BAB II

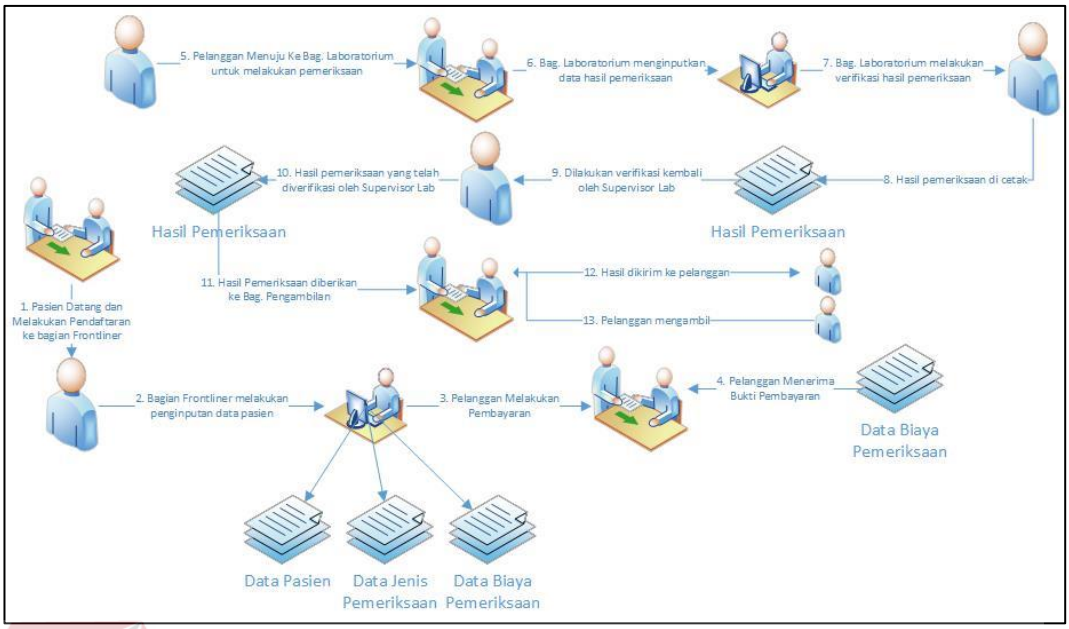
LANDASAN TEORI

2.1. Sistem Informasi

Menurut Beynon (2004) Sistem informasi merupakan perpaduan antara teknologi informasi dengan aktivitas yang menggunakan teknologi dalam mendukung kinerja kerja, manajemen perusahaan serta dalam pembuatan keputusan dalam suatu perusahaan. Sistem informasi tidak hanya menggambarkan tentang komputer dan perangkatnya serta interaksinya dengan organisasi melainkan juga digunakan dalam menggambarkan interaksi antara seluruh komponen yang terlibat dalam proses bisnis suatu organisasi tersebut.

2.2. Sistem Informasi Parahita

Sistem informasi parahita merupakan sistem yang telah terintegrasi dan terpusat yang digunakan PDC dalam menunjang proses bisnis secara keseluruhan meliputi proses keuangan, proses marketing, proses SDM, proses pendaftaran pasien, proses pemerikasaan hingga proses keluarnya hasil laboratorium. PARIS menyediakan berbagai informasi penting, antara lain: informasi data pasien, data hasil pemeriksaan, data dokter, data keuangan, data karyawan serta data perusahaan yang bekerjasama dengan Parahita. PARIS digunakan oleh berbagai bagian yang terkait di PDC, yaitu bagian laboratorium, bagian pelayanan, bagian penjualan, bagian keuangan, bagian sumber daya insani (SDI) & umum, bagian penanggung jawab lab dan penanggung jawab medis. Sistem Informasi Parahita tersebut dapat dilihat pada Gambar 2.1.



Gambar 2. 1 Alur Sistem PARIS

2.3. Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya memastikan atau menjamin keberlangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*), dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno dan Iffano, 2009). Contoh Kemanan Informasi menurut (Sarno dan Iffano, 2009) adalah.

1. *Physical Security* adalah keamanan informasi yang menfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup '*Physical Security*'.

3. *Operation Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut agar beroperasi tanpa adanya gangguan.
4. *Communications Security* adalah keamanan informasi yang bertujuan untuk mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya, dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Aspek kemanan informasi meliputi tiga hal, yaitu : *Confidentiality*, *Integrity*, dan *Availability* (CIA). Aspek tersebut dapat dilihat pada Gambar 2.2 yang lebih lanjut akan dijelaskan sebagai berikut.

Gambar 2. 2 Aspek Keamanan Informasi
(Sumber: Sarno dan Iffano, 2009)

a. *Confidentiality* : Keamanan informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tersebut.

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

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

2.4. Audit

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

2.5. Audit Sistem Informasi

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

1. Tinjauan terkait fisik dan lingkungan, yakni : hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperature, kontrol kelembaban, dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database, seluruh prosedur administrasi sistem dan pelaksanaanya.
3. Tinjauan perangkat lunak. Perangkat unak yang dimaksud adalah bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjuan keamanan jaringan yang encakup tinjauan jaringan internal dan eksternal yang terhubung ke dalam sistem, batasan tingkat keamanan, tinjuan terhadap firewall, daftar kontrol akses router, port scanning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana atau kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang diterapkan.

2.6. Audit Keamanan Sistem Informasi

Menurut Ahmad (2012) audit keamanan sistem informasi adalah suatu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada dan untuk melakukan verifikasi apakah perlindungan yang ada berjalan dengan baik dan benar.

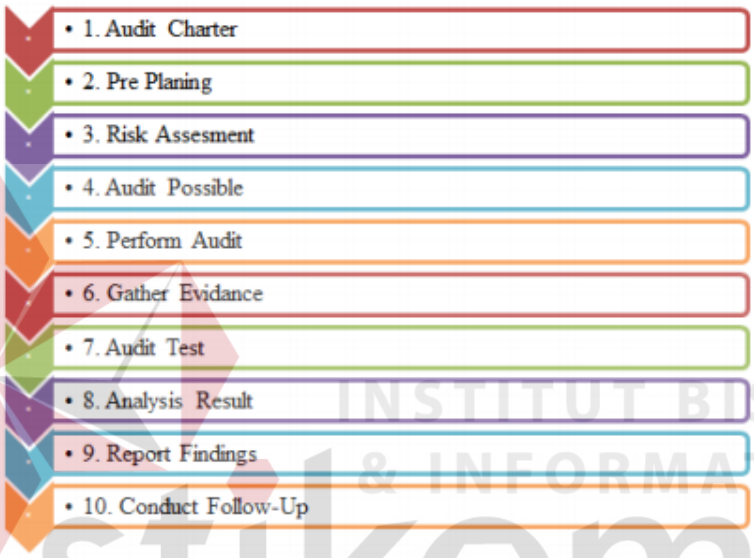
Adapun tujuan utama audit keamanan sistem informasi adalah memberikan perlindungan sesuai dengan suatu kebijakan dan standar keamanan yang ada serta melakukan verifikasi apakah perlindungan sudah berjalan dengan baik. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan audit keamanan pada sistem informasi yang digunakan. Penerapan audit keamanan sistem informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non teknis dalam suatu sistem teknologi informasi dalam sebuah organisasi.

2.7. Tahapan Audit

Sebelum mengetahui tahapan dari audit maka terlebih dahulu harus mengenal mengenai auditor dan *auditee*. Menurut Haryono (2001) auditor adalah orang yang melakukan audit untuk mendapatkan bukti yang akurat sesuai dengan yang telah ditetapkan dan melaporkan hasilnya kepada para pihak yang berkepentingan. Sedangkan *auditee* adalah seseorang yang diaudit atau diperiksa oleh auditor untuk mendapatkan informasi yang dibutuhkan dalam upaya untuk mencapai tujuan yang diinginkan.

Dalam melaksanakan audit, ada banyak berbagai macam versi dalam menjalankan tahapan audit, salah satunya tahapan dari David Cannon yang

mengacu ISACA. Menurut Cannon (2010) terdapat sepuluh tahapan yang harus dilakukan dalam proses audit, yaitu: 1. Membuat dan mendapatkan surat persetujuan audit, 2. Perencanaan audit, 3. Analisis risiko, 4. Persiapan audit, 5. Pelaksanaan audit, 6. Pengumpulan bukti dan temuan, 7. Tes audit, 8. Pemeriksaaan hasil audit, 9. Pelaporan audit, 10. Pertemuan penutup, lebih jelasnya dapat dilihat pada Gambar 2.3.



Gambar 2. 3 Tahapan-tahapan Audit Sistem Informasi
(Sumber: Canon, 2011)

Pada gambar 3 diatas menjelaskan tentang sepuluh tahapan yang dilakukan dalam proses audit, yaitu.

1. **Membuat dan Mendapatkan Persetujuan Engagement Letter**

   Sebelum melakukan audit, seorang auditor harus membuat surat kesepakatan atau keterikatan dengan clien untuk berkomitmen menjaga dan mentaati persetujuan dan peraturan yang telah dibuat selama audit dilakukan. Surat atau perjanjian yang dibuat oleh auditor internal dinamakan *audit charter* sedangkan untuk auditor eksternal dinamakan

engagement letter. *Engagement letter* adalah surat yang dikirimkan pada client pada awal permulaan audit yang didalamnya terdapat kontrak untuk menghindari kesalahpahaman antara clien dan auditor. Pada *engagement letter* didalamnya terdapat enam poin, yaitu:

1. Tanggung jawab
2. Wewenang
3. Tujuan
4. Peran
5. Objek Audit
6. Waktu awal sampai akhir

2. Perencanaan Audit

Auditor harus mengetahui tentang auditee (*know your auditee*) dan harus mampu mempelajari dokumen-dokumen organisasi, yaitu: profil, rencana strategis, prosedur, standar operasi, kebijakan, portofolio, arsitektur, infrastruktur, aplikasi sistem informasi dan laporan audit sebelumnya. Auditor melakukan *interview* manajemen dan staf dan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan. Pelajari regulasi yang mempengarui proses bisnis.

3. Analisis Risiko

Setelah melakukan perencanaan auditor melakukan penilaian risiko TI untuk menentukan objek-objek TI mana yang perlu mendapatkan perhatian dan alokasi sumber daya audit yang lebih dibandingkan dengan objek-objek lainnya. Teknik Penilaian Risiko TI:

a. *Judgemental.*

b. *Numeric rating.*

c. *Combination of judgemental and numeric rating*

4. Penentuan Apakah Audit Dimungkinkan

Auditor harus bertanggung jawab dalam pelaksanaan audit. Penetapan objek audit TI dan skala prioritasnya dilakukan berdasarkan hasil penilaian risiko yang telah dilakukan sebelumnya. Objek audit TI yang berisiko tinggi harus memperoleh prioritas yang lebih tinggi dari objek audit yang berisiko lebih rendah. Auditor harus bekerjasama dengan auditee dalam melakukan audit, audit tanpa bukti berarti audit tersebut sia-sia atau tidak berguna.

5. Pelaksanaan Audit

Sebelum melakukan atau melaksanakan audit seorang auditor akan melakukan persiapan. Terdapat beberapa langkah dalam tahap persiapan audit, yaitu :

a. Melakukan Pertemuan Pendahuluan Audit TI

Pertemuan pendahuluan dilakukan untuk.

1. Mendapatkan pemahaman yang sama atas audit TI yang dilakukan.
2. Mendapatkan penjelasan dari pemimpin *auditee* tentang kondisi terakhir.

Objek audit dan hal-hal yang perlu menjadi perhatian. Pertemuan pendahuluan didokumentasikan dalam bentuk risalah atau notulen pertemuan pendahuluan.

b. Penyampaian Surat Penugasan

Tim auditor TI dalam setiap melaksanakan tugasnya harus berdasarkan surat penugasan yang ditanda tangani oleh kepala direksi. Surat penugasan merupakan bentuk pendelegasian wewenang kepala kepada tim auditor TI untuk melaksanakan audit.

c. Koordinasi Tim Auditor

Koordinasi perlu dilakukan agar setiap anggota tim auditor TI memahami tugas dan tanggung jawabnya secara jelas sesuai dengan AWP yang telah disusun sebelumnya oleh ketua tim auditor sehingga audit dapat.

1. Dilaksanakan secara efektif dan efisien.
2. Mencapai tujuan yang telah ditetapkan.
3. Memenuhi kebutuhan manajemen.

d. Penyusunan *Audit Working Plan* (AWP)

Audit Working Plan adalah dokumen yang dibuat oleh Ketua Tim Auditor TI yang digunakan untuk merencanakan dan memantau pelaksanaan Audit TI secara terperinci.

e. Penyampaian Kebutuhan Data

Data yang diperlukan auditor TI dapat disampaikan terlebih dahulu kepada auditee agar dapat dipersiapkan terlebih dahulu. *Field Work* dilaksanakan auditor TI setelah auditee menginformasikan ketersediaan semua data yang diperlukan auditor TI, sehingaa *field work* dapat dilaksanakan oleh auditor TI secara efektif dan efisien.

f. Persiapan Kertas Kerja Audit

Auditor mempersiapkan kertas kerja audit TI yang didalamnya terdapat semua dokumentasi proses audit TI yang dilakukan oleh. Contoh: AWP, Dokumen Administrasi Audit TI, Program Audit TI beserta kertas kerja pendukungnya, Form analisa data, interview, observasi, data dan bukti audit, daftar temuan dan laporan audit. Setelah persiapan telah dilakuan selanjutnya Audit dapat dilaksanakan. Pelaksanaan Audit terdapat beberapa langkah, yaitu.

a. Penyusunan Daftar Temuan

Daftar temuan disampaikan secara lugas dan objektif dilengkapi dengan.

1. Deskripsi / penjelasan singkat dari temuan yang diungkap.
2. Kriteria (peraturan, standard an praktik terbaik yang menjadi acuan).
3. Risiki-risiko yang mungkin timbul jika temuan tidak ditindaklajuti.
4. Rekomendasi dari auditor TI yang perlu ditindaklanjuti oleh *auditee* agar risiko-risiko yang ada tidak terjadi.
5. Harus didukung data, bukti, dan fakta yang benar.
6. Mengacu pada kriteria yang relevan dengan kebutuhan dan kewajiban *auditee* dan telah ditetapkan menjadi acuan pelaksanaan audit TI.

b. Konfirmasi Temuan

Temuan harus dikonfirmasikan terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal (Kepada Bidang dan Sekretaris) dalam bentuk

laporan TI. Konfirmasi temuan didokumentasikan dalam bentuk risalah / konfirmasi temuan.

6. **Melakukan Pemeriksaan Data dan Bukti**

   Setiap langkah pemeriksaan yang ada dalam program audit dilaksanakan oleh auditor TI dengan menggunakan satu atau lebih teknik audit yang sesuai dan disertai data atau bukti pendukung yang menandai atau mencukupi.

7. **Melakukan Tes Audit**

   Pemeriksaan data dan bukti dapat dilakukan melalui 2 tahap tes, yaitu.

   1. *Compliance* tes: Pengujian untuk mengetahui keberadaan atau penerapan pengendalian dalam kegiatan operasioanal obyek audit.
   2. *Substantive* tes: Pengujian memastikan kelengkapan, integritas, dan keakuratan (kebenaran dan konsistensi) data dan informasi.

   Dalam melakukan tes audit terdapat beberapa teknik yaitu.

   a. Teknik *Review*: pemeriksaan ulang terhadap dokumentasi dan konfigurasi TI.

      Contoh: Dengan memeriksa ulang kelengkapan dan kepatuhan dalam pelaksanaan kebijakan, standar dan prosedur TI dan memeriksa kelengkapan dan pengembangan staf yang ada dalam struktur organisasi TI.

   b. Teknik *Interview*: pemeriksaan secara langsung terhadap *brainware* yang menjadi pengelola dan pengguna TI organsasi.

Contoh: *interview* terhadap pengelola departemen terkait dengan kegiatan operasional pemeliharaan, pengaman, dan *interview* terhadap pengguna TI terkait dengan keputusan terhadap ketersediaan layanan TI.

c. Teknik *Observation*: Pemeriksaan secara langsung pada operasional objek TI.

Contoh: meninjau dan memeriksa infrastruktur kelistrikan, pengaturan udara dan pengaman ruang. Ikut serta dan mengamati pegguna dalam menggunakan aplikasi untuk mendukung kegiatan operasional sehari-hari. Meninjau dan memeriksa *software-software* yang *terinstall* di dalam komputer-komputer *client*.

d. *Trial* tes: Menguji secara langsung fungsi perangkat TI untuk mengetahui kelayakan dan kinerja operasionalnya.

Contoh: menguji fungsi sistem pendeteksi dan pemadam kebakaran (*fire suppression system*), mematikan aliran listrik ke komputer untuk menguji fungsi UPS dan genset.

8. Pemeriksaan Hasil Audit

Setiap langkah pemeriksaan yang ada dalam Program Audit dilaksanakan oleh auditor TI dengan menggunakan satu atau lebih Teknik Audit yang sesuai dan dengan disertai data atau bukti pendukung yang memadai atau mencukupi.

9. Pelaporan Audit

Setelah Audit dilaksanakan auditor akan membuat laporan terdapat beberapa tahapan dalam pembuatan laporan, tahapan tersebut yaitu.

a. Penyusunan Laporan Audit TI

Berdasarkan seluruh kertas kerja audit, temuan dan tanggapan auditee, auditor TI harus menyusun draf laporan audit TI sebagai peratanggun jawaban atas penugasan audit TI yang telah dilaksanakan. Laporan audit TI ditujukan kepada pihak berhak saja karena laporan audit TI merupakan dokumen yang bersifat rahasia. Isi (*draf*) Laporan Audit TI.

1. Laporan Audit
    a. Penerima Laporan.
    b. Opini Laporan.
    c. Standar pelaksanaan audit yang dipergunakan.
2. Ringkasan Eksekutif
    a. Periode audit TI.
    b. Tanggal pelaksanaan audit TI.
    c. Ringkasan hasil pemeriksaan TI.
3. Pendahuluan
    a. Dasar pelaksanaan audit TI.
    b. Tujuan audit TI.
    c. Ruang lingkup audit.
    d. Periode pemeriksaan.
4. Metode pemeriksaan
5. Daftar Temuan
6. Lampiran

a. Permintaan Tanggapan Atas Temuan

Atas temuan yang telah disampaikan Auditor TI, *Auditee* harus memberikan tanggapan dan komitmen penyelesaiannya. Tanggapan secara formal atas setiap temuan Audit TI.

b. Persetujuan Laporan Audit TI

Draft laporan audit TI yang telah disusun harus dimintakan persetujuan terlebih dahulu kepada auditee sebelum dterbitkan sebagai laporan audit TI yang resmi dan formal. Persetujuan harus dilakukan oleh pejabat dii tingkat atas yang memadai (minimal Kepala Divisi TI).

10. Pertemuan Penutup Audit

Pertemuan Penutup Audit TI dilakukan untuk melaporkan hasil audit TI kepada manjemen, memberikan penjelasan pada manajemen tentang kondisi kelemahan dan rekomendasi utama. Pertemuan di dokumentasikan dalam bentuk risalah atau notulen pertemuan.

2.8. Standar Sistem Keamanan Manajemen Informasi

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

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

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

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

Berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

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

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

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

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

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

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

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

Dokumen panduan pelaksanaan manajemen risiko.

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

Dokumen panduan untuk sertifikasi SMKI perusahaan.

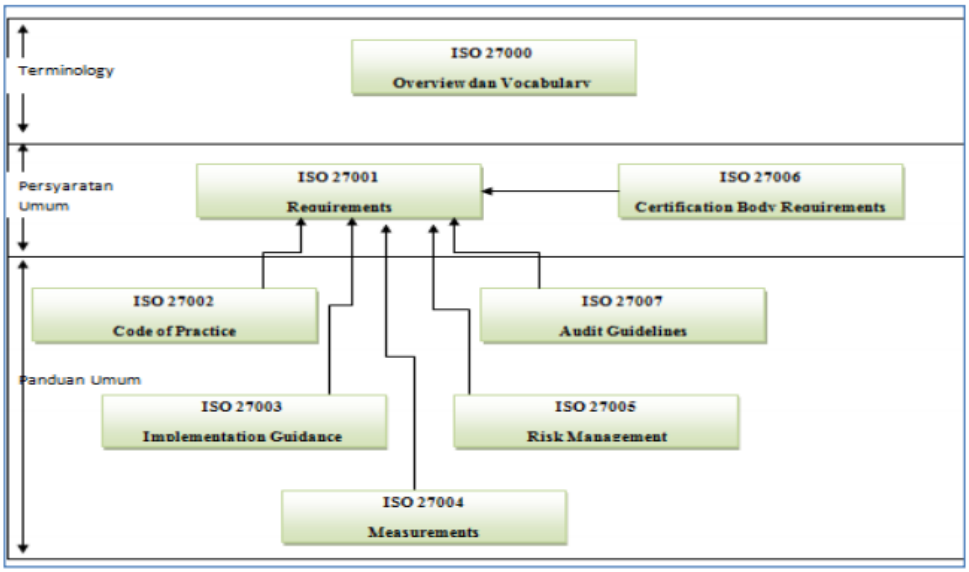
h. ISO/IEC 27007 – *Guidelines for ISMS Auditing*

Dokumen panduan audit SMKI perusahaan.

Adapun penjelasan dari standar ISMS tersebut dijelaskan sebagai berikut.

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

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



Gambar 2. 4 Hubungan Antar Standar Keluarga SMKI
(Sumber: DIrektorat Keamanan Informasi,2011)

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

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

ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi masyarakat penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

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

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

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

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

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

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

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

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

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

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

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

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

Standar ini memaparkan panduan bagaimana melakukan audit SMKI perusahaan.

2.9. ISO/IEC 27002:2005

ISO 27002:2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya mencakup 12 kontrol area, 41 kontrol objektif, dan 133 kontrol sebagaimana ditetapkan dalam ISO/IEC 27001, dapat dilihat pada Tabel 2.1.

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

Tabel 2. 1 Jumlah Klausul, Obyektif Kontrol dan Kontrol ISO 27002:2005

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

Dalam penelitian ini, audit keamanan sistem informasi akan difokuskan pada 4 klausul, yaitu klausul 7 tentang manajemen asset, klausul 8 tentang keamanan sumber daya manusia, klausul 9 tentang keamanan fisik dan lingkungan, klausul 11 tentang kontrol akses yang sudah disesuaikan dengan kesepakatan audit dan PDC dalam *engagement letter* untuk detail struktur dokumen kontrol keamanan yang digunakan sebagai acuan audit dari ISO/IEC 27002:2005 dapat dilihat pada Tabel 2.2.

Tabel 2. 2 Detail Struktur ISO/IEC 27002:2005

Klausul: 10 Manajemen Komunikasi dan Operasi	
Kategori Keamanan Utama: 10.1 Tanggung jawab dan prosedur operasional	
Objektif Kontrol Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilita-fasilitas pemrosesan Informasi	
Kontrol : 10.1.1	Pendokumentasian prosedur operasi
Kontrol : 10.1.2	Manajemen pertukaran
Kontrol : 10.1.3	Pemisahan tugas
Kontrol : 10.1.4	Pemisahan pengembangan, pengujian dan operasional Informasi
Kategori Keamanan Utama: 10.2 Manajemen pengiriman oleh pihak ketiga	
Objektif Kontrol Untuk mengimplementasikan dan memelihara tingkat Keamanan Informasi yang sesuai dalam hal layanan pengiriman yang berhubungan dengan perjanjian layanan pengiriman dengan pihak ketiga.	
Kontrol : 10.2.1	Layanan Pengiriman
Kontrol : 10.2.2	Pemantauan dan pengkajian ulang layanan pihak ketiga
Kontrol : 10.2.3	Manajemen penggantian layanan pihak ketiga
Kategrori Keamanan Utama : 10.3 Perencanaan Sistem dan Penerimaan	
Objektif Kontrol Untuk meminimalisasi kegagalan sistem	
Kontrol : 10.3.1	Manajemen Kapasitas
Kontrol : 10.3.2	Penerimaan Sistem
Kategori Kemanan Utama : 10.4 Perlindungan terhadap *malicious* dan *mobile code*	
Objektif Kontrol Untuk melindungi integrasi perangkat lunak (*software*) dan informasi	
Kontrol : 10.4.1	Kontrol terhadap kode berbahaya (*malicious code*)
Kontrol : 10.4.2	Kontrol terhadap *mobile code*

Tabel 2. 3 (Lanjutan)

Klausul: 10 Manajemen Komunikasi dan Operasi	
Kategori Keamanan Utama : 10.5 Backup	
Objektif Kontrol Untuk memelihara integritas dan ketersediaan Informasi dan fasilitas pemrosesan informasi	
Kontrol : 10.5.1	Back up Informasi
Kategori Keamanan Utama : 10.6 Manajemen Kemanan jaringan	
Objektif Kontrol Untuk memastikan keamanan pengiriman informasi di jaringan dan serta melindungi infrastruktur pendukungnya	
Kontrol : 10.6.1	Kontrol Jaringan
Kontrol : 10.6.2	Kemanan dalam layanan jaringan
Kategori Keamanan Utama : 10.7 Penanganan Waktu	
Objektif Kontrol Untuk mencegah pengaksesan, modifikasi, penghapusan atau pengrusakan aset secara ilegal serta gangguan aktifitas bisnis.	
Kontrol : 10.7.1	Manajemen pemindahan media
Kontrol : 10.7.2	Pemusnahan atau pembuangan medua
Kontrol : 10.7.3	Prosedur penanganan Informasi
Kategori Keamanan Utama : 10.8 Pertukaran Informasi	
Objektif Kontrol Untuk memelihara keamanan pertukaran informasi dan perangkat lunak di dalam organisasi dan dengan pihak luar	
Kontrol : 10.8.1	Kebijkan dan prosedur penukaran Informasi
Kontrol : 10.8.2	Perjanjian Pertukaran
Kontrol : 10.8.3	Transportasi media fisik
Kontrol : 10.8.4	Pesan elektronik
Kontrol : 10.8.5	Sistem Informasi Bisnis
Kategori Keamanan Utama : 10.9 Layanan *E-Commerce*	
Objektif Kontrol Untuk memastikan keamanan dalam layanan dan penggunaan E-Commerce	
Kontrol : 10.9.1	E-Commerce

Tabel 2. 4 (Lanjutan)

Klausul: 10 Manajemen Komunikasi dan Operasi	
Kategori Keamanan Utama : 10.9 Layanan *E-Commerce*	
Objektif Kontrol Untuk memastikan keamanan dalam layanan dan penggunaan E-Commerce	
Kontrol : 10.9.2	Transaksi On-Line
Kontrol : 10.9.3	Informasi untuk public
Kategori Keamanan Utama : 10.10 Monitoring	
Objektif Kontrol Untuk mendeteksi aktifitas pemrosesan Informasi secara ilegal	
Kontrol : 10.10.1	Rekamana Audit
Kontrol : 10.10.2	Monitoring penggunaan sistem
Kontrol : 10.10.3	Proteksi catatan Informasi
Kontrol : 10.10.4	Catatan administrator dan operator
Kontrol : 10.10.5	Catatan Kesalahan
Kontrol : 10.10.6	Sinkronisasi waktu
Klausul : 12 Akuisi Sistem Informasi, Pengembangan dan Pemeliharaan	
Kategori Kemanan Utama: 12.1 Persyaratan keamanan untuk Sistem Informasi	
Objektif Kontrol Untuk memastikan bahwa keamanan adalah bagian dari Sistem Informasi.	
Kontrol : 12.1.1	Analisa dan spesifikasi persyaratan keamanan
Kategori Kemanan Utama: 12.2 Pemrosesan yang benar dalam aplikasi	
Objektif Kontrol Untuk mencegah kesalahan, kehilangan, modifikasi tanpa hak atau kesalahan penggunaan Informasi dalam aplikasi	
Kontrol : 12.2.1	Validasi data input
Kontrol : 12.2.2	Kontrol untuk pemrosean internal
Kontrol : 12.2.3	Integritas pesan
Kontrol : 12.2.4	Validasi data output

Tabel 2. 5 (Lanjutan)

Klausul : 12 Akuisi Sistem Informasi, Pengembangan dan Pemeliharaan	
Kategori Keamanan Utama : 12.3 Kontrol Kriptografi	
Objektif Utama Untuk melindungi kerahasiaan, autentifikasi dan keutuhan Informasi dengan menggunakan sistem kriptografi.	
Kontrol : 12.3.1	Kebijakan dalam penggunaan kontrol kriptografi
Kontrol : 12.3.2	Manajemen kunci
Kategori Keamanan Utama : 12.4 Keamanan file sistem	
Objektif Kontrol Untuk memastikan keamanan file sistem	
Kontrol : 12.4.1	Kontrol operasional software
Kontrol : 12.4.2	Perlindungan data pengujian sistem
Kontrol : 12.4.3	Kontrol akses ke *source* program
Kategori Keamanan Utama : 12.5 Keamanan dalam pembangunan dan proses-proses pendukung	
Objektif Kontrol Untuk memelihara keamanan informasi dan aplikasi sistem software	
Kontrol : 12.5.1	Prosedur tambahan *control*
Kontrol : 12.5.2	Tinjauan teknis aplikasi setelah dilakukan perubahan sistem operasi
Kontrol : 12.5.3	Pembatasan perubahan paker software
Kontrol : 12.5.4	Kelemahan Informasi
Kontrol : 12.5.5	Pembangunan software yang di *outsource* kan
Kategori Keamanan Utama : 12.6 Manajemen teknik kelemahan	
Objektif Kontrol Untuk mengurangi resiko yang disebelahkan oleh terpublikasinya teknik-teknik kelemahan yang dimiliki	
Kontrol : 12.6.1	Kontrol terhadap kelemahan secara teknis

Tabel 2. 6 (Lanjutan)

Klausul : 13 Manajemen kejadian Keamanan Informasi	
Kategori Keamanan Utama: 13.1 Pelaporan kejadian dan kelemahan kelemahan informasi	
Objektif Kontrol Untuk memastikan kejadian dan kelemahan keamanan Sistem Informasi dikonversikan dan ditangani tepat waktu	
Kontrol : 13.1.1	Pelaporan kejadian Keamanan Informasi
Kontrol : 13.1.2	Pelaporan kelemahan keamanan
Kategori Keamanan Utama : 13.2 Manajemen kejadian keamanan informasi dan pengembangannya	
Objektif Kontrol Untuk memastikan konsistensi dan ke efektifitasan pendekatan yang di aplikasikan ke dalam manajemen kejadian Keamanan Informasi	
Kontrol : 13.2.1	Tanggung jawab dan prosedur
Kontrol : 13.2.2	Belajar dari kejadian Keamanan Informasi
Kontrol : 13.2.3	Pengumpulan bukti
Klausul : 14 Manajemen Kelangsungan Bisnis	
Kategori Kemanan Utama: 14.1 Aspek keamanan dalam manajemen kelangsungan bisnis	
Objektif Kontrol Untuk menghindari gangguan terhadap aktivitas bisnis serta untuk menjaga proses-proses bisnis yang kritis dari kegagalan dan banyak yang lebih besar atau bencana terhadap sistem Informasi	
Kontrol : 14.1.1	Memasukan keamanan Informasi dalam proses manajemen kelangsungan bisnis
Kontrol : 14.1.2	Kelangsungan bisnis dan penilaian resiko
Kontrol : 14.1.3	Pembangunan dan rencana kelangsungan yang di dalamnya meliputi Keamanan Informasi
Kontrol : 14.1.4	Kerangka kerja rencana kelangsungan bisnis
Kontrol : 14.1.5	Pengujian pemeliharaan dan penilaian ulang

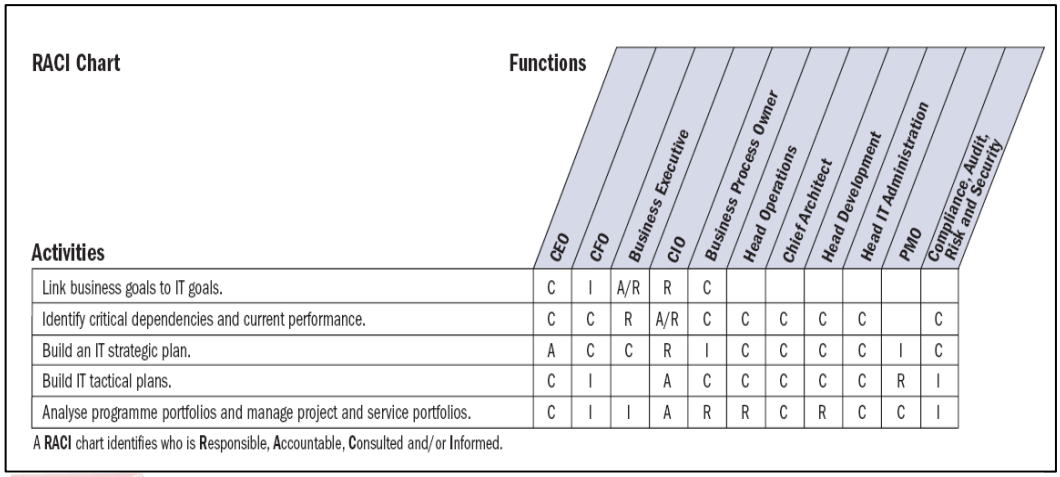
Tabel 2. 7 (Lanjutan)

Klausul : 15 Kepatuhan	
Kategori Kemanan Utama: 15.1 Kepatuhan terhadap persyaratan legal	
Objektif Kontrol Untuk mencegah pelanggan terhadap hukum, perundangan peratuaran atau kewajiban kontrak dan suatu persyaratan keamaanan	
Kontrol : 15.1.1	Identifikasi perundangan yang dapat diaplikasikan
Kontrol : 15.1.2	Hak kelayakan intelektual
Kontrol : 15.1.3	Perlindungan dokumen organisasi
Kontrol : 15.1.4	Perlindungan penyalahgunaan fasilitas pemrosesan informasi
Kontrol : 15.1.5	Pencegahan penyalahgunaan fasilitas pemrosesan informasi
Kontrol : 15.1.6	Peratutan kontrol kriptografi
Kategori Keamanan Utama : 15.2 Kepatuhan dengan kebijakan keamanan, standar dan kepatuhan teknik	
Objektif Kontrol Untuk memastikan kepatuhan terhadap sistem di dalam kebijakan keamanan organisasi dan standar	
Kontrol : 15.2.1	Kepatuhan dengan kebijakan keamanan dan standar
Kontrol : 15.2.2	Pemeriksaan kepatuhan teknik
Kategori Keamanan Utama : 15.3 Audit Sistem Informasi dan pertimbangan	
Objektif Kontrol Untuk memaksimalkan keefektifitasan dan meminimalisir interfensi dari atau ke dalam proses audit Sistem Informasi.	
Kontrol : 15.3.1	Kontrol Audit Sistem Informasi
Kontrol : 15.3.2	Perlindungan terhadap perangkat audit Sistem Informasi

2.10. Tabel RACI

Tabel RACI merupakan matriks yang menggambarkan peran berbagai pihak dalam penyelesaian suatu pekerjaan dalam suatu proyek atau proses bisnis. matriks ini sangat bermanfaat dalam menjelaskan peran dan tanggung jawab antarbagian yang ada dalam suatu proyek atau proses. Raci sedniri merupakan

singkatan dari *Responsible*, *Accountable*, *Consulted* dan *Informed*. Hal tersebut dapat dilihat pada gambar 2.5.



RACI Chart — Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Gambar 2. 5 RACI Chart
(Sumber: IT Governance Institute, 2007)

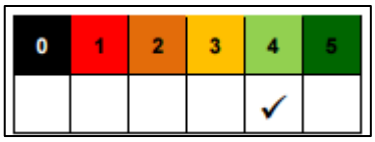
Berikut penjelasan dari RACI Chart antara lain.

1. *Responsible* (Pelaksana) : Orang yang melakukan suatu kegiatan atau melakukan pekerjaan.
2. *Accountable* (Penanggung jawab) : Orang yang akhirnya bertanggung jawab dan memiliki otoritas untuk memutuskan suatu perkara.
3. *Consulted* (Penasehat) : Orang yang diperlukan umpan balik atau sarannya dan berkontribusi akan kegiatan tersebut.
4. *Informed* (Terinformasi) : Orang yang perlu tahu hasil dari suatu keputusan atau tindakan.

2.11. Tingkat Kedewasaan (Maturity Level)

Menurut IT Governance Institute (2007: 17) model kedewasaan (*maturity level*) merupakan model yang digunakan dalam mengendalikan suatu proses TI yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat melakukan pengukuran dirinya sendiri. Menurut DISC Infosec (2009) salah

satu cara untuk dapat mencapai kontrol keamanan informasi yang optimal adalah menilai keamanan informasi organisasi berdasarkan ISO 27002 dan pemetaan setiap kontrol keamanan menggunakan *Capability Maturity Model Integration* (CMMI). CMMI memiliki lima tingkatan kematangan proses yang dapat dilihat pada gambar 2.6.



Gambar 2. 6 Tingkat Kematangan CMMI
(Sumber: DISC Infosec, 2009)

Dalam penilaian *maturity level* dilakukan menggunakan lima tingkatan proses rangkaian kesatuan kedewasaan berdasarkan metodologi CMMI. Metode CMMI digunakan sebagai acuan untuk perbandingan serta memiliki peran sebagai alat bantu untuk memahami tingkah laku, praktek, dan proses-proses dalam organisasi. Lima tingkatan kerangka kesatuan CMMI 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.