. Adanya semacam surat edaran dari manajemen atas untuk dapat melakukan langkah-langkah efektif untuk melakukan proses kemanan TIpada *call center*. (e) Kebutuhan bagi manajemen kemanan sistem secara utuh telah dipahami dan tindakan yang diperlukan sudah diterima secara luas di organisasi. Secara berkala diadakan forum internal perusahaan untuk dapat mencari solusi bersama atas permasalahan yang timbul dalam kemanan sistem pada *call center*. (f) Kebutuhan manajemen kemanan sistem dan pemahamannya atas langkah yang diperlukan telah dipahami dan diterima di organisasi. Keperluan dan kebutuhan kedepan senantiasa digali secara proaktif. Mengikuti forum berskala nasional maupun internasional untuk dapat melihat kecenderungan kedepan terkait dengan permasalahan dalam keamanan sistem pada *call center* yang juga merupakan peluang pengembangan kedepan.	

No	Pertanyaan	Jawaban					
		a	b	c	d	e	f
1.	Sejauhmana tingkat kesadaran pihak manajemen sampai saat ini terkait dengan keamanan TI pada *call center*?						
2.	Apa harapan di masa yang akan datang terkait dengan kesadaran akan kebutuhan keamanan call center?						

Jawaban kuisioner I Management Awarness DS5

No	Kode	Jawaban kuisioner																																		
		1			2			3			4			5			6			7			8			9			10			11			12		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
1	k1		1			1			1			1			1			1			1				1			1			1			1			1	
2	k2		1			1			1			1				1			1					1			1				1			1			1
3	k3		1				1	1					1		1				1			1				1					1			1			1
4	k4			1			1		1			1				1		1			1				1			1			1			1			1	
5	k5			1		1			1			1				1			1		1				1				1			1			1		
6	k6		1			1			1			1				1			1		1				1			1				1			1			1
7	k7			1		1			1			1			1			1		1				1		1					1			1			1	
8	k8		1			1			1				1			1		1				1		1			1			1			1			1	
9	k9		1			1				1		1				1		1				1			1			1			1			1			1	
10	k10		1				1			1			1		1			1				1			1		1			1			1				1
11	k11			1			1			1			1			1			1			1		1			1			1				1			1
12	k12			1		1			1		1			1			1			1				1			1			1			1			1	
13	k13		1			1			1			1			1				1			1	1			1				1			1				1

Jawaban kuisioner I Management Awarness DS11

No	Kode	Jawaban kuisioner																																										
		1			2			3			4			5			6			7			8			9			10			11			12			13			14		
		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
1	k1		1			1			1			1			1			1		1					1			1	1	1			1			1			1			1		
2	k2		1			1			1			1			1			1		1				1			1				1			1			1				1		
3	k3		1			1			1				1		1			1		1		1			1		1				1			1			1				1		
4	k4			1		1			1				1		1			1		1					1		1			1				1			1				1		
5	k5			1			1		1				1		1			1			1			1				1			1			1			1				1		
6	k6			1		1			1				1		1				1		1			1			1				1			1			1				1		
7	k7			1		1				1			1			1			1		1			1			1				1			1				1			1		
8	k8			1		1				1			1			1			1		1			1			1				1			1				1			1		
9	k9			1		1				1			1			1			1		1			1			1				1			1				1			1		
10	k10			1		1	1			1			1			1			1		1			1			1				1			1				1					1
11	k11			1		1	1			1			1			1			1			1		1			1				1				1				1					1
12	k12			1		1				1	1		1			1			1			1			1		1				1			1				1					1

Daftar pertanyaan interview

1. Apakah call center itu?

   Jawab: *Call center* merupakan aplikasi berbasis web based yg di gunakan oleh tim telemarketing, tim telecorporate, *finance*, dan BM.

   5. Tim telemarketing menggunakan *call center* utuk *call* dan registrasi *customer* yang akan mengikuti training.
   6. Tim telecorporate menggunakan *call center* untuk registrasi customer yang akan mengikuti training.
   7. Finance untuk memvalidasi pembayaran *training*.
   8. BM untuk monitoring jumlah peserta yg mengikuti *training* dan jumlah *call/day* yang di *call* oleh tim *telemarketing*.

2. Mendukung untuk apa aplikasi call center?

   Jawab: sudah di jawab

3. Apa tujuan call center?

   Jawab: seluruh kantor cabang dapat terintegrasi dalam hal melihat jumlah peserta *training*, Data tersimpan lebih baik di server.

4. Bagaimanakah arsitektur call center?

   Jawab: digambar

5. Bagaimana proses bisnis call center?

   Jawab:sudah tergambar di pertanyaan awal

6. Apakah sudah ada kebijakan untuk pengelolaan data dan keamanan sistem call center?

   Jawab: ada

7. Bagaimana proses pengelolaan data?

   Jawab: melakukan backup setiap hari

8. Bagaimana prosedur keamanan call center?

   Jawab: menggunakan firewall

9. Apakah ada peraturan eksternal (hukum, regulasi, perjanjian kontrak) yang berhubungan dengan pengelolaan data dan keamanan sistem?

   Jawab: ada

10. Apakah ada peraturan internal (standar, panduan dan prosedur) untuk pengelolaan data dan memastikan keamanan sistem?

    Jawab: ada

11. Bagaimanakah mengoperasikan aplikasi call center?

    Langsung melihat praktiknya.