BAB II
TINJAUAN PUSTAKA

A. PENELITIAN TERDAHULU

Pada penelitian sebelumnya yang dilakukan oleh (Witjaksono, 2019), dikatakan bahwa tingkat *capability* keseluruhan berdasarkan keseluruhan rata-rata adalah berada di level 4, yang berarti sebagian besar aktivitas pada domain DSS untuk Sistem Informasi Akademik Universitas Telkom telah dilakukan dengan baik, ada standar kontrol dan standar pengukuran yang sudah berjalan dengan baik. Optimasi proses maka harus dilakukan perbaikan-perbaikan proses dan pencapaian tujuan proses, dengan cara melakukan semua aktivitas pada *process practice* yang telah direkomendasikan oleh COBIT 5.

Berikutnya dari penelitian oleh (Ekowansyah et al., 2017a), menyatakan bahwa penggunaan Teknologi Informasi (TI) dalam perguruan tinggi akan bermanfaat jika penerapannya sesuai dengan visi dan misi organisasi. Oleh karena itu, audit sistem informasi akademik yang menggunakan COBIT 5 perlu dilakukan untuk mengidentifikasi tingkat kematangan TI yang diterapkan di lingkungan kampus Universitas Jenderal Achmad Yani. Tujuan penelitian ini adalah untuk mengukur dan mengetahui tingkat kematangan teknologi informasi akademik di Unjani berdasarkan data yang diperoleh dari sampel lingkungan kampus Unjani. Sebagai metode pengukuran teknologi informasi, peneliti memilih COBIT 5 karena metode ini lebih berfokus pada proses yang diinginkan dan akan menghasilkan kegiatan operasional yang baik jika dilakukan dengan baik. Dengan hasil audit sistem informasi akademik yang baik, diharapkan pihak manajemen TI dapat menemukan solusi dari proses yang dirasa kurang maksimal dan layanan yang diberikan kepada pengguna dapat maksimal.

Berikutnya oleh (Mz et al., 2021), dilakukan penelitian tentang tata kelola audit sistem informasi perpustakaan dengan menggunakan framework COBIT 5. Penelitian ini bertujuan untuk memastikan sistem informasi di

lembaga perpustakaan berjalan dengan baik sehingga dapat mempengaruhi kualitas pelayanan yang terintegrasi TI dan SI. Audit dilakukan dengan menggunakan domain Delivery Service and Support (DSS) pada COBIT 5, dengan fokus pada DSS01 dan DSS04 untuk meninjau layanan TI perpustakaan. Hasil audit menunjukkan capability level yang didapat terletak pada established process dan predictable process yang ditentukan sebagai level target. Rekomendasi yang diberikan antara lain membuat laporan hasil pelaksanaan prosedur setiap bulan, melakukan monitoring dan analisis laporan perbaikan untuk prosedur kedepan, melakukan monitoring dan analisis terhadap sistem informasi perpustakaan, dilakukan pengecekan aset setiap bulan, membuat katalog tertulis yang berisi manajemen problem, dan membuat kebijakan business continuity. COBIT 5 menjadi alat bantu dalam melakukan audit dan DSS fokus pada tingkatan layanan yang berkelanjutan.

Pada penelitian selanjutnya yang dilakukan oleh (Yauma Dzikri, Widhyhardika & Admaja Dwi H, 2019). Penelitia melakukan penelitian tentang Evaluasi Tata Kelola Keamanan Informasi Menggunakan Cobit 5 Pada Domain APO13 dan DSS05 (Studi pada PT Gas Energi Indonesia). Dalam penelitian ini mencoba untuk melakukan evaluasi terkait kemanan system informasi yang telah diimplementasikan pada sebuah system untuk mendapatkan kemanan bagi pengguna system. COBIT 5 mengukur tingkat pengelolaan keamanan informasi yang diterapkan pada perusahaan dengan menyediakan proses-proses yang memiliki kaitan dengan pengelolaan keamanan informasi. Proses tersebut adalah APO13 (Manage Security) dan DSS05 (Manage Security Services) yang merupakan proses utama pada COBIT 5 untuk mengukur pengelolaan keamanan informasi (ISACA, 2013). Sementara merujuk pada penelitian Matin et.al (2017) yang berjudul “Analisis Keamanan Data Center Menggunakan COBIT 5”, proses lain untuk melakukan pengukuran pada pengelolaan keamanan informasi EDM03, APO12 dan BAI06. Penelitian yang dilakukan oleh Matin et.al (2017) juga menjelaskan pentingnya melakukan keamanan informasi untuk menjaga aset, terutama pada organisasi yang belum melakukan evaluasi dan audit keamanan informasi.

Secara teori, keamanan informasi adalah usaha untuk melindungi informasi yang dimiliki agar tidak diakses oleh yang tidak berhak untuk mengakses informasi tersebut (Andress, 2014). Keamanan informasi memiliki 3 aspek utama yaitu confidentiality (kerahasiaan) yaitu usaha perlindungan dari akses yang tidak berhak, integrity (integritas) yaitu pencegahan data dari perubahan oleh yang tidak memiliki hak dan availability (ketersediaan) yaitu informasi tersedia ketika ada pihak yang membutuhkannya Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 5928 Fakultas Ilmu Komputer, Universitas Brawijaya (Andress, 2014).

Lalu penelitian selanjutnya oleh (Malik, Arini & Wardhani, 2017). Penelitia melakukan analisis keamanan system informasi data center pada sebuah institusi. Data center pada sebuah institusi telah diamati dan di analisa untuk mendapatkan deskripsi mengenai keamanan informasinya. Data center pernah mengalami insiden keamanan informasi berupa shell Injection. Akibatnya, beberapa situs web tidak dapat diakses dibeberapa saat. Insiden ini dapat mempengaruhi proses bisnis institusi. Untuk menghindari masalah ini di masa depan, diperlukan audit keamanan informasi. Audit ini dapat dilakukan dengan menggunakan framework COBIT 5. Dalam penelitian ini, audit keamanan informasi dilakukan terhadap keamanan informasi data center dengan fokus pada proses APO13 (Manage Security) dan DSS05 (Manage Security Service). Penelitian ini Penelitian ini dilakukan melalui tahap Initiation, Planning the Assessment, Briefing, Data Collection, Data Validation, Process Attribute Level dan Reporting the Result. Hasil penelitian ini diketahui tingkat kemampuan APO13 dan DSS05 pada saat ini (As Is) bernilai 1,54 dan 1,68 atau pada level 2, yang berarti proses APO13 dan DSS05 telah dilakukan dan dipelihara sesuai dengan rencana kerja. Oleh karena itu tingkat berikutnya (to be) ditetapkan pada level 3.

Lalu adapun, sebuah penelitian dengan judul "*Risk assessment and recommendation strategy based on COBIT 5 for risk: Case study sikn Jikn helpdesk service*" oleh (Wulandari et al., 2019). Penelitian ini berkaitan dengan National Archive Information System dan National Archive Information

Network (SIKN JIKN) yang merupakan program prioritas nasional dari Arsip Nasional Republik Indonesia (ANRI) sebagai sebuah lembaga arsip. ANRI menyediakan layanan helpdesk nasional untuk mendukung manajemen dan operasi SIKN JIKN. Namun, aplikasi helpdesk yang disediakan tidak digunakan secara optimal dan menyebabkan risiko seperti kehilangan data dan permintaan atau masalah yang diajukan oleh anggota SIKN JIKN sebagai pengguna sistem. Jika risiko tidak ditangani, hal ini akan menyebabkan kehilangan node jaringan potensial serta hilangnya ANRI. Oleh karena itu, dalam penelitian ini dilakukan analisis risiko terhadap aktivitas helpdesk SIKN JIKN dengan menggunakan pedoman dan kerangka kerja COBIT 5 untuk Risiko dan COBIT 5 Enabling Process. Penelitian ini berfokus pada domain yang mendukung aktivitas helpdesk, yaitu domain DSS01 untuk prosedur operasional dan APO12 untuk mengelola risiko. Hasil penilaian dapat digunakan sebagai rekomendasi untuk meningkatkan layanan helpdesk dan meminimalkan dampak risiko untuk memastikan keberlanjutan layanan helpdesk SIKN JIKN.

Selanjutnya, dalam penelitian yang dilakukan oleh (Wolden et al., 2015), disebutkan bahwa serangan *cyber espionage* dan malware memiliki potensi bahaya yang besar bagi organisasi yang mengandalkan teknologi modern untuk meningkatkan efisiensi. Meskipun aplikasi baru yang tersedia untuk perencanaan sumber daya perusahaan dan manajemen memberikan ketersediaan yang lebih tinggi dan layanan yang lebih baik, namun aplikasi tersebut sering kali disesuaikan dengan kebutuhan khusus, yang dapat meninggalkan celah keamanan. Meskipun organisasi telah menerapkan langkah-langkah keamanan yang ketat, pengguna akhir jahat memanfaatkan celah keamanan yang ditemukan dalam berbagai sistem untuk melakukan kejahatan siber umum seperti penolakan layanan, hacking dan pengubah situs web, malware, spam, dan phishing. Sistem Manajemen Rantai Pasokan (SCMS) juga bukanlah hal baru dalam hal kejahatan siber seperti itu dan tentunya membutuhkan Kerangka Keamanan Sistem Informasi (IS) dalam melawan serangan malware. Penelitian ini meneliti efektivitas implementasi

Kerangka Keamanan Informasi COBIT 5 dalam mengurangi risiko Serangan Siber pada SCMS. Dalam upaya ini, data kualitatif dikumpulkan untuk kuesioner keamanan yang komprehensif yang ditargetkan pada administrator dan manajer SI yang bertanggung jawab terhadap organisasi Rantai Pasokan yang menggunakan kerangka COBIT 5 untuk keamanan. Hasil penelitian menunjukkan bahwa COBIT 5 menambah dimensi baru untuk tata kelola keamanan SI melalui kebijakan yang ketat dan aturan yang lebih menguatkan keamanan aplikasi perusahaan. Secara keseluruhan, penelitian ini menunjukkan bahwa organisasi mendapatkan manfaat dari menerapkan langkah-langkah keamanan kerangka COBIT 5 pada sistem SCMS dan ERP.

B. KAJIAN PUSTAKA

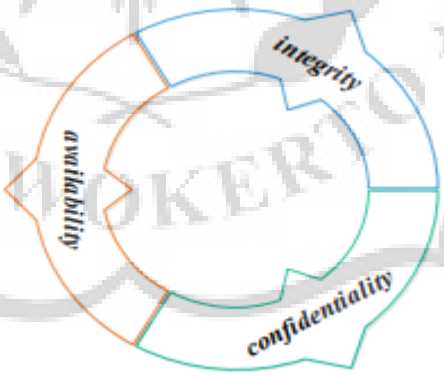
1. Analisis

Dalam Kamus Bahasa Indonesia Kontemporer karangan Peter Salim dan Yenni Salim (2002) menjabarkan pengertian analisis sebagai berikut:

a. Analisis adalah penyelidikan terhadap suatu peristiwa (perbuatan, karangan, dan sebagainya).
b. Analisis adalah penguraian pokok persoalan atas bagian – bagian, penelahan bagian – bagian tersebut dan hubungan antar bagian untuk mendapatkan pengertian yang tepat dengan pemahaman secara keseluruhan.
c. Analisis adalah sebuah penjabaran (pembetangan) sesuatu hal, dan sebagainya setelah ditelaah secara seksama.
d. Analisis adalah proses pemecehan masalah yang dimulai dengan hipotesis (dugaan, dan sebagainya) sampai terbukti kebenarannya melalui beberapa kepastian (pengamatan, percobaan, dan sebagainya).
e. Analisis adlaah proses pemecahan masalah melalui akal ke dalam bagian – bagiannya berdasarkan metode yang konsisten untuk mencapai pengertian tentang prinsip – prinsip dasarnya.

2. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan salah satu topik dalam perkembangan teknologi informasi dan komunikasi di era digitalisasi (Umar et al., 2018). Untuk memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi (Yunanri et al, 2016). Keamanan informasi dapat dicapai dengan menerapkan seperangkat kontrol yang sesuai. Kontrol ini perlu ditetapkan, diterapkan, dimonitor, direview, ditingkatkan dimana yang perlu untuk memastikan bahwa tujuan bisnis dan keamanan yang spesfifik bagi organisasi dipenuhi (Raichel et al., 2005). Penerapan keamanan informasi bertujuan untuk mengatasi masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan *(availability)*, kerahasiaan *(confidentiality)*, dan kesatuan *(integrity)* sehingga dapat dinilai tingkat keamanan informasinya (Riadi, 2016). Keamanan informasi adalah perlindungan karakteristik informasi *(confidentiality, integrity*, dan *availability)* baik itu dalam memperoses informasi, menyimpan serta mengirimkanya dalam upaya untuk menjaga keberlangsungan dan memperluas kesempatan bisnis (Kurniawan et al., 2017).



Gambar 1 Aspek Keamanan Informasi

Keamanan sistem informasi yang baik harus menerapkan standar *deming cycle of quality* (Hicham et al, 2012). Dalam area keamanan sistem informasi terdapat 4 poin *deming cycle of quality* yaitu:

a. *Plan* (Merencanakan): keamanan berencana untuk pindah postur yang reaktif ke postur proaktif.
b. *Develop* (Mengembangkan): serangkaian proses yang harus dilakukan dikembangkan mengikuti patokan keamanan.
c. *Check* (Periksa): Keamanan dikontrol melalui tes audit dan penetrasi, dan metode yang paling umum.
d. *Act* (Tindakan): Semua aktivitas kontrol dilakukan selama fase "Periksa" kemungkinan akan menyoroti sejumlah malfungsi yang perlu disediakan untuk tindakan korektif, tindakan pencegahan dan tindakan perbaikan.

3. Pendaftaran

Pendaftaran adalah pencatatan hal atau identitas seperti nama, alamat dan sebagainya dalam suatu lembaga pendidikan, pendaftaran merupakan hal yang sangat penting.

Pengertian pendaftaran disini pada dasarnya untuk memperlancar dan mempermudah dalam penerimaan Mahasiswa sehingga terorganisir, teratur, dengan cepat atau tepat. Jumlah mahasiswa pada tiap tahunnya tidak sama, maka untuk mempermudah pendataan mahasiswa dibuatlah Sistem Informasi Penerimaan Mahasiswa dengan menggunakan perantara komputer untuk menyimpan file mahasiswa.

4. Penerimaan Mahasiswa Baru (PMB) UMP

Penerimaan Mahasiswa Baru (PMB) merupakan salah satu kegiatan penting dalam sebuah perguruan tinggi. Kegiatan ini dilakukan setiap tahunnya dan bertujuan untuk merekrut calon mahasiswa baru yang berkualitas untuk bergabung di perguruan tinggi tersebut. PMB UMP dilaksanakan setiap tahun dengan 3 gelombang pendaftaran dengan beberapa tahapan seperti pembuatan akun, mengisi kelengkapan data diri, pemilihan jalur, hingga metode pembayaran. Sistem informasi PMB UMP diakses secara online berbasis website, dengan beberapa jalur seleksi pendaftaran yaitu sebagai berikut.

a. Jalur Minat, Prestasi, Organisasi

b. Jalur CBT/Reguler
c. Jalur SMART/Nilai Raport
d. Jalur Nilai UTBK
e. Jalur Kedokteran
f. Program Pascasarjana
g. Program Profesi Apoteker
h. Program Profesi Ners
i. Program D2 Bahasa Arab
j. Mahad PAI Plus
k. Transfer / Alih Jenjang TLM
l. Alih Jenjang Kebidanan S1
m. Rekognisi Pembelajaran Lampau (RPL)

5. Cobit

COBIT adalah singkatan dari *Control Objective for Information and related Technology*, yang merupakan sebuah kerangka kerja (*framework*) yang dikembangkan oleh ISACA (*Information System and Control Association*) pada tahun 1992 untuk mendukung tata kelola teknologi informasi. COBIT dapat membantu perusahaan dalam mencapai tujuan melalui pengelolaan dan manajemen TI. Prinsip dasar dari framework COBIT adalah memberikan informasi yang diperlukan untuk mencapai tujuan perusahaan atau organisasi. Untuk mencapai hal tersebut, perusahaan atau organisasi perlu mengelola sumber daya teknologi informasi dengan menggunakan serangkaian proses teknologi informasi yang terstruktur sehingga dapat memberikan informasi yang dibutuhkan. (Ekowansyah et al., 2017b)

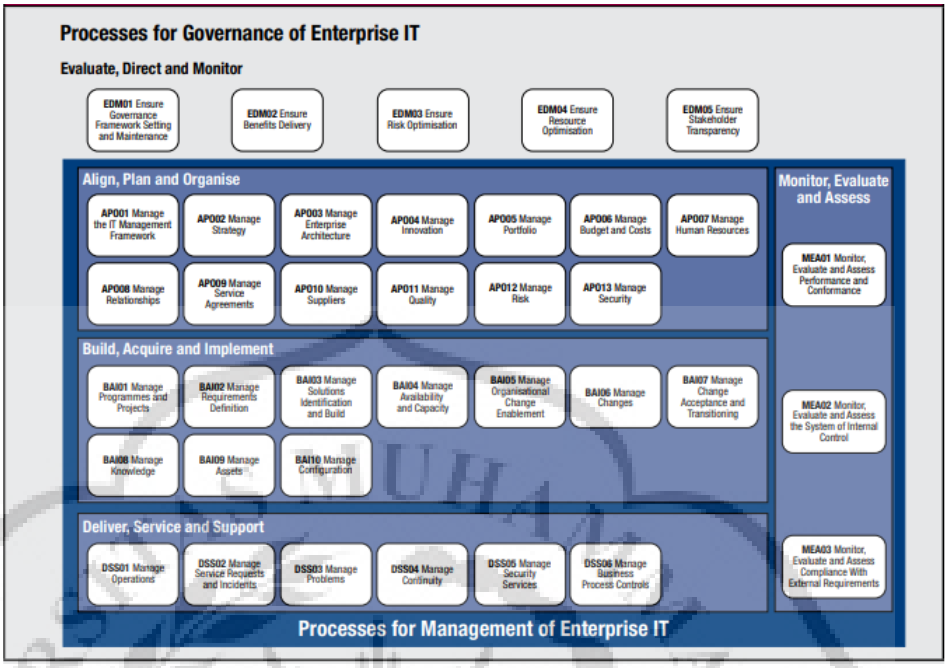
Seiring waktu, COBIT telah mengalami perkembangan sejak tahun 1996. Dimulai dari COBIT 1 pada tahun 1996 yang hanya membahas tentang audit, COBIT 2 pada tahun 1998 membahas sampai pada pengendalian, COBIT 3 pada tahun 2000 membahas sampai level manajemen, COBIT 4.0/4.1 pada tahun 2005 yang membahas sampai pada

tata kelola TI, dan COBIT 5 pada tahun 2012 yang membahas sampai pada tata kelola TI perusahaan secara keseluruhan.

6. Cobit 5

COBIT 5 adalah pembaruan dari framework COBIT yang menggabungkan pemikiran terkini tentang teknik dan tata kelola teknologi informasi perusahaan. *Framework* ini menyediakan prinsip-prinsip, praktik-praktik, dan alat analisis yang umumnya diterima untuk meningkatkan kepercayaan dan nilai sistem informasi. COBIT 5 dikembangkan dengan mengintegrasikan *Val* IT dan *Risk* IT dari ISACA, ITIL, serta standar-standar relevan dari ISO, dan merupakan perkembangan dari COBIT 4.1. (Lutfiyana et al., 2020).

COBIT 5 menyajikan sebuah model referensi proses yang rinci, terperinci, dan menyeluruh dalam menjelaskan proses tata kelola dan manajemen TI. Dalam model referensi proses COBIT 5 terdapat 37 proses tata kelola dan manajemen, yang dapat menggambarkan semua proses yang biasa ditemukan di perguruan tinggi. Model referensi proses ini juga menyediakan panduan yang mudah dipahami sebagai acuan. Oleh karena itu, setiap perguruan tinggi harus mampu menentukan alur proses bisnisnya sendiri sesuai dengan keadaan yang ada.



Gambar 2. Model Referensi Proses (Cobit 5 Enabling Processes, 2012)

Model referensi proses COBIT 5 dibagi menjadi dua domain proses utama, yaitu tata kelola dan manajemen. Domain tata kelola terdiri dari lima proses yang masing-masing memiliki praktik-prosak, yaitu *Evaluate, Direct*, dan *Monitor* (EDM). Sementara itu, domain manajemen memiliki empat area tanggung jawab, yaitu *Plan*, *Build*, *Run*, dan *Monitor*. Keempat area tanggung jawab tersebut mencakup ruang lingkup TI yang komprehensif, seperti *Align*, *Plan*, and *Organize* (APO), *Build*, *Acquire*, and *Implement* (BAI), *Deliver*, *Service and Support* (DSS), dan *Monitor*, *Evaluate*, and *Assess* (MEA).

a. Domain dan proses yang ada pada COBIT 5 yaitu:
   1) *Align, Plan and Organise* (terdiri dari 13 proses)
   2) *Build, Acquire and Implement* (terdiri dari 10 proses)
   3) *Deliver, Service and Support* (terdiri dari 6 proses)
   4) *Monitor, Evaluate and Assess* (terdiri dari 3 proses)
   5) *Evaluate Direct and Monitor* (terdiri dari 5 proses)

b. Prinsip-prinsip COBIT 5 adalah sebagai berikut:

1) *Meeting stakeholders needs* (memenuhi keinginan pemangku kepentingan). Perusahaan menciptakan nilai bagi stakeholder dengan mempertahankan keseimbangan antara realisasi manfaat dan optimalisasi risiko serta penggunaan sumber daya.
2) *Covering the enterprise end-to-end* (Mencakup *Enterprise End-to-end*). Mengintegrasikan tata kelola perusahaan TI dalam tata kelola perusahaan: mencakup semua fungsi dan proses dalam perusahaan menganggap semua tata kelola dan manajemen TI enabler untuk perusahaan.
3) *Applying a single integrated framework* (Menerapkan *Single Framework* yang Terpadu) Berkaitan dengan IT standar dan praktik terbaik, masing-masing memberikan bimbingan pada subset dari kegiatan TI.
4) *Enabling a Holistic Approach* (Mengaktifkan tata Pendekatan yang menyeluruh). Manajemen TI perusahaan yang efisien dan efektif memerlukan pendekatan yang menyeluruh, mempertimbangkan beberapa komponen yang berinteraksi. Cobit 5 mendefinisikan satu set enabler untuk mendukung pelaksanaan tata kelola yang komprehensif dan sistem manajemen TI untuk perusahaan.
5) *Separating Governance from Management* (Memisahkan Tata Kelola dari Manajemen) Kerangka COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup berbagai jenis kegiatan, memerlukan berbagai struktur organisasi dan melayani tujuan yang berbeda.

c. RACI *Chart*

RACI *Chart Responsible, Accountable, Consulted,* dan *Informad*. Dalam perusahaan, RACI *Chart* merupakan sebuah alat yang digunakan untuk pengambilan keputusan dan membantu pihak manajemen dalam mengidentifikasikan peran dan tanggung jawab keryawannya. pada Pembagian tugas yang jelas serta peran dan

tanggung jawab akan menyebabkan kebingungan yang akhirnya akan mengakibatkan berkurangnya produktivitas kerja karyawannya pada perusahaan (Cahyani et al., 2018). Pengertian *responsible, accountable, consulted,* dan *informed* telah dijelaskan dalam ISACA, COBIT 5 Enabling Process Tahun 2012 sebagai berikut:

1) *Responsible* (R) merupakan orang yang secara langsung bertanggung jawab menangani pekerjaan tersebut
2) *Accountable* (A) merupakan orang yang memiliki wewenang serta tanggung jawab terhadap keputusan ketika terjadi suatu masalah pada perusahaan.
3) *Consulted* (C) merupakan orang yang memberi nasehat terhadap aktivitas yang dilakukan pada perusahaan.
4) *Informed* (I) merupakan orang yang memberikan keputusan apa yang akan diambil.

7. *Domain Deliver, Service and Support* (DSS)

Domain yang berhubungan dengan keamanan teknologi informasi adalah domain DSS. Domain DSS *(Deliver, Service and Support)* merupakan sebuah domain yang digunakan dalam analisa teknologi informasi dalam area menajemen yang di dalamnya terdapat beberapa proses. (Firmansyah, 2015). Dalam dosmain DSS terdapat Sub-doman DSS05 dimana sub domain ini merupakan prosedur yang lebih intensif terhadap kemanan informasi. Sub domain tersebut adalah manage security services dimana sub domain ini melaksanakan beberapa akatifitas atau pernyataan sebanyak 49 pernyatan yang di kelompokan dalam 7 proses sebagai berikut:

a. *Protect against malware* (DSS05.01) melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada diseluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak.

b. *Manage network and connectivity security* (DSS05.02) digunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.
c. *Manage endpoint security* (DSS05.03) memberikan kepastian terhadap titik akhir keluaran (end poin) (missal: Laptop, desktop, dan server) dijamin tingkat yang sama atau lebih besar dari persyaratan keamanan yang disetujui.
d. *Manage user identity and logical access* (DSS05.04) memberikan kepastian terhadap semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis. Mereka dan berkoordinasi dengan devisi bisnis yang mengelola hak akses.
e. *Manage physical access to* IT *assets* (DSS05.05) menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan fisik. Bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau.
f. *Manage sensitive documents and output devices* (DSS05.06) menetapkan pengamanan fisik. Dalam segi dokumen yang berhubungan dengan istansi. Sehingga semua keluaran dokumen terstandar dalam keamanan.
g. *Monitor the infrastructure for security-related events* (DSS05.07) menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk hak akses yang tidak sah dan memastikan setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian.

8. *Capability Level*

Capability Level adalah suatu teknik penilaian yang digunakan untuk mengukur seberapa matang atau berkapabilitas sebuah organisasi. Skor kapabilitas ini dinyatakan dalam rentang level 0 hingga level 5.

Tabel 2. 1. Level dan Process Attribute dari Process Capabillity

Level	PA	Deskripsi
Level 0	0	Tidak dilakukan atau gagal
Level 1	1	Dilakukan tapi belum ada manajemennya
Level 2	2.1	Dilakukan dan ada perencanaan serta dimonitor
	2.2	Dilakukan, ada perencanaan dan monitor kemudian hasil kerja dikelola dengan baik (ditentukn kebutuhannya dan didokumentasikan)
Level 3	3.1	Dilakukan aktivitas terrtulis di SOP/kebijakan/aturan atau dibuat standar pengoperasiannya, merupakan unsur pentng yang wajib dilakukan
	3.2	Dilakukan aktivitas tertulis di SOP/kebijakan/aturan atau mempunyai standar penerapan, serta ada alokasi tanggung jawab dan sumber daya yang tepat
Level 4	4.1	Dilakukan aktivitas tertulis di SOP/kebijakan/aturan berjalan dengan baik dan ada penerapan ukuran layanan/informasi optimal yang dihasilkan
	4.2	Dilakukan aktivitas tertulis di SOP/kebijakan/aturan atau dan menghasilkan layanan/informasi optimal kemudian dimonitor dan dianalisis
Level 5	5.1	Dilakukan, inovasi dan strategi pengembangan aktivitas, sesuai hasil analisi dari aktivitas yang telah terstandarisasi sebelumnya
	5.2	Dilakukan, ada inovasi dan strategi pengembangan aktivitas, diukur pengaruhnya terhadap sasaran bisnis dan dievaluasi

Tabel 1. Level dan Process Attribute dari Process Capability

Berdasarkan Tabel 2.1. maka penjelasan untuk setiap level menurut ISO/IEC 15504 adalah sebagai berikut:

a. Level 0 - *Incomplete Process*

   Level 0 dimana pada tingkat ini proses manajemen tidak ada sama sekali, tidak ada pengetahuan tentang pentingnya manajemen sumber daya manusia dan TI dengan perencanaannya.

b. Level 1 - *Performed Process* (satu atribut)

Level 1 dimana pada tingkat ini proses bersifat tidak terorganisir. Manajemen mengetahui akan kebutuhan sumber daya dan TI tetapi tidak diformalisasikan pada suatu proses yang terencana

c. Level 2 - *Managed Process* (dua atribut)

Level 2 dimana pada tingkat ini proses sudah mengikuti pola yang teratur. Terdapat pemahaman kebutuhan untuk manajemen sumber daya dan TI. Sehingga dalam proyek kebutuhan-spesifik menerapkan sumber daya dan TI. Level 2 ini terdapat dua parameter yang diukur yaitu PA 2.1. Manajemen Kerja untuk mengukur sejauh mana kinerja proses dikelola, dan PA 2.2 Manajemen Work Product untuk mengukur sejauh mana Work Product yang dihasilkan oleh proses telah dikelola dengan tepat. Work Product (atau hasil dari proses) terdefinisikan dan terkontrol.

d. Level 3 - *Established Process* (dua atribut)

Level 3 dimana pada tingkat ini proses terdokumentasi dan dikomunikasikan/dijelaskan. Proses untuk pengaturan sumber daya dan TI telah dikembangkan. Terdapat suatu pendekatan straegi untuk menyewa dan mengatur personil TI dan rencana pelatihan formal yang di desain untuk menemukan kebutuhan-kebutuhan bisnis dari sumber daya. Pengembangan program yang rotasional didesain untuk memperluas skil manajemen teknikal dan bisnis yang dibangun. Terdapat 2 parameter yang dinilai dalam level 3. Parameter pertama yaitu, PA 3.1 Pendefinisian proses untuk mengukur sejauh mana standar dipelihara untuk mendukung penyebaran proses yang ditentukan. Parameter kedua yaitu, PA 3.2 Process Deployment untuk mengukur sejauh mana proses standar diterapkan secara efektif sebagai proses yang telah ditetapkan untuk mencapai hasil prosesnya.

e. Level 4 - *Predictable Process* (dua atribut),

Level 4 dimana pada tingkat ini proses dimonitor dan diukur. Sebuah organisasi/institusi ada tanggung jawab untuk pengembangan dan pemeliharaan dari suatu rencana manajemen sumber daya dan TI yang

diberikan kepada tenaga ahli khusus. Organisasi/Institusi memiliki ukuran standarisasi untuk mengatur proses bisnisnya dan mengidentifikasi penyimpanan-penyimpanan dari rencana yang mungkin terjadi. Level 4 ini terdapat dua parameter yang akan ukur. Parameter pertama PA 4.1 Pengukuran proses untuk mengukur sejauh mana hasil pengukuran digunakan untuk memastikan bahwa kinerja prosesnya mendukung tujuan kinerja proses yang relevan untuk mendukung tujuan bisnis yang ditetapkan. Parameter yang kedua PA 4.2 Pengendalian Proses untuk mengukur sejauh mana proses secara kuantitatif dikelola untuk menghasilkan sebuah proses yang stabil, memiliki kemampuan dan dapat diprediksi dalam batasan yang telah ditentukan.

f. Level 5 - *Optimized Process* (dua atribut)

Level 5 dimana pada tingkat ini organisasi/institusi memiliki rencana manajemen sumber daya TI yang efektif sehingga dapat digunakan untuk memenuhi kebutuhan dan mendukung bisnis. Manajemen sumber daya manusia TI diintegrasikan dengan perencanaan teknologi sehingga dapat digunakan dan dikembangkan secara optimal. Level 5 ini terdapat dua parameter yang diukur. Parameter pertama PA 5.1 Inovasi Proses untuk mengukur sejauh mana perubahan proses diidentifikasi dari analisis penyebab umum dari terjadinya variasi kinerja, dan dari penyelidikan pendekatan inovatif terhadap pendefinisian dan penerapan proses. Parameter kedua PA 5.2 Proses optimasi untuk mengukur tingkat perubahan terhadap definisi, pengelolaan, dan kinerja proses menghasilkan dampak efektif sehingga mencapai sasaran peningkatan proses yang relevan.