BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Terdapat beberapa penelitian mengenai audit tata kelola TI menggunakan COBIT 5, diantaranya adalah penelitian yang membahas mengenai tata kelola keamanan sistem informasi menggunakan COBIT 5 dengan judul "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5". Permasalahan dalam penelitian ini yaitu sejak tujuh tahun berlalu ditetapkan Peraturan walikota tentang standar operasional dan prosedur manajemen pengamanan sistem informasi Pemerintah Kota Yogyakarta belum pernah melakukan audit terhadap keamanan sistem informasi. Sehingga penelitian ini dilakukan untuk mengetahui tingkat kapabilitas keamanan sistem informasi pada Pemerintah Kota Yogyakarta. Penelitian melakukan pengumpulan data dari kuesioner berdasarkan COBIT 5. Hasil dari penelitian menunjukkan bahwa tidak ada yang mampu mencapai level yang ditargetkan yaitu level 3 *(Established Process)*. Penelitian dilakukan melalui 5 proses dalam COBIT 5 dan hanya mampu mencapai level 1 *(Incomplete Process)* dengan rincian Proses EDM03 dengan nilai sebesar 1,13. Proses APO12 dengan nilai sebesar 1,24. Proses AP013 dengan nilai 1,22. Proses BAI06 dengan nilai 1,18 dan Proses DSS05 dengan nilai 1,54 [3].

Penelitian lain mengenai tata kelola TI menggunakan COBIT 5 yaitu "Audit TeNOSS Menggunakan COBIT 5 pada Domain *Deliver, Service and Support (DSS)* pada PT Telkom Malang. Permasalahan pada aplikasi TeNOSS ini masih terjadi loading yang lama dan rumitnya dalam melakukan input data pelanggan, sehingga penelitian ini dilakukan untuk dapat merekomendasikan perbaikan atau pengembangan TeNOSS. Penelitian melakukan pengumpulan data dari kuesioner, *interview* dan observasi berdasarkan COBIT 5. Hasil dari penelitian didapat dari

domain DSS (DSS02, DSS05 dan DSS06) diperoleh *capability level* dari kondisi saat ini DSS02 dan DSS06 berada pada level 3 *(Established Process)* target yang ingin dicapai level 4 *(Predictable Process)* dan DSS05 berada pada level 2 *(Managed Process)* target yang ingin dicapai level 3 *(Established Process)* dari perbandingan hasil dan yang ingin dicapai didapatkan nilai *gap* sebesar 1 [4].

Tabel 0.1 Penelitian Terkait Analisis Tata Kelola TI Berdasarkan COBIT 5

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Dewi Ciptaningrum ,dkk, 2015	Sejak tujuh tahun ditetapkan Peraturan walikota tentang standar operasional dan prosedur manajemen pengamanan sistem informasi Pemerintah Kota Yogyakarta belum pernah melakukan audit terhadap keamanan sistem informasi. Sehingga diperlukan audit keamanan sistem informasi yang diharapkan mampu mengetahui tingkat kapabilitas keamanan sistem informasi.	Kerangka kerja COBIT 5 (Proses EDM03, APO12, APO13, BAI06 dan DSS05).	Kelima proses hanya bisa mencapai level 1 dan tidak ada proses yang mampu mencapai level yang ditargetkan yaitu pada level 3.

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
2.	Desepta Isna Ulumi,dkk, 2015	Pada aplikasi TeNOSS masih terjadi loading yang lama dan rumit dalam melakukan input data pelanggan dan dalam penerapanya tidak ada tindak lanjut dari PT. Telkom, sehingga diperlukan Audit TeNOSS untuk rekomendasi perbaikan dan pengembangan sistem.	*Capability Level* COBIT 5 (Proses DSS02, DSS05 dan DSS06).	*Capability Level* yang diperoleh dari DSS02, DSS06 adalah level 3 *(Established Process)* dengan *gap* sebesar 1 untuk mencapai level 4 dan DSS05 adalah level 2 *(Managed Process)* dengan *gap* 1 untuk mencapai level 3.

2.2 Tata Kelola TI *(IT Governance)*

Tata kelola TI merupakan suatu kebijakan, proses/ aktivitas yang mencakup sistem informasi, teknologi dan komunikasi, bisnis dan hukum serta isu-isu lain yang melibatkan hampir seluruh pemangku kepentingan organisasi, baik direktur, manajemen eksekutif, pengguna TI bahkan pengaudit SI/TI yang dapat mendukung pengoperasian TI agar dapat memperluas strategi dan tujuan perusahaan [5].

Tujuan dari tata kelola TI adalah menyelaraskan bisnis dan TI untuk menjamin kinerja TI memenuhi dan sesuai dengan tujuan, sebagai berikut [5]:

1. Menyelaraskan TI dengan strategi dalam organisasi untuk merealisasikan keuntungan-keuntungan yang telah dijanjikan dalam penerapan TI.
2. Penggunaan TI memungkinkan organisasi dapat memaksimalkan manfaat yang ada serta dapat memperbesar peluang-peluang dari hasil menerapkan TI.
3. Pertanggungjawaban dalam penggunaan sumber daya TI untuk mendukung strategi dan tujuan bisnis TI.
4. Manajemen yang sesuai dengan resiko-resiko yang berkaitan dengan TI.

Fokus utama dari area tata kelola TI dibedakan menjadi lima bagian area utama yaitu [5]:

Gambar 2.1 Fokus Area Tata Kelola TI [5]

Penjelasan singkat mengenai tata kelola TI pada gambar 2.1 adalah sebagai berikut :

1. *Strategic Alignment*, berfokus pada kepastian terhadap keterkaitan antara startegi bisnis dan TI serta penyelarasan antara operasional TI dengan bisnis.
2. *Value Delivery*, berfokus pada penyampaian nilai untuk memastikan bahwa TI dapat memenuhi manfaat yang dijanjikan dengan memfokuskan pada pengoptimalan biaya dan pembuktian nilai hakiki keberadaan TI.

3. *Resource Management,* berkaitan dengan pengoptimalan dan pengelolaan secara tepat dari sumber daya TI yang kritis, meliputi : aplikasi, informasi, infrastruktur dan SDM. Hal-hal penting yang berkaitan dengan area ini adalah pengoptimalan pengetahuan dan infrastruktur yang ada.
4. *Risk Managemet,* fokus pada resiko dan bagaimana perhatian perusahaan terhadap keberadaan resiko, pemahaman kebutuhan akan kepatutan, transparasi akan resiko terhadap proses bisnis perusahaan serta tanggung jawab untuk mengatasi resiko-resiko yang masuk ke dalam organisasi.
5. *Performance Measurement,* pengukuran dan pengawasan implementasi dari kinerja teknologi informasi yang berjalan, penggunaan SDM dan kinerja proses sesuai dengan tujuan kebutuhan bisnis organisasi yang akan dicapai.

2.3 Audit Tata Kelola Teknologi Informasi

Audit tata kelola TI dapat diartikan sebagai aktivitas pengumpulan dan pengevaluasian dari bukti-bukti yang ada untuk proses penentuan apakah proses TI yang berlangsung dalam organisasi tersebut telah dikelola sesuai dengan standar dan dilengkapi dengan objektif kontrol untuk mengawasi penggunannya serta apakah telah memenuhi tujuan bisnis organisasi secara efektif dengan menggunakan sumber daya yang efektif [5].

Elemen utama dalam aktivitas audit tata kelola TI dapat diklasifikasikan dalam tinjauan penting berikut [5] :

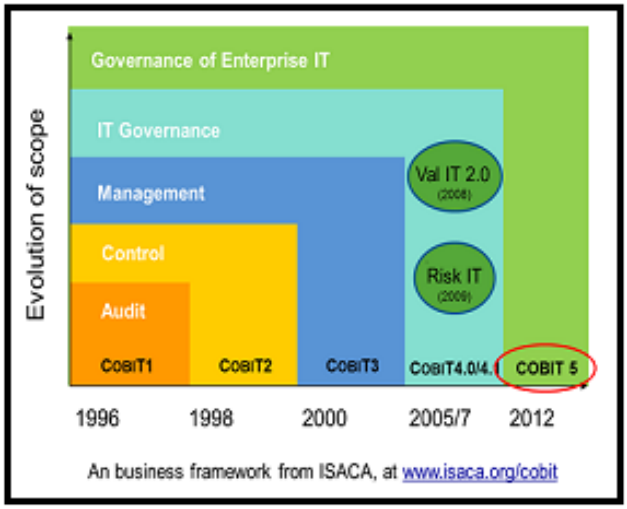
1. Tinjauan terkait dengan fisik dan lingkungan, mencakup hal-hal yang tekait dengan keamanan fisik, sumber daya, temperatur dan faktor lingkungan lainnya.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem informasi, database seluruh prosedur administrasi sistem.
3. Tinjauan perangkat lunak, tinjauan yang mencakup aplikasi bisnis organisasi berupa sistem berbasis web yang menjadi inti dari jalannya proses bisnis suatu organisasi.

4. Tinjauan keamanan jaringan, yang mencakup jaringan internal maupun eksternal yang terhubung dengan sistem dalam organisasi. Tinjauan terhadap tingkat keamanan serta pendeteksian akan gangguan ancaman yang masuk ke dalam sistem.
5. Tinjauan kontinuitas bisnis, memastikan ketersedian *backup* data dan penyimpanan jika sewaktu-waktu terjadi bencana.
6. Tinjauan integritas bisnis, memastikan ketelitian data yang sedang beroperasi.

2.4 COBIT *(Control Objectives for Information and related Technology)*

COBIT merupakan salah satu kerangka kerja TI yang dapat digunakan untuk membantu penyelasaran strategi bisnis dan tujuan tata kelola TI. Pengertian COBIT adalah suatu standar dalam kerangka kerja domain yang terdiri dari sekumpulan proses TI dan sekumpulan dokumentasi *best practices* untuk aktivitas dalam tata kelola TI yang dapat digunakan untuk membantu pendefisian strategi dan kontrol pada manajemen tingkat atas dalam menganalisa kesenjangan *gap* antara resiko bisnis, kebutuhan pengendalian dan permasalahan-permasalan yang yang ada dan dapat dipakai sebagai acuan langsung terkait pengelolaan TI. COBIT dibuat oleh *IT Governance Institute (ITGI)* dan merupakan bagian dari *Information Systems Audit and Control Association (ISACA).* COBIT terdiri dari tujuan pengendalian, pedoman audit dan pedoman manajemen serta pelaksanaannya yang sangat berguna untuk para auditor, pemakai TI dan para manajer.

COBIT pertama kali keluar pada tahun 1996 dengan COBIT versi 1 yang lebih menekankan pada audit, kemudian pada tahun 1998 keluar COBIT versi kedua yang menekankan pada pengendalian. Pada tahun 2000 keluar COBIT versi 3 yang berorientasi pada manajemen. Dan kemudian COBIT versi 4 keluar pada bulan desember 2005 dan COBIT versi 4.1 keluar pada bulan mei 2007 yang berorientasi pada tata kelola TI. Dan yang terakhir sampai saat ini COBIT versi 5 keluar pada bulan juni 2012 yang lebih menekankan tata kelola TI pada perusahaan [6].

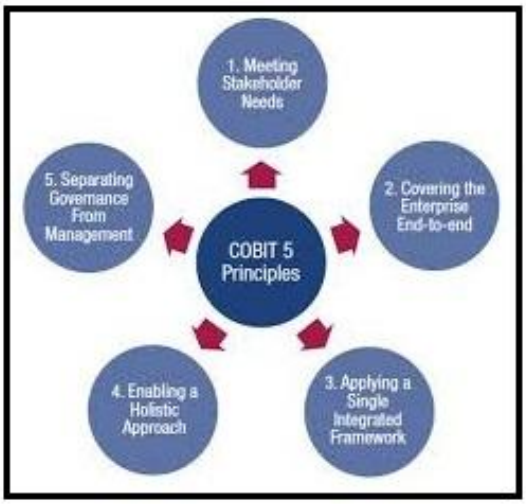


Gambar 2.2 Sejarah Perkembangan COBIT [6]

2.5 COBIT 5

COBIT 5 menyediakan kerangka kerja yang dapat membantu perusahaan atau organisasi untuk menciptakan nilai yang optimal dari tata kelola TI dengan mempertahankan, menyeimbangkan antara mewujudkan manfaat dan mengoptimalkan tingkat resiko dan sumber daya TI. COBIT 5 memungkinkan tata kelola TI untuk dapat mengatur dan mengelola seluruh bisnis perusahaan atau organisasi yang berkaitan dengan bidang fungsional TI [7].

COBIT 5 didasarkan pada lima prinsip utama untuk tata kelola dan manajemen TI perusahaan. Kelima prinsip ini diharapkan dapat membangun tata kelola perusahaan atau organisasi yang dapat mengoptimalkan tingkat resiko dan memberikan keuntungan bagi perusahaan atau organisasi [7].



Gambar 2.3 Lima Prinsip Utama COBIT 5 [7]

1. Prinsip 1 : Memenuhi Kebutuhan *Stakeholder*. Perusahaan menciptakan nilai bagi para *Stakeholder* dengan merealisasikan manfaat dan mengoptimalkan resiko. COBIT 5 menyediakan semua proses yang diperlukan perusahaan untuk memenuhi dalam pencapaian nilai bisnis melalui penggunaan TI. Karena setiap perusahaan memiliki tujuan yang berbeda sehingga peusahaan dapat menyesuaikan sendiri tujuan bisnisnya melalui COBIT 5.
2. Prinsip 2 : Melingkupi Seluruh Perusahaan. COBIT 5 dapat mencakup semua fungsi di dalam perusahaan, tidak hanya fokus pada fungsi TI, tetapi semua aset yang ada di dalam perusahaan. COBIT 5 mengintegrasikan semua tata kelola TI dan manajemen TI agar dapat digunakan dalam seluruh perusahaan dari segala aspek dan semua sumber daya baik internal maupun eksternal yang berhubungan dengan tata kelola TI dan manajemen TI.
3. Prinsip 3 : Menerapkan Satu Kerangka Tunggal yang Terintegrasi. Banyak standar yang berkaitan dengan TI. COBIT 5 selaras dengan standar kerja yang relevan lainnya dan kerangka kerja tingkat tinggi, dengan demikian COBIT 5 dapat berfungsi sebagai kerangka kerja untuk tata kelola TI dan manajemen TI pada perusahaan.
4. Prinsip 4 : Menggunakan Sebuah Pendekatan yang Menyeluruh. Tata kelola TI dan manajemen TI perusahaan yang efektif dan efisien memerlukan pendekatan dengan mempertimbangkan beberapa komponen yang saling

berinteraksi. COBIT 5 dapat mendefinisikan pendekatan-pendekatan tersebut untuk membantu perusahan atau organisasi dalam mencapai tujuan perusahaan atau organisasi. COBIT 5 mendefinisikan tujuh kategori pendekatan :

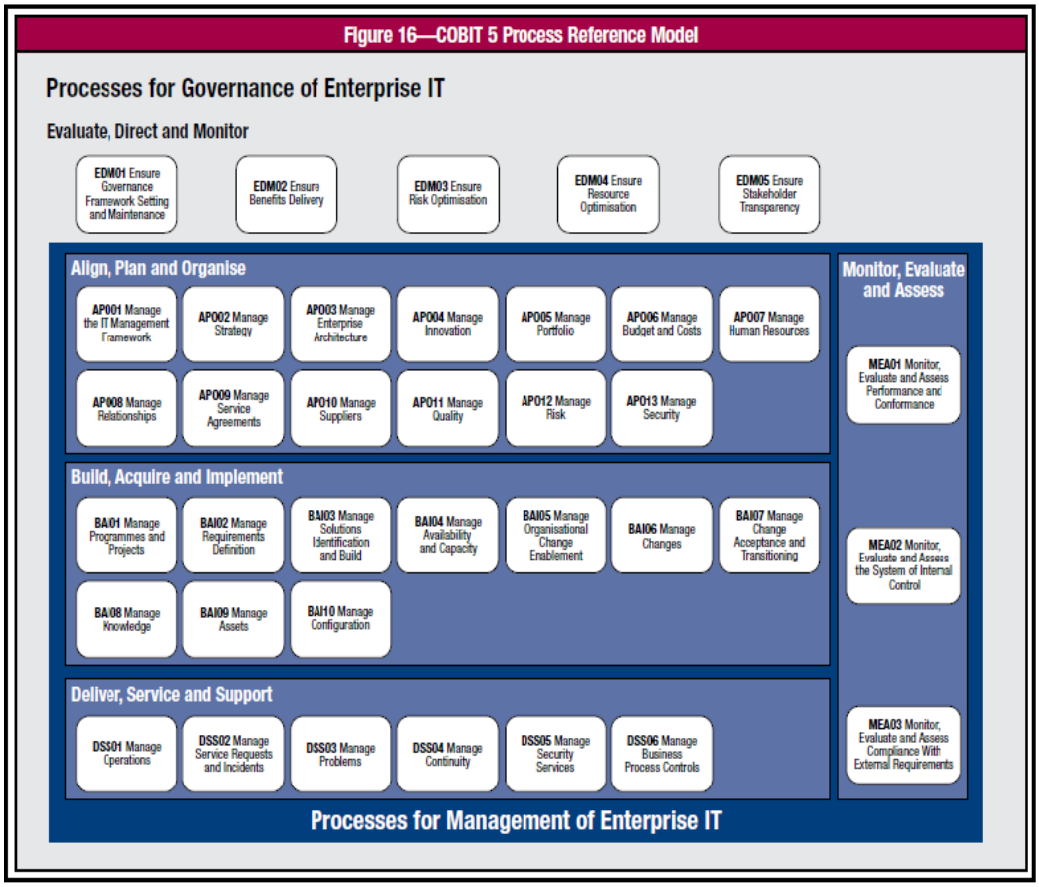
a. Prinsip, kebijakan dan kerangka kerja
b. Proses
c. Struktur organisasi
d. Budaya, etika dan perilaku
e. Informasi
f. Layanan, infrastruktur dan aplikasi
g. Sumber daya, keterampilan dan kompetensi

5. Prinsip 5 : Pemisahan Tata Kelola Dari Manajemen. Kerangka kerja COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen. Dua disiplin mencakup berbagai jenis kegiatan, struktur organisasi dan tujuan. Pebedaan utama antara tata kelola dan manajemen :
   a. Tata Kelola. Tata kelola memastikan kepentingan kebutuhan, kondisi, pilihan yang akan dievaluasi, menetapkan arah perusahaan, pengambilan keputusan, pemantauan kinerja sumber daya dan kepatuhan yang disepakati untuk dapat mencapai tujuan perusahaan yang ingin dicapai. Pada kebanyakan perusahaan, tata kelola keseluruhan merupakan tanggung jawab dewan direksi di bawah kepemimpinan ketua.
   b. Manajemen. Manajemen mempunyai rencana, membangun, menjalankan dan monitoring semua kegiatan supaya dapat sejalan dengan arah yang telah ditetapkan dalam perusahaan serta dapat mencapai tujuan yang telah ditetapkan perusahaan. Pada kebanyakan perusahaan, manajemen adalah tanggung jawab manajemen eksekutif di bawah kepemimpinan CEO.

2.5.1 Model Referensi Proses COBIT 5

Model referensi COBIT 5 merupakan suatu model yang mendefinisikan dan menjelaskan secara rinci mengenai tata kelola dan manajemen. Model tersebut

mewakili semua proses yang ada di organisasi yang berkaitan dengan kegiatan TI, menyediakan model referensi yang mudah dipahami oleh operasional TI dan manajer bisnis. Model referensi COBIT 5 merupakan evolusi dari model referensi COBIT 4.1 yang diitegrasikan dengan model proses RiskIT dan ValIT [7].



Gambar 2.4 Model Referensi COBIT 5 [7]

Gambar di atas menunjukkan 37 proses tata kelola dan manajemen pada proses COBIT 5. Model referensi COBIT 5 dibagi menjadi 2 proses utama yaitu tata kelola dan manajemen [7].

1. Tata kelola *(Governance)*

   Memuat lima proses tata kelola, di dalam domain evaluasi, pengarahan dan pengawasan. EDM *(Evaluate, Direct and Monitoring),* tujuan domain EDM adalah untuk menetapkan arah melalui prioritas dan pengambilan keputusan,

melakukan pemantauan kinerja dan memberikan arahan kepada TI. Kelima proses tersebut terdiri dari :

a. EDM01 Memastikan adanya pengaturan dan pemeliharaan kerangka kerja tata kelola *(Ensure governance framework setting and maintenance).*
b. EDM02 Memastikan mendapat manfaat *(Ensure benefits delivery).*
c. EDM03 Memastikan optimalisasi resiko *(Ensure risk optimisation).*
d. EDM04 Memastikan optimalisasi sumber daya *(Ensure resource otimisation).*
e. EDM05 Memastikan transparasi terhadap *stakeholder (ensure stakeholder transparency).*

2. Manajemen

Memuat empat proses yang sejajar dengan area tanggung jawab dari merencanakan, membangun, menjalankan dan memantau *(Plan, Run, and Monitoring)*. Serta menyediakan cakupan yang menyeluruh dari ruang lingkup TI, yaitu :

a. Domain menyelaraskan, merencanakan dan mengatur. APO *(Align, Plan and Organise),* tujuan domain APO adalah untuk memberikan taktik dan mengidentifikasi cara terbaik yang dapat digunakan oleh perusahaan untuk membantu mencapai tujuan dan sasaran perusahaan. Domain APO juga memperhatikan bentuk organisasi dan infrastrukutur guna untuk mencapai hasil yang optimal dan memberikan manfaat dari penggunaan TI. Domain APO terdiri dari 13 proses yaitu :
    1) APO01 Mengelola manajemen kerangka TI *(Manage the IT management framework).*
    2) APO02 Mengelola strategi *(Manage strategy).*
    3) APO03 Mengelola arsitektur informasi *(Manage enterprise architecture).*
    4) APO04 Mengelola inovasi *(Manage innovation).*
    5) APO05 Mengelola portopolio *(Manage portofolio).*
    6) APO06 Mengelola anggaran dan biaya *(Manage budget and costs).*

7) APO07 Mengelola sumber daya manusia *(Manage human resources).*
8) APO08 Mengelola hubungan (*Manage relationships).*
9) APO09 Mengelola perjanjian layanan *(Manage service agreements).*
10) APO10 Mengelola pemasok *(Manage suppliers).*
11) APO11 Mengelola kualitas *(Manage quality).*
12) APO12 Mengelola risk *(Manage risk).*
13) APO13 Mengelola keamanan *(Manage security).*

b. Domain membangun, memperoleh dan melaksanakan. BAI *(Build, Acquire and Implement),* tujuan domain BAI adalah untuk mengidentifikasi solusi TI yang perlu dikembangkan dan diterapkan ke dalam proses bisnis perusahaan. Domain BAI terdiri dari 10 proses yaitu :
   1) BAI01 Mengelola program dan proyek *(Manage programmes and projects).*
   2) BAI02 Mengelola definisi kebutuhan *(Manage requirements definition).*
   3) BAI03 Mengelola solusi otomatis *(Manage solutions identification and build).*
   4) BAI04 Mengelola ketersediaan dan kapasitas *(Manage availability and capacity).*
   5) BAI05 Mengelola perubahan pemberdayaan organisasi *(Manage organisational change enablement).*
   6) BAI06 Mengelola perubahan *(Manage changes).*
   7) BAI07 Mengelola penerimaan perubahan dan transisi *(Manage Change acceptance and transitioning).*
   8) BAI08 Mengelola pengetahuan *(Manage knowledge).*
   9) BAI09 Mengelola aset *(Manage assets).*
   10) BAI10 Mengelola konfigurasi *(Manage configuration).*

c. Domain menghasilkan, melayani dan mendukung. DSS *(Deliver, Service and Support),* tujuan domain DSS adalah untuk memberikan pelayanan seperti memberikan pelayanan aplikasi di dalam proses TI, pengelolaan

keamanan dan dukungan pelaksanaan proses TI yang lebih efektif dan efisien. Domain DSS terdiri dari 6 proses yaitu :

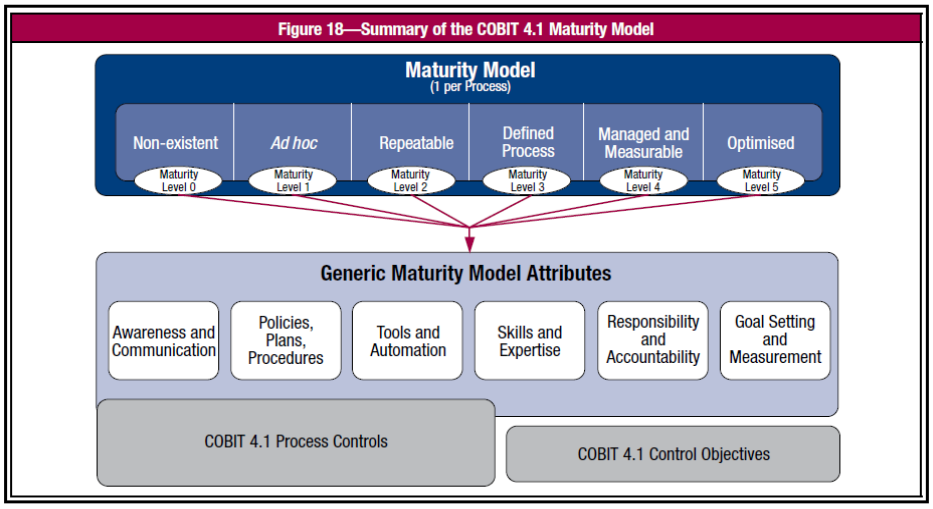
1) DSS01 Mengelola operasi *(Manage operations).*
2) DSS02 Mengelola layanan permintaan dan insiden *(Manage service requests ans incidents).*
3) DSS03 Mengelola permasalahan *(Manage problems).*
4) DSS04 Mengelola layanan yang berkelanjutan *(Manage continuity).*
5) DSS05 Mengelola layanan keamanan *(Manage security services).*
6) DSS06 Mengelola proses bisnis kontrol *(Manage business process controls).*

d. Domain mengawasi, mengevaluasi dan menilai. MEA *(Monitor, Evaluate and Assess),* tujuan domain MEA adalah untuk menilai kebutuhan perusahaan terhadap proses TI saat ini terhadap kepatuhan dari peraturan tata kelola. Serta penilaian terhadap proses TI pada kemampuannya untuk memenuhi tujuan bisnis dan proses kontrol perusahaan. Domain MEA terdiri dari 3 proses yaitu :

1) MEA01 Monitor, evaluasi dan menilai kinerja dan kesesuaian *(Monitor, evaluate and assess performance and performance).*
2) MEA02 Memantau, mengevaluasi dan menilai sistem pengendalian internal *(Monitor, evaluate and assess the system of internal control).*
3) MEA03 Memantau, mengevaluasi dan menilai kepatuhan dan kebutuhan eksternal *(Monitor, evaluate and assess compliance with external requirements).*

2.5.2 Model Kapabilitas Proses Pada COBIT 5

Penggunaan COBIT 4.1, dikenal dengan model proses kematangan termasuk dalam kematangan kerangka kerja. Model yang digunakan untuk mengukur kematangan terkait dengan proses tata kelola TI dan untuk mengukur tingkat kesenjangan *gap* serta menentukan bagaimana meningkatkan proses untuk mencapai tingkatan yang diinginkan [7].



Gambar 2.5 Model Kematangan Proses COBIT 4.1 [7]

Untuk model kapabilitas proses COBIT 5 yang telah diakui secara internasional oleh ISO/IEC 15504 mengenai *software egineering* dan *process assessment.* Pada model kapabilitas proses dilakukan penilaian dan proses dukungan perbaikan dengan menyediakan sarana kinerja dari tiap-tiap proses tata kelola dan proses manajemen, dimana akan dilakukan evaluasi atau perbaikan untuk meningkatkan performasinya [7].

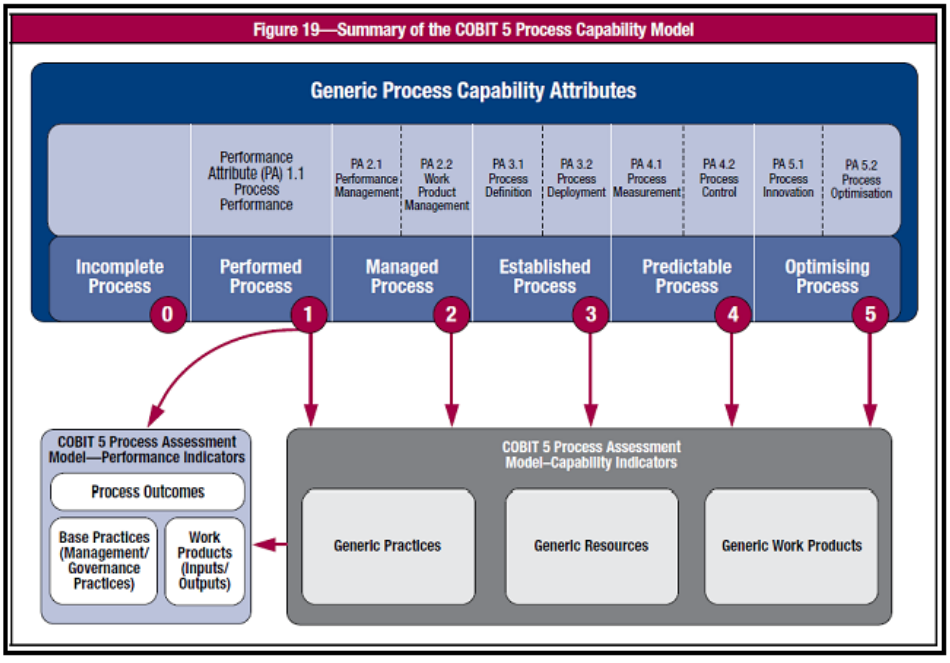
Indikator kapabilitas proses adalah kemampuan proses dalam meraih tingkat kapabilitas yang dibentuk oleh atribut proses. Bukti atas indikator kapabilitas proses akan mendukung penilaian atas pencapaian atribut proses [7].

Kapabilitas proses yang ada kemudian dituangkan pada suatau penilaian kapabilitas proses yang disebut *Process Assessment Model.* Model ini digunakan sebagai dokumen basis referensi untuk menilai peforma kapabilitas TI organisasi serta [8]:

1. Mendefinisikan kebutuhan-kebutuhan minimun untuk melakukan penilaian (*output-output* yang dibutuhkan).
2. Mendefinisikan proses kapabilitas dalam dua dimensi yaitu proses dan kapabilitas.
3. Menggunakan indikator proses kapabilitas dan proses performa untuk menentukan apakah atribut proses telah terpenuhi.

4. Mengukur performa proses berdasarkan sebuah urutan praktik dasar dan aktivitas-aktivitas untuk memenuhi *work product*.
5. Mengukur proses kapabilitas melalui pencapaian atribut berdasarkan bukti spesifik (level 1) dan *generic* (level yang lebih tinggi) *practies* dan *work product.*

Dimensi kapabilitas dalam model penilaian proses mencakup enam tingkat kapabilitas. Di dalam enam tingkat tersebut terdapat sembilan atribut proses. Level 0 mengenai keberadaan proses. Ada perbedaan penilaian antara penilaian untuk level 1 dan level yang lebih tinggi. Hal ini dilakukan karena level 1 menentukan apakah suatu proses mencapai tujuannya, dan oleh karena itu sangat penting untuk dicapai dan juga menjadi pondasi dalam meraih level yang lebih tinggi. Pada level yang tertinggi 5 ini sudah menjadi prestasi yang sangat penting bagi suatu organisasi atau peusahaan. Masing-masing dalam organisasi atau perusahaan harus menentukan berdasarkan biaya manfaat dan kelayakan untuk dapat mencapai tingkatan kapabilitas yang diinginkan.



Gambar 2.6 Model Kapabilitas Proses COBIT 5 [7]

Ada enam tingkatan kapabilitas yang dapat dicapai oleh masing-masing proses, yaitu [8]:

1. Level 0 *(Incomplete Process)*

   Merupakan proses yang gagal mencapai tujuan. Pada tingkat ini, ada sedikit atau tidak ada bukti dari setiap pencapaian sistematis tujuan proses. Proses ini tidak memiliki atribut.

2. Level 1 *(Performed Process)*

   Merupakan proses yang dijalankan. Proses yang telah diimplementasikan dan berhasil mencapai tujuannya. Tingkat ini hanya memiliki "*Process Performance"* sebagai proses atribut yaitu pengukuran mengenai seberapa jauh tujuan dari suatu proses yang berhasil diraih. Pencapaian penuh atas atribut ini mengakibatkan proses tersebut meraih tujuan yang sudah ditentukan.

3. Level 2 *(Managed Process)*

   Merupakan proses yang teratur. Proses yang telah dijalankan mencapai tujuannya dan diimplementasikan dengan cara yang lebih teratur dengan cara di kelola mencakup perencanaan, pengawasan dan penyesuaian. *Work products* nya dijalankan, dikendalikan dan dipertahankan dengan tepat. Ketentuan atribut proses pada level 2 adalah sebagai berikut :

   a. PA 2.1 *Performance Management*

      Mengukur sampai dimana performa proses dikelola.

   b. PA 2.2 *Work Product Management*

      Mengukur sejauh mana hasil kerja yang dihasilkan oleh proses dikelola. Hasil kerja yang dimaksud dalam hal ini adalah hasil dari proses.

4. Level 3 *(Established Process)*

   Merupakan proses yang tetap. Dimana proses yang telah diimplementasikan dengan cara yang teratur kemudian telah berhasil ditetapkan dan mampu untuk mencapai *outcome* yang telah diharapkan. Ketentuan atribut proses pada level 3 adalah sebagai berikut :

a. PA 3.1 *Process Definition*

Mengukur sejauh mana proses standar dikelola untuk mendukung pengerjaan dari proses yang telah didefinisikan.

b. PA 3.2 *Process Deployment*

Mengukur sejauh mana proses standar secara efektif telah dijalankan seperti yang telah didefinisikan untuk mencapai hasil dari proses.

5. Level 4 *(Predictable Process)*

Merupakan proses yang dapat diprediksi. Proses yang telah berjalan kemudian dioperasikan dengan batasan yang ditentukan untuk mencapai *outcome* yang diharapkan. Ketentuan atribut proses pada level 4 adalah sebagai berikut :

a. PA 4.1 *Process Measurement*

Mengenal seberapa jauh hasil pengukuran digunakan untuk memastikan bahwa performa proses mendukung pencapaian tujuan proses untuk mendukung tujuan organisasi. Pengukuran bisa pengukuran proses ataupun pengukuran produk atau pengukuran kedua-duanya.

b. PA 4.2 *Process Control*

Pengukuran tentang seberapa jauh suatu proses secara kuantitatif bisa menghasilkan proses yang stabil, mampu dan bisa diprediksi dalam batasan yang telah ditentukan.

6. Level 5 *(Optimizing Process)*

Merupakan proses optimasi. Proses yang dijalankan diatas ditingkatkan secara berkelanjutan untuk memenuhi tujuan bisnis organisasi baik di saat ini dan di masa depan. Ketentuan proses pada level 5 adalah sebagai berikut :

a. PA 5.1 *Process Innovation*

Mengukur sebuah perubahan proses yang telah diidentifikasi dari analisis penyebab umum dari adanya variasi di dalam performa dan dari investigasi pendekatan inovatif untuk mendefinisikan dan melaksanakan proses.

b. PA 5.2 *Process Optimization*

Mengukur perubahan untuk definisi, manajemen dan performa proses agar memiliki hasil yang berdampak secara efektif untuk mencapai tujuan dari proses peningkatan.

2.5.3 Skala Penilaian

Skala penilaian digunakan setelah memperoleh hasil dari analisa tingkat kapabilitas. Setiap atribut dinilai menggunakan standar skala penilaian yang dijelaskan dalam standar ISO/IEC 15504. Skala penilaian terdiri atas [8]:

1. N *(Not achieved* atau Tidak tercapai)
   Dalam kategori ini tidak ada atau hanya terdapat sedikit bukti atas pencapaian atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar 0% sampai 15%.
2. P *(Partically achieved* atau Tercapai sebagian)
   Dalam kategori ini terdapat beberapa bukti mengenai pendekatan dan beberapa pencapaian atribut atas proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar antara >15% sampai 50%.
3. L *(Largely achieved* atau Secara garis besar tercapai)
   Dalam kategori ini terdapat bukti atas pendekatan sistematis dan pencapaian signifikan atas proses tersebut, meski mungkin masih ada kelemahan yang tidak signifikan. *Range* nilai yang diraih pada kategori ini berkisar antara >50% sampai 85%.
4. F *(Fully achieved* atau Tercapai penuh)
   Dalam kategori ini terdapat cukup bukti atas pendekatan sistematis dan lengkap, dan pencapaian penuh atas atribut proses tersebut serta tidak ada kelemahan terkait atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar antara >85% sampai 100%.

Suatu proses cukup meraih kategori *Largely achieved* (L) atau *Fully achieved* (F) untuk dapat dinyatakan bahwa proses tersebut telah meraih suatu level kapabilitas tersebut, namun proses tersebut harus meraih kategori *Fully achieved* (F) untuk

dapat melanjutkan penilaian ke level kapabilitas selanjutnya. Jadi misalnya suatu proses untuk meraih level kapabilitas 3, maka level 1 dan level 2 proses tersebut harus mencapai kategori *Fully achieved* (F), sementara level kapabilitas 3 cukup mencapai kategori *Largely achieved* (L) atau *Fully achieved* (F) [8].

2.6 Analisis Kesenjangan *(Gap Analysis)*

Analisis kesenjangan *(gap analysis)* dilakukan untuk mencari perbedaan antara tingkat kapabilitas yang diperoleh dengan tingkat yang diharapkan. Analisis dilakukan dengan melakukan identifikasi perbaikan untuk peningkatan tingkat kapabilitas berdasarkan proses atribut kerangka kerja COBIT 5. Hasil dari analisis ini adalah saran perbaikan untuk tata kelola TI [7].

2.7 COBIT 5 Proses *Deliver, Service and Support* (DSS05)

Domain DSS proses *Deliver, Servise and Support* (DSS05) merupakan proses yang berfokus pada upaya perlindungan aset informasi pada organisasi untuk mempertahankan tingkat resiko keamanan informasi yang dapat diterima organisasi sesuai kebijakan keamanan. Melakukan pemantauan keamanan dan pengujian berkala serta menerapkan tindakan korektif untuk mengidentifikasi kelemahan keamanan dan insiden keamanan [9].

Tujuan dari proses *Deliver, Servise and Support* (DSS05) adalah mengklasifikasi masalah proses bisnis dan mencari akar penyebab permasalahan untuk mencegah kerentanan informasi dan insiden. Meningkatkan tingkat layanan kenyamanan pelanggan dan kepuasan pelanggan dengan mengurangi jumlah masalah operasional yang ada [9].

Pada DSS05 mengandung 5 praktek manajemen, diantaranya [9] :

1. DSS05.01 *(Protect against malware)*

   Merupakan praktek untuk memberikan perlindungan terhadap *malware.* Praktek tata kelola yang dilakukan adalah menerapkan dan memelihara pencegahan, dan langkah-langkah perbaikan di tempat seluruh organisasi untuk melindungi informasi dan teknologi dari *malware* seperti virus, worm spyware dan spam.

2. DSS05.02 *(Manage network and connectivity security)*
   Merupakan praktek pengelolaan jaringan dan keamanan konektivitas. Praktek tata kelola yang dilakukan adalah menggunakan keamanan dan prosedur yang terkait untuk melindungi informasi atas keamanan konektivitas.
3. DSS05.03 *(Manage enpoint security)*
   Merupakan praktek mengelola keamanan *endpoint.* Praktek tata kelola yang dilakukan adalah memastikan perangkat *endpoint.* Seperti laptop, dekstop, server terjamin pada tingkatan yang sama dengan atau lebih besar dari prosedur keamanan yang telah didefinisikan.
4. DSS05.04 *(Manage user identity and logical access)*
   Merupakan praktek pengelolaan identitas pengguna dan hak akses. Praktek tata kelola yang dilakukan adalah memastikan bahwa semua pengguna memiliki akses informasi hak sesuai dengan kebutuhan mereka.
5. DSS05.05 *(Manage physical security)*
   Merupakan praktek mendefinisikan dan menerapkan prosedur, membatasi dan mencabut akses sesuai dengan kebutuhan bisnis serta keadaan darurat. Mengelola keamanan akses ke tempat yang berwenang atas akses tersebut. Memantau orang yang memasuki tempat akses termasuk staf, staf sementara, klien, vendor dan pengunjung atau pihak ketiga.
6. DSS05.06 *(Manage sensitive documents and outputs devices)*
   Merupakan prektek mengelola keamanan dokumen. Praktek tata kelola yang dilakukan adalah membangun pengamanan fisik yang sesuai, inventarisasi dokumen penting dan persediaan manajemen atas aset TI seperti surat berharga, token keamanan.
7. DSS05.07 *(Manage Information Security Incidents)*
   Merupakan praktek pendefinisian dan mengkomunikasikan karakteristik insiden keamanan potensial dan memberikan bimbingan kepada manajemen proses tentang bagaimana untuk menangani insiden keamanan.
8. DSS05.08 *(Manage Information Handling)*
   Mengelola keamanan aset informasi seluruh siklus hidup organisasi.

2.8 RACI *Chart*

RACI *Chart* memiliki fungsi pada tingkat proses tanggung jawab untuk peran pada struktur organisasi suatu perusahaan. RACI *Chart* mendefinisikan kewenangan seseorang di dalam suatu perusahaan yang berbasis TI. RACI *Chart* terdapat berbagai tingkatan dengan karakter sebagai berikut:

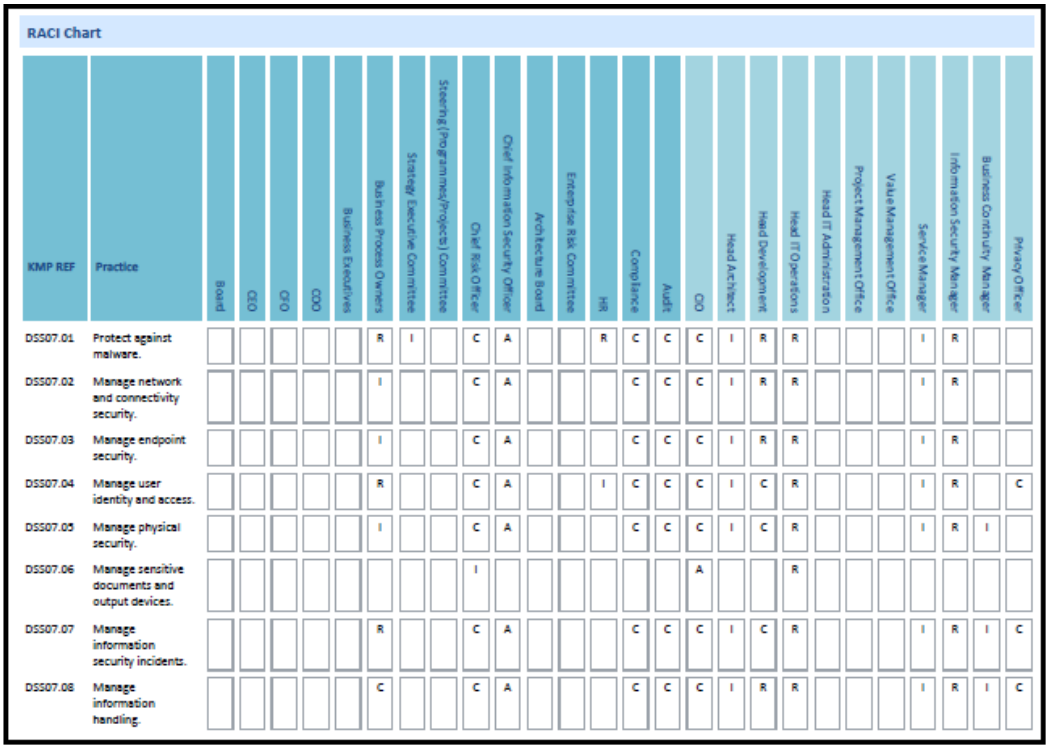
1. *Responsible* (pelaksana)

   Merupakan pihak yang melakukan suatu pekerjaan. Hal ini berkaitan pada peran utama di dalam organisasi untuk memenuhi kegiatan yang telah direncanakan dan menciptakan hasil yang diharapkan.
2. *Accountable* (Bertanggung jawab)

   Merupakan pihak yang bertanggung jawab atas semua pekerjaan. Dengan memperhatikan hal tersebut pada tingkat terendah akuntabilitas yang sesuai memiliki tingkat yang paling tinggi pertanggung jawabannya.
3. *Consulted* (Penasehat)

   Merupakan pihak yang dimintai pendapat tentang suatu pekerjaan. Peran ini tergantung pada peran *responsible* dan *accountable* untuk mendapat informasi-informasi dari unit-unit lain.
4. *Informed* (Informasi)

   Merupakan pihak yang mendapatkan informasi tentang kemajuan suatu pekerjaan. Peran yang diberi informasi mengenai peran atau penyerahan tugas.



RACI Chart

KMP REF	Practice	Board	CEO	CFO	COO	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (programmes/Projects) Committee	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	HR	Compliance	Audit	CIO	Head Architect	Head Developement	Head IT Operations	Head IT Administration	Project Management Office	Value Management Office	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS07.01	Protect against malware.						R	I		C	A			R	C	C	C	I	R	R				I	R		
DSS07.02	Manage network and connectivity security.						I			C	A				C	C	C	I	R	R				I	R		
DSS07.03	Manage endpoint security.						I			C	A				C	C	C	I	R	R				I	R		
DSS07.04	Manage user identity and access.						R			C	A			I	C	C	C	I	C	R				I	R		C
DSS07.05	Manage physical security.						I			C	A				C	C	C	I	C	R				I	R	I	
DSS07.06	Manage sensitive documents and output devices.									I							A			R						
DSS07.07	Manage information security incidents.						R			C	A				C	C	C	I	C	R				I	R	I	C
DSS07.08	Manage information handling.						C			C	A				C	C	C	I	R	R				I	R	I	C

Gambar 2.7 Diagram RACI [9]

2.9 Keamanan Sistem Informasi

Keamanan sistem informasi dapat diartikan sebagai suatu perlindungan dari kejahatan teknologi terhadap sistem yang sudah berbasis informasi dari berbagai ancaman-ancaman seperti penipuan, pencurian data penting, virus, terjadinya perubahan program atau melakukan akses sistem yang tidak sah. Penanganan keamanan sistem informasi dapat ditingkatkan melalui prosedur-prosedur dan peralatan-peralatan pengamanan sistem perangkat keras komputer, jaringan komputer dan data [10].

2.10 Pentingnya Keamanan Sistem Informasi

Keamanan sistem informasi merupakan komponen yang sangat penting bagi organisasi atau perusahaan yang telah menggunakan teknologi berbasis TI. Keamanan sistem informasi menggambarkan adanya perlindungan terhadap komputer, fasilitas, data dan informasi dari pihak-pihak yang tidak bertanggung jawab. Namun pada praktek yang terjadi di dalam organisasi atau perusahaan

masalah keamanan sistem informasi ini kurang mendapat kepedulian dari pihak pengelola sistem informasi [10].

Kemampuan dalam sistem informasi sangatlah banyak memberikan fungsi bagi organisasi atau perusahaan, antara lain mudahnya mengakses atau memberikan informasi yang cepat akurat dan efisien, namun sering kali informasi tersebut jatuh ke pihak yang tidak bertanggung jawab dan ini dapat menimbulkan kerugian bagi organisasi atau perusahaan yang memiliki informasi tersebut. Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama [10], yaitu :

1. Kerahasiaan

   Aspek ini lebih ke dalam memberikan perlindungan informasi dan data organisasi atau perusahaan dari orang-orang yang tidak bertanggung jawab. Inti utama dari aspek kerahasiaan adalah untuk menjaga informasi agar informasi tersebut lebih bersifat *privacy* dan agar terhindar dari orang-orang yang tidak berhak mengakses informasi tersebut.
2. Ketersediaan

   Aspek ini yang menyatakan bahwa informasi tersebut benar-benar asli adanya, atau jika ada orang akan mengakses informasi bahwa informasi tersebut adalah informasi yang benar-benar dimaksud. Biasanya masalah utama dalam ketersediaan adalah pembuktian keaslian dokumen, ini dapat di buktikan menggunakan teknologi *watermarking* dan *digital signature.* Masalah kedua yaitu akses kontrol, berkaitan dengan siapa saja yang berhak mengakses informasi atau dokumen. Dalam hal ini biasanya pengguna menunjukkan bahwa dia sah atau berhak menggunakannya.
3. Integritas

   Aspek ini lebih menekankan bahwa informasi tidak boleh diubah tanpa ijin dari pemilik informasi. Adanya ancaman virus, trojan horse atau pengguna lainnya yang mengubah informasi tersebut tanpa seijin pemilik informasi.

2.11 Manajemen Keamanan Sistem Informasi

Manajemen keamanan sistem informasi merupakan suatu perlindungan untuk perangkat komputer supaya sumber daya informasi tetap aman dari orang yang tidak berkepentingan atau tidak berwenang. Serta memberikan perlindungan kepada perusahaan agar sistem informasi tetap berfungsi setelah terjadinya bencana atau kerusakan sistem informasi [10].

Terdapat empat tahapan dalam proses manajemen keamanan sistem informasi :

1. Mengidentifikasi berbagai ancaman yang dapat mengganggu sumber daya informasi perusahaan.
2. Mengidentifikasi resiko yang dapat ditimbulkan dari ancaman tersebut.
3. Menyusun kebijakan keamanan sistem informasi.
4. Mengimplementasikan kontrol untuk mengatasi tiap-tiap resiko tersebut.

2.12 Tipe Ancaman Informasi

Ancaman informasi merupakan sutau kejadian yang dapat merugikan organisasi atau pihak-pihak terkait yang sedang membutuhkan informasi tersebut. Terdapat beberapa ancaman informasi yang dapat mengganggu kinerja pada suatu organisasi yaitu [11]:

1. *Interruption*

   Merupakan ancaman terhadap informasi dan data yang ada di dalam sistem komputer dirusak atau dihapus sehingga tidak dapat mengaksesnya kembali. Contoh : *server down*, penghancuran bagian perangkat keras komputer.
2. *Interception*

   Merupakan ancaman terhadap kerahasiaan. Informasi yang ada di akses oleh orang lain yang tidak memiliki hak akses atas informasi tersebut. Contoh : mencuri data rahasia, meng*copy* file tanpa diotorisasi.
3. *Modification*

   Sumber daya yang tidak berhak mengakses berhasil mengakses informasi kemudian merubah nilai dari sumber daya tersebut. Contoh : mengubah

program sehingga program dijalankan akan berbeda hasilnya, mengubah nilai-nilai file data.

4. *Fabrication*

   Sumber daya mampu menyisipkan dan memasukkan objek-objek palsu ke dalam sistem. Contoh: memasukkan pesan palsu ke dalam jaringan, penambahan *record* ke file.

2.13 Pengamanan Jaringan

Jaringan merupakan yang sangat rentan dengan serangan-serangan dan gangguan. Untuk itu diperlukan suatu pengamanan jaringan untuk meminimalisir gangguan-gangguan pada infrastruktur jaringan.

Pengamanan jaringan dibagi menjadi 3 yaitu [12] :

1. Pengamanan Sistem Jaringan
   a. Penggunaan *digest authentication* pada web server, sehingga *password* yang dikirimkan melalui *network* tidak berupa *clear text.*
   b. Pencatatan log melalui program atau fasilitas yang disediakan. Administrator sistem berkewajiban melakukan pengecekan terhadap kejadian-kejadian yang terekam dalam log setiap bulan.
   c. Menggunakan beberapa program untuk mendeteksi adanya penyusupan *(intrusion detection).* Beberapa program sederhana yang dapat dilakukan antara lain *chkwtmp, tcplogd* dan *hostsentry.*
   d. *Firewall* digunakan untuk membatasi *port-port* yang dapat diakses dari luar. Sedangkan akses internet dari dalam ke luar untuk situs-situs tertentu dilarang.
   e. *Switch* harus memiliki fungsi *Routed Access Control List* yang dapat digunakan untuk menjamin hanya *user* yang memiliki akses saja yang dapat menggunakan *secured* dan *restricted network.*
   f. *Application-Proxy Firewall* ini digunakan untuk memfilter informasi-informasi yang lewat dari *proxy sever* tersebut. *Proxy server* dapat

memilih informasi-informasi yang akan diteruskan atau tidak berdasarkan *setting* atau *logic* dari *proxy server* tersebut.

g. *Backup harddisk* secara keseluruhan untuk semua *server* ke dalam tape.

h. *Backup* basis data.

2. Pengamanan Sistem Operasi

a. *Server* tidak diperkenankan menggunakan atau menyediakan *floppy drive.* Hal ini untuk menghindari penyusup dapat menggubah *password root* dengan menggunakan disket *boot.*

b. Setiap aplikasi yang digunakan wajib menyediakan fungsi login yang memaksa pengguna untuk memasukkan *username* dan *password* setiap kali akan menggunakan aplikasi tersebut termasuk ketika melakukan koneksi jaringan.

c. Aplikasi internal tidak dapat diakses dari luar. Untuk mencegah akses dari luar terhadap aplikasi internal, maka digunakan *firewall* dan IP internal untuk *server-server* yang digunakan oleh aplikasi internal. Dengan IP internal dan *firewall* diharapkan *server-server* tersebut hanya bisa dikenali oleh komputer yang ada pada jaringan lokal saja.

d. Adanya sesi untuk membatasi lamanya koneksi yang *idle.* Untuk aplikasi-aplikasi berbasis *web*, jika *browser* sudah dibuka dan user tidak menggunakan aplikasi yang diakses dalam waktu tertentu atau *idle* yang diperkenankan tersebut juga dengan lamanya sesi.

e. Mengingat banyak lubang keamanan dikirimkan melalui *e-mail*, maka penggunaan antivirus yang *up-to-date* merupakan sebuah keharusan. Antivirus ini harus dipasang pada setiap *workstation* dan *server.*

f. Bagi pemakai aplikasi, pengaksesan basis data harus melalui aplikasi yang sudah dikembangkan.

g. *Username* dan *password* untuk mengakses basis data hanya boleh diketahui oleh kalangan terbatas.

3. Pengamanan Jaringan

a. Ruangan tempat menyimpan semua *server, router* serta data *backup* berada di ruang yang berbeda dengan ruang kerja. Ruangan tersebut selalu

terkunci dan hanya dapat diakses oleh *operation* dan *network administrator.*

b. *Server-server* yang ada diletakkan pada ruangan *server* yang khusus. Pintu masuk dan keluar dari dan ke ruangan ini hanya ada satu pintu. Tembok dan pintu ruangan ini berupa kaca anti pecah. Pintunya berupa pintu elektronik, diperlukan kartu akses magnetik untuk membukanya. Lantainya menggunakan *raised floor.* AC yang digunakan untuk mendinginkan ruangan *server* merupakan AC central. Perlu juga menyediakan alat untuk memadamkan api, alarm kebakaran, sensor deteksi kebakaran melalui panas dan asap.
c. Mengasuransikan aset-aset yang dimiliki khususnya *server* dan PC.
d. Menyediakan mesin diesel untuk menyuplai arus listrik secara otomatis jika listrik yang disediakan oleh PLN mengalami gangguan.
e. Menyediakan UPS *(Uninterruptible Power Supply)* untuk server aplikasi ataupun basis data untuk mencegah kerusakan fisik pada *server* tersebut.