BAB 2
TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Banyak penelitian yang telah dilakukan tentang audit tata kelola Teknologi Informasi menggunakan framework COBIT 5, salah satunya adalah penelitian yang membahas mengenai tata kelola keamanan sistem informasi menggunakan COBIT 5 yang berjudul "Audit Tata Kelola Teknologi Informasi Berbasis COBIT 5 (DSS05) Untuk Evaluasi Keamanan Sistem Informasi Pada Dinas Komunikasi Dan Informasi Kabupaten Kendal". Dalam penelitian ini terdapat masalah pada Dinas Komunikasi dan Informasi Kabupaten Kendal yaitu belum diterapkannya SOP (*Standart Operating System*) secara jelas mengenai permasalahan pada sistem informasi dan komunikasi terutama tentang keamanan dalam pengolahan atau penyimpanan data. Oleh karena itu penelitian ini dilakukan untuk mencari tingkat kapabilitas keamanan sistem informasi pada Dinas Komunikasi dan Informasi Kabupaten Kendal sebagai ukuran tingkat keamanan pada pengolahan data. Tenik pengumpulan data yang dilakukakan dalam penelitian ini yaitu melalui metode wawancara, studi pustaka, serta penyebaran kuesioner berdasarkan COBIT 5. Maka dari penelitian ini diperoleh hasil yang menunjukan bahwa tingkat kapabilitas tata kelola terkait sistem informasi pada Dinas Kominfo Kabupaten Kendal adalah 2 yaitu *managed process* dengan status *Largely Achieved* sebesar 76,45% atau setara dengan nilai 2,76 yang belum memenuhi target pada level 3 [2].

Masih terdapat beberapa penelitian lain yang dilakukan mengenai tata kelola TI menggunakan COBIT 5 yaitu "Audit Tata Kelola TI menggunakan COBIT 5 (MEA02) pada BPPT Kota Semarang". Permasalahan pada penelitian ini yaitu masih sering terjadi kesalahan pada sistem BPPT kota Semarang sehingga dibutuhkan proses pengawasan, evaluasi, dan penilaian pengendalian internal terhadap sistem, guna memperoleh suatu strategi dalam perbaikan. Data yang

digunakan sebagai acuan dalam penelitian berdasarkan wawancara, dan kuesioner sesuai dengan kerangka kerja COBIT 5. Hasil dari penelitian ini yaitu tingkat kapabilitas tata kelola TI pada BPPT kota Semarang telah tercapai dengan baik sebesar 78,16% atau setara 2,78 dimana *Inclomplete* (Level 0) dan *Performed* (Level 1) sudah mencapai *Fully Achieved* dengan target yaitu *Established* (level 3) [3].

Tabel 2.1 Penenelitian Terkait Audit Tata Kelola TI Berdasarka COBIT 5

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Tri Rachmawati Sari, et all, 2016	Dinas Komunikasi dan Informasi Kabupaten Kendal belum menerapkannya SOP (*Standart Operating System*) secara jelas mengenai permasalahan pada sistem informasi dan komunikasi terutama tentang keamanan dalam pengolahan atau penyimpanan data.	Kerangka kerja pada COBIT 5 dengan domain DSS05.	Tingkat kapabilitas tata kelola terkait sistem informasi yang diperoleh pada Dinas Komunikasi dan Informasi Kabupaten Kendal saat ini adalah 2 yaitu *managed process* dengan status *Largely Achieved* sebesar 76,45% atau setara dengan nilai 2,76 yang belum memenuhi target pada level 3.

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
2.	Lutfiani Anngraeni, et all, 2016	Masih seringnya terjadi kesalahan pada sistem BPPT kota Semarang sehingga dibutuhkan proses pengawasan, evaluasi, dan penilaian pengendalian internal terhadap sistem, guna memperoleh suatu strategi dalam perbaikan.	Kerangka kerja COBIT 5 dengan domain MEA02	Pengukuran tingkat kapabilitas tata kelola TI pada BPPT kota Semarang telah tercapai dengan baik sebesar 78,16% atau setara 2,78 dimana *Inclomplete* (Level 0) dan *Performed* (Level 1) sudah mencapai *Fully Achieved* dengan target yaitu *Established* (level 3)
3.	Rio Kurnia Candra, et all, 2013	Analisa tata kelola TI serta evaluasi, menilai kapabilitas dan menyusun rekomendasi untuk TI.	*Capability Level* dengan kerangka kerja COBIT 5 (DSS)	Rata-rata *Capability Level* pada DSS ini adalah83% berada pada level 3 yaitu *Establish Process*. Yang artinya setiap aktivitas telah dilakukan dengan standarpenerapannya, sudah terdokumentasi dan setiap komunikasi berjalan dengan baik.

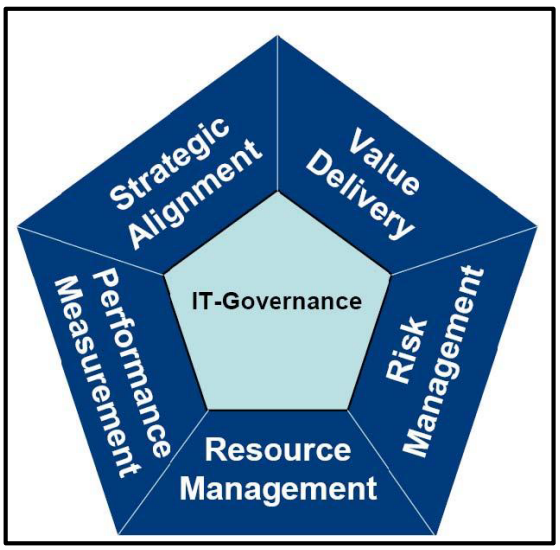
2.2 Tata Kelola TI (*IT Governance*)

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 SI/TI yang dapat mendukung pengoperasian TI agar dapat memperluas strategi dan tujuan perusahaan [4].

Tujuan dari tata kelola TI adalah menyelaraskan bisnis dan TI untuk menjamin kinerja TI memenuhi dan sesuai dengan tujuan , sebagai berikut [4]:

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. Pertanggung jawaban 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 [4] :



Gambar 2.1 Fokus Area Tata Kelola TI [4]

1. *Strategic Alignment*, berfokus pada kepastian terhadap ketertiban antara strategi 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 Management*, 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 penggunaannya serta telah memenuhi tujuan bisnis organisasi secara efektif dengan menggunakan sumber daya efektif [4].

Elemen utama dalam aktifitas audit tata kelola TI dapat diklasifikasikan dalam tinjauan penting berikut [4] :

1. Tinjauan terkait dengan fisik dan lingkungan , mencakup hal-hal yang terkait dengan keamanan fisik, sumber daya, temperatur dan faktor lingkungan lainnya.

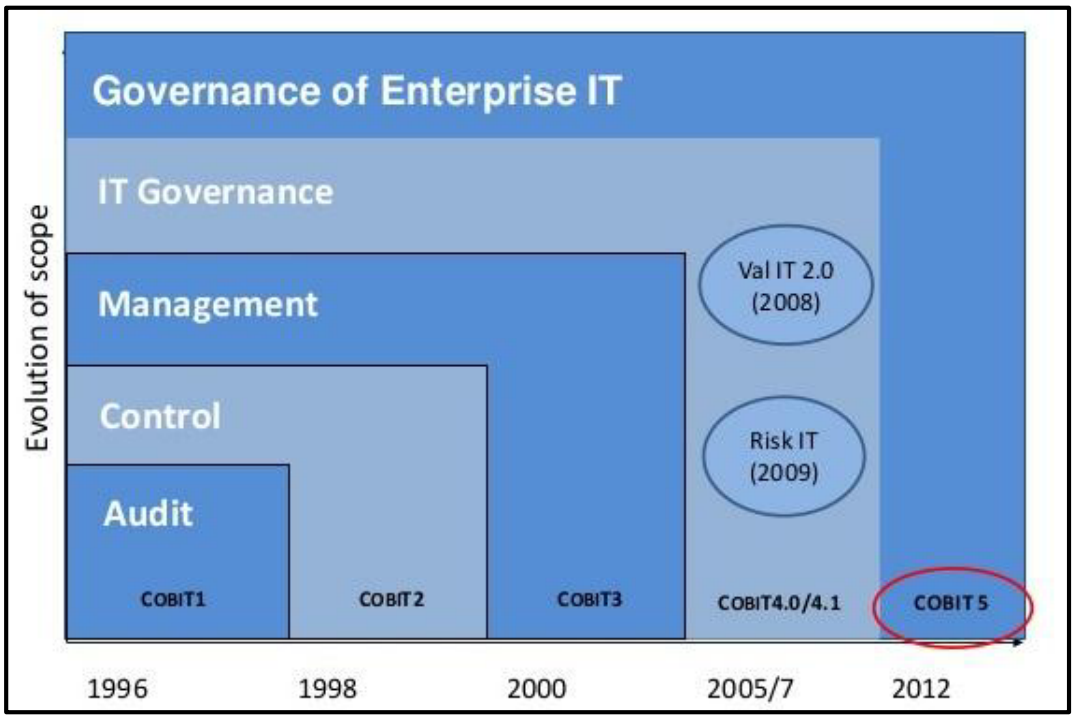
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem informasi, database seluruh prosedur administrasi sistem.
3. Tinjauan perangkat lunak, tinjauan yang mencakup aplikasi bisnis organisasi berupa sistem berbasis web yang menjadi inti dari jalannya proses bisnis suatu organisasi.
4. Tinjauan keamanan jaringan, yang mencakup jaringan internet 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 ketersediaan backup data dan penyimpanan jika sewaktu-waktu terjadi bencana.
6. Tinjauan integritas bisnis, memastikan ketelitian data yang sedang beroperasi.

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

COBIT adalah suatu bentuk kerangka kerja TI yang berfungsi sebagai pembantu dalam mengevaluasi strategi bisnis dan tujuan tata kelola TI. Untuk lebih jelasnya pengertian dari COBIT merupakan suatu standar dalam kerangka kerja domain yang terdiri dari sekumpulan proses TI dan sekumpulan dokumentasi *best practices* untuk aktivitas dalam tata kelola TI yang digunakan untuk membantu pendefinisian strategi serta kontrol pada manajemen tingkat atas untuk menganilis kesenjangan *gap* antara resiko bisnis, yang berfungsi sebagai acuan dalam dalam menemukan masalah-masalah serta solusi untuk perbaikan terkait tata kelola TI. COBIT merupakan bagian dari *Information System Audit and Control Association* (*ISACA*) yang dibuat oleh *IT Governance Institute* (*ITGI*).

COBIT pertama kali diluncurkan pada tahun 1996 dengan COBIT versi 1 yang lebih berorientasi pada penekanan audit, lalu tahun 1998 dirilis COBIT versi 2 dengan penekanan pada pengendalian, kemudian tahun 2000 dirilis kembali COBIT versi ketiga yang menekankan pada manajemen. Pada tahun 2005 COBIT kembali mengeluarkan versi terbaru yaitu versi 4 dan dua tahun kemudian kembali mengalami pembaruan dengan merilis COBIT versi 4.1 pada tahun 2007. Namun

pada tahun 2012 COBIT kembali mengeluarkan versi terbarunya dengan COBIT versi 5 yang lebih menekankan tata kelola TI pada perusahaan [5].

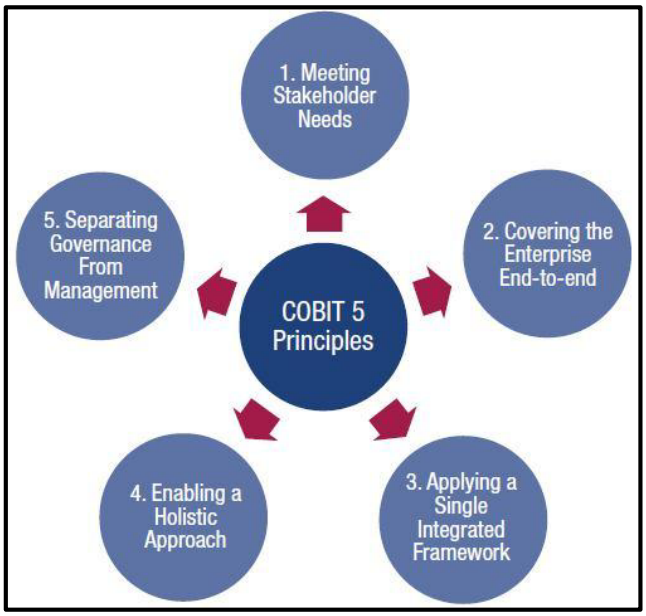


Gambar 2.2 Sejarah Perkembangan Cobit

2.5 COBIT 5

COBIT 5 merupakan versi terbaru yang menyediakan kerangka kerja yang digunakan untuk membantu perusahaan atau organisasi dalam mencapai nilai yang optimal dari tata kelola TI dengan mempertahankan , menyeimbangkan antara mewujudkan manfaat dan memaksimalkan 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 [6].

Terdapat lima prinsip utama dalam COBIT 5 sebagai dasar dalam tata kelola manajemen TI suatu organisasi. Dari lima prinsip tersebut diharapkan dapat mengoptimalkan tingkat resiko dan memberikan keuntungan bagi perusahaan atau organisasi [6].



Gambar 2.3 Prinsip-Prinsip Dalam Cobit 5

Prinsip 1 : Memenuhi kebutuhan *Stakeholder*. Perusahaan menciptakan nilai bagi para *Stakeholder* dengan merealisasikan manfaat dan mengoptimalkan resiko. COBIT 5 menyediakan semua proses-proses yang diperlikan perusahaan untuk memenuhi dalam pencapaian nilai bisnis melalui pengguna TI. Karena setiap perusahaan memiliki tujuan yang berbeda sehigga perusahaan dapat menyesuaikan sendiri tujuan bisnisnya melalui COBIT 5.

Prinsip 2 : Melindungi seluruh Perusahaan. COBIT 5 dapat mencapai 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 sunber daya baik internal maupun eksternal yang berhubungan dengan tata kelola TI dan manajemen TI.

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.

Prinsip 4 : Menggunakan Sebuah Pendekatan yang Menyeluruh. Tata kelola TI dan manajemen TI perusahaan yang efektif dan efiien memerlukan pendekatan dengan mempertimbangkan beberapa komponen yang saling berinteraksi. COBIT 5 dapat mendefinisikan pendekatan-pendekatan tersebut untuk membantu perusahaan atau organisasi dalam mencapai tujuan perusahaan atau organisasi. COBIT 5 mendefinisikan tujuh kategori pendekatan :

1. Prinsip, kebijakan dan kerangka kerja
2. Proses
3. Struktur organisasi
4. Budaya, etika dan perilaku
5. Informasi
6. Layanan, infrastruktur dan aplikasi
7. Sumber daya, keterampilan dan komponen

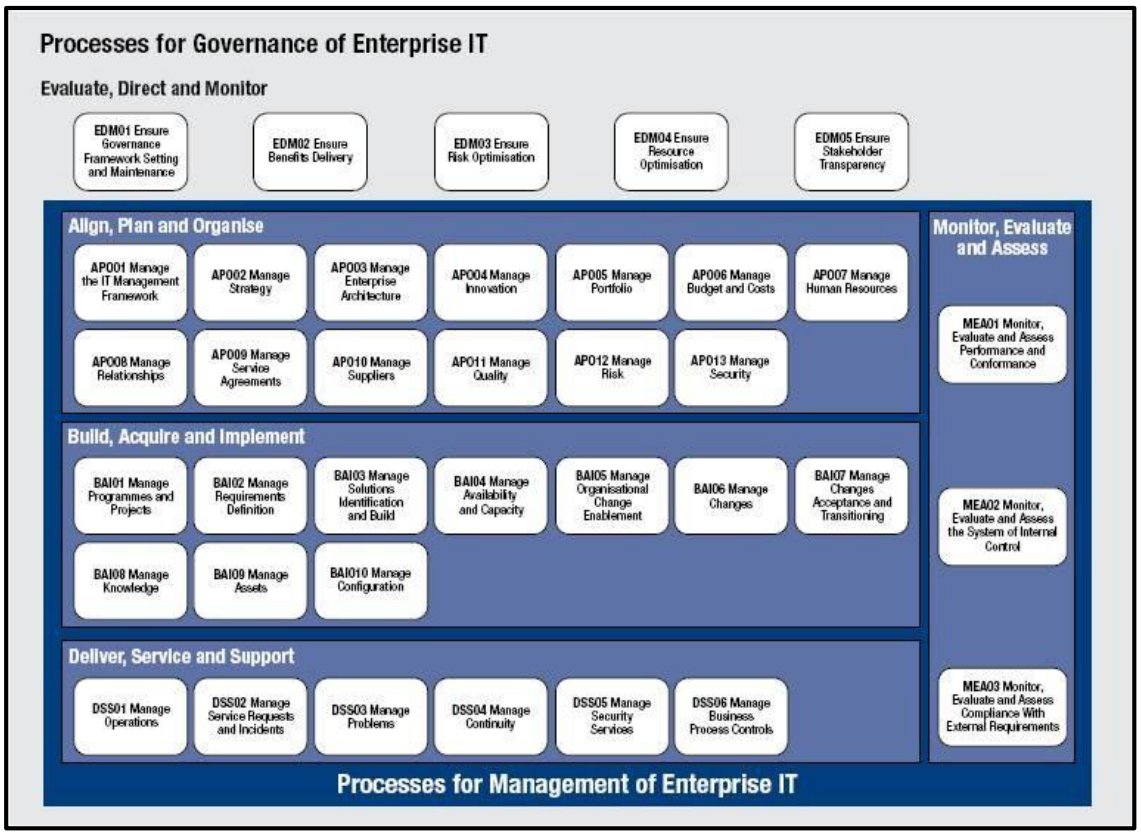
Prinsip 5 : Pemisahan Tata Kelola Dari Manajemen. Kerangka kerja COBIT 5 memuat perbedaan yang jelas antara tata kelola dan manajemen. Dua disiplin mencakup berbagai jenis kegiatan, struktur organiasi dan tujuan.

Perbedaan utama antara tata kelola dan manajemen :

1. 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 keola keseluruhan merupakan tanggung jawab dewan direksi di bawah kepemimpinan ketua.
2. Manajemen : Manajemen mempunyai rencana, membagun, menjalankan segala arah 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 *evolution* dari referensi COBIT 4.1 yang diintegrasikan dengan model proses *RiskIT* dan *ValIT* [6].



Gambar 2.4 Model Referensi COBIT 5 [6]

Gambar diatas menunjukan 37 proses tata kelola dan manajemen pada prose COBIT 5. Model referensi COBIT 5 dibagi menjadi 2 proses utama yaitu tata kelola dan manajemen [6] :

1. Tata kelola (*Governance*)

   Mempunyai 5 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 optimalisasiresiko (*Ensure risk optimisation*).
   d. EDM04 Memastikan optimalisasi sumber daya (*Ensure resource optimisation*).
   e. EDM05 Memastikan transparansi terhadap *stakeholder* (*ensure Stakeholder transparancy*).

2. Manajemen

   Memuat 4 proses yang sejajar dengan area tanggung jawab dari merencaakan, membangun, menjalankan dan mamantau (*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 meberikan taktik dan mengidentifikasi cara terbaik yang dapat digunakan oleh perusahaan untuk membantu mencapai tujuan dan sasaran perusahaan. Domain APO juga memperhatikan bentuk organisasi dan Infrastruktur guna untuk mencapai hasil yang optomal dan meberikan manfaat dari penggunaan IT. Domain APO terdiri dari 13 proses yaitu :
      1) APO01 Mengelola manajemen kerangka IT (*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 anggran dan biaya (*Manage budget and cost*).
7) APO07 Mengelola sumber daya manusia (*Manage human resource*).
8) APO08 Mengelola hubungan (*Manage relationships*).
9) APO09 Mengelola perjanjian layanan (*Manage agreements*).
10) APO10 Mengelola pemasok (*Manage suppliers*).
11) APO11 Mengelola kualitas (*Manage quality*).
12) APO12 Mengelola resiko (*Manage risk*).
13) APO13 Mengelola keamanan (*Manage Security*).

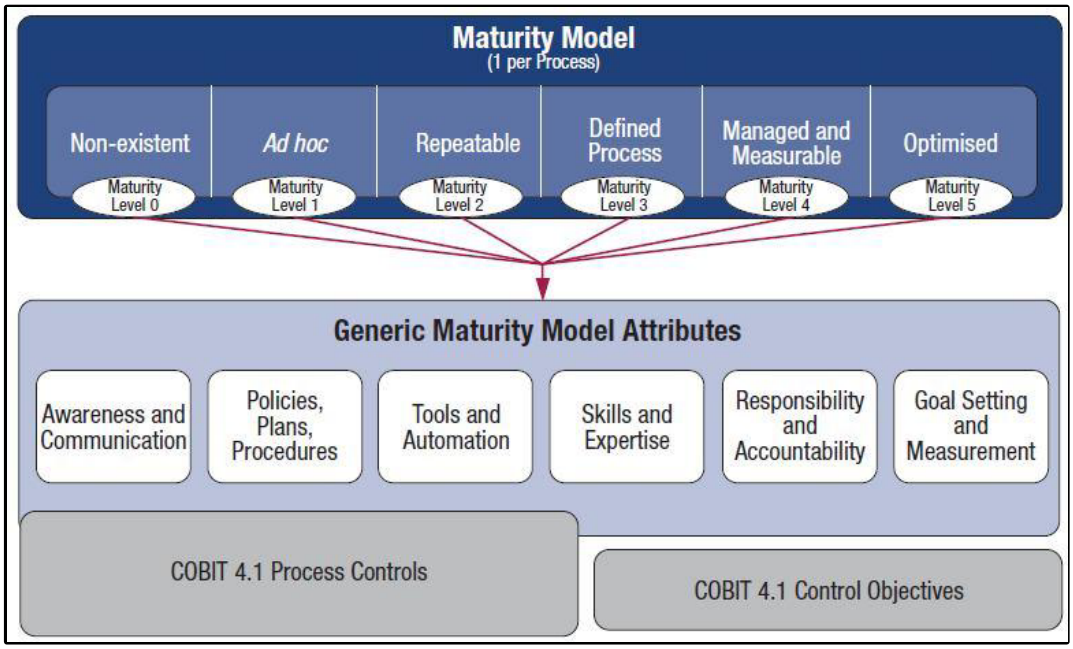
b. Domain membangun, memperoleh dan melaksakan. BAI (*Build, Aquire and Implement*), tujuan domain BAI adalah untuk mengidentifikasi solusi TI yang perlu dikembangkan dan diterapkan ke salam prose bisnis perusahaan. Domain BAI terdiri dari 10 proses yaitu :
   1) BAI01 Mengelola program dan proyek (*Manage programmes and project*).
   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 accepted and transitionsing*).
   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 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 request and incident*).
   3) DSS03 Mengelola permasalahan (*Manage problems*).
   4) DSS04 Mengelola layanan yang berkelanjutan (*Manage security service*).
   5) DSS05 Mengelola layanan keamanan (*Manage security service*).
   6) DSS06 Mengelola proses bisnis kontrol (*Manage business process control*).

d. Domain, 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 untukmemenuhi tujuan bisnisdan 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*).

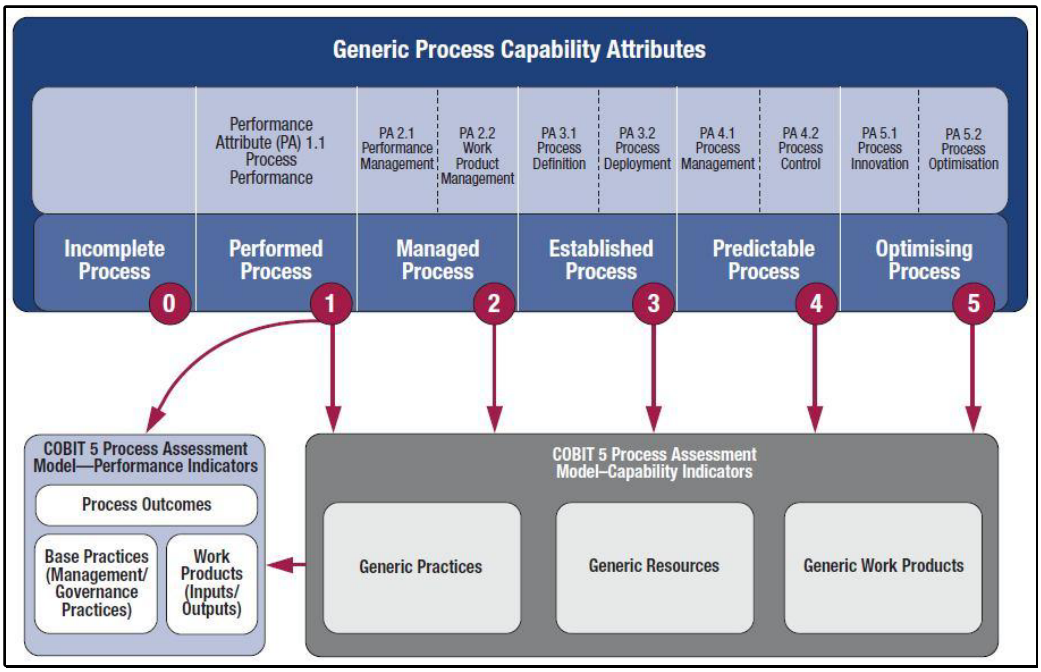
2.5.2 Model Kapabilitas Proses Pada COBIT 5

Para auditor yang mengunakan COBIT 4.1, *ValIT* dan *RiskIT* mungkin telah mengetahui adanya model kematangan proses dalam proses-proses tersebut. Model ini dipakai untuk mengukur tingkat kematangan proses yang berhubungan dengan teknologi informasi dalam suatu organisasi, untuk mendefinisikan persyaratan tingkat kapabilitas atau kematangan, dan untuk menemukan kekurangan diantara tingkat-tingkat kematangan dan strategi yang digunakan untuk meningkatkan proses guna mencapai tingkatan kematangan yang diharapkan [6].



Gambar 2.5 Model Kematangan Pada Cobit 4.1 [6]

Berbeda dengan COBIT 5, yang mengenalkan adanya model kapabilitas proses, berdasarkan pada ISO/IEC 15504, standar mengenai *Software Engineering* dan *Process Assessment*. Model ini mengukur performansi tiap-tiap proses tata kelola (*EDM-based*) atau proses manajemen (*PBRM based*), dan dapat mengidentifikasi area-area yang perlu untuk ditingkatkan performansinya. Model ini berbeda dengan model proses *maturity* dalam COBIT 4.1, baik itu pada desain maupun penggunaannya [6].



Gambar 2.6 Model Kapabilitas dalam COBIT 5

Ada enam tingkatan kapabilitas yang dapat dicapai oleh masing-masing proses, yaitu [7] :

1. ***Incomplete Process*** – Proses tidak lengkap; Proses tidak diimplementasikan atau gagal mencapai tujuannya. Pada tingkatan ini, hanya ada sedikit bukti atau bahkan tidak ada bukti adanya pencapaian sistematik dari tujuan proses tersebut.
2. ***Performed Process*** – Proses dijalankan (satu atribut); Proses yang diimplementasikan berhasil mencapai tujuannya.
3. ***Managed Process*** – Proses teratur (dua atribut); Proses yang telah dijalankan seperti diatas telah diimplementasikan dalam cara yang lebih teratur (direncanakan, dipantau, dan disesuaikan), dan produk yang dihasilkan telah ditetapkan, dikendalikan, dan dijaga dengan baik.
4. ***Established Process*** – Proses tetap (dua atribut); Proses di atas telah diimplementasikan menggunakan proses tertentu yang telah ditetapkan, yang mampu mencapai *outcome* yang diharapkan.

5. ***Predictable Process*** – Proses yang dapat diprediksi (dua atribut); Proses di atas telah dijalankan dalam batasan yang ditentukan untuk mencapai *outcome* proses yang diharapkan.
6. ***Optimising Process*** – Proses Optimasi (dua atribut); Proses diatas terus ditingkatkan secara berkelanjutan untuk memenuhi tujuan bisnis saat ini dan masa depan.

Keuntungan model kapabilitas proses COBIT 5 dibandingkan dengan model kematangan proses dalam COBIT 4.1, diantaranya :

1. Meningkatkan fokus pada proses yang sedang dijalankan, untuk meyakinkan apakah sudah berhasil mencapai tujuan dan memberikan *outcome* yang diperlukan sesuai dengan yang diharapkan.
2. Konten yang lebih disederhanakan dengan mengeliminasi duplikasi, karena penilaian model kematangan dalam COBIT 4.1 memerlukan penggunaan sejumlah komponen spesifik, termasuk model kematangan umum, model kematangan proses, tujuan pengendalian dan proses pengendalian untuk mendukung proses penilaian model kematangan dalam COBIT 4.1.
3. Meningkatkan keandalan dan keberulangan dari aktivitas penggunaan kapabilitas proses dan evaluasinya, mengurangi perbedaan pendapat diantara *stakeholder* dan hasil penilaian.
4. Meningkatkan kegunaan dari hasil penilaian kapabilitas proses, karena model baru ini memberikan sebuah dasar bagi penilaian yang lebih formal dan teliti.

2.5.3 Perbedaan Antara C OBIT 4.1 dan COBIT 5

Ada beberapa perbedaan antara COBIT 5 dengan COBIT 4.1 sebagai berikut :

1. *Governance of Enterprise IT (GEIT),* merupakan sebuah prisnsip terbaru dalam tata kelola TI untuk organisasi. Pada COBIT 5 seperti halnya *ValtIT* dan *RiskIT* lebih menekankan kepada prinsip dibandingkan proses. Dari beberapa *fedback* didapati bahwa penggunaan prinsip-prinsip tersebut dapat dipahami dengan mudah dan diimplementasikan secara lebih baik dalam konteks *enterprise*.

2. Dalam COBIT 5 lebih berorientasi terhadap *Enabler*, walaupun demikian sebenarnya di dalam COBIT 4.1 juga terdapat *enabler* akan tetapi berbeda dalam penyebutan istilah. COBIT 5 menyebutkan bagian-bagian dalam *enable* secara lebih detail didalam pengimplementasian. Berikut merupakan perbandingan pada bagian *enabler* di antara COBIT 4.1 dan COBIT 5 dari sudut pandang yang sama :
   a. Prinsip-prinsip, kebijakan dan kerangka kerja.
      Di dalam COBIT 4.1, terdapat beberapa poin yang tersebar dalam proses-proses COBIT 4.1
   b. Proses-proses.
      Proses merupakan bagian yang sentral dari COBIT 4.1.
   c. Struktur Organisasi.
      Pada COBIT 4.1, struktur organisasi dapat dilihat didalam RACI *chart (Responsible, Accountable, Consulted*, dan *Informed)* yang menjelaskan peran serta tanggung jawab oleh pihak-pihak terkait dalam setiap proses..
   d. Kultur, etika dan perilaku.
      Poin-poin tersebut telah tercermin dalam beberapa proses COBIT 4.1
   e. Informasi.
      Informasi adalah salah satu sumber daya TI yang terpenting pada COBIT 4.1
   f. Layanan, Infrastruktur, dan Aplikasi.
      Infrastruktur dan aplikasi merupakan bagian yang menjadi satu dalam sebuah layanan, yang menjadi sumber daya TI.
   g. Orang, keterampilan (*skills*) dan kompetensi.
      Istilah “orang” di dalam COBIT 4.1 hanya sebagai salah satu pendukung sumber daya, tanpa menyebutkan keterampilan dan kompetensinya.
3. COBIT 5 merupakan modifikasi dari model-model yang lama dengan tambahan *governance* dan terdapat juga beberapa proses yang baru yang mencakup aktivitas perusahaan seperti *end-to-end.* COBIT 5 menggabungan antara COBIT 4.1, *Risk IT* dan *Val IT* kedalam sebuah kerangka

kerja yang dapat digunakan untuk menyelaraskan dengan *best practices* yang tersedia seperti ITIL v3 dan TOGAF.

4. Terdapat penambahan beberapa proses baru pada COBIT 5 yang belum ada didalam COBIT 4.1 dan modifikasi pada beberapa proses yang telah ada dalam COBIT 4.1. Dapat diartikan bahwa model COBIT 5 merupakan pengintegrasian konten COBIT4.1, *Risk IT* dan *Val IT*. Oleh karena itu COBIT 5 merupakan suatu framework yang lebih efektif digunakan sebagai evaluasi bisnis perusahaan secara *end-to-end*.

2.5.4 Skala Penilaian

Skala penilaian digunakan setelah memperoleh hasil dari tingkat kapabilitas, setiap atribut dinilai menggunakan standar skala penilaian yang dijelaskan dalam standar ISO/IEC 15504. Skala penilaian terdiri atas [7] :

1. N (*Not achieved* atau Tidak tercapai)
   Pada kategori ini, belum diketemukan atau hanya terdapat sedikit bukti berdasarkan pencapaian dari atribut prosesi tersebut. *Range* nilai yang diperoleh dalam kategori ini berkisar 0% sampai 15%.
2. P (*Partically achieved* atau Tecapai sebagaian)
   Pada kategori ini, ditemukan beberapa bukti mengenai pendekatan dan beberapa pencapaian atribut atas proses tersebut. *Range* nilai yang diperoleh pada kategori ini berkisar antara >15% sampai 50%.
3. L (*Largely achieved* atau Secara garis besar tercapai)
   Pada kategori ini terdapat bukti atas pendekatan sistematis dan pencapaian signifikan atas proses tersebut, meski mungkin masih ada kelemahan yang tidak signifikan. *Range* nilai yang diperoleh pada kategori ini berkisar antara >50% sampai 85%.
4. F (*Fully achieved* atau Tercapai penuh)
   Di dalam kriteria ini ditemukan beberapa bukti atas pendekatan sistematis dan lengkap, serta tercapai secara penuh atas atribut proses tersebut serta tidak diketemukan kelemahan - kelemahan terkait atribut proses tersebut. *Range*

nilai yang diperoleh 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 kapabiliitas itu, akan tetapi proses itu harus meraih kategori *Fully acvieved* (F) agar dapat melanjutkan penilaian pada level kapabilitas selanjutnya. Jadi semisalnya suatu proses agar meraih level kapabilitas 3, maka level 1 dan level 2 pada proses itu harus mencapai kategori *Fully achieved* (F), sedangkan level kapabilitas 3 cukup mencapai kategori *Large achieved* (L) atau *Fully achieved* (F) [7].

2.6 Penggunaan COBIT 5 Pada Lembaga Penjamin Mutu Pendidikan Jawa Tengah

Ada beberapa framework yang dapat digunakan sebagai proses audit yaitu seperti ITIL, ISO, dan COBIT. Akan tetapi dari beberapa framework tersebut COBIT 5 berisi arahan yang lebih umum dan spesifik mengenai apa saja yang harus dilakukan sesuai topik yang dibahas dalam penelitian ini mengenai proses keamanan TI. Pemilihan COBIT 5 sebagai framework audit tata kelola pada LPMP Jawa Tengah karena implementasi pada COBIT 5 dapat membantu instansi dalam hal meningkatkan pendekatan audit, mendukung audit kerja dengan arahan audit secara rinci, sebagai penilaian untuk kendali IS/IT, meningkatkan kontrol IT, dan sebagai standarisasi pendekatan/program audit dalam LPMP Jawa Tengah.

Adapun kelebihan dari COBIT 5 yaitu antara lain :

1. Rahasia.
2. Proteksi terhadap informasi yang sensitif dari akses yang tidak bertanggung jawab.
3. Integritas.
4. Berhubungan dengan penyediaan informasi yang sesuai untuk manajemen.
5. Secara umum dapat dikatakan bahwa COBIT merupakan sebuah model tata kelola TI yang memberikan sebuah arahan yang lengkap mulai dari sistem

mutu, perencanaan, manajemen proyek, keamanan, pengembangan dan pengelolaan layanan.

Dari hasil observasi yang dilakukan peneliti sebelumnya terdapat beberapa kelemahan dalam hal proses keamanan TI dalam LPMP Jawa Tengah, sebagai contoh tidak adanya pengamanan secara khusus pada ruang server, standarisasi ruang server dinilai sangat kurang, kurangnya SDM yang berkompeten di dalam lingkup ICT LPMP Jawa Tengah sehingga perlu dilakukan pelatihan, dan masih banyak lagi yang dirasa perlu untuk diperbaiki dalam hal keamanan sistem informasi pada LPMP Jawa Tengah sebagai instansi pemerintahan.

Berdasarkan masalah-masalah yang terjadi di atas, COBIT 5 dapat memberikan suatu model referensi yang menjelaskan secara rinci mengenai tata kelola TI. Proses tersebut berada pada domain DSS (*Deliver, Service, Support*) yang memberikan pelayanan seperti pengelolaan keamanan dan dukungan proses IT yang lebih efektif dan efisien, sehingga dinilai mampu memperbaiki permasalahan yang terjadi pada LPMP Jawa Tengah. Lebih khususnya seperti isi domain DSS05 yang mengandung praktek manajemen diantaranya :

1. Melindungi terhadap malware, yang berisi standarisasi tentang pengamanan sistem informasi dari virus, worm, dll.
2. Mengelola keamanan jaringan dan konektivitas, yang berisi standarisasi pengamanan jaringan serta penataan sistem pengkabelan yang baik dan aman pada LPMP Jawa Tengah.
3. Mengelola keamanan *endpoint*, memberikan prosedur keamanan seperti laptop, PC, dan server.
4. Mengelola identitas pengguna dan akses logis, mengatur tentang prosedur keamanan hak akses sesuai kebutuhan kepada masing-masing staf.
5. Mengelola keamanan fisik, berisikan standar prosedur yang mengatur seperti pengamanan ruang server, standarisasi ruang server yang dirasa masih kurang didalam LPMP Jawa Tengah.

Dari penjelasan-penjelasan diatas maka peneliti memilih menggunakan COBIT 5 pada domain DSS05 (*Manage Security Service*) untuk melakukan proses audit tata kelola terkait keamanan informasi pada LPMP Jawa Tengah.

2.7 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 [6].

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

Domain DSS proses *Deliver, Service and Support* (DSS05) merupakan proses yang berfokus pada upaya perlindungan aset informasi pada organisasi untiuk mempertahankan tingkat resiko keamanan informasi yang dapat diterima organisasi sesuai kebijakan keamanan [8].

Tujuan dari proses *Deliver, Service 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 operasional yang ada [8].

Pada DSS05 mengandung praktek manajemen, diantaranya [8] :

1. DSS05.01 (*Protect Agains 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 perusahaan guna melindungi teknologi informasi dari ancaman *malware* seperti *worm, virus, spam,* dll.

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 perangkatn *endpoint.* Seperti laptop, desktop, 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 seta 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 Output Devices)*

   Merupakan praktek 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 keamanan 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.

2.9 RACI Chart

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

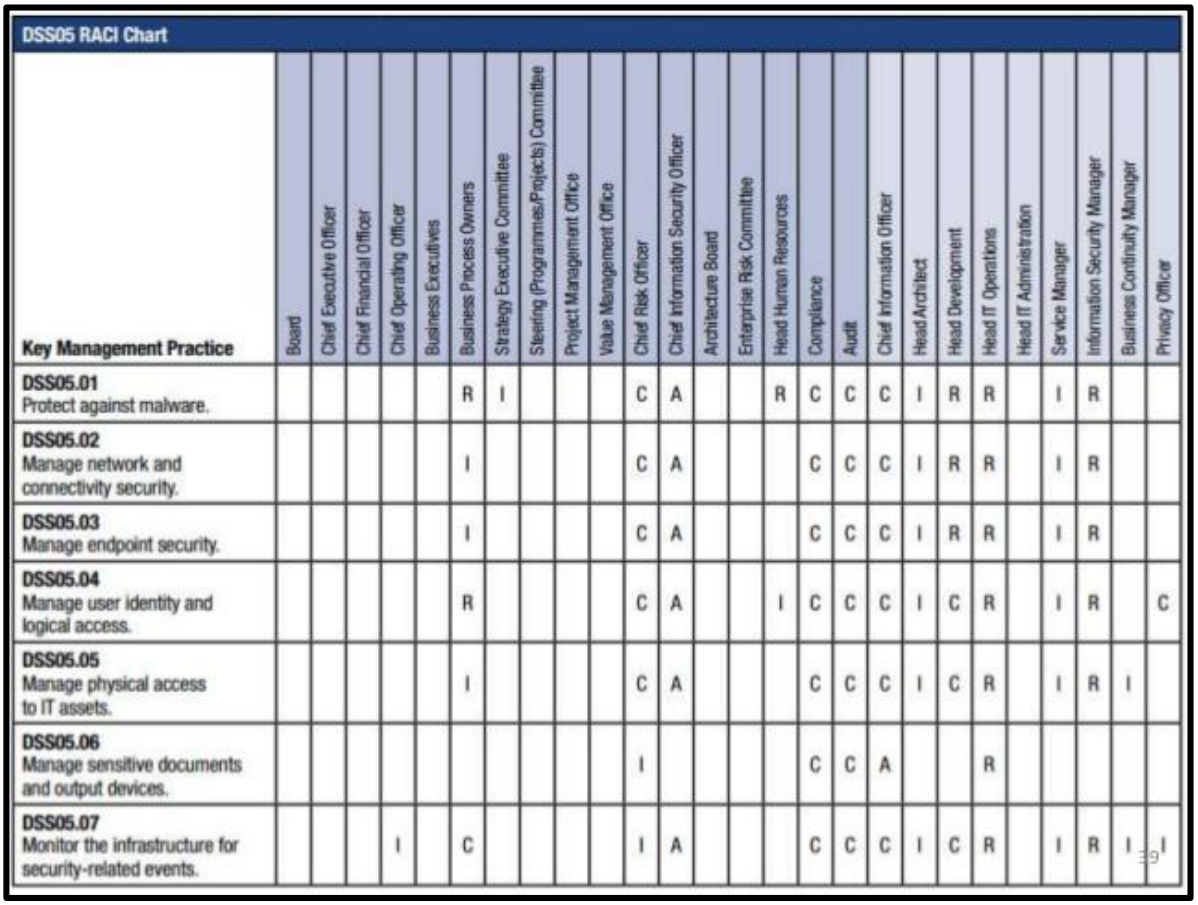
1. *Responsible* (pelaksana)

   Merupakan pihak yang melakukan suatu pekerjaan. Hal ini berkaitan pada peran utama di dalam organisasi guna mencapai kegiataan yang telah direncanakan serta dapat mencapai hasil sesuai yang diharapkan.
2. *Accountable* (Bertanggung jawab)

   Merupakan pihak yang bertanggung jawab atas semua pekerjaan. Dengan memperhatikan hal tersebut pada tingkatan paling rendah dalam akuntabilitas yang sama, memiliki tingkat yang paling tinggi pertanggung jawabannya.
3. *Consulted* (penasehat)

   Merupakan pihak yang diminta pendapat tentang suatu pekerjaan. Posisi seperti ini tergantung pada peranan *responsible* serta *accountable* guna mendapat informasi-informasi dari bagian-bagian lainnya dalam perusahaan.
4. *Informed* (Informasi)

   Merupakan pihak yang mendapat informasi tentang kemajuan suatu pekerjaan. Jabatan ini sebagai informan suatu perusahaan seperti peran dan penyerahan tugas.



DSS05 RACI Chart																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Gambar 2.7 RACI Chart DSS 05

2.10 Keamanan Sistem Informasi

Kemanan sistem informasi dapat diartikan sebagai suatu perlindugan dari kejahatab 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, jaringan komputer dan data [9].

2.11 Pentingnya Keamanan Sistem Informasi

Keamanan sistem informasi merupakan komponen yang sangat penting bagi organisasi atau perusahaan yang telah menggunkan teknologi berbasis TI. Kemanan sistem informasi menggambarkan adanya perlindungan terhadap komputer,

fasilitas, data dan informasi dari pihak-pihak yang tidak bertanggung jawab. Namun pada prakteknya yang terjadi di dalam organisasi atau perusahaan masalah keamanan sistem informasi ini kurang mendapat kepedulian dari pihak pengelola sistem informasi [9].

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, yaitu [9] :

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 menunjukan 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.

2.12 Manajemen Kemananan Sistem Informasi

Manajemen keamana 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 4 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.

2.13 Tipe Ancaman Informasi

Ancaman informasi merupakan suatu 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 [10]:

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 sebagian perangkat keras komputer.

2. *Interception*

   Merupakan ancaman terhadap kerahasiaan. Informasi yang ada di akses oleh orang lain yang tidak memiliki hak akses tersebut. Contoh : mencuri data rahasia , mengcopy file tanpa diotorisasi.

3. Modification

Sumber daya yang tidak berhak mengakses berhasil megakses informasi kemudian merubah nilai dari sumber daya tersebut. Contoh : mengubah program sehingga program dijalankan akan berbeda hasilnya, megubah nilai-nilai file data.

2.14 Pengamanan Jaringan

Dalam dunia teknologi informasi, jaringan merupakan bagian yang sangat rentan terhadap gangguan-gangguan atau serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Maka dari itu diperlukan suatu pengaman jaringan untuk meminimilasir gangguan-gangguan pada infrastruktur.

Pengaman sistem jaringan dapat digolongkan menjadi 3 bagian [11] :

1. Pengaman Sistem Jaringan
    a. Menggunakan *digest authentications* pada web server, yang dapat menjaga *password* yang dikirim melalui *network* agar tidak berbentuk *clear texts.*
    b. Proses mencatat log melalui program atau fasilitas yang telah tersedia. Administrator sistem mempunyai kewajiban untuk melakukan pengecekan pada aktifitas-aktifitas yang tercatat pada log setiap bulannya.
    c. Memanfaatkan beberapa program yang mempunyai fungsi untuk pendeteksi jika terjadi penyusupan (*intrusion detection).* Banyak program yang telah disediakan untuk melakukan deteksi seperti *chektmp, tcplogd,* serta *hotsentry.*
    d. Penggunaan *Firewall* yang berfungsi untuk memberi batasan kepada *port-port* atas akses dari luar. Serta pengaksesan untuk beberapa situs dari dalam ke luar situs dilarang.
    e. Fungsi utama dari *switch* yaitu *Routed Acces Control List* yang berguna untuk menjamin *user* yang mempunyai hak akses khusus untuk dapat menggunakan *restriceted* dan *secured network*.

f. Untuk memfilter informasi yang melalui *proxy server* dapat menggunakan *Application-Proxy Firewall.* Sehingga *proxy server* dapat memilah informasi yang masuk untuk dapat diteruskan atau tidak sesuai *setting* atau *logic* yang telah ditentekan.

g. Melakukan *Bakcup harddisk* secara berkala pada setiap server yang digunakan kedalam tape.

h. Memback up basis data secara rutin.

2. Pengamanan Sistem Operasi

a. Pelarangan dalam menggunakan media penyimpanan *portable* pada *server.* Hal tersebut dilakukan agar tidak terjadi proses penyusupan pada *server* yang dapat megubah mengubah *password* root menggunakan *flash disk* dan sebagainya.

b. Wajib menyediakan sistem login pada setiap aplikasi, agar pengguna memasukan username dan password untuk mengetahui siapa saja yang telah mengakses aplikasi tersebut jika terjadi hal-hal yang tidak diinginkan.

c. Pencegahan terhadap akses dari luar untuk aplikasi-aplikasi internal. Yaitu dengan cara menggunakan *firewall* dan *IP Internal* serta *firewall* untuk server-server pada aplikasi internal yang dipakai. Sehingga server-server hanya dapat mengenali alamat IP pada jaringan komputer lokal saja.

d. Melakukan pembatasan sesi koneksi sehingga dapat mengatur lamanya koneksi yang idle. Seperti aplikasi yang berbasis website, apabila browser telah dijalankan dan pengguna tidak menjalankan aplikasi tersebut dalam rentang waktu yang ditentukan atau idle yang diperbolehkan, maka koneksi akan dihentikan.

e. Karena banyak celah keamanan yang dikirimkan melalui e-mail, maka dari itu penggunaan antivirus yang selalu terupdate adalah suatu keharusan yang wajib diaplikasikan di setiap server dan komputer.

f. Dalam pengaksesan basis data melalui aplikasi, harus menggunakan aplikasi yang telah dikembangkan .

g. Pemegang hak akses pada basis data hanya dapat diketahui oleh beberapa orang, untuk menjaga kerahasiaan *username* dan *password*.

3. Pengamanan Jaringan
   a. Ruang untuk menyimpan *server, backup data,* dan *router* harus dipisah dengan ruang kerja. Tempat tersebut harus memiliki keamanan dalam mengakses, sehingga harus tertutup dengan rapat serta hanya bagian *operation* dan *network administrator* yang diperbolehkan untuk masuk.
   b. Ruang server harus berada pada ruang khusus yang memiliki satu pintu untuk akses keluar masuk. Sistem keamanan pada ruang server harus pada tingkat VVIP dengan pintu elektronik yang menggunakan kartu akses magnetik, tembok serta kaca sekat yang digunakan memiliki kriteria tertentu yang susah dirusak. Pendingin udara dalam ruangan harus selalu menyala sebagai pendingin server, dengan saluran khusus AC sentral. Serta ruang server harus memiliki sensor tedeksi api, yang dilengkapi alat pemadam kebakaran portable.
   c. Mengasuransikan aset yang dimiliki seperti *server* dan PC
   d. Penyediaan mesin diesel otomatis guna mengantisipasi apabila terjadi pemadaman listrik yang dilakukan oleh pihak PLN.
   e. Setiap server baik server aplikasi maupun basis data harus dilengkapi dengan UPS (*Uninterruptible Power Supply*) untuk meminimalisir terjadinya kerusakan secara fisik pada server.