BAB 2

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian sebelumnya telah dilakukan berdasarkan framework ISO/IEC 27001. Diantaranya adalah penelitian yang dilakukan oleh Lussianty, dkk, penelitian tersebut membahas tentang pengukuran risiko pada PT. Street Directory Indonesia dengan judul penelitian "*Pengukuran Risiko Informasi Teknologi Pada PT. Street Directory Indonesia dengan Menggunakan ISO/IEC 27001/2"* penelitian tersebut dilakukan untuk mengidentfikasi praktek keamanan dan memberikan solusi untuk mengelola keamanan informasi dan meminimalisir dapak risiko yang terdapat pada PT. Street Directory Indonesia. [1]

Penelitian lainnya dilakukan oleh Riawan Arbi Kusuma yang membahas tentang keamanan system informasi dengan judul *"Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta"*

Penelitian tersebut dilakukan untuk memformulasikan hasil audit keamanan Sistem Informasi Akademik UIN SUNAN KALIJAGA YOGYAKARTA dengan menggunakan standar SNI ISO 27001.[2]

2.2 Landasan Teori

2.2.1 Sistem Informasi

Rainer & Cegielski (2013:5) mendefinisikan sistem informasi sebagai berikut : "*An information system collecting, process, store, analyze, and disseminate information for specific purposes. It has been said that the purpose of information system is to get the right information to right people, at the right time, in the right amount, and in the right format.*"[3] Dari kutipan tersebut dapat diterjemahkan sebagai berikut: Sebuah sistem informasi mengumpulkan, memproses, menyimpan, menganalisis, dan menyebarkan informasi untuk tujuan spesifik. Telah mengatakan bahwa tujuan dari sistem informasi

adalah untuk mendapatkan informasi yang tepat untuk orang yang tepat, pada waktu yang tepat, dalam jumlah yang tepat, dan dalam format yang tepat.

Menurut *Satzinger, Jackson, & Burd* (2009:6), "*Information system a collection of interrelated components that collect, process, store, and provide as output the information needed to complete business tasks."* Dari kutipan tersebut dapat diterjemahkan sebagai berikut: Sistem informasi sebuah kumpulan komponen yang saling terkait yang mengumpulkan, memproses, menyimpan, dan menyediakan output informasi yang dibutuhkan untuk menyelesaikan tugas-tugas bisnis. [1]

2.2.2 Teknologi Informasi

Menurut *Rainer & Cegielski (2011:7)*, "*Information Technology (IT) relates to any computer-based tool that people use to work with information and to support the information and information-processing needs if an organization.*"[3] Dari kutipan tersebut dapat diterjemahkan sebagai berikut: Teknologi Informasi (TI) berhubungan dengan beberapa alat berbasiskan komputer yang digunakan orang untuk bekerja dengan menggunakan dan mendukung informasi, serta pemprosesan informasi yang dibutuhkan oleh organisasi.

2.2.2.1 Infrastruktur Teknologi Informasi

1. Hardware

   Menurut *Rainer* (2013:13), *hardware* terdiri dari perangkat seperti prosesor, monitor, keyboard, dan printer. Bersamaan, perangkat ini menerima, mengolah, dan menampilkan data dan informasi. Sehingga dari kedua kutipan tersebut dapat disimpulkan bahwa pengertian dari hardware adalah sebuah perangkat system yang terdiri dari prosesor, monitor, keyboard, dan printer. Perangkat tersebut merupakan bagian dari sistem pengendalian keamanan informasi yang dapat menerima, mengolah, dan menampilkan data dan informasi. [3]

2. Software

   Menurut *Rainer* (2013:12), Software adalah program atau kumpulan program yang memungkinkan hardware untuk memproses data. Menurut *Turban & Volonino* (2012:9), "*Software is a set of applications or programs that instruct the hardware to process data or other inputs such as voice commands*." Dari kutipan tersebut dapat diterjemahkan sebagai berikut: Software adalah seperangkat aplikasi atau program yang menginstruksikan perangkat keras untuk memproses data atau masukan lain seperti perintah suara. Sehingga dari kedua kutipan tersebut dapat disimpulkan bahwa pengertian dari software adalah sekumpulan program atau seperangkat aplikasi yang memberikan perintah kepada hardware untuk memproses data. [3]

3. Jaringan

   Jaringan adalah kumpulan dari beberapa perangkat yang saling terhubung satu sama lain guna melakukan suatu komunikasi data dengan memanfaatkan protokol komunikasi melalui media komunikasi (kabel atau nirkabel) sehingga dapat saling berbagi informasi, data, program dan dapat menggunakan perangkat secara bersama. Jaringan komputer terbagi atas jaringan internal dan eksternal, jaringan komputer internal adalah jaringan komputer yang menghubungkan antar host-host yang terhubung satu sama lain baik dalam lingkup satu gedung maupun antar gedung, sedangkan jaringan eksternal adalah jaringan yang menghubungkan antar host dimana host satu dengan yang lain beda perusahaan atau pihak ketiga.

   Keamanan jaringan adalah suatu cara berupa sebuah sistem yang digunakan untuk menjaga, melindungi tau memberikan proteksi pada suatu jaringan agar terhindar dari ancaman baik dari dalam maupun dari luar yang mengakibatkan rusaknya jaringan dan bocornya suatu informasi yang yang berasa pada suatu jaringan sehingga orang lain yang tidak mempunyai hak tidak bisa memperoleh informasi tersebut.

Keamanan jaringan komputer bagi suatu perusaan sangatnya krusial melihat dari segi bisnis dan informasi sehingga diperlukan suatu sistem yang dapat menjaga informasi yang ada pada perusahaan agar tidak digunakan, modifikasi, interupsi, dan diganggu oleh orang yang tidak berwenang.

4. Sistem komputer

   adalah suatu yang terdiri dari software dan hardware yang mempunyai tugas tertentu berupa input, proses data, penyimpanan data serta memberikan outputan berupa informasi.

   Informasi adalah suatu aset yang berharga demi kelangsungan hidup suatu perusahaan atau bisnis yang berupa catatan, audio, visual atau berupa file.

2.2.2.2 Fungsi Teknologi Informasi

Fungsi dari Teknologi Informasi adalah menangkap, memproses data masukan yang diterima untuk menjadi suatu informasi. Pengolahan atau pemprosesan dapat berupa pengubahan data kebentuk lain, analisis, perhitungan, penggabungan, segala bentuk data dan informasi sehingga membentuk informasi yang berguna yang dapat disimpan kedalam suatu media penyimpanan data dan dapat dicari kembali informasi yang diperlukan. Informasi tersebuat dapat dipindah atau dikirim ke lokasi lain dengan melalui jaringan komputer

2.2.3 Firewall

2.2.3.1 Pengertian Firewall

Firewall adalah piranti berupa perangkat lunak yang di tempatkan pada ujung koneksi jaringan yang berfungsi sebagai *Network Border Security officer* (Petugas Keamanan Pembatasan Jaringan). Piranti ini mengawasi seluruh aliran yang keluar dan masuk ke koneksi, memilah milah aliran data yang dapat dihentikan atau ditolak berdasarkan aturan yang telah dibuat. [1]

2.2.3.2 Fungsi Firewall

Firewall dirancang dapat melakukan sebagai berikut :

1. Mengontrol dan mengatur lalu lintas jaringan
2. Autentifikasi terhadap akses
3. Melindungi sumberdaya dalam jaringan privat, mencatat dan melaporkan semua kejadian dalam suatu jaringan kepada *administrator*

2.1.1 Malware

1. Trojan

Trojan horse adalah suatu program yang mereplikasi dirinya seperti tampak suatu program aplikasi yang sebenarnya, padahal sesungguhnya sebuah program yang sangat menyerang dengan menipu user. Trojan akan aktif ketika, sebuah program dijalankan. Mungkin saja dapat berisi kode yang dapat merusakkan komputer. Trojan dapat juga menciptakan suatu dobrakan ke dalam suatu sistem yang membiarkan hackers dapat memperoleh akses.

2. Virus

Virus adalah suatu program yang aktif dan menyebar dengan memodifikasi program atau file lain. Virus tidak bisa aktif dengan sendirinya; melainkan perlu diaktipkan. Sekali diaktipkan, dia akan mereplikasi dirinya dan menyebar.

Meskipun demikian sederhana, bahkan virus ini sangat berbahaya karena dapat dengan cepat menggunakan semua memori yang tersedia dan dapat berakibat mesin komputer tak bisa berjalan sebagaimana mestinya. Virus dibuat untuk menghapus atau merusak file tertentu, yang dipancarkan biasanya melalui email, downolad file, media storage non permanen, dsb. alat penyimpan data.

3. Worm

Worm serupa dengan virus, tetapi tidak sama sebagaimana virus, dia tidak mereplikasi dirinya. Worm menggunakan jaringan yang terhubung. Worm dapat aktif dan menyebar dengan cepat dan tidak perlu memerlukan intervensi manusia

atau diaktifkan. Sistem kerja Worm dapat mempunyai dampak jauh lebih besar dibanding virus tunggal dan dapat menyebar dan menginfeksi bagian-bagian dari jaringan dengan cepat

2.1.2 IT Audit

IT Audit merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (*Weber, 2000*)[9]

2.1.2.1 Prosedur Audit

Prosedur audit merupakan suatu alat bantuan yang digunakan untuk mengidentifikasi sebuah peristiwa. Dalam proses audit ada 4 prosedur audit yang harus dilakukan yaitu inspeksi, observasi, penyelidikan, dan konfirmasi (Bastian, 2007)[9]. Beberapa prosedur audit yang dapat kita jumpai saat ini yaitu :

1. Inspeksi

   Merupakan pemeriksaan secara rinci dan spesifik terhadap dokumen atau kondisi fisik suatu dokumen. Prossedur ini banyak dilakukan oleh auditor.
2. Pengamatan

   Merupakan prosedur audit yang digunakan oleh auditor untuk melihat, memantau atau menyaksikan pelaksanaan suatu kegiatan.
3. Konfirmasi

   Merupakan bentuk penyelidikan yang memungkinkan auditor memperoleh informasi secara langsung dari pihak ketiga yang bebas, dalam hal ini auditor mendapatkan informasi langsung dari pihak luar atau disebut pihak ketiga yang bebas
4. Permintaan keterangan

   Merupakan prosedur audit yag dilakukan dengan meminta keterangan secara lisan. Bukti audit yang dihasilkan oleh prosedur ini adalah bukti lisan dan dokumenter.

5. Penelusuran

   Dalam pelaksanaan prosedur auditing dan melakukan penelusuran informasi sejak mula-mula informasi tersebut direkam pertama kali dalam dokumen, dilanjutkan dengan pelacakan pengolahan informasi tersebut.

6. Pemeriksaan dokumen pendukung (Vouching)

   Merupakan prosedur audit yang meliputi:

   a. Inspeksi terhadap dokumen-dokumen yang mendukung suatu transaksi atau informasi keuangan untuk menentukan kewajaran dan kebenarannya.
   b. Pembandingan dokumen tersebut dengan catatan yang berkaitan.

7. Perhitungan (Counting)

   Prosedur ini meliputi:

   a. Penghitungan fisik terhadap sumber daya berwujud seperti persediaan di tangan.
   b. Pertanggung jawaban semua formulir bernomor urut cetak.

8. Scanning

   Merupakan review secara cepat terhadap dokumen, catatan, dan daftar untuk mendeteksi unsur-unsur yang tampak tidak biasa yang memerlukan penyelidikan lebih mendalam.

9. Pelaksanaan ulang (Reperforming)

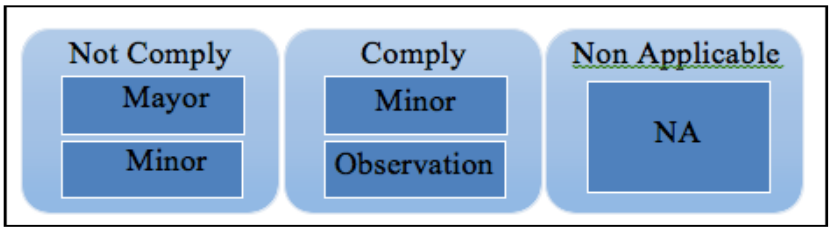
   Merupakan pelaksanaan ulang (reperforming) perhitungan dan rekonsiliasi yang dibuat oleh pelanggan.

10. Teknik audit dengan bantuan komputer

    Apabila catatan pelanggan diselenggarakan dalam media elektronik, auditor perlu menggunakan teknik audit bantuan komputer (computer-assisted audit techniques) dalam menggunakan prosedur audit.

2.1.2.2 Kategori Temuan Audit

Terdapat beberapa kategori temuan untuk analisa hasil audit yaitu :



Gambar 2.1 Kategori Temuan Audit

Penjelasan :

1. *Not Comply* : Tidak memenuhi persyaratan pada kontrol keamanan.
2. *Comply* : Memenuhi persyaratan pada kontrol keamanan.
3. *Non Applicable* (NA) : Persyaratan pada kontrol keamanan tidak berlaku di dalam proses.
4. *Major Finding* : Apabila tidak ada sama sekali aktivitas yang dilakukan dan tidak terdapat dokumen yang mendukung serta memiliki dampak yang besar.
5. *Minor Finding* : Aktivitas telah dilakukan namun tidak ada dokumen yang mendukung. Apabila dampak yang dihasilkan cukup besar maka termasuk Not Comply.
6. *Observation* : Aktivitas telah dilakukan dan sudah ada dokumen yang mendukung namun terdapat beberapa hal yang masih belum lengkap. Temuan ini tidak bisa dijadikan masukan kedalam kategori ketidaksesuaian, serta tidak melanggar dokumentasi sistem manajemen yang telah ditetapkan sebelumnya.

2.1.2.3 Sifat Temuan Audit

Temuan Audit mempunyai beberapa ukuran dan bentuk diantaranya :

1. Tindakan yang seharusnya diambil tetapi tidak dilakukan
2. Tindakan yang seharusnya tidak boleh dilakukan, seperti memberikan user dan password kepada orang lain
3. Eksposur-eskposur risiko yang harus dipertimbangkan

2.2 Teori Khusus

2.2.1 Manajemen Risiko

2.2.1.1 Pengertian

Peltier (2005:325) mengatakan bahwa, "*Risk is the probability that a particular critical infrastructure's vulnerability is being exploited by a particular threat weighted by the impact of that exploitation.*"[4] Dari kutipan tersebut dapat diterjemahkan sebagai berikut : Risiko adalah kemungkinan bahwa kerentanan suatu infrastruktur yang bersifat kritis sedang dieksploitasi oleh ancaman tertentu tertimbang dengan dampak dari eksploitasi tersebut.

Menurut *Schwalbe (2011:425), "Risk is an uncertainty that can have a negative or positive effect on meeting project objectives."* Dari kutipan tersebut dapat diterjemahkan sebagai berikut: Risiko adalah ketidak pastian yang dapat memiliki dampak negatif atau positif dalam memenuhi tujuan proyek.[9]

Sehingga dari dua kutipan di atas dapat diambil kesimpulan bahwa pengertian dari risiko adalah kemungkinan bahwa kerentanan suatu infrastruktur yang bersifat kritis sedang dieksploitasi oleh ancaman tertentu yang dapat memiliki dampak negatif atau positif dalam memenuhi tujuan proyek.

2.2.1.2 Penilaian Risiko

Organisasi menggunakan penilaian risiko untuk menentukan ancaman apa yang terdapat pada suatu aset dan tingkat risiko yang terkait pada ancaman tersebut. Prioritas pada ancaman (penentuan tingkat risiko) memberikan informasi yang dibutuhkan oleh organisasi untuk memilih langkah yang tepat dalam mengendalikan, melindungi, atau melakukan tindakan untuk menurunkan risiko ke tingkat yang dapat diterima (*Peltier, 2005 : 16*)[4]. Menurut *Peltier (2005 : 16)*, penilaian risiko dibagi menjadi enam langkah yaitu :

a. Definisi Aset

Tim penilaian risiko dan pemilik perusahaan akan mendefinisikan proses, aplikasi, sistem, atau aset yang sedang ditinjau. Pada penilaian risiko sebuah proyek, definisi aset harus sesuai dengan ruang lingkup dan hasil yang diinginkan. Seperti setiap proyek, penyampaian dari langkah definisi aset adalah untuk mencapai kesepakatan dengan pemilik perusahaan pada apa yang dinilai dan penggunaan semua parameter yang relevan.

b. Identifikasi Ancaman

Ancaman merupakan suatu peristiwa yang tidak diinginkan yang dapat mempengaruhi tujuan atau misi dari unit bisnis atau perusahaan bisnis. Terdapat tiga kategori utama dari sumber ancaman :

1) Natural Threat : seperti banjir, gempa bumi, tornado, tanah longsor.
2) Human Threat : ancaman yang disebabkan oleh manusia seperti tindakan yang tidak disengaja (kesalahan dan kelalaian) atau tindakan yang disengaja (melakukan kecurangan, instalasi perangkat lunak yang berbahaya, akses yang tidak sah),
3) Environmental Threat : seperti pemadaman listrik jangka panjang, polusi, tumpahan bahan kimia, kebocoran cairan

c. Menentukan Probabilitas Kejadian

Setelah daftar ancaman telah selesai dan tim telah menyepakati definisi dari setiap ancaman, maka diperlukan untuk menentukan seberapa besar kemungkinan ancaman dapat terjadi.

Berikut ini adalah definisi dari probabilitas atau kemungkinan ancaman yang mungkin terjadi:

1) *Probability* : kemungkinan bahwa ancaman akan terjadi
2) *High probability* : Sangat mungkin bahwa ancaman akan terjadi dalam tahun berikutnya.

3) *Medium probability* : Kemungkinan bahwa ancaman mungkin terjadi selama tahun berikutnya.
4) *Low probability* : Sangat tidak mungkin bahwa ancaman akan terjadi selama tahun berikutnya.

d. Menentukan Dampak Dari Ancaman

Setelah menentukan kemungkinan ancaman yang terjadi, maka diperlukan untuk menentukan dampak dari ancaman pada organisasi. Penilaian risiko akan memerlukan definisi dari dampak tersebut serta tabel matriks yang akan memungkinkan tim untuk menetapkan tingkat risiko. Berikut ini adalah definisi dari dampak yang dapat digunakan untuk menentukan tingkat risiko :

1) *Impact* : Ukuran besarnya kerugian atau kerusakan pada nilai aset.
2) *High Impact* : penutupan pada unit bisnis yang bersifat penting. Dampak ini mengarah pada kerugian yang signifikan pada bisnis, perusahaan, atau keuntungan
3) *Medium Impact* : gangguan jangka pendak pada proses bisnis atau system yang menyebabkan kerugian pada sebagian bidang keuangan pada unit bisnis tunggal
4) *Low Impact* : tidak menyebabkan kehilangan atau kerugian.

Tabel 2.2 *Probabilitas-Impact Matrix*

IMPACT

PROBABILITAS

	High	Medium	Low
High	High	High	Medium
Medium	High	High	Medium
Low	Medium	Medium	Low

Keterangan :

High	: Tindakan korektif harus diterapkan.
Medium	: Tindakan korektif sebaiknya diterapkan.
Low	: Tidak ada tindakan yang diperlukan

e. Kontrol yang Direkomendasikan

Setelah tingkat risiko telah ditetapkan, kemudian akan mengidentifikasikan control atau perlindungan yang mungkin dapat menghilangkan risiko, atau setidaknya mengurangi risiko ke tingkat yang dapat diterima. Ketika memilih jenis pengendalian, maka diperlukan untuk mengukur dampak operasional untuk organisasi. Tujuan dari daftar kontrol yang direkomendasikan adalah untuk mengidentifikasi kategori kontrol yang akan mengarahkan tim untuk menentukan kontrol khusus yang diperlukan.

f. Dokumentasi

Setelah analisis risiko selesai dilakukan, hasil analisa risiko perlu didokumentasikan dalam format standar dan laporan yang ditujukan kepada pemilik aset. Laporan ini akan membantu perusahaan untuk mengambil keputusan tentang kebijakan, prosedur, anggaran, system, dan perubahan manajemen. Laporan analisis risiko harus disajikan secara sistematis dan analitis sehingga perusahaan akan memahami risiko dan mengalokasikan sumber daya untuk mengurangi risiko ke tingkat yang dapat diterima.

2.2.2 SMKI (Sistem Manajemen Keamanan Informasi)

Arnanson & Willett (2008:14) mengatakan bahwa, "I*SO defines ISMS to be "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security"*. Dari kutipan tersebut dapat diterjemahkan sebagai berikut : ISO mendefinisikan SMKI menjadi "bagian dari system manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan,

menerapkan, mengoperasikan, memantau, mengkaji, memelihara, dan meningkatkan keamanan informasi".

2.2.2.1 Keamanan Informasi

Keamanan informasi merupakan salah satu hal penting yang harus diperhatikan oleh perusahaan, kebocoran informasi dan kegagalan sistem dapat menyebabkan kerugian baik di sisi finansial maupun produktifitas perusahaan. Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan database pada level obyek, keamanan informasi pada pengguna, dimana pengguna tersebut memiliki akses informasi tertentu.

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi risiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dalam peluang bisnis. (*ISO/IEC 27001, 2005*)[8].

mengenai keamanan informasi terutama akan ditentukan berdasarkan seberapa jauh tingkat keamanan yang akan dibangun untuk informasi dalam database. Tingkat keamanan informasi juga bergantung pada tingkat sensitifitas informasi dalam database, biasanya informasi yang tidak terlalu sensitif sistem keamanannya tidak ketat sedangkan informasi yang sangat sensitif perlu pengaturan keamanan yang ketat untuk akses ke informasi tersebut.

Ancaman-ancaman keamanan informasi (Threats) meliputi orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan, ancaman dapat bersifat internal maupun internal serta disengaja maupun tidak disengaja.

Keamanan informasi terdiri dari perlindungan terhadap beberapa aspek. Aspek-aspek yang dimaksud adalah sebagai berikut :

1. *Confidentiality* (kerahasiaan): aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang

yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. *Integrity* (Integritas) : aspek yang menjamin bahwa data tidak dirubah tanpa ada izin dari pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.
3. *Availability* (Ketersediaan) : aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).
4. *Privasi* (Privasi)

   Adalah prinsip yang menjamin bahwa informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi digunakan hanya untuk tujuan tertentu oleh pemilik informasi pada saat informasi dikumpulkan. “Information that is collected, used, and stored by an organization is intended only for the purposes stated by the data owner at the time it was collected,” (Whitman & Mattord, 2010)[1]
5. *Identification* (Identifikasi)

   Adalah prinsip yang menjamin bahwa informasi memiliki karakteristik identifikasi ketika informasi dapat mengenali penggunanya. Identifikasi adalah langkah pertama dalam memperoleh akses ke informasi yang diamankan, dan berfungsi sebagai dasar untuk otentifikasi dan otorisasi. “An information system possesses the characteristic of identification when it is able to recognize individual users. Identification is the first step in gaining access to secured material, and it serves as the foundation for subsequent authentication and authorization,” (Whitman & Mattord, 2010)[1]
6. *Authentificatin* (Autentifikasi)

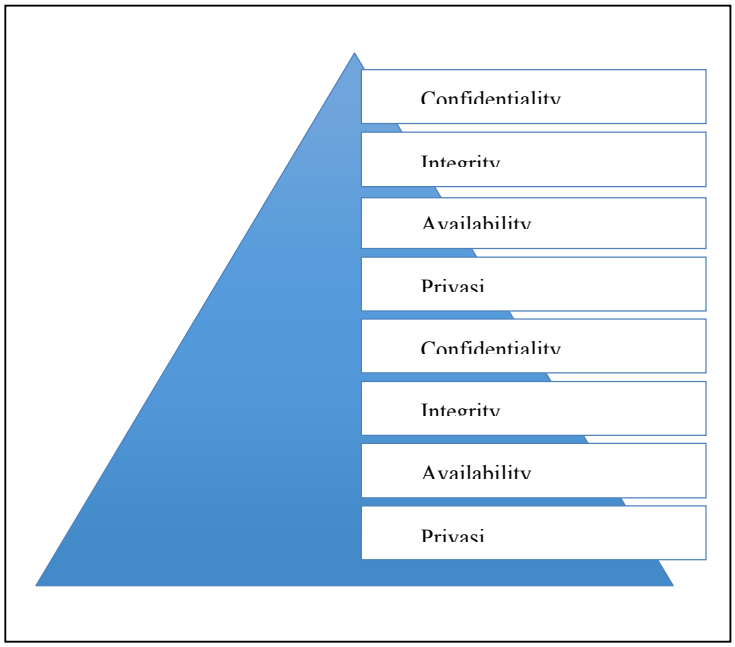
   Adalah prinsip yang menjamin bahwa saat otentifikasi terjadi ketika sistem dapat membuktikan bahwa pengguna memiliki hak klaim. “Authentication occurs when a control proves that a user possesses the identify that he or she claims,” (Whitman & Mattord, 2010)[1]

7. Authorization (Otorisasi)

   Adalah prinsip yang menjamin bahwa pengguna telah mendapatkan otorisasi sehingga dapat mengakses, mengupdate atau menghapus informasi. "After the identify of a user is authenticated, a process called authorization assures that the user has been specifically and axplicitly authorized by the proper authority to access, update, or delete the contents of information," (Whitman & Mattord, 2010)[1]

8. Accountability (Akuntabilitas)

   Akuntabilitas dari informasi dikatakan eksis ketika sistem dapat menyajikan semua aktifitas terhadap informasi, dan siapa yang melakukan aktifitas itu. "Accountability of information exist when a control provides assurance that every activity undertaken can be attribute to a named person," (Whitman & Mattord, 2010)[1]



Gambar 2.2. Prinsip Keamanan Informasi

2.2.2.2 Ruang Lingkup Keamanan Informasi

Ruang lingkup keamanan informasi ada 4 yaitu organization, people, process, dan technology, lebih lanjutnya akan dijelaskan sebagai berikut

1. Organization

   Sebuah organisasi adalah jaringan yang terdiri atas manusia, aset dan proses interaksi satu dengan yang lain yang didefinisikan dengan peran dan pekerjaan yang bertujuan untuk menyelesaikan tujuan bersama. “An organization is a network of people, assets, and processes interacting with each other in defined roles and working toward a common goal,” (ISACA, 2010, p. 38). [9]

2. People

   Sumber daya manusia dan isu-isu keamanan informasi yang berkaitan. Siapa yang mengimplementasi setiap bagian dari strategi yang ada. Representasi kolektif manusia dan nilai-nilai perilaku, serta nilai-nilai yang masih bias harus diperhitungkan,

   “The human resources and security issues that surround them. It defines who implements (throught design) each part of the strategy. It represent a human collective and must take into account values, behaviors and biases,” (ISACA, 2010, p. 38). [9]

3. Process

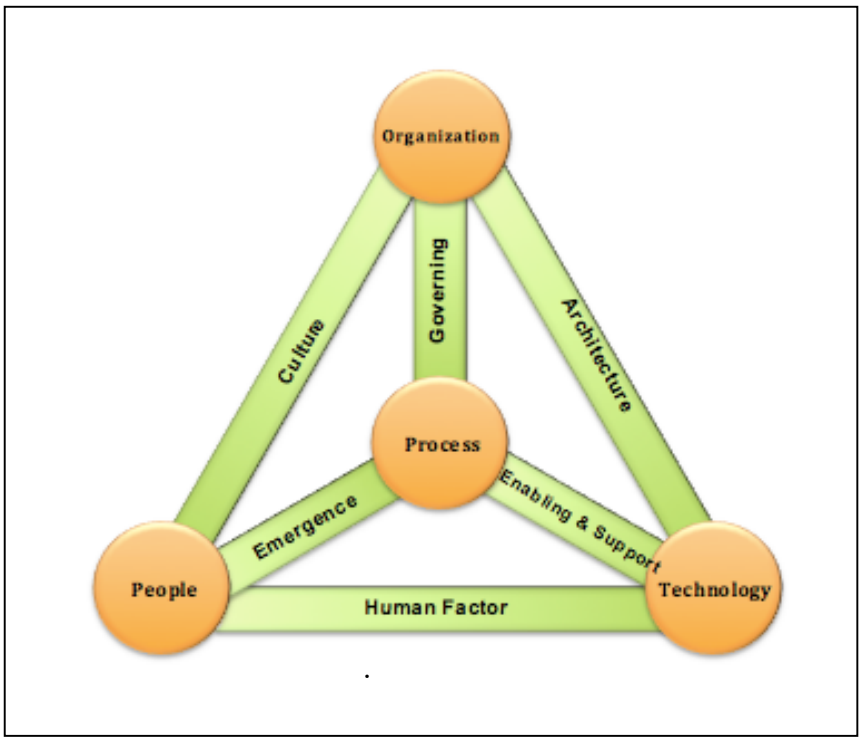
   Proses yang dimaksud adalah semua proses yang ada termasuk mekanisme formal dan informal (besar dan kecil, sederhana dan kompleks) untuk menyelesaikan dan menyediakan link vital untuk semua interkoneksi yang dinamis.

   “Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections,” (ISACA, 2010, p. 38).[9]

4. Technology

   Teknologi terdiri atas semua alat, aplikasi dan infrastruktur yang membuat proses lebih efisien.

"Composed of all of tools, applications and infrastructure that make processes more efficient," (ISACA, 2010, p. 39) [9]



Gambar 2.3 Ruang Lingkup Keamanan Informasi (ISACA, 2010)

Pengamanan informasi tersebut dapat dicapai dengan melakukan suatu kontrol yang terdiri dari kebijakan, proses, prosedur, struktur organisasi, serta fungsi-fungsi infrastruktur TI. Sedangkan *Information Security Management System* (ISMS) adalah suatu cara untuk melindungi dan mengelola informasi berdasarkan pendekatan yang sistematis terhadap risiko bisnis, untuk mempersiapkan, mengimplementasikan, mengoperasikan, mengawasi, meninjau kembali, memelihara, serta meningkatkan pengamanan informasi. ISMS merupakan suatu pendekatan secara organisasi untuk pengamanan informasi.[10]

2.2.3 ISO/IEC 27000

ISO (*International Organization for Standarzitation*) adalah pengembang terbesar di dunia standar internasional secara sukarela memberikan keamanan yang lebih spesifik, layanan yang baik, membantu industri lebih efisien dan efektif.

Dikembangkan melalui kesepakatan global, mereka membantu untuk mengatasi hambatan perdagangan internasional.

ISO 27000 Information Security Management System International Standards Organization (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000. Adapun beberapa standar di seri ISO ini adalah sebagai berikut (IsecT Ltd, 2012):

1. *ISO 27000:2009 - Information Security Management System – overview and vocabulary*
2. *ISO 27001:2005 - Information Security Management System - Requirements*
3. *ISO 27002:2005 - Code of Practice for Information Security Management System.*
4. *ISO 27003:2010 - Information Security Management System Implementation Guidance*
5. *ISO 27004:2009 - Information Security Management System Measurement*
6. *ISO 27005:2008 - Information Security Risk Management System.*
7. *ISO 27006:2011 - Requirements for Bodies Providing Audit and Certification of Information Security Management System.*
8. *ISO 27007:2011 - Guidelines for Information Security Management System Auditing (Focused on the Management System).*
9. *ISO 27008:2011 - Guidance for Auditors on ISMS Controls (Focused on Information Security Controls)*
10. *ISO 27010:2011 - Information Technology – Security Techniques - Information Security Management for Inter-sector and Inter-organizational Communications.*
11. *ISO 27011:2008 - Information Security Management Guidelines for Telecommunication Organizations based on ISO/IEC 27002.*
12. *ISO 27013:2012 - Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001*
13. *ISO 27014 : Information Security Governance Framework*

14. *ISO 27015 : Information Security Management Guidelines for the finance and Insurance Sectors*
15. *ISO 27016 – Information security management – Organizational economics [DRAFT]*
16. *ISO 27017 – Security in cloud computing [DRAFT]*
17. *ISO 27018 – Code of practice for data protection controls for public cloud computing services [DRAFT]*
18. *ISO 27019 – Information security management guidelines based on ISO 27002 for process control systems specific to the energy industry [DRAFT]*
19. *ISO 27031:2011 - Guidelines for Information and Communication Technology Readiness for Business Continuity.*
20. *ISO 27032:2012 - Guidelines for Cyber Security*
21. *ISO 27033:2009 - IT Network Security, A Multi-part Standard Based on ISO/IEC 18028:2006.*
22. *ISO 27034:2011 - Guideline for Application Security (part 1 published, rest in DRAFT)*
23. *ISO 27035:2011 – Information Security Incident Management*
24. *ISO 27036 – Information security for supplier relationship [DRAFT]*
25. *ISO 27037:2012 - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.*
26. *ISO 27038 – Specification for digital redaction [DRAFT]*
27. *ISO 27039 – Selection, deployment and operations of intrusion detection (and preventation) systems (IDPS) [DRAFT]*
28. *ISO 27040 – Storage security [DRAFT]*
29. *ISO 27041 – Guidelines for the analysis and interpretation of digital evidence [DRAFT]*
30. *ISO 27042 – Guidelines for the analysis and interpretation of digital evidence [DRAFT]*
31. *ISO 27043 – Digital evidence investigation principles and process [DRAFT]*

32. *ISO 27799:2008 - Information Security Management in Health using ISO/IEC 27002*[8]

2.2.4 ISO/IEC 27001

ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. Standar ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Management Syestem*, biasa disebut *ISMS* yang diterbitkan pada bulan Oktober 2005 oleh *International Organization for Standarization dan International Electrotechnical Commission* yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan berdasarkan "*best practise*" dalam pengamanan informasi.

Adapun 11 klausul dari ISO/IEC 27001 yaitu :

A.5. *Security policy* (kebijakan keamanan informasi)

Untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh jajaran organisasi.

A.6. *Organization of information security* (Organisasi keamanan informasi)

Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggung jawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah.

A.7. *Asset management* (Manajemen aset)

Manajemen Aset didefinisikan menjadi sebuah proses pengelolaan aset (kekayaan) baik berwujud dan tidak berwujud yang memiliki nilai ekonomis, nilai komersial, dan nilai tukar, mampu mendorong tercapainya tujuan dari individu dan organisasi. Melalui proses manajemen *planning*, *organizing*, *leading* dan *controling*. bertujuan mendapat keuntungan dan mengurangi biaya (*cost*) secara effisien dan effektif.

A.8. *Human resources security* (Keamanan sumber daya manusia)

Organisasi harus menetapkan dan menyediakan sumber daya manusia yang dibutuhkan untuk menerapkan, mengoperasikan, memantau, meningkatkan dan memelihara keamanan informasi.

A.9. *Physical and environmental security* (Keamanan fisik dan Lingkungan)

Untuk mencegah akses tanpa otoritas, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis harus berada di wilayah yang aman, terlindungi secara aman dengan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Prlindungan harus disesuaikan dengan identifikasi resiko.

A.10. *Communications and operations management* (Manajemen Komunikasi dan Operasi)

Untuk menjamin bahwa fasilitas pemprosesan informasi berjalan dengan benar dan aman harus ditetapkan tanggung jawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan operasi yang tepat dan prosedur penanganan insiden. Di mana harus ditetapkan pemisah tugas untuk mengurangi penyalahgunaan sistem karena kecerobohan atau kesenjangan.

A.11. *Access control* (Akses kontrol)

Untuk mencegah akses tanpa ijin terhadap sistem informasi. Akses kontrol adalah bagaimana hanya administrator yang mempunyai akses control saja yang dapat mengakses tempat pemrosesan informasi.

A.12. *Information system acquisition, development, and maintenance* (Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi)

Untuk memastikan bahwa keamanan dibangun dalam system informasi. Persyaratan keamanan system mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna.

A.13. *Information security incident management* (Manajemen insiden keamanan informasi)

Manajeman insiden keamanan informasi adalah bagaimana memanajemen agar satu atau serangkaian kejadian keamanan informasi yang tidak diinginkan atau tidak diharapkan yang mempunyai kemungkinan secara signifikan dapat mengganggu operasi bisnis dan mengancam keamanan informasi.

A.14. *Business continuity management* (Manajemen kelangsungan usaha)

Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha dari kegagalan atau bencana. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan yang mungkin terjadi seperti bencana alam, kecelakaan, kegagalan alat dan keterlambatan sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Rencana darurat harus disiapkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Manajemen kelangsungan bisnis harus mencakup control untuk mengidentifikasi dan mengurangi risiko, membatasi konsekuensi kesalahan

yang merusak, dan memastikan penyimpulan terhadap operasional yang penting.

A.15. *Compliance* (Kesesuaian)

Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, atau kewajiban kontrol serta ketentuan keamanan lainnya.[8]