BAB II

LANDASAN TEORI

2.1 Sistem Informasi

Menurut Hall dalam Sarno (2009: 26) sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas, yang menggunakan teknologi untuk mendukung kinerja, manajemen dan pembuatan keputusan (Beynon, 2004). Agar dapat berdaya guna maka SI seharusnya merupakan rangkaian prosedur formal yang melakukan pengelompokan data pemrosesan dan pendistribusian kepada pengguna. Dalam hal ini, sistem informasi digunakan tidak hanya untuk menggambarkan komputer dan perangkatnya serta interaksinya dengan organisasi, tetapi juga digunakan untuk menggambarkan interaksi seluruh komponen yang terlibat dalam proses bisnis organisasi tersebut.

Berdasarkan definisi sistem informasi tersebut, menurut Kristanto (2003: 15-16) peranan sistem informasi dalam bisnis, antara lain:

1. Mendukung operasi bisnis
2. Mendukung dalam pengambilan keputusan manajerial
3. Meraih keuntungan strategi

2.2 Audit

Definisi secara umum tentang audit adalah bahwa "*Auditing is an independent investigation of some particular activity*". Sebetulnya kata Audit itu sendiri berasal dari Bahasa Latin *Audire* yang dalam Bahasa Inggris berarti *to hear*.

Makna yang dimaksud disini adalah "*hearing about the account's balances*" oleh para pihak terkait terhadap pihak ketiga yang netral (tidak ada *vested interest*) mengenai catatan keuangan perusahaan yang dikelola oleh orang-orang tertentu yang bukan sekaligus pemiliknya (Gondodiyoto, 2007 : 28). Tujuan dari audit adalah untuk menentukan dan melaporkan tingkat kesamaan antara informasi yang dinilai dengan ukuran atau kriteria yang ada (Surendro, 2004).

Menurut Susilo (2003: 80), audit adalah kegiatan mengumpulkan informasi faktual dan signifikan melalui interaksi (pemeriksaan, pengukuran dan penilaian yang berujung pada penarikan kesimpulan) secara sistematis, obyektif dan terdokumentasi yang berorientasi pada azas penggalian nilai atau manfaat.

Audit juga dapat didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (ISACA, 2006).

2.3 Audit Sistem Informasi

Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif (Weber, 1999). Beberapa elemen utama

tinjauan penting dalam Audit Sistem Informasi yaitu dapat diklasifikasikan sebagai berikut.

1. Tinjauan terkait dengan fisik dan lingkungan, yakni: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database, seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap *firewall*, daftar kontrol akses *router*, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur *backup* dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/kontinuitas bisnis yang dimiliki.

6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

Tahapan audit sistem informasi dibagi menjadi 4 (empat) tahapan yaitu: 1. Tahap perencanaan audit, 2. Tahap persiapan audit, 3. Tahap pelaksanaan audit, 4. Tahap pelaporan audit (Hermawan, 2011). Keempat tahapan tersebut adalah sebagai berikut.

1. Tahap Perencanaan Audit Sistem Informasi

Tahap perencanaan ini dilakukan oleh auditor untuk mengetahui tentang *auditee* (*how your auditee*) dan mempelajari tentang proses bisnis perusahaan yang diaudit. Pada tahap ini ditentukan ruang lingkup dan tujuan dari audit sistem informasi yang hendak dikerjakan.

2. Tahap Persiapan Audit Sistem Informasi

Pada tahap persiapan, auditor merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci, kemudian mempersiapkan kertas kerja audit sistem informasi yang akan dipakai.

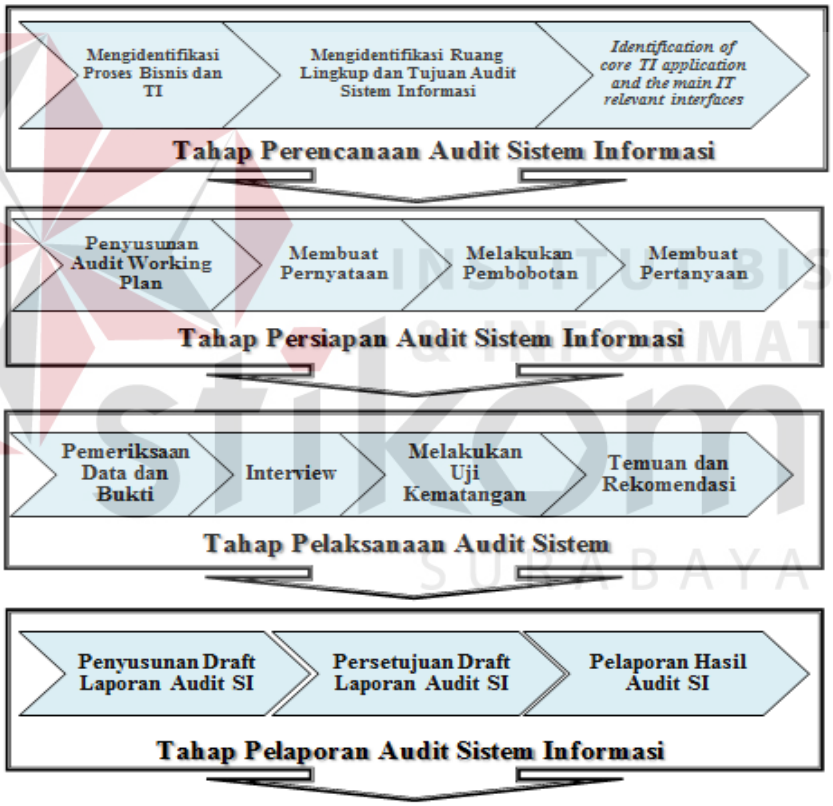
3. Tahap Pelaksanaan Audit Sistem Informasi

Pada tahap pelaksanaan, auditor melakukan pengumpulan dan evaluasi bukti dan data audit sistem informasi yang dilakukan, serta melakukan uji kepatutan (*complience test*), yakni dengan menyesuaikan keadaan ada dengan standar pengelolaan proses TI yang didefinisikan dalam kerangka kerja ISO 27002. Selanjutnya dilakukan penyusunan temuan serta rekomendasi guna diberikan kepada *auditee*.

4. Tahap Pelaporan Audit Sistem Informasi

Pada tahap pelaporan, auditor membuat *draft* pelaporan yang obyektif dan komperehensif yang nantinya ditunjukan ke *auditee*.

Tahapan-tahapan dalam audit sistem informasi merupakan langkah sekuensial. Setiap tahapan terdapat langkah-langkah yang harus dilakukan (Dhipiya, 2012). Tahapan-tahapan dalam audit sistem informasi dapat dilihat pada Gambar 2.1.



Gambar 2.1 Tahapan-Tahapan dalam Audit Sistem Informasi
(Sumber: Dhipiya, 2012)

2.4 Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno dan Iffano, 2009: 26). Contoh Keamanan Informasi menurut Sarno dan Iffano (2009: 27) adalah:

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

isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Aspek Keamanan Informasi meliputi ketiga hal, yaitu: *Confidentiality*, *Integrity*, dan *Availability* (CIA). Aspek tersebut dapat dilihat pada Gambar 2.2 di halaman 16 yang lebih lanjut akan dijelaskan sebagai berikut.

a) *Confidentiality*: Keamanan Informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses Informasi tertentu.
b) *Integrity*: Keamanan Informasi seharusnya menjamin kelengkapan Informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah Informasi dari aslinya.
c) *Availability*: Keamanan Informasi seharusnya menjamin pengguna dapat mengakses Informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses Informasi.

Gambar 2.2 Aspek Keamanan Informasi
(Sumber: Sarno dan Iffano, 2009: 37)

2.5 ISO/IEC 27002:2005

International Standards Organization (ISO) mengelompokkan standar keamanan informasi yang umum dikenali secara internasional ke dalam struktur penomoran yang standar yakni ISO 17799. ISO IEC 17799 tahun 2005, resmi dipublikasikan pada tanggal 15 Juni 2005. Pada tanggal 1 Juli 2007, nama itu secara resmi diubah menjadi ISO IEC 27002 tahun 2005. Konten tersebut masih persis sama. Standar ISO IEC 17799:2005 (sekarang dikenal sebagai ISO IEC 27002:2005) dikembangkan oleh IT *Security Subcommittee* (SC 27) dan *Technical Committee on Information Technology* (ISO/IEC JTC 1) (ISO 27002, 2005).

ISO 27002:2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan

seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27001.

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

Pada Gambar 2.3 dapat dilihat bahwa *International Standards Organization* (ISO) mengelompokkan semua standard keamanan informasi ke dalam satu struktur penomoran, yaitu pada serial ISO 27000 (Sarno, 2009:57). Penjelasan singkat mengenai masing-masing penomoran dalam Gambar 2.3 akan dipaparkan sebagaimana berikut.

<table>
<tr><td colspan="2">27000 Fundamental & Vocabulary</td></tr>
<tr><td rowspan="4">27005
RISK
MANAGEMENT</td><td>27001: ISMS</td></tr>
<tr><td>27002: Code of Practice for ISMS</td></tr>
<tr><td>27003: Implementation Guidance</td></tr>
<tr><td>27004: Metric & Measurement</td></tr>
<tr><td colspan="2">27006: Guidelines on ISMS Accreditation</td></tr>
<tr><td colspan="2">27007: Guidelines on ISMS Auditing</td></tr>
</table>

Gambar 2.3 ISO/IEC 27000 *Family*
(Sumber: Sarno dan Iffano, 2009: 56)

a. **ISO 27000:** dokumen definisi-definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.

b. **ISO 27001:** berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

c. **ISO 27002:** terkait dengan dokumen ISO 27001, namun dalam dokumen ini berisi panduan praktis (*code of practice*) teknik keamanan informasi.

d. **ISO 27003:** panduan implementasi sistem manajemen keamanan informasi perusahaan.

e. **ISO 27004:** berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

f. **ISO 27005:** dokumen panduan pelaksanaan manajemen resiko.

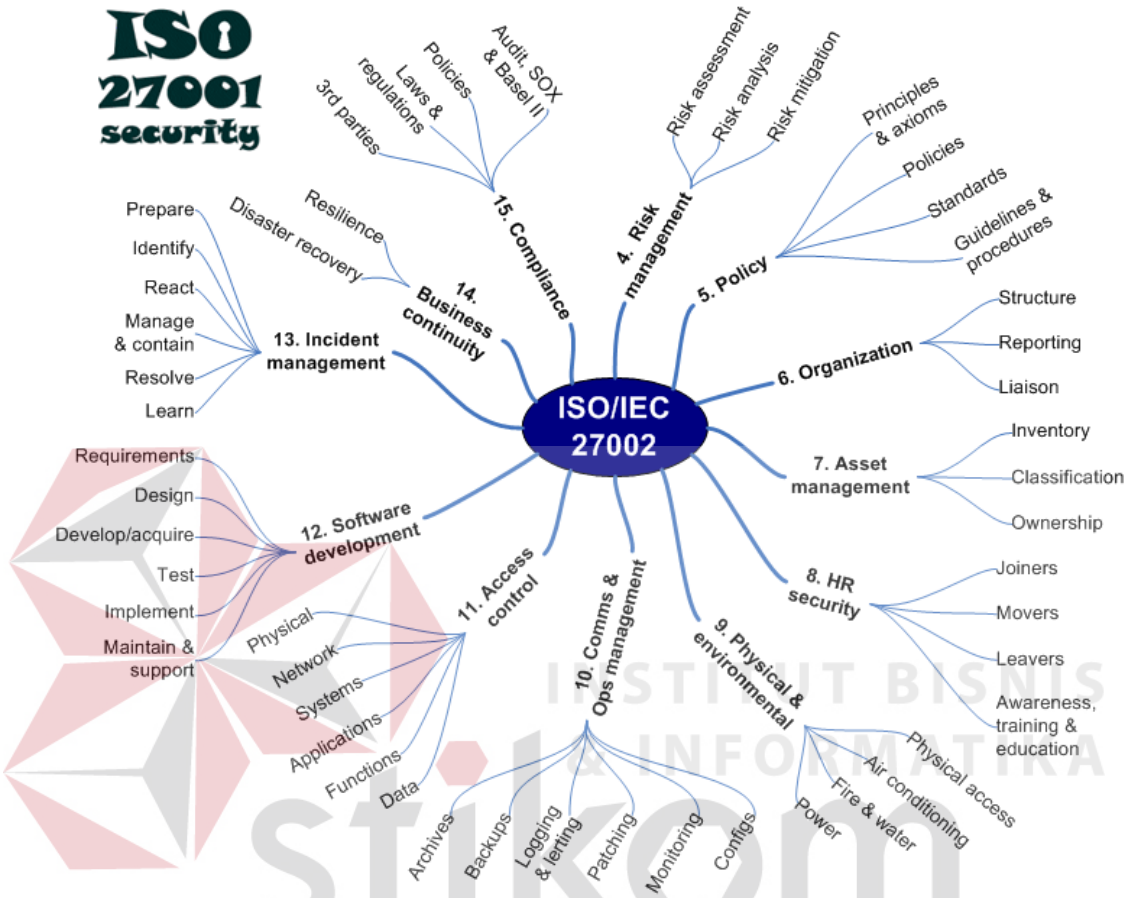
g. **ISO 27006:** dokumen panduan untuk sertifikasi SMKI perusahaan.

h. **ISO 27007:** dokumen panduan audit SMKI perusahaan.

Pemetaan terhadap ISO 27002 dapat dilihat pada Gambar 2.4 di halaman 19. Untuk detail struktur dokumen kontrol keamanan dari ISO/IEC 27002 dapat dilihat pada Lampiran Detail Struktur Dokumen Kontrol Keamanan ISO/IEC 27002.

2.6 Kebijakan Kontrol Akses

Kontrol akses adalah kumpulan dari metode dan komponen yang dipergunakan untuk melindungi asset informasi (Winarta, dkk, 2005:10). Kontrol akses mendukung baik kerahasiaan dan integritas dari sebuah sistem yang aman. Kontrol akses kita gunakan untuk memastikan hanya orang-orang yang berhak saja yang dapat melihat informasi. Kontrol akses memberikan kemampuan untuk mendikte mana informasi yang bisa dilihat atau dimodifikasi oleh user.



Gambar 2.4 Pemetaan ISO 27002 (Sumber: ISO/IEC, 2005)

Menurut Winarta, dkk (2005:10) tujuan dari kebijakan kontrol akses adalah mengijinkan hanya subyek yang mempunyai otorisasi yang bisa mengakses obyek yang sudah diijinkan untuk diakses. Hal ini mungkin juga ada subyeks yang sudah mempunyai otorisasi tapi tidak melakukan akses terhadap spesifik obyek tertentu.

Persyaratan bisnis kontrol akses harus ditetapkan dan didokumentasikan. Peraturan dan hak kontrol akses untuk setiap pengguna atau kelompok pengguna harus dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.

Pengguna dan penyedia layanan harus diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses (Sarno dan Iffano, 2009:303). Menurut Sarno dan Iffano (2009: 303) kebijakan harus mencakup hal berikut:

1. Persyaratan keamanan dari aplikasi bisnis perorangan;
2. Identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis;
3. Kebijakan diseminasi dan otorisasi Informasi. Misalnya kebutuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi Informasi;
4. Konsistensi antara kontrol akses dan kebijakan klasifikasi Informasi dari sistem dan jaringan yang berbeda;
5. Peraturan yang relevan dan setiap kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan;
6. Profil standar akses pengguna untuk kategori pekerjaan yang umum;
7. Manajemen hak akses di lingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia.

2.7 Registrasi Pengguna

Menurut Winarta, dkk (2005: 11) Organisasi-organisasi menggunakan beberapa kebijakan dalam menerapkan peraturan kontrol akses. Filosofi yang paling tidak aman adalah memberikan hak akses kepada setiap orang secara *default*. Memang kelihatannya mudah akan tetapi hal ini mudah juga untuk ditembus. Jadi pada metode ini, kita harus memastikan bahwa semua akses harus dibatasi, administrasi yang buruk bisa menyebabkan lubang keamanan. Filosofi dari *least privilege* adalah sebuah subyek hanya diberikan hak sesuai dengan keperluannya

tidak lebih. *Least privilege* membantu menghindari *authorization creep*, yaitu sebuah kondisi dimana sebuah subyek memiliki hak akses lebih dari apa sebenarnya dibutuhkan. Mereka memberikan hak tertentu kepada *user* yang memang memiliki tanggung jawab untuk menjaga semua operasi yang melibatkan database berjalan lancar tanpa gangguan. Sehingga orang tersebut diberikan *user id* dan *password* yang bisa dipakai untuk melakukan monitor terhadap beberapa server untuk keperluan operasional.

Menurut Sarno dan Iffano (2009: 305) harus ada prosedur pendaftaran dan pengakhiran secara formal terhadap sebagai pengguna untuk memberikan akses menuju Sistem Informasi dan layanan seluruh kelompok pengguna. Akses dari pengguna layanan bagi Informasi harus di Kontrol melalui proses pendaftaran pengguna secara formal, yang harus meliputi:

1. Penggunaan ID pengguna yang unik, agar pengguna dapat terhubung dan bertanggung jawab atas tindakannya. Penggunaan ID kelompok harus mendapat ijin apakah mereka diperbolehkan sesuai pekerjaan yang dilakukan;
2. memeriksa apakah pengguna yang mempunyai otorisasi dari pemilik sistem, menggunakan untuk akses Sistem Informasi atau layanan. Persetujuan terpisah tentang hak akses dari manajemen juga diperlukan;
3. memeriksa apakah tingkatan akses yang diberikan sesuai dengan tujuan bisnis dan konsisten dengan kebijakan organisasi tentang sistem keamanan, misalnya tidak menyalahgunakan pemisahan pemisahan tugas;
4. memberikan pengguna pernyataan secara tertulis tentang hak akses mereka;

5. keharusan pengguna untuk menadatangani pernyataan yang menandakan bahwa mereka memahami tentang kondisi dari aksesnya;
6. memastikan penyedia layanan tidak menyediakan akses hingga prosedur otorisasi dilengkapi;
7. memelihara catatan resmi seluruh individu yang terdaftar untuk menggunakan layanan;
8. mengakhiri hak akses pengguna yang telah pindah dari pekerjaannya atau meninggalkan organisasi;
9. memeriksa secara periodik, dan mengakhiri, pengulangan penggunaan ID dan catatan pengguna;
10. menjamin bahwa ID pengguna yang sama tidak dikeluarkan kepada pengguna lain.

Pertimbangan yang diberikan harus mencakup klausa tentang kontrak kerja dengan staf dan kontrak pemberian layanan yang menjelaskan sanksi tertentu jika akses tanpa ijin dilakukan oleh staf atau agen pemberi layanan.

2.8 Manajemen Hak Istimewa atau Khusus

Tujuan dari kontrol ini adalah untuk memastikan bahwa proses formal yang didirikan untuk mengurangi resiko penipuan ID dan akses yang tidak sah. Proses ditetapkan untuk *user registration* dan *de-registration*. Proses pendaftaran dimulai dari waktu seseorang bergabung organisasi. ID pengguna dalam aplikasi sistem dan akses harus berdasarkan tanggung jawab pekerjaan atau peran seseorang. Tim sumber daya manusia (SDM) bekerja sama dengan tim TI untuk memberikan ID pengguna

untuk karyawan baru. Proses otorisasi harus dibentuk untuk memvalidasi kebutuhan penciptaan user ID dalam sistem. Sebuah proses yang khas memiliki permintaan penyediaan akan melalui persetujuan yang diperlukan sebelum pengguna ID ditugaskan di sistem produksi. Semakin banyak perusahaan yang mengadopsi sistem *self-provisioning*, di mana peran dan ID pengguna yang diperlukan dalam sistem dikodifikasikan pada identitas dan akses sistem manajemen (IAM). IAM sistem juga menyediakan *Workflow* yang diperlukan untuk authorisations. Dalam sistem *self-provisioning*, pengguna dapat pergi untuk mengakses portal dan permintaan untuk aplikasi sistem.

Setelah persetujuan diberikan, *user id* tersedia secara otomatis di beberapa aplikasi dimana pengguna diizinkan akses. Hak akses yang diperlukan juga ditetapkan berdasarkan peran atau profil dalam aplikasi. *Critical factor success* adalah bahwa peran pengguna bisnis harus terhubung ke peran dan hak istimewa dalam aplikasi ini didokumentasikan dan disetujui oleh manajemen. Otomatisasi menggunakan sistem IAM adalah praktik terbaik dan dapat mengurangi overhead proses. Proses serupa harus tersedia untuk *de-registrasi*. Tim SDM harus memberitahukan hal itu segera setelah seseorang telah meninggalkan organisasi, lalu tim IT harus menghapus atau menonaktifkan user ID untuk jangka waktu tertentu sebelum penghapusan. Skenario lain adalah proses harus dapat mengatasi pengguna lintas divisi, terkait promosi, perubahan dalam id pengguna dan hak istimewa (Vasudevan, dkk, 2008).

Alokasi dan penggunaan hak khusus sebagai contoh fitur atau fasilitas Sistem Informasi dengan kelompok pengguna yang beragam memungkinkan adanya peluang

pengguna untuk menembus sistem atau kontrol aplikasi sehingga harus dibatasi dan dikontrol. Penggunaan hak khusus tentang sistem yang tidak semestinya sering ditemukan sebagai faktor penyebab utama kegagalan sistem. Sistem kelompok pengguna yang mensyaratkan perlindungan terhadap akses tanpa ijin harus mempunyai alokasi hak khusus yang dikontrol melalui proses otorisasi formal (Sarno dan Iffano, 2009: 306). Menurut Sarno dan Iffano (2009: 304) beberapa langkah berikut harus dipertimbangkan:

1. hak khusus yang terkait dengan setiap produk sistem, misalnya sistem operasi, sistem manajemen database dan setiap aplikasinya, dan kategori staf yang akan dialokasikan harus diidentifikasi.
2. hak khusus harus dialokasikan kepada individu berdasarkan kebutuhan pengguna dan kasus per kasus, sebagai contoh persyaratan minimum untuk peran fungsionalnya, jika diperlukan.
3. proses otorisasi dan catatan seluruh hak khusus yang dialokasikan harus dipelihara. Hak khusus harus tidak boleh diberikan sampai proses otorisasi dilengkapi.
4. perkembangan dan penggunaan sistem yang umum harus dipromosikan untuk menghindari kebutuhan pemberian hak khusus kepada pengguna.
5. hak khusus harus diberikan pada identitas pengguna yang berbeda dari identitas yang digunakan untuk kepentingan bisnis secara umum.

2.9 Manajemen *password* user

Password adalah alat umum untuk memvalidasi identitas pengguna untuk mengakses Sistem Informasi atau layanan Sadikin (2010:8). Kebijakan *password* akun *user* menurut:

1. Semua *user* dilarang untuk membagikan *password* akun milik sendiri ke orang lain (termasuk keluarga, sahabat karib, dan sebagainya).
2. Semua *user* dilarang menggunakan akun milik orang lain.
3. Akun *user* hanya dapat digunakan sekali pada waktu yang bersamaan (menggunakan kabel atau *wireless*)
4. Tamu yang akan memakai koneksi internet diberi nama *user* "*guest*" dengan *password* yang selalu berbeda tiap hari. *Password guest* diberikan oleh *admin*.

Alokasi dari *password* harus dikontrol melalui proses manajemen yang formal, menurut Sarno dan Iffano (2009: 307) pendekatannya sebagai berikut:

1. Pengguna harus menandatangani pernyataan untuk menjaga *password* pribadi secara rahasia dan *password* kelompok hanya untuk anggota kelompok tersebut.
2. menjamin, pengguna untuk memelihara *password*-nya. *Password* sementara yang aman disediakan sistem dan mengharuskan *user* mengganti *password* sesegera mungkin. *Password* sementara yang diberikan ketika pengguna lupa *password*-nya hanya boleh disediakan jika terdapat identifikasi pengguna yang jelas;
3. mensyaratkan *password* sementara diberikan ke pengguna secara aman. Penggunaan pihak ketiga atau pesan surat elektronik secara terbuka harus dihindarkan. Pengguna harus memberitahukan bahwa mereka telah menerima *password*.

Password tidak boleh disimpan dalam sistem komputer bila tidak terlindungi untuk identifikasi dan otentifikasi pengguna, misalnya biometrik, yaitu pengesahan sidik jari, tanda tangan dan penggunaan piranti keras token, sebagai contoh kartu chip, tersedia dan harus dipertimbangkan jika perlu.

2.10 Tinjauan terhadap hak akses user

Pengertian kontrol akses dalam aplikasi dimulai dengan definisi dari peran pengguna dan otorisasi yang sesuai atau hak akses *user* berdasarkan kebutuhan bisnis. Setelah peran dan otorisasi jelas, baru dapat diimplementasikan dalam aplikasi. Aplikasi harus memiliki modul administrasi agar dapat mendefinisikan peran dan hak-hak user. Kebanyakan aplikasi perusahaan memiliki dukungan untuk fungsi tersebut namun biasanya ada kesenjangan dalam implementasi. Aplikasi juga harus memiliki cara intuitif untuk mendefinisikan otorisasi tersebut. Otorisasi lebih tinggi perlu disediakan oleh tim IT untuk memastikan bahwa fungsi utama aplikasi tidak terpengaruh (Vasudevan, dkk, 2008).

Menurut Sarno dan Iffano (2009: 308) untuk memelihara kontrol yang efektif terhadap akses ke data dan layanan informasi, manajemen harus mengarahkan satu proses formal secara berkala untuk mengkaji ulang hak pengguna terhadap akses agar:

1. hak akses pengguna dapat dikaji ulang dalam rentang waktu secara berkala setiap 6 bulan sekali dan setelah ada perubahan;
2. otorisasi untuk hak khusus harus dikaji ulang dalam rentang waktu yang lebih sering kurang lebih setiap 3 bulan sekali;

3. alokasi hak khusus diperiksa dalam rentang waktu secara berkala untuk memastikan bahwa tidak ada hak khusus diminta tanpa ijin.

2.11 Penggunaan Password

Pengguna harus mengikuti latihan keamanan yang baik dalam pemilihan dan penggunaan *password*. *Password* disediakan untuk memvalidasi identitas pengguna dan dengan demikian menetapkan hak akses ke fasilitas pemrosesan informasi atau layanan. Menurut Sadikin (2010: 10) ketentuan kebijakan *password* sebagai berikut.

1. Panjang *password user* minimal 8 karakter dengan perpaduan antara huruf kapital, huruf kecil, angka, dan karakter khusus (!@#$%^&*()_+|).
2. Disarankan semua *user* mengganti *password*-nya dalam 1 bulan.
3. *Password* yang menggunakan 1 karakter dengan panjang 8 digit atau lebih akan tetap kena pinalti.
4. *User* yang mengganti *password*-nya akan dicatat dalam file *log server*.

Menurut Sarno dan Iffano (2009: 309) seluruh pengguna harus disarankan untuk:

1. menjaga *password* secara rahasia;
2. tidak menyimpan catatan tertulis *password*, kecuali bisa disimpan secara aman;
3. merubah *password* apabila ada indikasi kemungkinan sistem atau *password* disalahgunakan;
4. memilih *password* yang baik dengan panjang minimum enam karakter dengan catatan:
   a. gampang diingat;

b. tanpa dasar apapun seseorang dapat dengan mudah menebak atau memperoleh menggunakan informasi terkait, misalnya nama, nomor telepon, dan tanggal lahir dan sebagainya;

5. bebas dari karakter sejenis yang berurutan atau nomor atau huruf yang sama.
6. merubah *password* dalam rentang waktu secara berkala atau berdasarkan jumlah pengakses sebagai contoh *password* untuk hak khusus harus diganti lebih sering dari pada *password* yang umum dan menghindari penggunaan kembali atau pengulangan *password* yang lama;
7. merubah *password* sementara pada proses log-on otomatis misalnya disimpan dalam satu macro atau *function key*;
8. tidak membagikan *password* pengguna individu.

2.12 Peralatan Pengguna Yang Tidak Dijaga

Menurut Voicee (2010: 1) Pengguna harus memberikan perlindungan pada peralatan yang tidak dijaga. Peralatan yang dipasang di wilayah pengguna, misalnya *workstation* atau *file server*, harus mendapat perlindungan khusus dari akses tanpa ijin jika tidak dijaga untuk waktu tertentu. PC harus menggunakan *screen saver* yang dilindungi *password* dan *screen saver* harus diatur menyala secara otomatis setelah waktu wajar tidak aktif antara lima dan tujuh menit. Dengan mengunci layar dapat mencegah orang lain untuk mengakses PC dan membaca informasi yang masih terbuka dilayar PC. Seluruh pengguna dan kontraktor harus disadarkan dan diberi tanggung jawab untuk menerapkan sistem keamanan dan prosedur untuk melindungi

peralatan yang tidak dijaga. Menurut Sarno dan Iffano (2009:310) pengguna harus disarankan untuk:

1. menghentikan sesi aktif ketika selesai, kecuali dapat diamankan dengan mekanisme pengunci yang tepat, misalnya *screen saver* yang dilindungi dengan *password*;
2. *log-off* dari *mainframe* ketika sesi berakhir contoh tidak sekedar mematikan komputer atau terminal;
3. mengamankan PC atau terminal dari akses tanpa ijin dengan menggunakan *key lock* atau alat kontrol sejenis, seperti akses *password*, ketika tidak dipakai.

2.13 Kebijakan *clear desk* dan *clear screen*

Organisasi perlu merencanakan atau mengadopsi kebijakan *clear desk* untuk cetakan atau dokumen dan media penyimpanan yang dapat dipindah. Selain itu juga diperlukan kebijakan *clear screen* untuk fasilitas pemrosesan informasi untuk mengurangi resiko akses tanpa ijin, kehilangan, dan kerusakan informasi selama dan diluar jam kerja. Kebijakan tersebut harus memperhatikan klasifikasi keamanan informasi, resiko korespondensi dan aspek budaya organisasi (Sarno dan Iffano, 2009: 311).

Pedoman *clear desk* dan *clear screen* menurut Voicce (2010: 1):

a. Pada akhir setiap hari, atau ketika meja / kantor sedang kosong, dan terdapat informasi 'rahasia' (seperti kertas, *flashdisk*, disk, dan sebagainya) harus disimpan di tempat yang aman.

b. Brankas, lemari arsip, laci, dan kantor / pintu ruangan harus dikunci jika tanpa pengawasan. Pada akhir setiap sesi semua informasi sensitif harus dihapus dari tempat kerja dan disimpan di tempat terkunci.

c. Semua limbah kertas yang memiliki informasi pribadi atau rahasia, harus dihancurkan atau ditempatkan di daerah sampah yang benar. Dalam situasi ini jenis limbah kertas dibuang dengan sampah biasa.

d. Selalu kunci layar dengan menekan *'Ctrl, Alt, Delete*' dan kemudian masukkan password untuk mengunci PC setiap kali meninggalkan meja dan pastikan bahwa diperlukan *password* saat *login* kembali.

e. *Screen saver* yang dilindungi *password* harus digunakan saat PC tidak terkunci. *Screen saver* harus diatur menyala secara otomatis setelah waktu yang wajar tidak aktif kira-kira antara lima dan tujuh menit.

f. Mengunci layar tidak hanya mencegah orang lain menggunakan PC, tetapi juga dapat mencegah seseorang membaca informasi rahasia yang terbuka pada layar.

g. Jangan meletakkan *password* ditempat yang mudah di akses rang lain seperti di bawah meja atau dibawah PC.

h. Saat sedang mengerjakan informasi sensitif, dan ada tamu yang berkunjung ke meja, maka layar harus segera dikunci agar informasi yang sedang terbuka tidak dapat dibaca pengunjung.

i. Semua printer dan mesin faks harus dibersihkan dari kertas segera setelah selesai dicetak, ini membantu memastikan bahwa dokumen-dokumen sensitif tidak tertinggal di tempat printer.

Menurut Sarno dan Iffano (2009: 311) informasi yang tertinggal di meja juga dapat rusak atau hancur karena bencana seperti kebakaran, banjir, atau ledakan. Kontrol berikut harus diperhatikan:

1. Dimana mungkin, cetakan dan media komputer harus disimpan dalam rak yang terkunci baik dan atau bentuk perangkat keamanan kantor lain pada saat tidak digunakan, khususnya di luar jam kerja.
2. Informasi bisnis yang sensitif dan penting harus disimpan terkunci idealnya di lemari besi atau rak tahan api jika tidak dipergunakan, khususnya pada saat kantor kosong.
3. Komputer pribadi dan terminal komputer dan printer tidak boleh ditinggal logged-on tanpa penjagaan dan harus dilindungi dengan kunci, *password* dan alat kontrol lain, ketika tidak dipergunakan.
4. Ruang surat masuk dan keluar, mesin faksimil dan telex yang tidak dijaga harus dilindungi.
5. Mesin fotocopy harus dikunci atau dilindungi dari penggunaan tanpa ijin diluar jam kerja umum.
6. Informasi sensitif atau berklarifikasi, jika tercetak, harus segera dipindahkan dari printer.

2.14 Prosedur *log-on* yang aman

Akses terhadap layanan informasi harus dapat dilakukan melalui proses *log-on* yang aman. Prosedur untuk masuk ke dalam sistem komputer harus didesain untuk memperkecil peluang akses tanpa ijin. Prosedur *log-on* harus membuka informasi

minimum tentang sistem, dengan tujuan menghindari pemberian bantuan yang tidak perlu kepada pengguna tanpa ijin. Menurut Sarno dan Iffano (2009: 319) prosedur *log-on* harus:

1. tidak menampilkan sistem atau aplikasi alat identifikasi sampai dengan proses *log-on* selesai dilakukan;
2. menampilkan peringatan umum bahwa komputer hanya boleh diakses oleh pengguna yang diijinkan;
3. tidak menyediakan pesan bantuan selama prosedur *log-on* yang dapat membantu pengguna tanpa ijin;
4. memvalidasi informasi *log-on* hanya setelah seluruh data masukan dilengkapi. Jika terjadi kesalahan, sistem tidak mengindikasikan bagian data mana yang benar atau salah;
5. membatasi jumlah kegagalan percobaan *log-on* yang diperbolehkan dianjurkan tiga kali dan mempertimbangkan:
   a. mencatat percobaan gagal;
   b. mengharuskan *time delay* sebelum percobaan *log-on* selanjutnya diperbolehkan atau menolak setiap percobaan selanjutnya tanpa otorisasi khusus;
   c. memutus koneksi sambungan data;
6. membatasi waktu maksimum dan minimum yang diperbolehkan untuk prosedur *log-on*. Jika melebihi, sistem akan menghentikan *log-on*;
7. menampilkan informasi berikut saat melengkapi *log-on* yang baik:
   a. tanggal dan waktu *log-on* berhasil terakhir;

b. rincian seluruh kegagalan *log-on* sejak *log-on* terakhir yang berhasil.

2.15 Identifikasi dan Otentifikasi User

Menurut Ningsih (2010: 6-8) ada beberapa metode otentifikasi *user* yaitu:

1. *Something you know*: Cara ini mengandalkan kerahasiaan informasi, ini berasumsi bahwa tidak ada seorang pun yang mengetahui rahasia itu kecuali anda seorang. Faktor *something you know* melibatkan pengetahuan informasi rahasia yang memungkinkan *user* meng-otentikasi dirinya sendiri ke sebuah server. Contohnya adalah password dan PIN.
2. *Something you have*: Cara ini biasanya merupakan faktor tambahan untuk membuat autentikasi menjadi lebih aman, melibatkan bahwa *user* harus memiliki alat secara fisik. Cara ini berasumsi bahwa tidak ada seorang pun yang memiliki barang tersebut kecuali anda seorang. Contohnya adalah kartu *magnetic/smartcard, hardware* token, USB token
3. *Something you are*: melibatkan bahwa *user* memiliki karakteristik yang unik yang membedakan dirinya dengan *user* lain untuk mengidentifikasi dirinya sendiri. Menggunakan metode identifikasi *biometrik* untuk meng-otentikasi *user*. Contoh meliputi sidik jari, pemindaian retina mata, dan garis tangan seseorang.
4. *Something you do*: melibatkan bahwa tiap *user* ketika melakukan sesuatu atau ketika menggunakan sesuatu dengan cara yang berbeda. Contoh: penggunaan analisis suara *voice recognition* atau analisis tulisan tangan.

Menurut Winarta, dkk (2005: 11) tambahan metode otentifikasi dan identifikasi *user*:

Single Sign-On: Semakin banyak informasi, atau faktor, yang diminta dari subjek, semakin menjamin bahwa subjek adalah benar-benar entitas yang diklaimnya. Oleh karenanya, otetikasi dua faktor lebih aman dari otentikasi faktor tunggal. Masalah yang timbul adalah bila subjek ingin mengakses beberapa sumber daya pada sistem yang berbeda, subjek tersebut mungkin diminta untuk memberikan informasi identifikasi dan otentikasi pada masing-masing sistem yang berbeda. Hal semacam ini dengan cepat menjadi sesuatu yang membosankan. Sistem *Single Sign-On* (SSO) menghindari login ganda dengan cara mengidentifikasi subjek secara ketat dan memperkenankan informasi otentikasi untuk digunakan dalam sistem atau kelompok sistem yang terpercaya. *User* lebih menyukai SSO, namun administrator memiliki banyak tugas tambahan yang harus dilakukan. Perlu perhatian ekstra untuk menjamin bukti-bukti otentikasi tidak tidak tersebar dan tidak disadap ketika melintasi jaringan. Beberapa sistem SSO yang baik kini telah digunakan. Tidak penting untuk memahami setiap sistem SSO secara detail. Konsep-konsep penting dan kesulitan-kesulitannya cukup umum bagi semua produk SSO.

Menurut Sarno dan Iffano (2009: 321) seluruh pengguna termasuk staf pendukung teknis, seperti operator, administrator database harus mempunyai alat pengidentifikasi khusus seperti ID pengguna untuk penggunaan pribadi dan terbatas agar aktifitas tersebut bisa dilacak sebagai pertanggung jawaban individu. ID pengguna tidak boleh memberikan indikasi tentang tingkatan hak khusus pengguna, misalnya manajer, pengawas. Dalam kondisi khusus, dimana ada keuntungan bisnis

yang jelas, penggunaan ID yang dapat digunakan bersama grup pengguna atau pekerjaan yang spesifik dapat digunakan. Pada kasus ini persetujuan manajemen harus terdokumentasi. Kontrol tambahan mungkin di butuhkan untuk menjaga akuntabilitas. Ada berbagai prosedur otentifikasi, yang dapat di pergunakan untuk membuktikan identitas pengguna. *Password* adalah cara umum untuk menyediakan identifikasi dan otentifikasi (I & O) berdasar pada satu kerahasiaan yang hanya diketahui pengguna. Hal yang sama juga dapat dicapai dengan metode kriptografis dan protokol otentikasi. Obyek seperti token memori atau kartu pintar yang dimiliki pengguna juga dapat digunakan untuk I & O. Teknologi otentikasi biometrik yang menggunakan karakteristik atau atribut khusus individu juga dapat digunakan untuk mengotentikasi identitas individu. Kombinasi teknologi dan mekanisme yang terhubung secara aman akan menghasilkan otentikasi yang lebih kuat.

2.16 Manajemen Password

Password adalah salah satu alat prinsip untuk memvalidasi otoritas pengguna dalam mengakses layanan komputer. Sistem manajemen *password* harus menyediakan fasilitas interaktif yang efektif yang memastikan *password* yang berkualitas. Menurut Ningsih (2010: 9) kaidah *strong password* merupakan suatu petunjuk/ tips yang perlu di ikuti oleh user individu atau dalam sebuah organisasi dalam membuat *username* dan *password* yang sulit untuk di tembus.

Berikut adalah petunjuk *strong password authentication*:

1. *User name* default yang di buat oleh sistem secara otomatis sebaiknya diganti untuk mencegah ditebak dengan mudah.

2. Password yang berisikan kata-kata yang terdapat dalam kamus sebaiknya di hindari karena dapat di pecahkan dengan menggunakan program perentas *password* atau *password cracking*.
3. Jika *user* memiliki *password* lebih dari satu untuk sistem jaringan dan situs web, biasanya mereka menyimpan daftar password tersebut dalam dalam sebuah file dalam sistem komputer mereka. Untuk melindungi file tersebut dari akses user yang tidak berhak, *user* seharusnya meng-enkripsi file tersebut dalam daftar *password*nya.
4. *Password* idealnya mudah di ingat tapi sulit untuk di tebak. Hindari penggunaan *password* lemah yang menggunakan pengenal pribadi seperti tanggal lahir, nama kecil. Contoh penggunaan *strong password* 12Ud!, yang mudah di ingat dengan menggunakan metode *mnemonic* rudi.

Beberapa aplikasi membutuhkan *password* untuk ditandatangani oleh otoritas independen. Dalam banyak kasus, *password* dipilih dan dijaga oleh pengguna. Menurut Sarno dan Iffano (2009: 322) sistem manajemen *password* yang baik seharusnya:

1. memastikan penggunaan *password* individu untuk menjaga tingkat kebenarannya;
2. membolehkan pengguna untuk memilih dan mengubah *password*nya dan termasuk prosedur konfirmasi utuk membolehkan kesalahan input;
3. pastikan pemilihan *password* berkualitas;
4. dalam hal pengguna mengelola *password* sendiri, pastikan mereka merubah *password*;

5. dalam hal pengguna memilih *password*, pastikan mereka merubah *password*nya pada *log-on* pertama;
6. menjaga catatan *password* pengguna sebelumnya, seperti 12 bulan sebelumnya, dan mencegah penggunaan ulang;
7. tidak menampilkan *password* di layar ketika dimasukkan;
8. menyimpan files *password* terpisah dari data sistem aplikasi;
9. menyimpan *password* dalam bentuk enkripsi menggunakan algoritma enkripsi *one-way*;
10. merubah *password default vendor* pada saat instalasi.

2.17 Penggunaan Utilitas Sistem

Sistem utilitas adalah alat yang digunakan untuk mengelola dan memecahkan masalah aplikasi dan data sistem. Contoh database administrasi perangkat lunak dan *registry* editor. Banyak dari utilitas alat ini yang dapat mengakses sumber daya sistem yang kritis. Oleh karena itu, di tangan yang salah, dapat menjadi alat-alat serangan yang efektif. *Database* administrator dapat memotong kontrol aplikasi dan langsung mengakses *database* dengan utilitas administrasi *database*. Ini adalah contoh dari mana utilitas sistem yang dapat digunakan untuk memotong kontrol aplikasi. Jadi tujuan dari kontrol ini adalah untuk membatasi penggunaan utilitas sistem tersebut.

Syarat-syarat sistem utilitas antara lain terpisah dari aplikasi sistem, menonaktifkan sistem utilitas sejauh mungkin dalam aplikasi sistem, hak akses ke utilitas ini hanya diberikan untuk pengguna tertentu, menjaga log akses dan penggunaan sistem utilitas (Vasudevan dkk, 2008).

Umumnya komputer mempunyai satu atau lebih fasilitas program sistem yang mampu menjalankan *overriding* sistem dan kontrol aplikasi. Sangatlah penting bahwa penggunaannya dibatasi dan di kontrol dengan ketat. Menurut Sarno dan Iffano (2009: 322) kontrol berikut harus diperhatikan:

1. penggunaan prosedur otentikasi untuk sistem fasilitas;
2. pemisahan sistem fasilitas dari piranti lunak aplikasi;
3. pembatasan penggunaan sistem fasilitas sampai ke minimum pengguna yang dipercaya dan diijinkan;
4. otorisasi untuk penggunaan sistem fasilitas;
5. pembatasan ketersediaan sistem fasilitas, yaitu untuk durasi waktu yang diijinkan;
6. proses pencatatan penggunaan fasilitas sistem
7. menetapkan dan mendokumentasikan tingkatan otorisasi fasilitas sistem;
8. penghapusan seluruh piranti lunak fasilitas dan sistem yang tidak diperlukan.

2.18 Sesi *Time-out*

Pengguna mungkin meninggalkan aplikasi terminal tanpa pengawasan untuk waktu yang lama. Hal ini menimbulkan risiko bahwa beberapa pengguna lain dapat memiliki hak akses sah ke aplikasi selama waktu ini, jadi aplikasi harus memiliki fitur *'time out'* setelah periode tertentu tidak aktif. (Vasudevan dkk, 2008).

Terminal yang tidak aktif pada lokasi yang beresiko tinggi, seperti wilayah publik atau wilayah eksternal di luar manajemen keamanan organisasi, atau yang melayani sistem beresiko tinggi, harus dimatikan setelah periode waktu tanpa aktivitas yang ditentukan untuk mencegah akses pihak tanpa otorisasi. Fasilitas time-

out ini harus menutup layar terminal dan menutup seluruh aplikasi dan network setelah periode pematian ditentukan. *Time-out delay* harus menggambarkan resiko keamanan wilayah dan pengguna terminal. Format terbatas dari fasilitas time-out terminal dapat disediakan untuk sebagian PC yang mati layarnya dan mencegah akses pihak tanpa otorisasi tetapi tidak menutup aplikasi jaringan (Sarno dan Iffano, 2009: 323)

2.19 Batasan Waktu Koneksi

Pelarangan terhadap waktu koneksi harus menyertakan sistem pengamanan tambahan untuk aplikasi yang beresiko tinggi. Membatasi periode selama koneksi terminal membolehkan layanan komputer mengurangi terbukanya peluang akses tanpa ijin. Kontrol semacam itu harus dipertimbangkan untuk aplikasi komputer yang sensitif, khususnya yang terpasang di lokasi beresiko tinggi, seperti wilayah publik atau eksternal di luar manajemen sistem pengamanan organisasi. Menurut Sarno dan Iffano (2009: 324) contoh pelarangan semacam itu meliputi:

1. menggunakan slot waktu yang telah ditetapkan, yaitu pengiriman *batch file*, atau sesi interaktif berkala untuk durasi singkat;
2. membatasi waktu koneksi pada jam kerja normal jika tidak ada kebutuhan lembur atau perpanjangan waktu operasi.

2.20 Pembatasan Akses Informasi

Kontrol akses lemah tetap merupakan risiko yang signifikan di sebagian besar perusahaan. ISO27001 memiliki satu set kontrol untuk mengelola hak akses dan

manajemen hak istimewa yang sesuai dalam aplikasi. Tujuan dari kontrol ini adalah untuk mengimplementasikan proses yang kuat untuk akses kontrol sehingga kemungkinan penipuan berkurang. Kontrol akses dalam aplikasi dimulai dengan definisi dari peran pengguna dan hak berdasarkan kebutuhan bisnis (Vasudevan, dkk, 2008).

Pengguna sistem aplikasi, termasuk staf pendukung, harus disediakan akses ke informasi dan fungsi sistem aplikasi sesuai dengan kebijakan kontrol akses yang ditentukan, berdasarkan kebutuhan aplikasi usaha individu dan tidak berubah terhadap kebijakan akses informasi organisasi. Menurut Sarno dan Iffano (2009: 325) aplikasi yang harus dipertimbangkan dalam mendukung kebutuhan pembatasan akses:

1. menyediakan menu untuk mengontrol akses terhadap fungsi sistem aplikasi;
2. membatasi pengetahuan pengguna atas informasi atau fungsi sistem aplikasi yang mereka tidak dapat otorisasi mengakses, dengan mengedit dokumentasi pengguna.
3. mengontrol hak akses pengguna, misalnya membaca, menulis, menghapus dan mengeksekusi
4. memastikan bahwa output dari sistem aplikasi yang menangani informasi penting, yang relevan untuk penggunaan output, terkirim hanya kepada terminal dan lokasi yang berijin, termasuk mengkaji ulang secara berkala. Output semacam itu untuk memastikan redudansi informasi hilang.

Menurut Sarno dan Iffano (2009: 325) fasilitas sistem keamanan harus digunakan untuk melarang akses ke sistem aplikasi. *Logical Access* terhadap *software*

dan informasi harus dilarang untuk pengguna, sistem aplikasi seharusnya terkait dengan hal-hal berikut:

a. mengontrol akses pengguna terhadap informasi dan fungsi sistem aplikasi, dalam hubungannya dengan kebijakan kontrol akses bisnis yang ditetapkan;
b. menyediakan perlindungan dari akses tidak berwenang untuk semua penggunaan dan sistem operasi *software* yang mampu menjalankan sistem atau kontrol aplikasi;
c. tidak menyalahgunakan sistem keamanan sistem lain yang sumber informasinya terbagi;
d. mampu untuk menyediakan akses informasi hanya untuk pemilik, individu lain yang diijinkan, dan kelompok pengguna yang ditetapkan.

2.21 Isolasi Sistem yang Sensitif

Sistem isolasi kedengarannya seperti istilah asing dalam lingkungan komputasi. Kontrol ini tidak bertujuan memotong akses ke sistem yang kritis. Sebaliknya, kontrol ini mencari cara untuk membatasi dampak operasional karena berbagi sumber daya antara sistem.

Implikasi dari kontrol ini adalah untuk merampingkan biaya dan untuk mengambil keuntungan maksimal dari sumber daya yang tersedia. Sebagai contoh, inti perbankan aplikasi perangkat lunak mungkin berjalan pada sistem *hardware* yang sangat canngih yang mungkin tidak sepenuhnya dimanfaatkan. Organisasi mungkin memutuskan bahwa itu akan berjalan satu aplikasi lain pada *hardware* yang sama

untuk lebih banyak laba atas investasi. Sementara ini mungkin menghemat biaya, ini juga mungkin menyebabkan *downtime* produksi (Vasudevan dkk, 2008).

Sistem sensitif membutuhkan lingkungan komputasi khusus terisolasi. Sebagian sistem aplikasi sangat sensitif terhadap potensi kehilangan sehingga membutuhkan penanganan khusus. Sensitivitas dapat mengindikasikan bahwa sistem aplikasi harus dijalankan pada komputer khusus, seharusnya hanya membagi resources dengan sistem aplikasi aplikasi yang dipercaya, atau tidak mempunyai batasan. Menurut Sarno dan Iffano (2009: 326) yang harus diperhatikan dalam isolasi sistem sensitif:

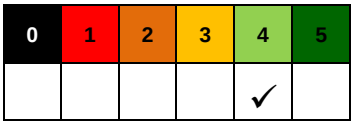
1. sensitivitas sistem aplikasi harus diidentifikasi secara eksplisit dan didokumentasikan oleh pemilik aplikasi.
2. ketika aplikasi sensitif dijalankan pada lingkungan bersama, sistem aplikasi yang akan dibagi resourcesnya harus teridentifikasi dan disetujui oleh pemilik aplikasi sensitif.

2.22 *Maturity Model*

IT Governance Institute (2007: 17) mendefinisikan model kedewasaan merupakan model yang digunakan untuk mengendalikan proses teknologi informasi yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri.

Menurut DISC Infosec (2009) salah satu cara untuk mencapai kontrol keamanan informasi yang optimal adalah menilai keamanan informasi organisasi berdasarkan ISO 27002 dan memetakan setiap kontrol keamanan dengan *Capability*

Maturity Model Integration (CMMI). CMMI memiliki lima tingkat tingkat kematangan proses yang dapat dilihat pada Gambar 2.5



Gambar 2.5 Tingkat Kematangan CMMI
(Sumber: DISC Infosec, 2009)

Penilaian *maturity level* dilakukan menggunakan lima tingkatan proses rangkaian kesatuan kedewasaan berdasarkan metodologi CMMI. Pendekatan CMMI digunakan sebagai patokan untuk perbandingan dan berperan sebagai alat bantu untuk memahami tingkah laku, praktek, dan proses-proses dalam organisasi. Lima tingkatan kerangka kesatuan CMM adalah sebagai berikut.

a. Level 0 (*non-existent*): Tidak ada kontrol sama sekali.
b. Level 1 (*initial*): Pada level ini, organisasi memiliki pendekatan yang tidak konsisten, kontrol keamanan dilakukan secara informal. Informal berarti tidak ada dokumentasi, tidak ada standar.
c. Level 2 (*limited/repeatable*): Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan.
d. Level 3 (*defined*): Pada level ini, kontrol keamanan telah didokumentasikan rinci dan dikomunikasikan melalui pelatihan, tetapi tidak ada pengukuran kepatuhan.
e. Level 4 (*managed*): Pada level ini, terdapat pengukuran efektivitas kontrol keamanan, tetapi tidak ada bukti dari setiap ulasan kepatuhan dan/atau kontrol

memerlukan perbaikan lebih lanjut untuk mencapai tingkat kepatuhan yang diperlukan.

f. Level 5 (*optimized*): Pada level ini, kontrol keamanan telah disempurnakan hingga sesuai dengan ISO 27002 berdasarkan pada kepemimpinan yang efektif, manajemen perubahan, perbaikan berkelanjutan, dan komunikasi internal.

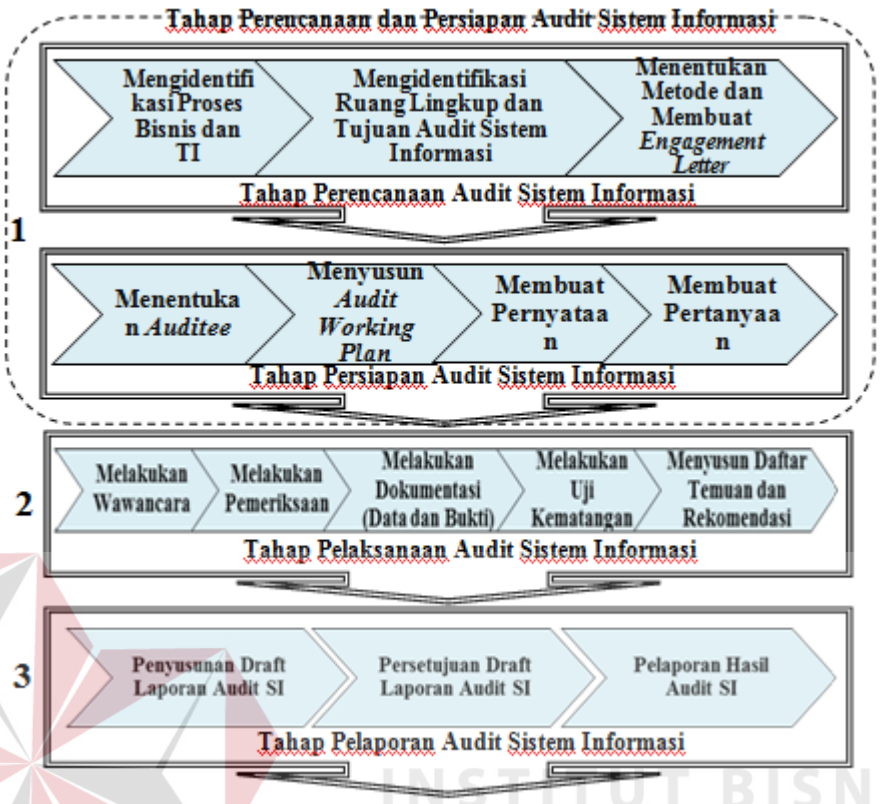
2.23 Tahapan-Tahapan dalam Audit Sistem Informasi

ISACA tahun 2010 menyatakan membagi tahapan audit sistem informasi menjadi 4 (empat) tahapan yaitu: 1. Tahap perencanaan audit, 2. Tahap persiapan audit, 3. Tahap pelaksanaan audit, 4. Tahap pelaporan audit. Keempat tahapan tersebut dilihat pada Gambar 2.6 di halaman 45.

1. Tahap Perencanaan dan Persiapan Audit Sistem Informasi

Tahap perencanaan dan persiapan ini dilakukan oleh auditor untuk mengetahui tentang *auditee* (*how your auditee*), mempelajari tentang proses bisnis perusahaan yang diaudit, merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci, menyusun audit *working plan*, serta mempersiapkan kertas kerja audit sistem informasi yang akan dipakai. Langkah-langkah yang terdapat di tahap perencanaan dan persiapan audit sistem informasi adalah sebagai berikut.

a. Mengidentifikasi proses bisnis dan TI



Gambar 2.6 Tahapan-Tahapan dalam Audit Sistem Informasi

Dalam perencanaan proses audit, auditor harus melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit *(auditee*). Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut bisa berupa profil perusahaan, rencana strategis, standard *operating procedure*, kebijakan, standar, prosedur, portopolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. Auditor juga harus mengetahui apakah sebelumnya perusahaan telah dilaksanakan proses audit. Apabila pernah melakukan audit maka, auditor perlu mengetahui dan memeriksa laporan audit periode sebelumnya.

Pengetahuan tentang *auditee* dapat dilakukan dengan cara melihat dokumen-dokumen yang terkait dengan proses audit dari media *online* bahkan auditor datang langsung ke perusahaan lalu melakukan wawancara manajemen dan staff, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan.

b. Mengidentifikasi ruang lingkup dan tujuan audit sistem informasi

Langkah selanjutnya yang dilakukan dalam audit sistem informasi adalah mengidentifikasi ruang lingkup. Ruang lingkup audit harus mengacu pada tujuan audit. Pada tahap ini auditor menentukan klausul, *objective control*, dan kontrol yang akan digunakan.

c. Menentukan metode dan membuat proposal ke perusahaan

Pada tahap ini auditor merancang dan menentukan metode-medote yang akan digunakan pada pelaksanaan audit keamanan sistem informasi. Auditor menuangkan keseluruhan perencanaan audit ke dalam *engagement letter* beserta data-data apa saja yang dibutuhkan selama proses audit. Rencana audit harus didiskusikan bersama pimpinan perusahaan sebelum disetujui oleh pimpinan perusahaan untuk memastikan kecukupan dukungan manajemen serta kesesuaian audit dengan kebutuhan manajemen (Hermawan, 2011).

d. Menentukan *auditee*

Auditee adalah entitas organisasi atau bagian/unit organisasi atau operasi/program termasuk kondisi tertentu yang diaudit. Penetapan *auditee* dilihat berdasarkan klausul yang telah ditetapkan. Selain itu, setelah dilakukan wawancara

awal dapat ditentukan dan diketahui bagian mana saja yang menangani kontrol keamanan yang ada pada setiap klausul yang ditetapkan.

e. Menyusun jadual audit (rencana kerja audit)

Rencana kerja audit merupakan dokumen yang digunakan untuk merencanakan dan memantau pelaksanaan Audit TI secara terperinci. Dimulai dari proses awal hingga proses pelaporan audit.

f. Membuat peryataan

Tahap selanjutnya dalam persiapan audit keamanan sistem informasi ini dilakukan dengan membuat pernyataan. Pernyataan dibuat berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah dipilih. Kontrol keamanan tersebut dapat dilihat pada panduan ISO 27002. Pada setiap kontrol keamanan dapat ditemukan pernyataan yang telah mendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut.

g. Membuat pertanyaan

Setelah dilakukan pembobotan pernyataan pada tiap proses TI, maka selanjutnya auditor membuat pertanyaan berdasarkan pernyataan tersebut. Pertanyaan tersebut akan dijadikan acuan dalam melakukan wawancara kepada pihak yang telah ditentukan sebelumnya.

Tabel 2.1 Tingkat Kepentingan dalam Pembobotan Pernyataan

No	Nilai Kualitatif	Skala	Keterangan
1	Tinggi	0,70 – 1,00	Pernyataan tersebut mempunyai peranan yang sangat penting dalam proses sistem informasi
2	Cukup	0,40 – 0,69	Pernyataan tersebut cukup mempunyai peran dalam proses sistem informasi
3	Rendah	0,00 – 0,39	Pernyataan tersebut dalam melengkapi peran dalam sistem informasi

Sumber: Niekerk dan Labuschagne (2006: 7)

2. Tahap Pelaksanaan Audit Sistem Informasi

Pada tahap pelaksanaan, auditor melakukan pengumpulan dan evaluasi bukti dan data audit sistem informasi yang dilakukan, serta melakukan uji kepatutan (*complience test*), yakni dengan menyesuaikan keadaan ada dengan standar pengelolaan proses TI. Selanjutnya dilakukan penyusunan temuan serta rekomendasi guna diberikan kepada *auditee*. Langkah-langkah yang terdapat di tahap ini adalah sebagai berikut.

a. Melakukan wawancara

Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Proses TI yang dapat terbagi menjadi 4 kelompok, yaitu: pihak yang bertanggung jawab terhadap kesuksesan aktivitas (*responsible*), pihak yang bertanggung jawab (*accountable*), pihak yang mengerti aktivitas (*consulted*), dan pihak yang senantiasa diinformasikan perihal perkembangan aktivitas (*informed*). Wawancara juga dapat dilaksanakan berdasarkan struktur organisasi.

b. Melakukan Pemeriksaan

Pemeriksaan terhadap data dan bukti dilakukan melalui 2 (dua) tahap test, yaitu: *compliance test* dan *substantive test*. *Compliance test* merupakan pengujian untuk mengetahui keberadaan/penerapan pengendalian dalam kegiatan operasional objek audit, sedangkan *substantive test* merupakan pengujian untuk memastikan kelengkapan, integritas, dan keakuratan (kebenaran dan kekonsistenan).

Pemeriksaan data dan bukti diambil saat pelaksanaan audit yang dilaksanakan berdasarkan pada program audit yang telah disiapkan pada tahap perencanaan dan persiapan audit dilakukan. Pembuatan kertas kerja dan pertanyaan-pertanyaan

wawancara yang digunakan untuk mengumpulkan fakta tiap proses yang ada di sistem informasi saat ini, dimana pertanyaan yang diajukan dalam kertas kerja maupun wawancara dibuat dengan mengacu pada masing-masing kontrol proses sesuai pedoman dari ISO yang dikembangkan sesuai dengan objek yang akan diaudit.

c. Melakukan dokumentasi (data dan bukti)

Pada tahap ini auditor telah memperoleh data dan melakukan wawancara ataupun observasi yang akan membantu anggota tim ini untuk menganalisis data-data dan bukti-bukti yang ada. Selama melakukan audit, auditor harus dapat mendokumentasikan pekerjaan mereka sehingga kesimpulan dapat dibuktikan. Tujuan mendokumentasikan pekerjaan harus cukup detail sehingga cukup informasi bagi orang untuk dapat memahami apa yang telah dilakukan dan dapat mencapai kesimpulan yang sama seperti auditor. Dokumentasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video.

d. Melakukan uji kematangan

Setelah dilakukan wawancara dan observasi pada tahap pengumpulan bukti, maka hasil audit yang diperoleh akan dianalisa dan dievaluasi. Analisa yang digunakan dalam audit keamanan sistem informasi kali ini adalah dengan menggunakan analisa tingkat kematangan. Uji kematangan dilakukan dengan menggunakan penilaian CMM *maturity level* dengan mengacu pada pernyataan dari ISO 27002. Uji kematangan ini dilakukan untuk mengukur tingkat keamanan yang ada pada perusahaan.

e. Menyusun daftar temuan dan rekomendasi

Selama proses audit, auditor akan memeriksa banyak catatan, mempelajari banyak jenis informasi, melihat banyak laporan, mengobservasi prosedur kerja dan melakukan wawancara dengan berbagai pihak. Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung diperusahaan. Bukti tersebut akhirnya dikumpulkan dan dievaluasi untuk memungkinkan auditor membentuk opini mengenai kecukupan dan keefektifan kontrol internal sehingga dapat merekomendasikan tindakan perbaikan dan korektif (Sarno, 2009: 49).

3. Tahap Pelaporan Audit Sistem Informasi

Berdasarkan seluruh kertas kerja audit, temuan, dan tanggapan *auditee*, maka *audite* harus menyusun *draft* laporan audit SI sebagai pertanggungjawaban atas penugasan audit SI yang telah dilaksanakan. Laporan audit harus ditunjukan kepada pihak yang berhak saja karena laporan audit SI merupakan dokumen yang bersifat rahasia. Tahap pelaporan audit sistem informasi yang dilakukan dimulai dengan penyusunan *draft* laporan hasil audit, persetujuan *draft* laporan hasil audit, dan pelaporan hasil audit.