BAB II

LANDASAN TEORI

2.1. Rumah Sakit

Rumah sakit merupakan sebuah institusi yang fungsi utamanya memberikan pelayanan kesehatan kepada masyarakat. Tugas rumah sakit adalah melaksanakan upaya kesehatan secara berdaya guna dan berhasil guna dengan mengutamakan upaya penyembuhan dan pemulihan yang dilaksanakan secara serasi dan terpadu dengan peningkatan dan pencegahan serta melaksanakan rujukan. Untuk dapat menyelenggarakan upaya-upaya tersebut dan mengelola rumah sakit agar tetap dapat memenuhi kebutuhan pasien dan masyarakat yang dinamis, maka setiap komponen yang ada di rumah sakit harus terintegrasi dalam satu sistem (Soejitno, 2002)

Menurut Depkes RI (1992) berdasarkan pembedaan tingkatan menurut kemampuan unsur pelayanan kesehatan yang dapat disediakan, ketenagaan, fisik dan peralatan, maka rumah sakit umum pemerintah pusat dan daerah diklasifikasikan menjadi:

1. Rumah Sakit Umum Kelas A adalah rumah sakit umum yang mempunyai fasilitas dan kemampuan pelayanan medis spesialistik luas dan subspesialistik luas.
2. Rumah Sakit Umum Kelas B adalah rumah sakit umum yang mempunyai fasilitas dan kemampuan pelayanan medis sekurang-kurangnya 11 spesialistik luas dan subspesialistik terbatas.

3. Rumah Sakit Umum Kelas C adalah rumah sakit umum yang mempunyai fasilitas dan kemampuan pelayanan medis spesialistik dasar.

4. Rumah Sakit Umum Kelas D adalah rumah sakit umum yang mempunyai fasilitas dan kemampuan pelayanan medis dasar.

2.2. Sistem Informasi

Menurut Al-Bahra Bin Ladjamudin dalam bukunya yang berjudul Analisis & Desain Sistem Informasi (2005: 13), menyebutkan sistem informasi dapat didefinisikan sebagai berikut:

a. Suatu sistem yang dibuat oleh manusia yang terdiri dari komponen-komponen dalam organisasi untuk mencapai suatu tujuan yaitu menyajikan informasi.
b. Sekumpulan prosedur organisasi yang pada saat dilaksanakan akan memberikan informasi bagi pengambil keputusan dan/atau untuk mengendalikan organisasi.

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 strategik.

Sistem informasi memberikan nilai tambah terhadap proses produksi, kualitas, manajemen, pengambilan keputusan, dan pemecahan masalah serta keunggulan kompetitif yang tentu saja sangat berguna bagi kegiatan bisnis (Kroenke dalam Kadir, 2003:5).

2.3. Sistem Informasi Manajemen Rumah Sakit (SIM-RS)

Menurut peraturan menteri kesehatan nomor 82 Tahun 2013 sistem informasi manajemen rumah sakit yang selanjutnya disingkat SIM-RS adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan rumah sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari sistem informasi kesehatan. Pelaksanaan pengelolaan dan pengembangan SIM-RS harus mampu meningkatkan dan mendukung proses pelayanan kesehatan di rumah sakit yang meliputi:

a. Kecepatan, akurasi, integrasi, peningkatan pelayanan, peningkatan efisiensi, kemudahan pelaporan dalam pelaksanaan operasional.
b. Kecepatan mengambil keputusan, akurasi dan kecepatan identifikasi masalah dan kemudahan dalam penyusunan strategi dalam pelaksanaan manajerial.
c. Budaya kerja, transparansi, koordinasi antar unit, pemahaman sistem dan pengurangan biaya administrasi dalam pelaksanaan organisasi.

2.4. Audit

Menurut Canon (2011) audit merupakan suatu 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. Sedangkan tujuan audit adalah untuk memberikan suatu Gambaran kondisi tertentu yang terjadi di

organisasi dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi.

2.5. Audit Sistem Informasi

Audit Sistem Informasi adalah suatu proses untuk mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan apakah sistem teknologi informasi yang digunakan mampu melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu tercapainya tujuan organisasi secara efektif, serta dapet menggunakan sumber daya yang dimiliki secara efisien (Weber, 1999).

Beberapa elemen utama (Weber, 1999) tinjauan penting dalam audit sistem informasi dapat diklasifikasikan sebagai berikut:

1. Tinjauan terkait fisik dan lingkungan, yaitu: suatu hal yang terkait dengan keamanan fisik, suplai sumber daya, *temperature*, kontrol kelembaban ruanganan, kualitas gedung, risiko bencana alam dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu: mencakup tinjauan keamanan sistem operasi, sistem manajemen *database*, seluruh prosedur administrasi sistem serta prosedur pelaksanaanya.
3. Tinjauan perangkat lunak, yaitu: perangkat lunak yang dimaksud adalah perangkat lunak untuk tujuan 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 ke dalam sistem dalam suatu organisasi, batasan tingkat keamanan, tinjuan terhadap *firewall*, daftar kontrol akses *router*, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem dalam suatu organisasi.
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 serta dampak dari kurangnya kontrol yang diterapkan.

2.6. Keamanan Informasi

Menurut Sarno dan Iffano (2009) keamanan informasi adalah suatu 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. Contoh kemanan informasi menurut (Sarno dan Iffano, 2009) adalah:

1. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

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

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

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

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 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 suatu informasi.

2.7. Audit Keamanan Sistem Informasi

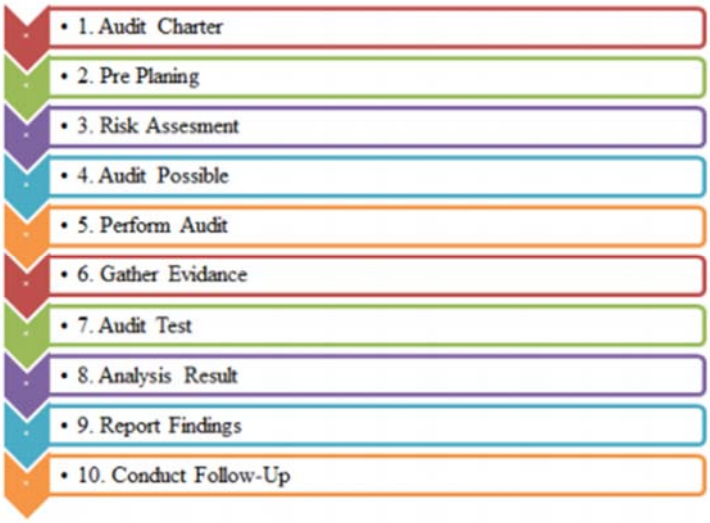
Menurut Ahmad (2012) audit keamanan sistem informasi adalah suatu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada dan untuk melakukan verifikasi apakah perlindungan yang ada berjalan dengan baik dan benar.

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.

2.8. 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 2.2.



Gambar 2.2 Tahapan-tahapan Audit Teknologi Informasi
(Sumber: Cannon, 2011)

2.9. 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.

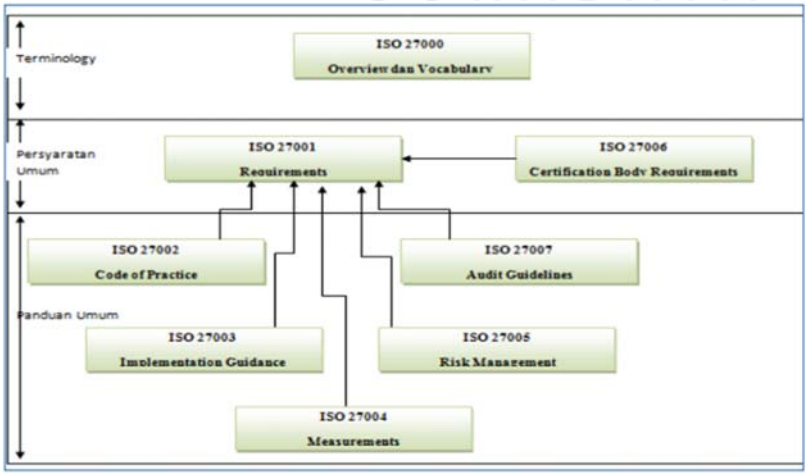
h. ISO/IEC 27007 – *Guidelines for ISMS Auditing*

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 2.3



Gambar 2.3 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.

2.10. 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 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 Ringkasan Jumlah Klausul Kontrol Keamanan, Obyektif Kontrol dan Kontrol Pada ISO 27002:2005

Klausul	**Jumlah**	
	Objektif Kontrol	Kontrol
4	2	-
5	1	2
6	2	11
7	2	5
8	3	9

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

Dalam penelitian ini, audit keamanan sistem informasi akan difokuskan pada 4 klausul, yaitu klausul 7 tentang manajemen aset, klausul 8 tentang keamanan sumber daya manusia, klausul 9 tentang keamanan fisik dan 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 Kontrol Acuan Audit Keamanan SIstem Informasi 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 fasilitas-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*
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*
Kontrol : 10.9.2	Transaksi *On-Line*
Kontrol : 10.9.3	Informasi untuk publik
Kategori Keamanan Utama : 10.10 Monitoring ***Objektif Kontrol*** Untuk mendeteksi aktifitas pemrosesan informasi secara ilegal.	
Kontrol : 10.10.1	Rekaman 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*

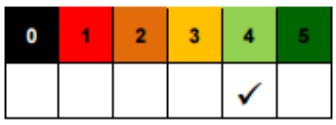
Kontrol : 12.2.2	Kontrol untuk pemrosean internal
Kontrol : 12.2.3	Integritas pesan
Kontrol : 12.2.4	Validasi data *output*
Kategori Keamanan Utama : 12.3 Kontrol Kriptografi ***Objektif Utama*** Untuk melindungi kerahasiaan, autentifikasi dan keutuhan Informasi dengan menggunakan sistem kriptografi.	
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 risiko yang disebabkan oleh terpublikasinya teknik-teknik kelemahan yang dimiliki.	
Kontrol : 12.6.1	Kontrol terhadap kelemahan secara teknis
Klausul : 13 Manajemen kejadian Keamanan Informasi	
Kategori Keamanan Utama: 13.1 Pelaporan Kejadian dan Kelemahan Keamanan 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 keefektifitasan pendekatan yang diaplikasikan 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 risiko
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
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

2.11. Tingkat Kedewasaan (Maturity Level)

IT Governance Institute (2007: 17) menjelaskan model kedewasaan (*maturity level*) merupakan model yang digunakan untuk mengendalikan suatu proses TI yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur 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 tingkat kematangan proses yang dapat dilihat di halaman selanjutnya pada Gambar 2.4.



Gambar 2.4 Tingkat Kematangan CMMI
(Sumber: DISC Infosec, 2009)

Dalam penilaian *maturity level* dilakukan dengan 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.