Analisis Audit Sistem Informasi Berbasis COBIT 5 Pada Domain *Deliver, Service, and Support (DSS)* (Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)

Tugas Akhir

Diajukan untuk memenuhi sebagian dari syarat
untuk memperoleh gelar Sarjana Teknik
Telkom Engineering School
Telkom University

Analysis-Based Information Systems Audit COBIT 5 In the Domain Deliver, Service, and Support (DSS) (Case Study: SIM-BL in unit CDC PT Telkom Centre. Tbk)

Achyar Al-Rasyid
1103091159

Program Studi Sarjana Teknik Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2015

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul ”Analisis Audit Sistem Informasi Berbasis COBIT , pada Domain *Deliver, Service, and Support (DSS)* (Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)” beserta seluruh isinya adalah benar-benar karya saya sendiri dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/ sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, 6 Mei 2015

Yang membuat pernyataan,

Achyar Al-Rasyid

NIM : 113091159

LEMBAR PENGESAHAN

Analisis Audit Sistem Informasi Berbasis COBIT 5
Pada Domain *Deliver, Service, and Support* (DSS)
(Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)

Analysis-Based Information Systems Audit COBIT 5
In the Domain Deliver, Service, and Support (DSS)
(Case Study: SIM-BL in unit CDC PT Telkom Centre. Tbk)

Achyar Al-Rasyid
NIM : 1103091159

Proposal ini diajukan sebagai usulan pembuatan Tugas Akhir pada Program Studi
Sarjana Teknik Informatika
Fakultas Informatika
Telkom University

Bandung, 1 Juni 2015
Menyetujui

Pembimbing 1	Pembimbing 2
Imelda Atastina, S.Si., MT.	Bambang Subagjo
NIP : 07770396-1	NIK : 621484

ABSTRAK

Teknologi informasi (TI) telah menjadi unsur penting dalam suatu organisasi dan merupakan investasi yang menjadi salah satu pembuat nilai tambah dan keuntungan kompetitif. TI perlu diatur agar dapat dimanfaatkan dengan baik. Tindakan untuk mengatur TI disebut dengan tata kelola TI. Tata kelola TI yang dijalankan dengan baik dapat membantu organisasi dalam upaya mencapai tujuannya. Tata kelola TI itu sendiri memerlukan audit yang bertujuan untuk mengevaluasi dan memastikan pemenuhannya ditinjau dari pendekatan objektif dari suatu standar. Unit *Community Development Centre* (CDC) PT Telkom merupakan salah satu organisasi yang mengimplementasikan tata kelola TI yaitu dengan Sistem Informasi Manajemen Bina Lingkungan (SIM-BL) untuk membantu merealisasikan sasaran dan mencapai tujuan mengenai pengelolaan dan penyaluran dana bantuan sosial perusahaan kepada masyarakat melalui pemanfaatan TI. Tata kelola TI dalam aplikasi SIM-BL memerlukan audit untuk mengevaluasi, menilai kapabilitas, dan menyusun rekomendasi terhadap tata kelola TI-nya karena unit aplikasi SIM-BL pada Unit CDC PT Telkom belum pernah melakukan evaluasi terhadap tata kelola TI tersebut yang telah diterapkan dari sisi kemajuan mencapai tujuan serta nilai tata kelola dan manajemen teknologi informasi. Sehingga sampai saat ini unit CDC PT Telkom belum dapat mengetahui sejauh mana manfaat dan dampak yang diperoleh dari penerapan TI tersebut terhadap progresivitas pencapaian tujuan dikaitkan dengan pengelolaan sistem informasi, apa yang menjadi kekurangan, serta apa tawaran solusinya. Standar audit yang digunakan adalah *Control Objectives for Information and Related Technology* (COBIT) 5. COBIT 5 merupakan *framework* yang komprehensif dan bersifat holistik sehingga sesuai dengan SIM-BL yang berskala *enterprise* dan menjalankan tata kelola TI yang sudah berjalan. Domain COBIT 5 yang dipilih adalah domain *Deliver, Service,* dan *Support* (DSS) yang fokus pada penilaian pengiriman dan layanan teknologi informasi serta dukungannya terhadap proses bisnis yang berlangsung termasuk pengelolaan masalah agar keberlanjutan proses bisnis tetap terjaga serta bagaimana mengontrol proses bisnis, mengevaluasi, dan merencanakan secara jangka panjang proses bisnis kedepan. Hasilnya adalah *Capability Level* yang didapat secara keseluhan pada SIM-BL Unit CDC PT Telkom adalah *Level* 4, yaitu *Predictable Process,* dan *Level* target yang ingin dicapai adalah 5 yaitu *Optimizing process*, sehingga berdasarkan analisis *gap* secara garis besar perlu adanya peningkatan *Capability Level* dari kondisi *existing* dari sisi peningkatan aktivitas dengan rekomendasinya yaitu memaksimalkan yang sudah berjalan baik dan melakukan inovasi dalam aktivitas untuk mempercepat tercapainya tujuan

Kata kunci : audit tata kelola teknologi informasi, COBIT 5, domain DSS, *Capability Level*, analisis *gap*, kondisi *existing*, rekomendasi

ABSTRACT

Information technology (IT) has become an important element in organization and investment that became one of the makers added value and competitive advantage. IT needs to be set to be put the good result, measures to regulate IT named governance IT. IT governance is executed properly can assist the organization in achieving their objectives. IT governance itself requires an audit that aims to evaluate and ensure compliance in terms of the objective of a standard approach. Unit Community Development Centre (CDC) PT Telkom is one of the organizations that implement IT governance with the Community Development Management Information System (MIS-BL) to help realize the objectives goals of the management and distribution of social aid fund company to the public through the use of Information Technology. IT governance in SIM-BL applications require audit to evaluate, assess capabilities, and make a recommendation to their IT governance, because unit-BL SIM application on CDC Unit PT Telkom has never been evaluated to their IT governance that have been applied from the side progress toward meeting the goals and values of governance and management of information technology. So far CDC unit PT Telkom has not been able to determine the extent of the benefits and impacts derived from the application of IT to the progression of the achievement of goals associated with the management of information systems, what the shortfall, as well as what the solution offer. Audit standard that used was COBIT 5. COBIT 5 framework is a comprehensive and holistic in accordance with the SIM-BL-scale enterprise and to run the IT governance that already running. Selected COBIT 5 domains are domains Deliver, Service, and Support (DSS) that focuses on the assessment and delivery of information technology services and support to business processes that take place including the management of sustainability issues so that business processes remain intact as well as how to control business processes, evaluate, and long-term planning of future business processes. The results are obtained Capability overall Level on SIM-BL Unit CDC PT Telkom is Level 4, which Predictable Process, and the target Level to be achieved 5 that is Optimizing process, so based on gap analysis outlined, need an improvement of the condition in Capability Level existing terms to increased activity with its recommendations is to maximize that already running well and to innovate in activities to accelerate the achievement of goals.

Keywords: audit of information technology governance, COBIT 5, the domain DSS, Capability Level, gap analysis, existing condition, recommendation

LEMBAR PERSEMBAHAN

Pada kesempatan ini saya ingin menyampaikan rasa terima kasih yang tulus kepada berbagai pihak yang telah membantu dan memberikan dukungan kepada saya dalam pengerjaan Tugas Akhir ini, dan khususnya yang pertama untuk Yang Maha Mengetahui dan Maha Kuasa Allah SWT, saya mengucapkan rasa syukur yang tiada henti karena dengan kehendak-Nya, saya dapat menyelesaikan Tugas Akhir ini dengan lancar. Saya ingin mengucapkan terima kasih juga kepada:

1. Nabi Muhammad, Sang Revolusioner Peradaban
2. Ibu saya : Penti Supiantini yang selalu sabar dalam mengingatkan
3. Ayah saya : Drs. H. Asep Hermawan, MH. yang selalu mendukung setiap aktivitas
4. Nakeisha Zahra Aliya, adik sepupu saya yang selalu menjadi hiburan di rumah
5. Seluruh keluarga besar alm. Bapak H. Subarna Wijaya dan alm. Ibu Hj. Atikah : Uwak-uwak dan seluruh kakak sepupu
6. Seluruh keluarga besar alm. KH. R. A. Memed dan Ibu Hj. Nonok Rokayah : Uwak-uwak, bibi, paman, dan sepupu
7. Dosen Pembimbing I saya : Ibu Imelda Atastina yang telah memberikan bimbingannya
8. Pembimbing II saya : Bapak Subagjo yang telah memberikan bimbingannya
9. Bapak Herry, SM BL PT Telkom Unit CDC PT Telkom, Bapak Shoheh Officer I BL Unit CDC PT Telkom
10. Bapak Hadary Mallafi, Unit ITSS yang telah berkenan diawawancarai memberikan data
11. Bapak Nazaruddin, Telkom Sigma, yang telah berkenan diwawancarai dan memberikan data
12. Bapak Ahmad Tri Hanuranto, Rektor IT Telkom terakhir banyak memberikan saya inspirasi, nasehat, dan semangat
13. Bapak Heroe Wijanto, Wakil Rektor Telkom University, banyak memberikan saya inspirasi, nasehat, dan semangat
14. Zartikazahra Nurulfiqri, yang telah memberikan dorongan semangat hingga TA dapat selesai
15. Seluruh teman-teman kelas IF 33-05 yang sudah lebih dulu lulus dan terus mengingatkan
16. Seluruh teman-teman aktivis mahasiswa HMI Komisariat IT Telkom, HMI Cabang Bandung, HMIF 2010, teman-teman aktivis BEM KBM IT Telkom
17. Seluruh teman-teman aktivis dan senior aktivis yang tidak bisa disebutkan satu per satu

KATA PENGANTAR

Bismillahirrohmanirrohiim.

Assalamu'alaikum wr. wb.

Puji dan syukur saya panjatkan kepada kehadirat Allah SWT yang selalu memberikan nikmat yang tiada henti serta hidayah dan kuasa-Nya dalam membimbing umat-Nya, serta tauladan bagi umat manusia Rasulullah SAW, sehingga penulis dapat menyelesaikan tugas akhir dengan **"**Analisis Audit Sistem Informasi **Berbasis COBIT , pada Domain *Deliver, Service, and Support (DSS)* (Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)"** sebagai salah satu syarat kelulusan program pendidikan Sarjana Teknik Informatika *Telkom University.*

Saya mengucapkan terimakasih kepada segenap pihak yang telah membantu dan memberikan dukungan terhadap saya serta motivasi yang tiada henti dalam proses pengerjaan Tugas Akhir ini. Saya menyadari bahwa penulisan buku Tugas Akhir ini masih belum sempurna. Oleh karena itu diharapkan mendapat masukan, baik saran maupun kritik dari berbagai pihak demi kesempurnaan Tugas Akhir ini. Semoga buku Tugas Akhir ini dapat bermanfaat bagi kemajuan penelitian segenap masyarakat dan khususnya seluruh civitas akademika *Telkom University*

Wassalamu'alaikum wr. wb.

Bandung, 6 Mei 2015

Penulis

Achyar Al-Rasyid

NIM : 113091159

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

PT Telkom memiliki Sistem Informasi Manajemen Bina Lingkungan (SIM BL) yang diharapkan dapat menjadi role model bagi seluruh BUMN maupun pembina dan pelaksana Bina Lingkungan (BL) dalam penyaluran dana publik. Namun, unit *Community Development Centre* (CDC) PT Telkom belum pernah melakukan evaluasi terhadap Sistem Informasi/Teknologi Informasi (SI/TI) yang telah diterapkan dari sisi kemajuan mencapai tujuan serta nilai tata kelola dan manajemen teknologi informasi. Sehingga sampai saat ini unit CDC PT Telkom belum dapat mengetahui sejauh mana manfaat dan dampak yang diperoleh dari penerapan SI/TI tersebut terhadap progresivitas pencapaian tujuan dikaitkan dengan pengelolaan sistem informasi, apa yang menjadi kekurangan, serta apa tawaran solusinya.

Ada beberapa standar yang dikembangkan peneliti mengenai penerapan teknologi informasi. Standar tersebut adalah *Control Objectives for Information and Related Technology* (COBIT) 5 dan *Information Technology Infrastructure Library* (ITIL). ITIL berfokus pada layanan untuk pelanggan dan tidak memberikan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan [7]. COBIT 5 merupakan standar komprehensif yang membantu perusahaan dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif. COBIT 5 menyediakan kerangka kerja *IT Governance* dan *control objectives* yang rinci bagi manajemen, pemilik proses bisnis, pemakai dan *auditor*, karena mengelola TI secara *holistic* sehingga nilai yang diberikan oleh TI dapat tercapai optimal dengan memperhatikan segala aspek tata kelola teknologi informasi mulai dari sisi *people, skills, competencies, services, infrastructure,* dan *applications* yang merupakan bagian dari *enabler* suatu tata kelola teknologi informasi [12]. Oleh karena itu COBIT 5 sesuai dan dapat membantu dalam mengaudit tata kelola teknologi informasi dengan tidak terpusat hanya pada masalah teknis dalam teknologi saja tetapi juga melihat sumber daya lain yang menjadi penggerak tata kelola teknologi informasi menuju tujuan organisasi.

Domain *Deliver, Service, and Support* (DSS) dipilih karena sesuai dengan kondisi tata kelola TI di Unit CDC PT Telkom yang diaplikasikan pada produk SIM-BL saat ini, yang telah direncanakan (*plan*), telah dibangun (*build*), dan sekarang sedang dijalankan (*run*) juga SIM-BL sangat berpatokan terhadap *workflow* dan *business process* dikarenakan berkaitan dengan penyaluran bantuan milik publik. Beberapa domain lain seperti *Align, Plan, and Organize* (APO) akan lebih sesuai jika diterapkan pada tata kelola TI yang belum dijalankan atau masih bersifat baru, domain *Build, Acquire, and Implement* (BAI) akan lebih sesuai jika diterapkan pada suatu unit yang khusus berperan sebagai pembangun (*developer*) atau jika ada intensi memperbaiki tata kelola TI yang telah dibangun dalam segi yang lebih teknikal, domain *Monitor, Evaluate and Asses* (MEA) akan lebih

sesuai jika tata kelola TI telah dibangun dan telah berjalan, serta pelaksanaan *monitoring* dilakukan oleh pihak internal, mengingat *monitoring* dengan audit mempunyai intensitas berbeda, *monitoring* lebih sering dilakukan dalam jangka waktu tertentu daripada audit sehingga MEA akan lebih sesuai untuk *monitoring*, bukan audit. [19] Dengan kondisi tata kelola TI di Unit CDC PT Telkom sekarang yang berada di area *run* yaitu sedang berjalan dengan diaplikasikannya SIM-BL dan kebutuhan unit CDC PT Telkom untuk mengirimkan layanan, melayani permintaan, dan mendukung keberlanjutan tata kelola TI, maka domain DSS adalah domain terpilih karena hal-hal tersebut sesuai dan tercakup di dalam domain DSS.

Audit efekivitas sistem dilakukan setelah suatu sistem berjalan beberapa waktu sampai manajemen mendapatkan evaluasi ataupun masukan untuk mengambil keputusan apakah kinerja sistem layak dipertehankan, harus ditingkatkan, atau perlu dimodifikasi atau sistem sudah baik. Audit seperti ini dilakukan ketika manajemen meminta auditor untuk melakukan audit guna menentukan sejauh mana sistem telah mencapai tujuan yang ditetapkan. Audi juga dapat dilakukan secara berkala. [22]

Dan langkah audit ini semata-mata demi semakin terwujudnya keselarasan kondisi SI/TI dengan tujuan unit CDC PT Telkom. Oleh karena itu, penulis menjadikan hal ini sebagai objek penelitian tugas akhir yang berjudul *"Analisis Audit Sistem Informasi Berbasis COBIT 5 Pada Domain Deliver, Service, and Support (DSS) (Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)".*

1.2 Rumusan Masalah

Beberapa permasalahan yang diteliti sehubungan dengan analisis COBIT 5 pada domain *Deliver, Service, and Support (DSS)* SI/TI pada SIM-BL Unit CDC PT Telkom, adalah sebagai berikut :

1. Bagaimana penerapan audit tata kelola TI pada SIM-BL Unit CDC PT Telkom berdasarkan domain DSS COBIT 5?
2. Bagaimana nilai *capability Level* dan rekomendasi berdasarkan hasil audit untuk diberikan kepada pihak Unit CDC PT Telkom terkait tata kelola TI pada domain DSS COBIT 5 pada SIM-BL?

1.3 Batasan Masalah

Adapun batasan masalah dalam tugas akhir ini diantaranya sebagai berikut:

a) Penelitian dilaksanakan pada sistem yang sedang berjalan baik dari segi aplikasi, infrastruktur, *service*, dan manajemen pada SIM-BL terutama yang menyangkut dengan kegiatan operasional Unit CDC PT Telkom.
b) Standar yang digunakan sebagai standar audit adalah COBIT 5 domain DSS.
c) Penelitian ini hanya menghasilkan rekomendasi solusi SI/TI yang dapat diterapkan pada SIM-BL, namun tidak sampai dilakukan pembuatan dokumen rancangan usulan SI/TI tersebut juga tidak sampai tahap implementasi aplikasi baru

d) Penelitian dilakukan pada Unit CDC PT Telkom, Tbk pusat, Jln. Japati no. 1 Kota Bandung

1.4 Tujuan

Tujuan yang diharapkan penulis dapat tercapai pada pembuatan tugas akhir ini diantaranya :

1. Mengetahui kondisi performansi tata kelola teknologi informasi pada SIM-BL Unit CDC PT Telkom berdasarkan domain DSS COBIT 5.
2. Menilai *Level* kapabilitas proses dan memberi rekomendasi berdasarkan temuan-temuan audit pada domain DSS COBIT 5 sebagai dasar-dasar perbaikan dan pengembangan tata kelola teknologi informasi pada SIM-BL Unit CDC PT Telkom

1.5 Metodologi Penyelesaian Masalah

Metode yang digunakan untuk menyelesaikan permasalahan pada Tugas Akhir ini adalah sebagai berikut:

a) Studi Literatur
   Melakukan pencarian referensi serta berbagai sumber lain yang digunakan sebagai penunjang dan acuan dalam proses pengerjaan tugas akhir ini. Mencari uraian-uraian tentang teori COBIT 5 dan beberapa teori pendukung lainnya yang digunakan penulis.

b) Pembuatan Draft Pertanyaan Wawancara dan Kuesioner
   Melakukan pembuatan poin – poin dari tiap aturan teori COBIT 5, khususnya domain *Deliver, Service, and Support* (DSS) yang perlu ditanyakan terhadap responden. Penentuan pertanyaan berdasarkan hasil *breakdown* teori COBIT 5. Pertanyaan ini dibutuhkan untuk mengetahui gambaran umum SIM-BL Unit CDC PT Telkom, arahan strategis perusahaan, pelayanan yang berlangsung, proses bisnis yang berlangsung, serta pertanyaan dalam kuesioner dibuat berdasarkan aktivitas-aktivitas yang telah tercantum dari tiap domain DSS01-DSS06

c) Pengumpulan Data
   Dilakukan dengan wawancara dan menyebar kuesioner. Wawancara yang dilakukan kepada Senior Manager Bina Lingkungan (SM-Bina Lingkungan / SM-BL) CDC PT Telkom, Manager Sistem Informasi Bagian Perencanaan dan Pengendalian (PRANDAL) CDC PT Telkom, *Officer* I Bagian Bina

Lingkungan, *Person In Charge* (PIC) SIM-BL Divisi *IT Service & Solution* (ITSS), PIC SIM-BL Telkom Sigma terkait kondisi dan arahan strategis beserta informasi-informasi yang dibutuhkan lainnya. Kuesioner diberikan kepada staff di Bagian PRANDAL Unit CDC PT Telkom, Unit ITSS, dan Telkom Sigma. Kuesioner ini diperlukan untuk mengetahui SIM-BL Unit CDC PT Telkom, yaitu mengenai DSS01 – Mengelola Operasi, DSS02 – Mengelola Permintaan Layanan dan Insiden, DSS03 – Mengelola Masalah, DSS04 – Mengelola Keberlanjutan, DSS05 – Mengelola Keamanan Layanan, dan DSS06 – Mengelola Kontrol Proses Bisnis

d) Proses Analisis Hasil
Analisis dilakukan pada hasil kuesioner dan pembobotan. Hasil dari perhitungan kuesioner dan penelitian akan direkap menggunakan *microsoft excel* serta penyajian diagram, setelah itu diperoleh *Capability Level* dari kondisi *existing* yang berikutnya dilakukan analisis *gap* kemudian dilanjutkan dengan rekomendasi

e) Penarikan Kesimpulan
Menarik kesimpulan dari hasil analisis yang didapat sehingga kelayakan dan perbaikan yang seharusnya dilakukan dapat diketahui.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

1. PENDAHULUAN
   Bab ini berisi uraian tugas akhir secara umum, meliputi latar belakang, rumusan masalah, tujuan, manfaat penelitian, batasan masalah, metodologi, dan sistematika penulisan.

2. LANDASAN TEORI
   Bab ini berisi mengenai teori-teori penunjang yang digunakan dalam penyelesaian tugas akhir.

3. METODOLOGI DAN IMPLEMENTASI
   Bab ini menjelaskan gambaran umum bagaimana proses penelitian yang akan dilakukan dan berisi langkah-langkah implementasi penelitian.

4. ANALISIS HASIL
   Bab ini berisi identifikasi dan analisis hasil penelitian berupa kondisi *existing*, analisis *gap* dan juga berisi rekomendasi.

5. KESIMPULAN DAN SARAN
   Bab ini berisi kesimpulan dari seluruh analisis yang telah dijalankan dan saran yang diperlukan untuk pengembangan tugas akhir lebih lanjut.

BAB II
TINJAUAN PUSTAKA

2.1 Konsep Dasar Sistem Informasi

Menurut *Robert A. Letch dan K Roscoe Davis*, "Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung informasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan." [16]

2.2 Definisi *IT Governance*

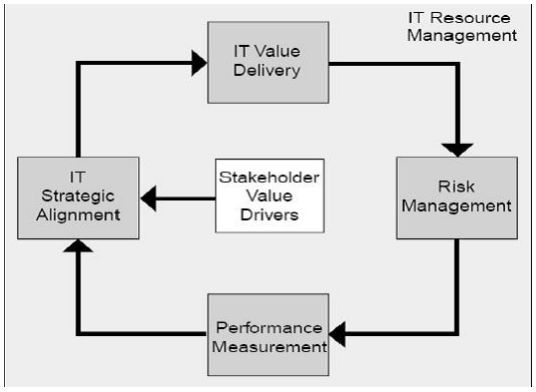
IT Governance adalah istilah yang menguraikan bagaimana suatu organisasi mengendalikan dan mengurus sumber daya TI dengan mempertimbangkan TI dalam pengawasan, monitoring, kendali, dan petunjuk terhadap sumber daya TI dan bagaimana TI diterapkan didalam entitas yang akan mempunyai suatu dampak yang besar terhadap pencapaian visi, misi, dan tujuan strategis suatu organisasi. [10]

Menurut ISACA (2000) [17], *IT Governance* adalah struktur yang terbentuk, hubungan dan proses untuk mengarahkan dan mengendalikan organisasi dalam rangka mencapai tujuan organisasi dengan cara menambahkan nilai melalui penyeimbangan antara resiko dan hasil pada TI dan prosesnya.
Sementara itu menurut *IT Governance Institute* (2000) [18], *IT Governance* deidefinisikan sebagai tanggungjawab eksekutif dan dewan direktur, dan terdiri atas kepemimpinan, struktur organisasi serta proses-proses yang memastikan TI perusahaan mendukung dan memperluas obyektif dan strategi organisasi.

Berdasarkan definisi-definisi tersebut, dapat disimpulkan bahwa penekanan *IT Governance* adalah pada penyelarasan antara TI dengan tujuan bisnis suatu perusahaan dimana ada kaitannya dengan kewenangan *top-Level management.* [10]

2.2.1 Fokus Area *IT Governance*

Ada lima area fokus yang terdapat pada *IT Governance* seperti yang terlihat pada Gambar:



Gambar 2. 1 Fokus Area Tata Kelola TI [3]

1. *Strategic Alignment*
   Fokus :
   a. Memastikan hubungan bisnis dengan perencanaan strategi TI, dan
   b. Penyelenggaraan operasional TI dengan operasional perusahaan secara keseluruhan.
2. *Value Delivery*
   Fokus :
   a. Mengoptimalkan biaya dan pembuktian nilai intrinsiknya
   b. Melaksanakan proporsi dan nilai seluruh siklus penyampaian
3. *Risk Management*
   Fokus :
   a. Titik beratnya ada pada proses-proses untuk memelihara nilai
   b. Identifikasi resiko, mitigasi resiko, dan menerapkan berbagai pengendalian
4. *Resource Management*
   Fokus :
   a. Pengoptimalan investasi, pengetahuan, dan infrastruktur
   b. Menentukan manajemen yang sesuai
5. *Performance Measurement*
   Fokus pada melakukan evaluasi dan penilaian. Kemudian membuktikan bahwa kebijakan telah ditetapkan

2.3 Manfaat Tatakelola Teknologi Informasi

Tatakelola teknologi informasi yang efektif akan memberikan manfaat yang sangat besar bagi perusahaan. Dengan adanya tatakelola teknologi informasi, maka perusahaan akan semakin mudah dalam pengelolaan manajemen, sehingga visi-misi perusahaan, tujuan bisnis, serta pelayanan yang baik akan dapat terwujud. Selain itu, resiko yang merupakan keniscayaan bagi tiap proses bisnis, akan mudah ditangani. [10]

2.4 Tata Kelola Korporasi (*Enterprise Governace)*

Tata kelola adalah kumpulan dari cara dan aturan untuk menjalankan sebuah prosedur serta standar operasional dalam mencapai suatu tujuan strategis. Istiliah yang perlu diketahui adalah *enterprise governace* yang dipakai dalam menjalankan organisasi. Dengan adanya standarisasi dalam *enterprise governance*, diharapkan organisasi dapat berjalan lebih transparan dan lebih mengutamakan kebutuhan *stakeholder* sehingga mencapai keuntungan serta cara kerja yang efektif [4].

Enterprise governance sendiri dilatar belakangi ketika terjadinya resersi di Amerika Serikat sehingga membuat para investor kehilangan rasa kepercayaannya terhadapat organisasi ataupun perusahaan yang ada saat itu. Dengan adanya *enterprise governance* yang baik diharapkan tingkat kepercayaan serta perlindungan investasi lebih terjamin.

Enterprise governance inipun belum mempunyai bentuk ataupun model yang spesifik agar bisa digunakan seragam diseluruh bagian usaha. *Enterprise governance* ini harus dirancang sesuai dengan kondisi sumber daya yang ada pada

organisasi ataupun negara tertentu. Beberapa bagian yang diperhatikan pada *enterprise governance* adalah [4]:

1. Akuntabilitas dan kepercayaan secara hukum.
   Dalam hal ini *enterprise governace* mengimplementasikan petunjuk dan mekanisme untuk memastikan manajemen menjalankan niat baik dan organisasi publik terlindungi dari perbuatan yang salah ataupun penipuan.

2. Cara pandang ekonomi yang efesien.
   Dalam hal ini melibatkan bagaimana sistem *enterprise governance* bertujuan untuk mencapai hasil optimal sehingga memenuhi tujuan yang diinginkan.

3. Cara pandang strategis yang efesien.
   Hal ini melibatkan kebijakan umum yang secara tidak langsung mengukur keadaan ekonomi seperti kemiskinan, akses pasar, kestabilan pendapatan, pelayanan kesehatan serta penciptaan lapangan kerja.

4. Cara pandang *stakeholder*.
   Lingkup ini memperhatikan kebutuhan dari *stakeholder* yang berhubungan. Tata kelola korporasi akan diturunkan menjadi tata kelola teknologi informasi yang difokuskan pada pengaturan penggunaan teknologi informasi pada perusahaan yang berjalan.

2.5 Audit Tata Kelola Teknologi Informasi

Dalam Dian, menurut Gondodiyoto, audit adalah proses pengumpulan dan penilaian bahan bukti tentang informasi untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan dan dilakukan oleh orang berkompeten dan independen [2].

Pengertian audit secara umum dapat disederhanakan sebagai berikut : audit adalah kegiatan mengumpulkan informasi faktual dan signifikan melalui interaksi (pemeriksaan, pengukuran, dan penilaian serta penarikan kesimpulan) secara sistematis, objektif dan terdokumentasikan yang berorientasi pada azas nilai manfaat. Sekarang ini jenis audit telah berkembang mencakup berbagai Bagian atau fungsi yang ada dalam organisasi, antara lain audit manajemen, audit operasional, audit mutu, audit keuangan, audit sistem informasi audit komunikasi, audit lingkungan, audit pemasaran, dan audit sumber daya manusia [14].

Audit eksternal adalah audit yang dilakukan oleh auditor eksternal dari pihak eksternal atau dari institusi independen. Audit dilaksanakan berdasarkan azas-azas formal/standar kriteria tertentu yang digunakan sebagai acuan untuk menilai. Hasil penilaian dikeluarkan oleh institusi independen tersebut berdasarkan data dan informasi yang diperoleh dari proses audit. Pernyataan auditor eksternal tersebut adalah kesimpulan yang dijadikan dasar bagi perusahaan maupun pihak-pihak lain yang berkepentingan untuk mengambil keputusan [14]. Esensi dari audit adalah:

1) Audit adalah proses interaktif

2) Audit adalah kegiatan yang dilakukan secara sistematis
3) Audit dilakukan dengan azas manfaat dan tujuan
4) Audit dilakukan secara objektif/independen
5) Audit berpijak pada data/fakta & kebenaran
6) Audit melibatkan proses analisis/evaluasi/penilaian/pengujian
7) Audit bermuara pada pengambilan keputusan
8) Audit dilaksanakan berdasarkan azas-azas/standar tertentu
9) Audit merupakan kegiatan berulang
10) Audit menghasilkan laporan [14].

Tujuan audit adalah mendapatkan informasi faktual dan signifikan berupa data hasil analisa, penilaian, rekomendasi auditor yang dapat digunakan oleh *auditee* atau manajemen untuk berbagai keperluan misalnya untuk dasar pengambilan keputusan, pengendalian manajemen, perbaikan dan/atau perubahan dalam berbagai aspek dalam upaya mengamankan kebijakan dan mencapai tujuan organisasi secara keseluruhan [14].

Dalam penelitian Vlasta, Ron Weber menyatakan beberapa alasan penting mengapa audit TI perlu dilakukan, antara lain:

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan
3. Risiko kebocoran data
4. Penyalahgunaan komputer
5. Kerugian akibat kesalahan proses perhitungan
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer [15].

Dari definisi tata kelola teknologi informasi dan definisi audit yang telah dijabarkan di atas maka bisa ditarik kesimpulan bahwa audit tata kelola teknologi informasi adalah kegiatan mengumpulkan informasi faktual dan signifikan melalui interaksi (pemeriksaan, pengukuran, dan penilaian serta penarikan kesimpulan) secara sistematis, objektif dan terdokumentasikan terhadap pengendalian infrastruktur teknologi secara menyeluruh, memastikan adanya alokasi penggunaan TI dan memastikan bahwa TI menopang dan mengembangkan strategi-strategi dan tujuan perusahaan, dimana audit dilaksanakan berdasarkan azas-azas formal/standar kriteria tertentu yang digunakan sebagai acuan untuk menilai.

2.6 Pengertian COBIT

Control Objectives for Information and Related Technology (COBIT) telah menjadi standar global untuk *IT Governance*, dibuat oleh ISACA dan ITGI pada tahun 1996 [8]. COBIT pertama kali dirilis pada tahun 1996 yaitu COBIT versi 1. Pada tahun 1998, versi 2 dirilis dengan penambahan *Management Guidelines*. Pada tahun 2000, versi 3 dirilis. Pada bulan Desember tahun 2005, versi 3 dirilis dan pada bulan Mei tahun 2007, versi 4.1 yang merupakan revisi dirilis. COBIT 5 dirilis pada bulan April tahun 2012 [15].

COBIT adalah kerangka *IT governance* yang ditujukan kepada manajemen, staf pelayanan TI, *control departement*, fungsi audit dan lebih penting lagi bagi

pemilik proses bisnis (*business process owners*), untuk memastikan *confidentiality, integrity dan availability* data serta informasi sensitif dan kritikal [7]. COBIT telah berkembang menjadi *IT Governance framework* yang paling signifikan dan juga cocok digunakan untuk audit karena COBIT menyediakan pedoman komprehensif di lingkungan proses-proses TI dan hubungannya dengan tujuan bisnis [13].

COBIT adalah sekumpulan dokumentasi *best practices* untuk *IT Governance* yang dapat membantu auditor, pengguna *(user),* dan manajemen, untuk menjembatani *gap* antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. COBIT bermanfaat bagi auditor karena merupakan teknik yang dapat membantu dalam identifikasi IT *control issues.* Adapun menurut ISACA standar untuk audit sistem informasi adalah [5]:

Tabel 2. 1 Standar Audit Sistem Informasi ISACA

010	*Audit Chapter*
010.010	*Responsibility, Authority and Accountability* Definisi dari tanggungjawab, otoritas, dan *accountability* dari fungsi audit sistem informasi lebih tepat bila didokumnetasikan dalam surat perjanjian.
020	*Independence*
020.010	*Profesional Independence* Dalam permasalahan yang berkaitan dengan audit, auditor sistem informasi harus bersikap independen dalam tingkah laku dan tindakannya.
020.020	*Organizational Relationship* Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektivitas dari suatu proses.
030	*Profesional Ethics and Standards*
030.010	*Code of Profesional Ethics* Auditor dari sistem informasi harus menghormati dan manaati etika profesional dari ISACA.
030.020	*Due Profesional Core* Standar *auditing* profesional harus diterapkan dalam segala aspek dalam pekerjaan yang dilakukan oleh auditor sistem informasi.
040	*Competence*
040.010	*Continuing Professional Education*
040.020	Auditor sistem informasi harus memaintain kompetensi teknikal

	melalui pendidikan lanjut profesional.
050	*Planning*
050.010	*Audit Planning* Auditor sistem informasi harus merencanakan perencanaan audit sistem untuk menempatkan tujuan audit dan untuk melengkapi standar profesioanl audit.
060	*Performance of Audit Work*
060.010	*Supervision* Staf dari audit sistem informasi harus tepat untuk dapat menjamin tujuan dari audit dijalankan dan standar profesional *auditing* dapat terpenuhi.
060.020	*Evidence* Selama masa pekerjaan audit, auditor sistem informasi harus mendapatkan bukti yang tepat, dapat dipercaya, relevan dan berguna untuk mencapai tujuan objektif dari suatu audit.
070	*Reporting*
070.010	*Report Content and Form* Auditor sistem informasi harus menyediakan *report* dalam bentuk yang tepat pada saat penyelesaian tugas audit. Laporan Audit berupa ruang lingkup, tujuan, periode audit, dan lingkungan dimana audit dijalankan. Laporan audit harus mengidentifikasikan permasalahan yang terjadi dalam jangka waktu audit. Laporan audit juga untuk memberikan rekomendasi dari layanan atau kualifikasi yang diberikan auditor terhadap tugas audit yang dijalankan.
080	*Follow Up Activities*
080.010	*Follow Up* Auditor sistem informasi harus meminta dan mengevaluasi informasi yang sesuai dari penemuan yang terdahulu dan rekomendasi yang dihasilkan pada periode audit terdahulu untuk mendefinisikan tindakan yang tepat yang harus diimplementasikan dalam satu periode waktu.

2.6.1 Kerangka COBIT 5

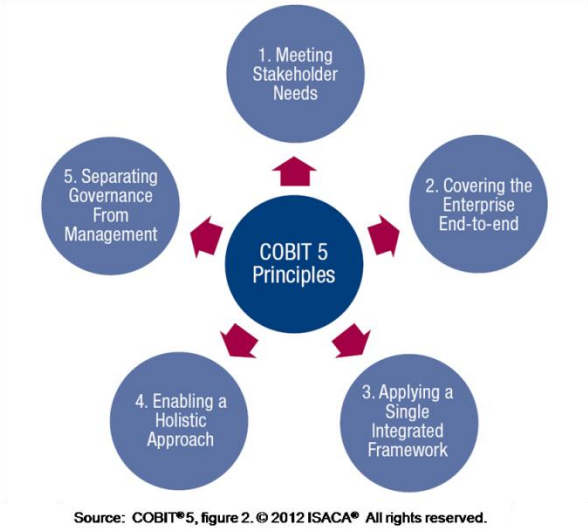
Secara sederhana, COBIT 5 membantu *enterprise* membangun nilai yang optimal dari TI dengan mengelola keseimbangan antara realisasi manfaat dan optimasi *Level* resiko dan penggunaan sumberdaya.

COBIT 5 memungkinkan informasi dan teknologi yang terkait untuk dikelola secara holistik bagi keseluruhan *enterprise*, mencakup area bisnis dan fungsional secara keseluruhan, dengan mempertimbangkan manfaat TI bagi *stakeholders* internal dan eksternal [6]

2.6.2 Prinsip-Prinsip COBIT 5

Menurut ISACA (2012), bahwa COBIT 5 memiliki 5 prinsip dasar [4] :

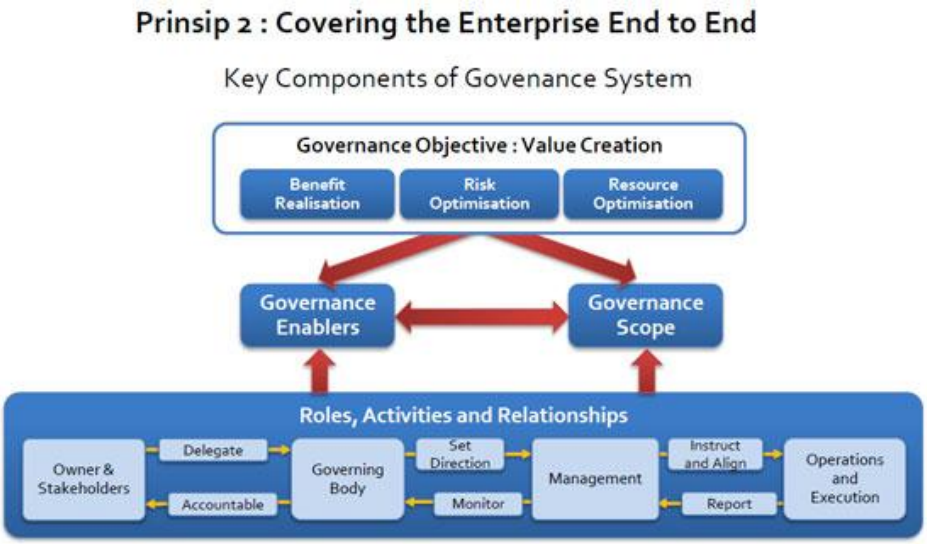
1. Memenuhi kebutuhan *stakeholder*.
2. Melingkupi tata kelola dan proses kerja *End-to-End Enterprise*
3. Mengaplikasikan sebuah kerangka-kerja yang terintegrasi.
4. Pendekatan keseluruhan untuk kemampuan tata kelola dan manajemen/pengaturan.
5. Pemisahan antara tata-kelola dengan manajemen/pengaturan.



Gambar 2. 2 Prinsip Dasar COBIT 5 [6]

1. ***Meeting stakeholder needs***, berguna untuk pendefinisan prioritas untuk implementasi, perbaikan, dan jaminan. Kebutuhan *stakeholder* diterjemahkan ke dalam *Goals Cascade* menjadi tujuan yang lebih spesifik, dapat ditindaklajuti dan disesuaikan, dalam konteks : Tujuan perusahaan (*Enterprise Goal*), Tujuan yang terkait IT (*IT-related Goal*), Tujuan yang akan dicapai *enabler (Enabler Goal).* Selain itu sistem tata kelola harus mempertimbangkan seluruh *stakeholder* ketika membuat keputusan mengenai penilaian manfaat, *resource* dan risiko. [6]

2. ***Covering enterprise end-to-end***, bermanfaat untuk mengintegrasikan tata kelola TI perusahaan kedalam tata kelola perusahaan. Sistem tata kelola TI yang diusung COBIT 5 dapat menyatu dengan sistem tata kelola perusahaan dengan mulus. [6]



Gambar 2. 3 Komponen-Komponen Inti Dari Sistem Tata Kelola [6]

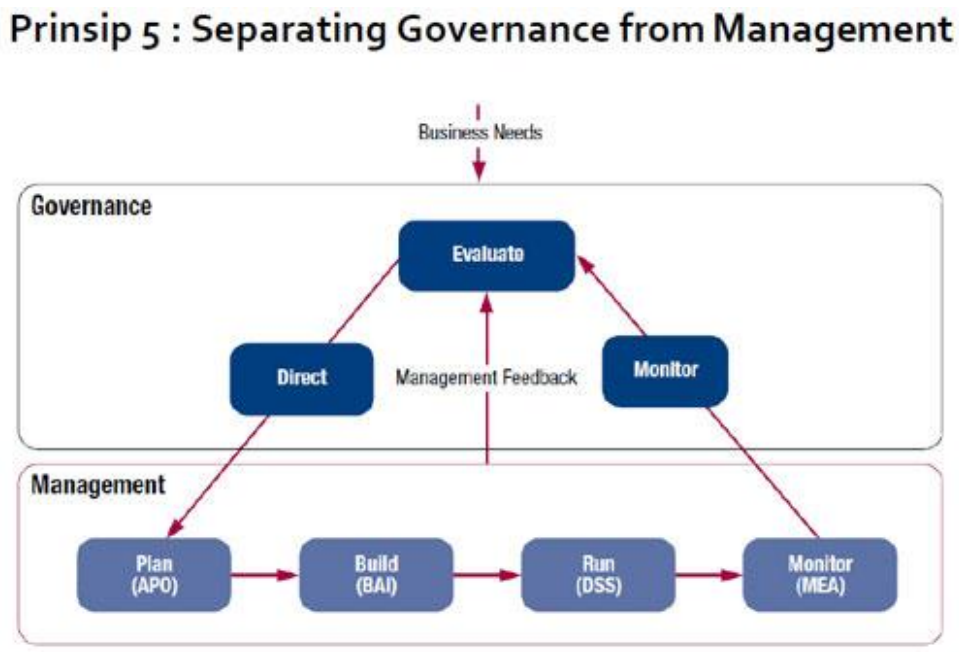
Prinsip kedua ini juga meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola TI perusahaan dimanapun informasi diproses. Dalam lingkup perusahaan, COBIT 5 menangani semua layanan TI internal maupun eksternal, dan juga proses bisnis internal dan eksternal. [6]

3. ***Applying a single intergrated framework***, sebagai penyelarasan diri dengan standar dan *framework* relevan lain, sehingga perusahaan memapu menggunakan COBIT 5 sebagai *framework* tata kelola umum dan *integrator*. Selain itu prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACA (COBIT, VAL IT, Risk IT, BMIS, ITAF, dll). [6]

4. ***Enabling a holistic approach***, yakni COBIT 5 memandang bahwa setiap *enabler* saling memperngaruhi satu sama lain dan menentukan apakah penerapan COBIT 5 akan berhasil. [6]

Gambar 2. 4 Saling Berpengaruhnya Enabler [6]

5. ***Separating governance from management***,
   COBIT membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup brbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani untuk tujuan yang berbeda pula.



Gambar 2. 5 Pemisahan Tata Kelola Dengan Manajemen [6]

Perbedaan *Governance* (Tata kelola) dengan *Management* (Manajemen) [9]

- *Governance* adalah tata kelola yang memastikan bahwa tujuan perusahaan dapat dicapai dengan melakukan evaluasi terhadap kebutuhan, kondisi, dan pilihan *stakeholder*, menerapkan arah melalui

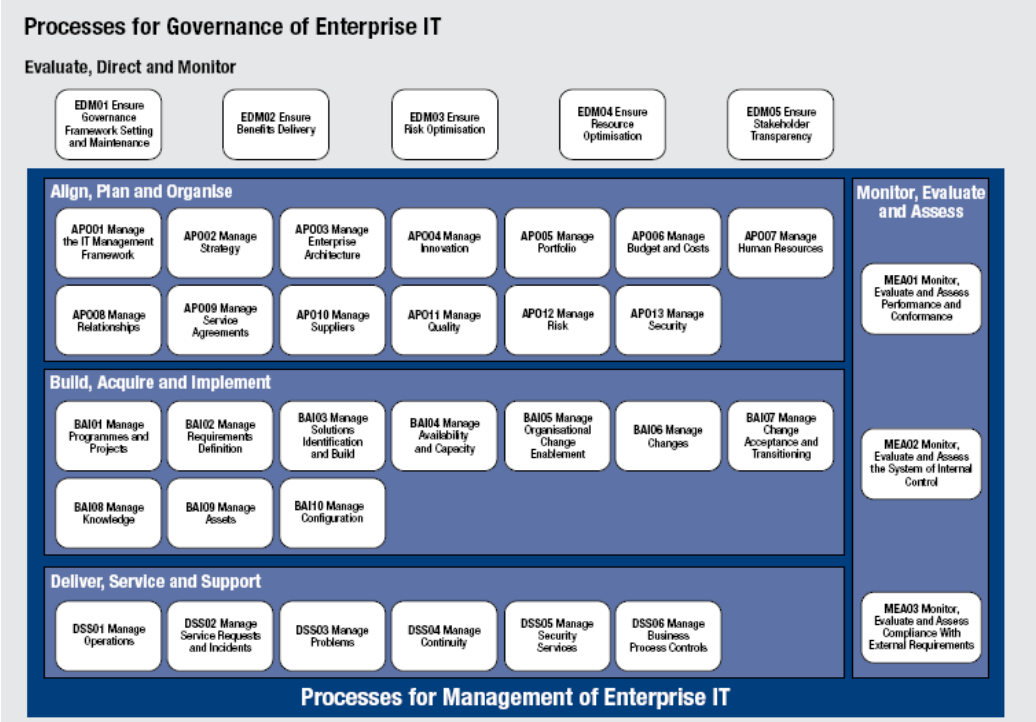
prioritas dan pengambilan keputusan terhadap arah dan tujuan yang telah disepakati. Pada perusahaan secara normatif, tata kelola adalah tanggung jawab dari dewan direksi dibawah kepemimpinan ketua. Tata kelola berisi lima proses yaitu proses itu sendiri, mengevaluasi, dan pemantauan langsung

- *Management* (Manajemen) berfungsi sebagai perencana, membangun, menjalankan dan memonitor aktifitas-aktifitas yang sejalan dengan arah yang ditetapkan oleh badan tata kelola untuk mencapai tujuan perusahaan. Manajemen-Berisi empat domain, sesuai dengan Bagian tanggung jawabnya yaitu merencanakan, membangun, menjalankan dan memantau (PBRM) falam cakupan *end-to-end*. 4 domain tersebut yaitu:

  - *Align, Plan and Organise (APO)*
  - *Build, Acquire and Implement (BAI)*
  - *Deliver, Service and Support (DSS)*
  - *Monitor, Evaluate and Assess (MEA)*

2.6.3 Domain dan Proses pada COBIT 5

COBIT 5 memiliki 5 domain yang terbagi dalam domain *governance* dan *management*, masing- masing domain memiliki proses yang memungkinkan untuk mencapai tujuannya [11]. Satu domain berasal dari *governance* dan empat lainnya berasal dari *management*. Domain yang berasal dari area *governance of enterprise* IT adalah (*Evaluate, Direct, and Monitor*) EDM yang terdiri dari 5 proses. Sedangkan domain yang berasal dari *management of enterprise* IT sejalan dengan tanggung jawab pada area *plan, build, run, and monitor* (PBRM). Terdapat 32 proses yang dipecah kedalam masing-masing domain sebagai berikut.
1. *Align, Plan and Organize* (APO) dengan13 proses.
2. *Build, Acquire and Implement* (BAI) dengan 10 proses.
3. *Deliver, Service and Support* (DSS) dengan 6 proses.
4. *Monitor, Evaluate and Assess* (MEA) dengan 3 proses.



Gambar 2. 6 Domain dan Proses COBIT 5 (Sumber : ISACA,2012)

2.6.4 Domain Deliver, Service, and Support (DSS)

Deliver, Service, and Support yang biasa dikenal dengan singkatan DSS merupakan salah satu domain di *framework* COBIT 5. Domain ini merupakan perluasan dari domain *Deliver and Support* (DS) pada versi COBIT sebelumnya, yakni COBIT 4.1. Domain DSS menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan, dan pengelolaan data yang sedang berjalan.

Sementara fokus domain DSS pada COBIT 5 yakni pada aspek pengiriman teknologi informasi, proses, dan dukungan yang memungkinkan untuk pelaksanaan sistem TI yang efektif dan efisien. Domain DSS terdiri dari 6 *control objective*, yakni sebagai berikut [12].

a. DSS01 – Mengelola Operasi
b. DSS02 – Mengelola Permintaan Layanan dan Insiden
c. DSS03 – Mengelola Masalah
d. DSS04 – Mengelola Keberlanjutan
e. DSS05 – Mengelola Keamanan Layanan
f. DSS06 – Mengelola Kontrol Proses Bisnis

2.6.5 Diagram RACI

Untuk melakukan penilaian dengan domain DSS, maka dilakukan *mapping* antara *sub control objective*s dan sumber daya manusia (SDM) yang ada di bagian pelaksana TI dengan menggunakan diagram RACI. Diagram RACI adalah bagian dari *Rensponsibility Assignment Matrix* (RAM) yang merupakan suatu bentuk pemetaan antara sumber daya dengan aktivitas dalam setiap prosedur. Berikut contoh salah satu diagram RACI pada DSS01 [12].

DSS01 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
DSS01.01 Perform operational procedures.																					A		C	C	C	
DSS01.02 Manage outsourced IT services.											I							A			R					
DSS01.03 Monitor IT infrastructure.				I		C					I						C	I		C	A		C	C		
DSS01.04 Manage the environment.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS01.05 Manage facilities.						I					C	A				C	C	C	I	C	R		I	R	I	

Gambar 2. 7 Diagram RACI DSS01 (Sumber : ISACA,2012)

Mapping tersebut dilakukan untuk seluruh *control objective* yang ada pada domain DSS. *Mapping* menggunakan diagram RACI. RACI merupakan singkatan dari *Responsible* (R), *Accountable* (A), *Consulted* (C), dan *Informed* (I). Berikut merupakan arti dari diagram RACI [12].

a. *Responsible* (R) menunjukkan bahwa bagian tersebut merupakan pihak pelaksana yang harus bertanggungjawab melaksanakan dan menyelesaikan aktivitas yang menjadi tanggung jawabnya.
b. *Accountable* (A) menunjukkan bahwa bagian tersebut merupakan pihak yang harus mengarahkan jalannya pelaksanaan aktivitas.
c. *Consulted* (C) menunjukkan bahwa bagian tersebut merupakan pihak yang akan menjadi tempat konsultasi selama pelaksanaan aktivitas.
d. *Informed* (I) menunjukkan bahwa bagian tersebut merupakan pihak yang diberikan informasi mengenai pelaksanaan aktivitas.

2.6.6 *Goals Cascade* Untuk Perencanaan Audit

Hubungan antara tujuan dan strategi bisnis dengan TI harus sejalan, untuk itu tujuan TI harus mendukung tujuan bisnis. Untuk perencanaan audit, terlebih dahulu melakukan *mapping enterprise goal* dengan IT-*related goal* guna memaparkan tujuan bisnis secara umum dengan beberapa tujuan TI yang mendukung tujuan bisnis organisasi. *IT-related goals* merupakan *IT balance scorecard* yang memandang TI berdasarkan empat perspektif, sedangkan *enterprise goal* merupakan *balance scorecard* yang memandang tujuan organisasi secara keseluruhan berdasarkan empat perspektif [12]. Hasil dari *mapping* ini tidak digunakan semua tetapi hanya yang relevan dengan kondisi objek audit. Untuk melakukan proses audit, sebelumnya dilakukan beberapa langkah sebagai berikut.

a. *Mapping* antara tujuan bisnis perusahaan dengan tujuan TI.
   Mapping dilakukan kedalam perspektif *IT Balance Scorecard* (IT BSC). Jika hubungan keterkaitan antara tujuan bisnis dan tujuan TI sangat kuat, maka diberi tanda "P" yang berarti *primary* (*strong relationship*). Jika terdapat

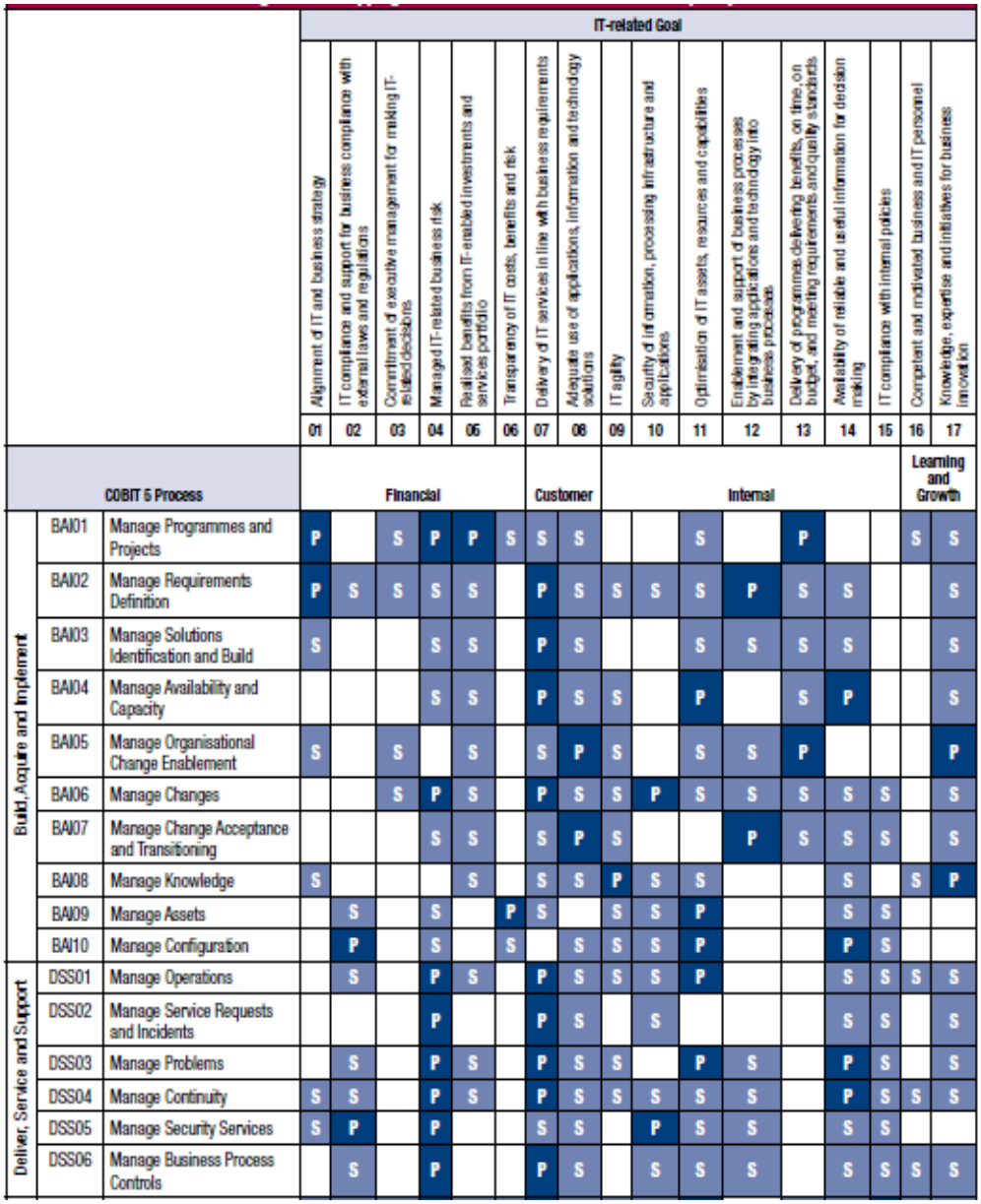
hubungan antara tujuan bisnis dengan tujuan TI tetapi hubungan tersebut tidak dominan, maka diberi tanda "S" yang berarti *secondary* (*medium relationship*). Jika tidak ada hubungan sama sekali, maka dikosongkan.

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		IT-related Goal	Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Gambar 2. 8 *Mapping Enterprise Goals* dengan *IT-related Goals* ISACA(Sumber: ISACA, 2012)

b. Melakukan *mapping* antara tujuan TI dengan proses TI

Setiap tujuan TI memiliki masing-masing proses TI yang relevan. Setelah dilakukan *mapping* terhadap tujuan bisnis perusahaan dengan tujuan TI, selanjutnya dilakukan *mapping* tujuan TI dengan proses TI [12].



			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		COBIT 5 Process	Financial						Customer		Internal							Learning and Growth	
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S		P	S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S

Gambar 2. 9 *Mapping IT-related Goals* dengan COBIT 5 *Process* ISACA (Sumber: ISACA, 2012)

2.6.7 *Process Capability Model*

Process capability model digunakan untuk mengukur kematangan *IT enterprise*, diadopsi dari ISO/IEC 15504 sebagai standar proses penilaian. Model ini menyediakan pengukuran performansi dari proses-proses pada area *governance* maupun manajemen, dan melakukan peningkatan pada area-area yang telah diidentifikasi.

Terdapat 6 *Level* kapabilitas proses yang bisa dicapai termasuk *incomplete process* jika prakteknya tidak tercapai sesuai dengan tujuan.

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Process optimization

Gambar 2. 10 *Process Capability Model* (Sumber: ISACA, 2012)

Berikut adalah penjelasan level dari *process capability* [13] :

a. Level 0 (*Incomplete*)
   Proses tidak melaksanakan atau gagal untuk mencapai tujuan proses. Pada tingkat ini, ada sedikit atau tidak sama sekali bukti (*evidence*) dari setiap pencapaian tujuan proses.
b. Level 1 (*Perfomed*)
   Proses diimplementasikan untuk mencapai tujuan bisnisnya.
c. Level 2 (*Managed*)
   Proses yang diimplementasikan dikelola (plan, monitor, and adjusted) dan hasilnya ditetapkan dan dikontrol.
d. Level 3 (*Established*)
   Proses didokumentasikan dan dikomunikasikan (untuk efisiensi organisasi).
e. Level 4 (*Predictable*)
   Proses dimonitor, diukur, dan diprediksi untuk mencapai hasil.
f. Level 5 (*Optimizing*)
   Sebelumnya proses telah di prediksikan kemudian ditingkatkan untuk memenuhi tujuan bisnis yang relevan dan tujuan yang akan dating.

Setiap proses yang dinilai akan menghasilkan 4 level rating point, yaitu :

a. *Not achieved*, apabila hasil penilaian antara 0% - 15%
b. *Partially achieved*, apabila hasil penilaian >15% - 50%
c. *Largely achieved*, apabilahasil penilaian >50% - 85%
d. *Fully achieved*, apabila hasil penilaian >85% - 100%

2.7 Profil Perusahaan

2.7.1 Visi Misi PT Telkom

a. VISION

To Become a Leading Telecommunications,Information, Media, Edutainment and Services ("TIMES") Player in The Region.

b. MISSION

- *To Provide TIMES with Excellent Quality & Competitive Price.*
- *To be The Role Model as the Best Managed Indonesian Corporation.*

c. Profil CDC PT Telkom

Dari historis perkembangan organisasi CDC, awalnya dimulai dari Proyek Pembinaan Usaha Kecil dan Koperasi (PPUKK) tahun 2001 dan mengalami perubahan menjadi *Community Development Center* (CDC) pada tahun 2003. Seiring dengan perubahan regulasi pemerintah dan tuntutan bisnis yang terus berkembang, maka Unit CDC dari tahun 2003 hingga tahun 2011 terus mengalami transformasi, baik dalam paradigma hingga pengelolaan organisasi, ruang lingkup tugas, wewenang dan tanggung jawabnya.

Lingkup Peran CDC hingga saat ini, telah berkembang menjadi lebih luas dengan berdasar pada Keputusan Direksi Nomor : KD. 18/PS180/COP-B0030000/2009 tanggal 12 Juni 2009 tentang Tambahan Tugas, Wewenang dan Tanggung Jawab Organisasi Pusat Pengelolaan Program Kemitraan dan Program Bina Lingkungan (CDC) terkait dengan Corporate Social Responsibility (CSR). CDC sebagai Unit Bisnis yang mendukung bisnis utama TELKOM, mempunyai posisi strategis terhadap unit bisnis lainnya dalam hal pemberdayaan komunitas. Pada posisi strategis tersebut CDC mengemban dua peran, yaitu sebagai pemegang mandat pelaksana PKBL dan sebagai pelaksanaan Telkom CSR.

d. Sejarah Perkembangan CDC

Bila ditinjau dari historisnya, cikal bakal CDC adalah Proyek Pembinaan Usaha Kecil dan Koperasi (PPUKK), yang pengelolaannya berdasarkan KEPMENKU Nomor : 316/KMK.016/1994 tentang Pedoman Pembinaan Usaha Kecil dan Koperasi melalui Pemanfaatan Dana dari bagian Lembaga Badan Usaha Milik Negara. Hal iniberlangsung sejak akhir tahun 2001 hingga tahun 2003. Adapun sebagai landasan pengelolaan PKBL adalah UU 19 tahun 2003 tentang BUMN, Pasal 88 dan Pasal 90, yang ditegaskan dengan KEPMEN BUMN Nomor: KEP-236/MBU/2003 tanggal 17 Juni 2003 tentang Program Kemitraan dan Program Bina Lingkungan Badan Usaha Milik Negara dengan Usaha Kecil.

Sebagai implementasi dari KEPMEN BUMN tersebut, maka ditetapkan Keputusan Direksi Nomor: KD.51/KU200/PUK-00/2003 tanggal 28 Agustus 2003 tentang Program Kemitraan dan Program Bina Lingkungan dan Keputusan Direksi Nomor : 61/PS150/CTG-10/2003 tanggal 9 September 2003 tentang Pembentukan Organisasi Selanjutnya, Pada tanggal 27 April 2007 Kementerian Negara BUMN menerbitkan Peraturan Menteri Negara BUMN Nomor : PER-05/MBU/2007 tentang Program Kemitraan BUMN dengan Usaha Kecil dan Program Bina Lingkungan, sebagai pengganti Keputusan

Menteri BUMN Nomor : KEP-236/MBU/2003. Sejalan dengan kondisi ini, CDC sebagai Unit Bisnis yang mendukung bisnis utama TELKOM, juga mengalami perubahan berdasarkan Keputusan Direksi Nomor: KD.12/PS150/COP-B0030000/2008 tanggal 5 Februari 2008 tentang Organisasi Pusat Pengelolaan Program Kemitraan dan Program Bina Lingkungan (CDC) sebagai pengganti Keputusan Direksi Nomor: KD.51/PS150/COP-B0030000/2006 tanggal 13 September 2006 tentang Organisasi Pusat Pengelolaan Program Kemitraan dan Program Bina Lingkungan (CDC). Perkembangan CDC selanjutnya, adalah berdasarkan Surat Edaran MENEG BUMN, Nomor : SE-07/MBU/2008 tentang Pelaksanaan PKBL dan Penerapan Pasal 74 UU. Nomor : 40 Tahun 2007 tanggal 5 Mei 2008 tentang Perseroan Terbatas, yang kemudian dipertegas dengan diterbitkannya SE-21/MBU/2008 tanggal 24 Desember 2008 tentang Pelaksanaan PKBL dan TJSL di Lingkungan BUMN. Hal ini menjadi dasar penyesuaian pelaksanaan PKBL dan CSR bagi TELKOM khususnya CDC, dengan dikeluarkan Keputusan Direksi nomor KD.18/PS180/COP-B0030000/2009 tanggal 12 Juni 2009 tentang Penambahan Tugas, Wewenang dan tanggung Jawab CDC terkait CSR.

e. Visi dan Misi CDC PT Telkom

TELKOM sebagai perusahan pelopor perusahaan telekomuniasi telah merumuskan dan menetapkan Visi dan Misi. Selanjutnya, sebagai Unit Bisnis yang mendukung bisnis utama TELKOM maka CDC mempunyai Visi dan Misi sebagai berikut:

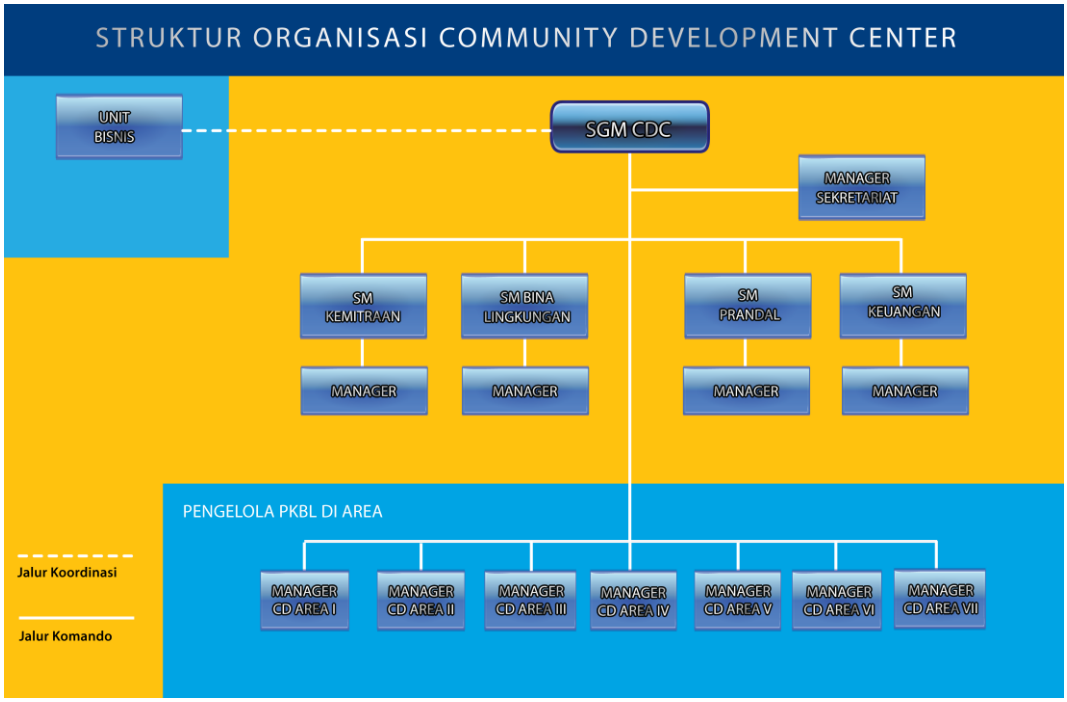
Visi

"Menjadi Perusahaan terbaik di dunia dalam membangun komunitas demi keberlanjutan bisnis dan reputasi perusahaan".

Misi

1. Membentuk atau memberdayakan komunitas Akses yang berhubungan dengan bisnis *Telecomunication, Information, Media, Edutainment* (TIME);
2. Membentuk atau memberdayakan komunitas Konten yang berhubungan dengan bisnis *Telecomunication, Information, Media, Edutainment* (TIME);
3. Membentuk atau memberdayakan komunitas Sosial, Ekonomi dan Lingkungan.

f. Struktur Organisasi CDC PT Telkom



Gambar 2. 11 Struktur Organisasi CDC PT Telkom

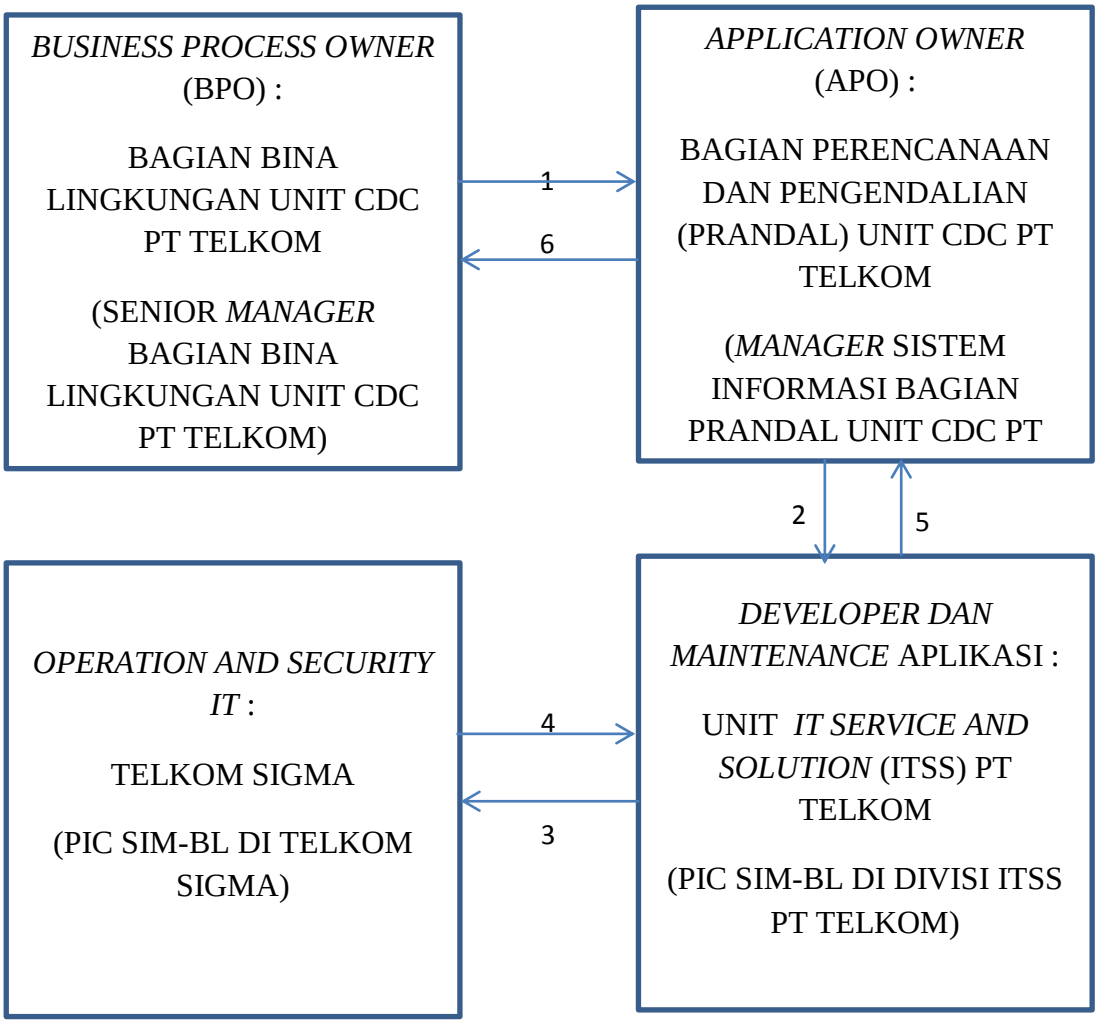
Struktur organisasi CDC sebagai berikut:

1. Pimpinan CDC yaitu *Senior General Manager* CDC
2. Pengelola Fungsi Dukungan Manajemen, yaitu Senior *Manager* Perencanaan & Pengendalian CDC dan Senior *Manager* Keuangan
3. Pengelola Operasional, yaitu Senior *Manager* Program Kemitraan, Senior Manager Program Bina Lingkungan dan *Manager Community Development* (CD) Area (Area I-VII).

Sasaran Strategis Bina Lingkungan

1. Melibatkan masyarakat dalam proses kinerja sosial perusahaan
2. Melakukan inovasi untuk melakukan transformasi dalam pengembangan teknologi TIME yang keberadaannya sangat dirasakan masyarakat
3. Menerapkan Investasi sosial (*social investment*) yang bertanggung jawab
4. Mendukung program pendidikan terutama yang mempunyai keterbatasan akses sumber daya, dan pengembangan budaya yang berbasis kearifan lokal
5. Memfasilitasi program kesehatan masyarakat melalui penggunaan IT dalam mengintegrasikan transaksi di bagian kesehatan

g. Bagan Pengelolaan Sistem Informasi Manajemen Bina Lingkungan Unit CDC PT Telkom



Gambar 2. 12 Bagan Pengelolaan Sistem Informasi

Proses 1 (BPO kepada APO) :

1. BPO memberikan diagram bisnis proses
2. *Change request*
3. Konsultasi

Proses 2 (APO kepada *Developer*) :

1. Meneruskan *change request*
2. Meneruskan jikalau terdapat problem
3. Konsultasi

Proses 3 (*Developer* kepada *Operator*) :

1. Meneruskan *change request* terkait teknis sistem, yaitu *operation* dan *security service*

Proses 4 (*Operator* kepada *Developer)* :

1. Hasil perbaikan dari teknis sistem, yaitu perihal *operation* dan *security service*

Proses 5 (*Developer* kepada APO) :

1. Hasil perbaikan (*follow up*) dari *change request*

Proses 6 (APO kepada BPO) :

1. Hasil akhir perbaikan (*follow up*) dari *change request*

2.8 Kebutuhan Untuk Mencapai Sasaran Strategis Bina Lingkungan

Untuk melakukan pemetaan *Enterprise Goals* dengan sasaran strategis Bina Lingkungan, diperlukan informasi tentang kebutuhan apa saja yang harus dipenuhi untuk mencapai sasaran strategis tersebut.

1. Melibatkan masyarakat dalam proses kinerja sosial perusahaan
2. Melakukan inovasi untuk melakukan transformasi dalam pengembangan teknologi TIME yang keberadaannya sangat dirasakan masyarakat
3. Menerapkan Investasi sosial (*social investment*) yang bertanggung jawab
4. Mendukung program pendidikan terutama yang mempunyai keterbatasan akses sumber daya, dan pengembangan budaya yang berbasis kearifan lokal
5. Memfasilitasi program kesehatan masyarakat melalui penggunaan IT dalam mengintegrasikan transaksi dibagian kesehatan

2.9 Statistika

Teknik pengumpulan data dengan kuesioner merupakan salah satu teknik yang digunakan dalam penelitian ini. Maka dari itu akan dipaparkan teori dasar yang berhubungan dengan statistika [10]

2.9.1 Pengertian Statistika

Menurut Wisnu Wardhana (2003) [1], Statistika adalah suatu pengetahuan mengenai pengumpulan, mengolah, menyajikan, dan menganalisa data dengan metode tertentu, serta menarik kesimpulan dan mengambil keputusan berdasarkan hasil analisis yang telah dilakukan melalui suatu metode statistika.

2.9.2 Populasi

Populasi adalah kelompok objek yang akan diteliti, yaitu [1] :

1. Populasi *Infinit*
   Populasi *infinit* adalah kumpulan objek yang tidak diketahui jumlahnya dengan pasti atau tak terbatas.
2. Populasi *Finit*
   Populasi *Finit* adalah kumpulan objek yang jumlahnya sudah diketahui dengan pasti atau kumpulan objek yang dapat diberi nomor identifikasi.

2.9.3 Validitas

Validiatas adalah tingkat kebenaran data yang menunjukan fakta yang dimaksud oleh peneliti. Data yang tdak valid menghasilkan kesimpulan yang tidak valid juga, meskipun data diolah dengan analisa statistik yang benar (*garbage in garbrbage out).* Berdasarakan acuan pengujianya, validitas terbagi menjadi dua jenis, yaitu [1]:

a. Validitas Eksternal

   Validitas eksternal adalah validitas yang pengujianya berdasarkan kriteria tertentu diluar alat ukur. Beberapa jenis validitas eksternal, yaitu:

   1. Validitas konkuren : mengacu pada hubungan antara tes skor yang dicapai dengan keadanaan sekarang. Pengujian validitas konkuren dilakukan dengan membandingkan hasil pengukuran alat ukur dengan pengukuran lainya yang lebih valid.
   2. Validitas Prediktif : cara pengujianya hampir sama dengan validitas konkuren, perbedaanya hanya pada ukuran referensi yang dipakai. Referensi validitas konkuren prediktif adalah tujuan dari pengukuran itu sendiri dimana pada saat pengukuran dilakukan keberhasilan tujuan tersebut belum tercapai.

b. Validitas Internal

   Validitas internal adalah validitas yang pengujianya terdapat dalam alat ukur. Ada beberapa jenis validitas internal, yaitu :

   1. Validitas konstruk : pengujian validitas ini dilakukan dengan melihat keselarasan setiap indikator yang dipakai. Suatu alat ukur dikatakan valid apabila sudah cocok dengan konstruksi teoritik dimana tes dibuat.
   2. Validitas Isi: validitas yang mengukur konsistensi variabel berdimensi jamak dengan kelengkapan aspek pengukuran variable tersebut. Untuk pengujian validitas ini dapat dilakukan dengan melihat referensi teori atau pendapta para ahli.

   Rumus yang digunakan untuk menguji validitas adalah rumus korelasi *product moment pearson*. Yaitu sebagai berikut:

$$r_i = \frac{N\sum XY - \sum X \sum Y}{\sqrt{\left\{N\sum X^2 - (\sum X)^2\right\}\left\{N\sum Y^2 - (\sum Y)^2\right\}}}$$

   (Azwar,2001:19)

   Keterangan :
   r : Korelasi antar instrument
   N : Jumlah sample
   X_i : Jumlah skor item
   Y_i : Jumlah skor total seluruh item

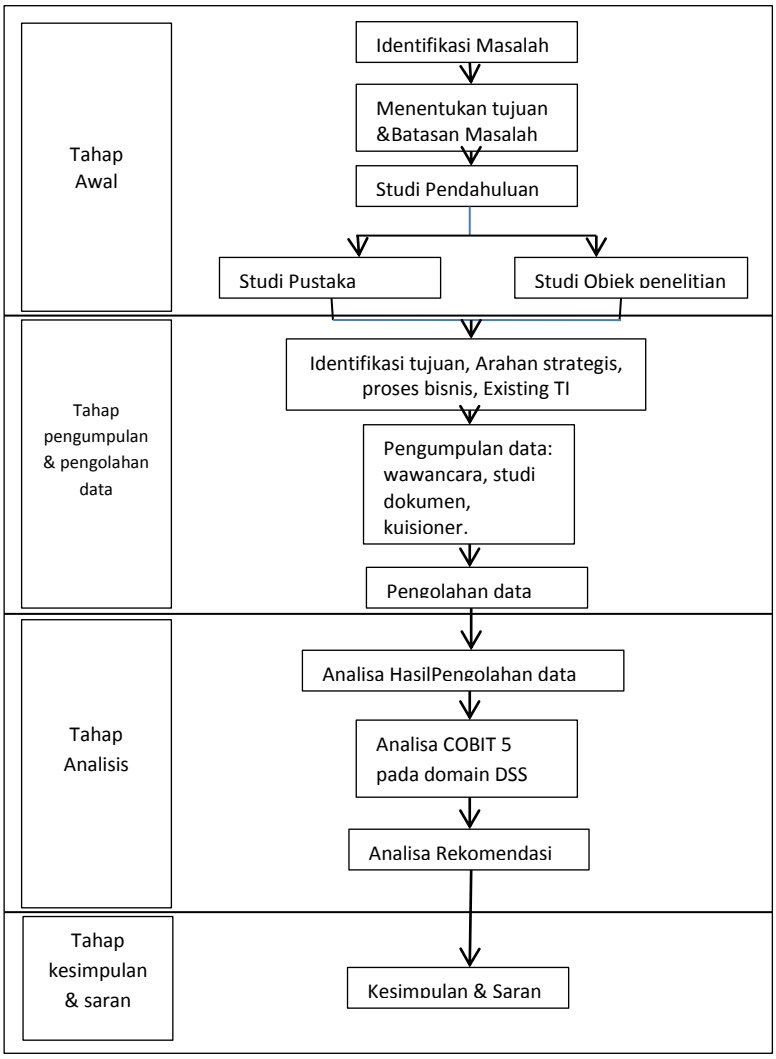
   Dasar pengambilan keputusan:

1) Jika r positif, serta r ≥ 0.30 atau r ≥ tabel maka item pertanyaan tersebut valid.
2) Jika r tidak positif, serta r < 0.30 atau < r tabel maka item pertanyaan tersebut tidak valid.

BAB III
METODOLOGI PENELITIAN

3.1 Metode Konseptual

Secara umum, metodologi yang digunakan untuk menyelesaikan permasalaham pada tugas akhir ini dapat dilihat pada gambar [10]



Gambar 3.1 Metodologi Penyelesaian Masalah

Setiap tahap merupakan proses yang saling berkaitan. Ada empat tahapan besar untuk menyelesaikan penelitian ini, yaitu:

3.1.1 Tahap Awal

Pada tahap ini dilakukan identifikasi masalah, menentukan tujuan dan batasan, serta melakukan studi pendahuluan, yaitu studi pustaka dan studi objek penelitian. Identifikasi masalah dilakukan untuk mengetahui fenomena apa yang dapat diangkat/diteliti, agar lebih mudah untuk menentukan tujuan penelitian.

Strudi pustaka dilakukan dengan membaca referensi seperti jurnal, artikel, tugas akhir, dan buku yang berkaitan dengan objek penelitian. Identifikasi masalah dilakukan untuk mengetahui fenomena apa yang dapat diangkat/diteliti, agar lebih mudah untuk menentukan tujuan penelitian. Studi pustaka dilakukan dengan membaca referensi seperti jurnal, artikel, tugas akhir, dan buku yang berkaitan dengan objek penelitian, yaitu SIM-BL dan audit sistem informasi menggunakan COBIT 5 pada domain DSS. [10]

Studi objek penelitian dilakukan dengan *meeting stakeholder* dan identifikasi kebutuhan lapangan, yaitu menyiapkan kebutuhan – kebutuhan yang dibutuhkan untuk audit, bertemu dengan *stakeholder* untuk mendiskusikan tujuan dari perusahaan dan pemetaan dalam COBIT 5, kemudian pihak – pihak divisi yang terkait untuk menjadi responden kuesioner dan wawancara, dan proses bisnis dan profil dari Bina Lingkungan CDC PT Telkom.

3.1.2 Tahap Pengumpulan dan Pengolahan Data

a. Tahap Pengumpulan Data

Identifikasi tujuan, arahan strategis dan proses bisnis.

Untuk memeperoleh hasil tujuan, arahan strategis dan proses bisnis perusahaan maka dilakukan pemetaan yang terdapat pada COBIT 5 itu sendiri. Pemetaan terdiri dari *Enterprise Goals, IT-Related Goals, Process Control* dan pemetaan RACI . Identisifkasi ini diperoleh dari hasil wawancara dengan Manager Sistem Informasi Bagian Perencanaan dan Pengendalian (PRANDAL) CDC PT Telkom.

1. Pemetaan *Enterprise Goals* dengan Sasaran Strategis Bina perusahaan

Tabel 3. 1 Pemetaan Enterprise Goals

BSC Dimension	**EG**	***Enterprise Goals***	**Sasaran Strategis Bina Lingkungan CDC PT Telkom**				
			Melibatkan masyarakat dalam proses kinerja sosial perusahaan	**Melakukan inovasi untuk melakukan transformasi dalam pengembangan teknologi TIME yang keberadaannya sangat dirasakan masyarakat**	**Menerapkan investasi sosial *(social investment)* yang bertanggungjawab**	**Mendukung program pendidikan terutama yang mempunyai keterbatasan akses sumberdaya, dan pengembangan budaya yang berbasis kearifan lokal**	**Memfasilitasi program kesehatan masyarakat melalui penggunaan IT dalam mengintegrasikan transaksi Bagian kesehatan**
Financial	1	*Stakeholder value of business investments*	P	P	P	P	P

	2	*Portfolio of competitive product and services*		P	P	P	P
	3	*Managed business risk (safeguarding of assets)*	P	P	P	S	S
	4	*Compliance with external laws and regulations*	P	S	P	S	
	5	*Financial transparency*			P		
Customer	6	*Customer-oriented service culture*	P	P	P	P	P
	7	*Business service continuity and availability*	S	S	S	S	S
	8	*Agile responses to a changing business environment*		P			S
	9	*Information-based strategic decision making*					
	10	*Optimisation of service delivery cost*					
Internal	11	*Optimisation of business process functionality*			P		

	12	*Optimisation of business process cost*					
	13	*Managed business change programmes*	S	S	S	S	S
	14	*Operational and staff productivity*					
	15	*Compliance with internal policies*	P		P		
Learning & Growth	16	*Skilled and motivated people*					
	17	*Product and business innovation culture*	S	S	S	S	S

Hasil dari pemetaan *Enterprise* pada Tabel 3.1 adalah EG1,EG2,EG3,EG,4EG,5,EG6,EG8,EG11,EG15. Keterangan dari pemetaan table diatas apabila pada suatu *Enterprise Goal* tidak terdapat nilai "P" yang berarti *primary*, maka *Enterprise Goals* tersebut tereliminasi.

2. Pemetaan *IT-Related Goals* dengan *Enterprise Goals*

Tabel 3. 2 Pemetaan IT-Related Goals dengan Enterprise Goals

			Enterprise Goal								
BSC DIMENSION	NO	*IT-realated Goals*	*1. Stakeholder value of business investments*	*2. Portfolio of competitive product and services*	*3. Manage business risk (safeguarding of assets)*	*4. Compliance with external laws and regulations*	*5. Financial Transparency*	*6. Custmer-orieted service culture*	*8. Agile responses to a changing business environtment*	*11. Optimisation of service business process functionality*	*15. Compliance with internal policies*

Financial	1	*Alignment of IT and business strategy*	P	p	S			P	P	P		
	2	*IT compliance and support for business compliance with external laws and regulation*			S	P					P	
	3	*Commitment of exective management for making IT-related decisions*	P	S	S				S	S		
	4	*Manage IT-related business risk*			P	S			S		S	
	5	*Realised benefits from IT-enabled investments and services portofolio*	P	P				S	S	S		
	6	*Transparancy of IT cost, benefits and risk*	S		S		P					

Customer	7	*Delivery of IT services in line with business requirement*	P	P	S	S		P	P	P		
	8	*Adequate use of applications,information and technology solution*	S	S	S			S		P		
Internal	9	*IT agility*	S	P	S			S	P	P		
	10	*Security of information, processing infrastructure and applications*			P	P					P	
	11	*Optimation of IT assets, resources, and capability*	P	S					S	S		
	12	*Enablement and support of business processes by integrating application and technology into business processes*	S	P	S			S	S	P		

	13	*Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards*	P	S	S			S				
	14	*Avaibility of reliable and useful information for decision making*	S	S	S	S				S		
	15	*IT compliance with internal policies*			S	S					P	
Learning & Growth	16	*Competent and motivated business and IT personel*	S	S	P			S	S			
	17	*Knwledge, expertise and initiatives for business innovation*	S	P				S	P	S		

Hasil dari pemetaan *IT-Related* pada Tabel 3.2 adalah IT-R1 – ITR13, kemudian IT-R15 – IT-R17. Keterangan dari pemetaan table diatas apabila pada suatu IT-*Related Goals* tidak terdapat nilai "P" yang berarti *primary*, maka *IT-Related Goals* tersebut tereliminasi.

3. Pemetaan *Process Control* dengan *IT-Related Goals*

Tabel 3. 3 Pemetaan Process Control dengan IT-Related Goals

Domain DSS	*IT-related Goals*																∑ P	∑ S	Nilai proses
	ITG1	ITG2	ITG3	ITG4	ITG5	ITG6	ITG7	ITG8	ITG9	ITG10	ITG11	ITG12	ITG13	ITG15	ITG16	ITG17			
DSS01 - Mengelola Operasi		S		P	S		P	S	S	S	P			S	S	S	3	8	0.44
DSS02 - Mengelola permintaan layanan dan insiden				P			P	S		S				S		S	2	4	0.25
DSS03 - Mengelola masalah		S		P	S		P	S	S		P	S		S		S	3	7	0.41
DSS04 - Mengelola keberlanjutan	S	S		P	S		P	S	S	S	S	S		S	S	S	2	11	0.47
DSS05 Mengelola layanan keamanan	S	P		P			S	S			S	S		S			2	6	0.31

DSS06 Mengelola kontrol proses bisnis		S		P			P	S		S	S	S		S	S	S	2	8	0.38

Hasil dari pemetaan *process control* pada Tabel 3.3 adalah DSS01 – DSS06, yang berarti semua domain DSS dijadikan sebagai cakupan proses audit. Keterangan dari pemetaan table diatas adalah menggunakan penilaian nilai proses, dimana proses yang memiliki nilai >0,15 makan dapat dijadikan cakupan audit, nilai 0,15 merupakan nilai urgenitas dari *process capability* kategori *Not Achived*.

a. Pemetaan RACI

Pemetaan RACI digunakan untuk menentukan objek yang akan terlibat dalam kegiatan audit.

Tabel 3. 4 Pemetaan RACI

Key Management Practices	SM BL	*Officer* I Bagian Bina Lingkungan	SM PRANDAL	*Manager* Sistem Informasi	*Officer* Sistem Informasi	*Manager* Perencanaan dan Pengembangan	*Officer* Perencanaan dan Pengembangan	PIC SIM-BL Unit ITSS	PIC SIM-BL Telkom Sigma
DSS01 - 01. Menjalankan prosedur operasional								CI	RACI
DSS01 - 02. Mengelola layanan *Outrsource IT*								CI	RACI

DSS01 - 03.Mengelola Infrastruktur								CI	RACI
DSS01 - 04.Mengelola lingkungan kerja								CI	RACI
DSS01 -05. Mengelola Fasilitas								CI	RACI
DSS02 - 01.Mendifinisikan skema klasifikasi insiden dan permintaan layanan				CI				RACI	R
DSS02 - 02.Mengklarifikasi & memproriataskan permintaan & insiden				CI				RACI	R
DSS02- 03.Memverifikasi, menyetujui dan memenuhi permintaan layanan				CI				RACI	R
DSS02-04. Mendiagnosis dan mengalokasikan insiden				CI				RACI	R

DSS02-05. Menyelesaikan dan Memenuhi insiden				CI				RACI	R
DSS02-06. Menutu permintaan layanan dan insiden				CI				RACI	R
DSS02-07. melacak status & membuat laporan				CI				RACI	R
DSS03-01. Mengidentifikasi dan mengklasifikasikan masalah				CI				RACI	R
DSS03-02. Menginvestigasi & diagnosis masalah				CI				RACI	R
DSS03-03. mencatat *Known Errors*				CI				RACI	R
DSS03-04. Menyelesaikan dan menutup masalah				CI				RACI	R

DSS03-05. Menjalankan manajemen masalah secara proaktif				CI				RACI	R
DSS04-01. Mendefinisikan kebijakan, tujuan, & ruang lingkup keberlangsungan bisnis	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-02. Menjaga strategi keberlanjutan	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-03. Mengembangkan& mengimplementasikan respon dari keberlangsungan bisnis	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-04. Latihan, tes, dan review dokumen *business continuity plan (BCP)*	A	R	RCI	RCI	RCI	RCI	RCI		

DSS04-05. *Review*, menjaga dan emngembangkan *continuity plan*	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-06. Mengadakan *Training* untuk *continuity plan*	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-07. Mengatur *backup*	A	R	RCI	RCI	RCI	RCI	RCI		
DSS04-08. Melakukan *review* ulang	A	R	RCI	RCI	RCI	RCI	RCI		
DSS05-01. Perlindungan dari *Maleware*								CI	RACI
DSS05-02. Mengelola jaringan dan keamanan konektifvitas								CI	RACI
DSS05-03. Mengelola keamanan *endpoint*							I	CI	RACI

DSS05-04. Mengelola identitas *user & logical access*								CI	RACI
DSS05-05. Mengelola akses fisik ke aset TI								CI	RACI
DSS05-06. Mengelola dokumen yang sensitif dan perangkat *output*								CI	RACI
DSS05-07. Memantau infrastruktur yang berhubungan dengan *security events*								CI	RACI
DSS06-01. Menyelaraskan aktivitas kontrol yang ada di proses bisnis dengan sasaran intitusi	A	R	RCI	RCI	RCI	RCI	RCI		
DSS06-02. Mengontrol pemrosesan informasi	A	R	RCI	RCI	RCI	RCI	RCI		

DSS06-03. Mengatur peran, tanggungjawab, hak akses dan Level otoritas	A	R	RCI	RCI	RCI	RCI	RCI		
DSS06-04. Mengelola kesalahan dan *exceptions*	A	R	RCI	RCI	RCI	RCI	RCI		
DSS06-05. Memastikan informasi dari event dapat ditelusi dan dipertanggungjawabkan	A	R	RCI	RCI	RCI	RCI	RCI		
DSS06-06. Mengamankan aset - aset informasi	A	R	RCI	RCI	RCI	RCI	RCI		

Keterangan dari RACI itu sendiri mengartikan:

R: Pihak pelaksanan yang bertanggung jawab melaksanakan dan menyelesaikan aktivitas yg menjadi tanggung jawabnya

A: Pihak yang mengarahkan jalannya pelaksanaan aktivitas

C: Pihak menjadi tempat konsultasi

I: Pihak sebagai informan

Proses penentuan RACI ini dilakukan dengan *stakeholder* agar data pemetaan dan pengumpulan data dapat akurat.

Sumber dan metode pengumpulan data, yaitu :

Sumber data primer
Data primer didapatkan langsung oleh peneliti dengan teknik sebagai berikut :

1. **Wawancara**
   Wawancara adalah teknik pengumpulan data/informasi dari narasumber dengan melontarkan beberapa pertanyaan. Pada penelitian ini, wawancara dilakukan untuk mengidentifikasi hal-hal yang berkaitan dengan kondisi existing SIM-BL, rencana strategis, visi-misi, dan data pendukung lainnya**.**

2. **Kuesioner**
   Kuesioner adalah teknik pengumpulan data dari sejumlah responden dengan daftar pertanyaan tertulis, lalu diolah untuk menghasilkan informasi yang utuh dan valid. Kuesioner dilakukan untuk mendapatkan data. Kuesioner dilakukan terhadap semua pegawai (semua populasi) yang memiliki tugas dan tanggungjawab menjalankan Program Bina Lingkungan. Sehingga yang dilakukan adalah melakukan penyebaran kuesioner kepada populasi *finit*

Tabel 3. 5 Pemetaan RACI

DSS-01 Mengelola Operasi													
Deskripsi	Mengkoordinasi dan mengeksekusi aktivitas dan prosedur operasional yang dibutuhkan, untuk mengirimkan layanan TI internal maupun dari luar, termasuk eksekusi dari standar prosedur operasional yang terdefinisi sebelumnya.												
Tujuan	Mengirimkan hasil layanan operasional TI sesuai dengan rencana.												
Pelaksanaan Manajemen (*Management Practice*)													
MP	Aktifitas	0	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2	Level	Output / Bukti
DSS-01.01 Menjalankan Prosedur Operasional	Memelihara prosedur operasional kegiatan TI.												
	Menjadwalkan dan melaksanakan aktivitas sesuai jadwal.												
	Memverifikasi data pemrosesan diterima dan terproses secara utuh, akurat dan tepat waktu.												

Form Kuesioner berisi daftar pertanyaan yang ditujukan ke responden dan diisi oleh koresponden secara langsung. Form kuesioner ini menghasilkan jawaban dari responden yang datanya dapat di analisis dan diolah kedalam proses audit.

Isi dari form kuesioner sebai berikut :

1) Lembar permohonan kesedian menjadi responden.
2) Identitas responden, responden mengisi identitas diri, seperti: nama, NIP, umur, jabatan/Divisi, lama kerja, jenis kelamin.
3) Petunjuk pengisian dan tabel kriteria jawaban
4) Tabel pertanyaan

3. Observasi

Setelah wawancara pertama dan kuesioner telah selesai, maka berikutnya yang dilakukan adalah melakukan wawancara kembali untuk mengetahui dokumentasi yang dimiliki oleh objek penelitian. Wawancara ini dilakukan kepada manajer atau minimal posisi yang setingkat diatas staff agar memperoleh dua jawaban hasil dari kuesioner yang diberikan kepada staff dan wawancara kepada minimal yang setingkat diatas staff. Juga untuk memastikan kondisi *existing* dengan keterangan dan bukti yang dimiliki.

.

Sumber Data Sekunder

Sumber data sekunder yang mendukung penelitian ini adalah dokumentesi yang di miliki oleh Unit CDC PT Telkom mengenai SIM-BL.

b. Tahap Pengolahan Data

Berikutnya setelah kuesioner terkumpul, maka dilakukan pengolahan data sebagai berikut:

1. Validitas

Uji validitas dilakukan terhadap isi instrumen, untuk mengukur kectepatan instrumen yang digunakan dalam suatu penelitian (Sugiyono, 2006) [1].

Tipe validitas pada penelitian ini adalah validitas internal, yaitu dengan mengkorelasikan jumlah skor tiap faktor (penjumlahan item dalam suatu faktor). Rumus yang digunakan untuk menguji validitas adalah rumus korelasi *product moment pearson*. Yaitu sebagai berikut:

$$r_i = \frac{N\sum XY - \sum X \sum Y}{\sqrt{\left\{N\sum X^2 - (\sum X)^2\right\}\left\{N\sum Y^2 - (\sum Y)^2\right\}}}$$

(Azwar,2001:19)

Keterangan :
r : Korelasi antar *instrument*

N : Jumlah sample
X_i : Jumlah skor item
Y_i : Jumlah skor total seluruh item

Dasar pengambilan keputusan:

3) Jika r positif, serta r ≥ 0.30 atau r ≥ tabel maka item pertanyaan tersebut valid.
4) Jika r tidak positif, serta r < 0.30 atau < r tabel maka item pertanyaan tersebut tidak valid.

2. **Pengolahan hasil kuesioner**

Untuk mengidentifikasi jawaban – jawaban atas hasil kuesioner dan wawancara kedalam form kerja audit dengan langkah sebagai berikut:

1. Mendefinisikan setiap jawaban dari item pertanyaan yang diberikan kepada responden yang sudah disusun. Nilai yang diperoleh dengan memberikan skor terhadap jawaban kuesioner yang diajukan kepada responden, dengan menggunakan 6 kriteria yang terdiri dari Level 0, 1, 2, 3, 4,5 sebagai berikut:

Tabel 3. 6 Indikator Level

Level	**PA**	**Deskripsi**
Level 0	0	Tidak dilakukan atau gagal
Level 1	1.1	Dilakukan dilakukan tetapi belum ada manajemennya
Level 2	2.1	Dilakukan dan ada perencanaan serta dimonitor
	2.2	Dilakukan , ada perencanaan dan dimonitor kemudian hasil kerja dikelola dengan baik (ditentukan *requirement*-nya & didokumentasikan)
Level 3	3.1	Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan atau dibuat standar pengoperasiannya, sebagai unsur penting yang wajib dilakukan
	3.2	Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan atau mempunyai standar penerapan, serta ada alokasi tanggung jawab dan sumber daya yang tepat
Level 4	4.1	Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan berjalan dengan baik dan ada penerapan ukuran layanan/informasi optimal yang harus dihasilkan
	4.2	Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan dan menghasilkan layanan/ informasi optimal kemudian dimonitor dan dianalisis
Level 5	5.1	Dilakukan, ada inovasi dan strategi pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya
	5.2	Dilakukan, ada inovasi dan strategi pengembangan aktifitas, diukur pengaruhnya terhadap sasaran bisnis dan dievaluasi

2. Memilih *Level* yang digunakan dengan menghitung frekuensi dari responden dengan pilihan jawabannya, kemudian diterapkan pada form kerja audit untuk hasil yang didapatkan.

Tabel 3. 7 Pemilihan Level

Level	Pilhan jawaban	Frekuensi
0	Tidak dilakukan atau gagal	0
1	1.1 Dilakukan dilakukan tetapi belum ada manajemennya	0
2	2.1 Dilakukan 44a nada perencanaan serta dimonitor 2.2 Dilakukan , ada perencanaan dan dimonitor kemudian hasil kerja dikelola dengan baik (ditentukan *requirement*-nya & didokumentasikan)	0
3	3.1 Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan atau dibuat standar pengoperasiannya, sebagai unsur penting yang wajib dilakukan 3.2 Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan atau mempunyai standar penerapan, serta ada alokasi tanggung jawab dan sumber daya yang tepat	0
4	4.1 Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan berjalan dengan baik 44a nada penerapan ukuran layanan/informasi optimal yang harus dihasilkan 4.2 Dilakukan, aktifitas tertulis di SOP/kebijakan/aturan dan menghasilkan layanan/ informasi optimal kemudian dimonitor dan dianalisis	0

5	5.1 Dilakukan, ada inovasi dan strategi pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya 5.2 Dilakukan, ada inovasi dan strategi pengembangan aktifitas, diukur pengaruhnya terhadap sasaran bisnis dan dievaluasi	0
Total		0

3.1.3 Tahap Analisis

Tahap analisis dibagi kedalam dua tahap, yaitu analisis COBIT dan analis rekomendasi

a. Analisis COBIT

Analisis *Capability Level*

Pada tahap ini dilakukan pengukuran *Level* dari tiap domain DSS yang diteliti. Pengukuran ini diperoleh berdasarkan pengolahan data hasil kuesioner yang telah diberikan kepada pihak terkait. Setelah itu akan diperoleh *capability Level* dari kondisi *existing* perusahaan.

b. Analisis rekomendasi

Setelah melakukan analisis berdasarkan COBIT 5, maka selanjutnya adalah mengidentifikasi rekomendasi yang sesuai dengan kebutuhan. Tahap ini berdasarkan analisa *gap* antara *Level existing* yang telah diperoleh dari hasil pengukuran dengan target *Level* kapabilitas perusahaan. Rekomendasi perbaikan ini diharapkan mampu membantu perusahaan dalam usaha pencapaian tujuan perusahaan. Adapun target *Level* kapabilitas yang diinginkan sebagai tujuan yang ingin dicapai, diperoleh berdasarkan wawancara yang dilakukan dengan pihak Unit CDC PT TelkomRekomendasi tersebut didapatkan dari analisis *gap* dari tingkat kematangan aktual dan kematangan yang diinginkan (ekspektasi)

Gap analysis

Pada bagian ini dilakukan analisis *gap* untuk mendefinisikan kesenjangan antara tingkat kematangan aktual dengan tingkat kematangan yang diinginkan (ekspektasi) dan menerjemahkan gaps tersebut menjadi peluang perbaikan.

Form ini digunakan untuk memperoleh hasil *Level Gap* yang ada yang nantnya di gunakan dalam proses penyusunan rekomendasi. Untuk memperoleh *Level Gap* dengan cara menganalisi hasil antara *Level* kondisi *existing* dengan Level targetnya. Kondisi *existing* didapat dari data yang diperoleh melalui kuesioner dan wawancara, kemudian *Level* target di peroleh dari wawancara dengan pihak *stakeholder*. Bentuk dari form ini berupa tabel.

Tabel 3. 8 Contoh Analisis Gap

Nama Proses	*Level Existing*	*Level Target*	*Gap*
DSS01 Manage Operations			
DSS02 Manage Service Requests and			

Incidents			
DSS03 Manage Problems			
DSS04 Manage Continuity			
DSS05 Manage Security Services			
DSS06 Manage Bussiness Process Controls			

Isi dari form pengambilan bukti sebagai berikut :

1) Nama Proses
2) Level Existing
3) Lavel Target
4) Gap

3.3 Tahap Kesimpulan dan Saran

Tahap ini merupakan tahap terakhir yang dilakukan. Kesimpulan berisi rangkuman dari proses dan hasil penelitian. Sedangkan saran berisi masukan atau rekomendasi tindakan lanjut penelitian berikutnya.

BAB IV
IMPLEMENTASI DAN ANALISIS HASIL

4.1 Teknik Pengumpulan Data

Tahap awal pelaksanaan audit ini adalah pengumpulan data, untuk mendukung penilaian, evaluasi lapangan dan juga untuk mengetahui kondisi nyata dari Bagian Bina Lingkungan Unit CDC PT Telkom terhadap audit yang dilakukan. Pengumpulan data dilakukan melalui kuesioner, wawancara, dan survey lapangan.

Dalam pengumpulan data melalui kuesioner dan wawancara ini dilakukan berdasarkan tabel *Raci Chart* yang sudah dipetakan dengan struktur organisasi dan sistem pengelolaan SI/TI di Bagian Bina Lingkungan Unit CDC PT Telkom .

4.1.1 Kuesioner

Pada tahap ini, dilakukannya kuesioner untuk mencari tanggapan-tanggapan dari para responden mengenai kondisi terkini yang ada pada Bagian Bina Lingkungan Unit CDC PT Telkom terkait dengan domain DSS (*Deliver, Service and Support*). Kuesioner ini berisikan pertanyaan – pertanyaan yang sesuai dengan proses – proses yang ada pada Domain DSS (*Deliver, Service and Support*).

Berikut adalah responden yang menerima kuisoner:

Tabel 4. 1 Responden Kuesioner

Divisi	Responden	Jumlah
Bagian Bina Lingkungan	Staff	3
Bagian PRANDAL	Staff	3
Divisi ITSS	Staff	6
TELKOM SIGMA	Staff	6
Total Responden	18	

Pada tabel 4.1 responden kuesioner dapat dilihat bahwa jumlah responden yang telah diberikan kuesioner ini adalah 18 orang, yang terdiri dari pihak – pihak internal di Bagian Bina Lingkungan Unit CDC PT Telkom, ITSS, dan Telkom Sigma. Sesuai dengan diagram RACI, yaitu untuk DSS 01 dan DSS 05 kuesionernya diberikan kepada Telkom Sigma, untuk DSS 02 dan DSS 03 diberikan kepada ITSS, dan untuk DSS 04 dan DSS 06 diberikan kepada PRANDAL dan Bina Lingkungan CDC PT Telkom.

4.1.2 Wawancara

Pada tahap wawancara ini, dilakukan untuk mengkroscek/mencari kebenaran dari tanggapan – tanggapan pada kuesioner yang telah di dapat, untuk melengkapi aktivitas yang respondennya hanya oleh pihak direktur/pihak manager dan juga untuk memperoleh bukti – bukti yang terkait dengan domain DSS (*Deliver, Service and Support*). Wawancara dilakukan secara *face to face* dengan responden didokumentasikan dengan notulensi wawancara.

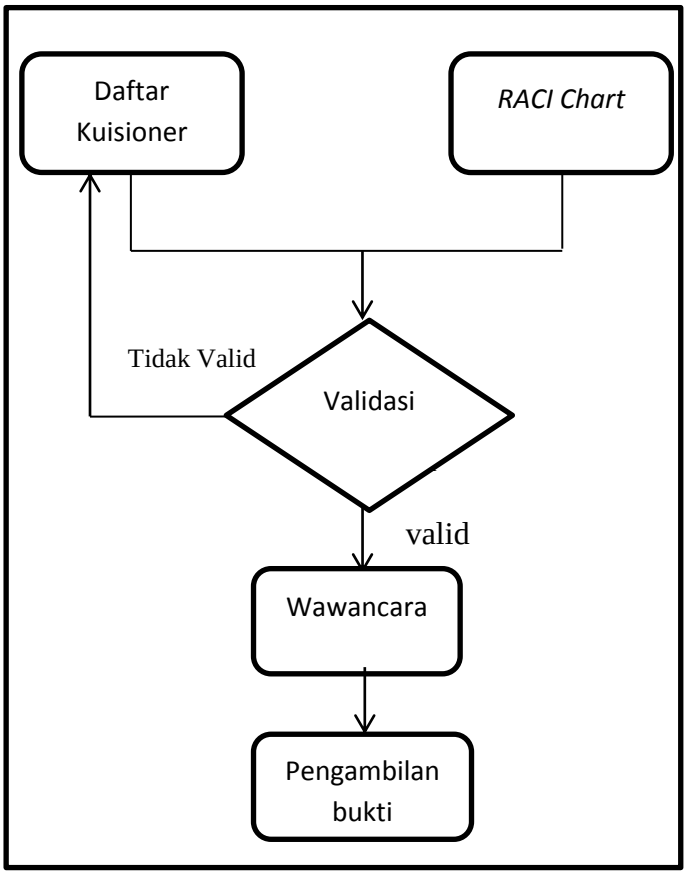
Berikut adalah responden untuk wawancara

Tabel 4. 2 Responden Wawancara

Nama	Nama Responden	Jumlah
Bapak Herry	SM Bina Lingkungan	1
Bapak Bambang Subagjo	*Manager* Sistem Informasi Bagian PRANDAL	1
Bapak Supriyono	*Manager* Perencanaan dan Pengembangan Bagian PRANDAL	1
Bapak Shoheh	*Officer I* Bagian Bina Lingkungan	1
Bapak Hadary Mallafi	PIC SIM-BL Divisi ITSS	1
Bapak Nazaruddin	PIC SIM-BL Telkom Sigma	1

4.1.2 Langkah Pengumpulan Data

Dalam pengumpulan data terdapat langkah tersendiri, berikut adalah langkah – langkah peneliti untuk melakukan pengumpulan data :



Gambar 4. 1 Pengumpulan Data

Langkah awal dari pengumpulan data ini mulai dari menyiapkan daftar kuesioner, kemudian di sesuai atau di petakan dengan hasil diagram RACI supaya daftar kuisoner tepat dengan sasaran. Setelah itu melakukan validasi hasil kuesioner, apabila data kuesioner ada yang tidak valid maka kuesioner yang tidak valid diulang kembali sampai menghasilkan hasil valid. Kemudian setelah semua data valid maka dilakukan kroscek dengan melakukan wawancara ke pihak yang memiliki jabatan tinggi di, kemudian disertai dengan pengambilan bukti.

4.2 Teknik Pengukuran Data

Pengukuran data digunakan untuk menilai apakah hasil dari kuesioner tersebut dapat dipercaya atau valid. Dalam teknik pengukuran data disini menggunakan validasi. Jenis – jenis dari validasi pun bermacam – macam, disini penulis mneggunakan jenis validasi korelasi *product moment* yang di kemukakan oleh *pearson*.

Pemilihan jenis validasi dengan korelasi *product moment* ini dirasa cocok karena instrument yang digunakan dalam pengukuran validasi ini serupa (menggunakan *variable interval*), dan cara perhitungan yang dapat diterapkan dengan baik. Pada validasi korelasi *product moment* ini item dikatakan valid jika nilai-nilai *Total Correlation* lebih besar dari nilai kritis. Item pertanyaan yang memiliki nilai koefisien validitas lebih besar dari nilai r-kritisnya dapat disimpulkan bahwa item tersebut valid dalam yang berarti bahwa item yang digunakan untuk mengukur suatu kajian dalam Bagian Bina Lingkungan Unit CDC PT Telkom dalam domain DSS (*Deliver, Service and Support*) menghasilkan data yang valid/dapat dipercaya.

Hasil nilai perhitungan validasi tiap item dapat dilihat pada lampiran.

4.3 Analisis Hasil

4.3.1 Analisis Validasi Kuesioner

Validasi dilakukan dengan menggunakan metode *product moment pearson*. Dengan menghitung masing-masing per sub bab domain DSS setelah dilakukan rekapitulasi di table (terdapat dilampiran). Validasi ini untuk mengetahui tingkat korelasi jawaban dengan pertanyaan yang diajukan. Hasilnya jikalau angka validasi yang didapat <0.3 maka terdapat ketidakvalidan, sehingga yang dilakukan adalah menjelaskan kembali maksud pertanyaan kepada responden jikalau masih belum valid maka perlu diperbaiki pertanyaan di sub bab tersebut sampai memperoleh angka >0.3 (valid).

4.3.2 Analisis Hasil Kuesioner

Dalam menentukan kondisi pada *Level* manakah aktifitas – aktifitas yang terdapat pada form kerja audit itu berada, maka dilakukan analisis berupa mencari *Level* yang tepat pada form hasil kuesioner. Penentuan *Level* ditiap aktifitas ini dilakukan dengan memilih nilai modus atau nilai yang paling banyak muncul pada tiap aktifitasnya. Dan apabila nilai yang muncul itu terdapat 2 *Level* atau mungkin lebih, maka yang di pilih adalah nilai *Level* yang terkecil diantaranya, misalkan pada DSS01-02 pada aktifitas ke 1 terdapat 5 responden, kemudian dari 5 responden yang memilih di *Level* 3 adalah 2 orang, di *Level* 4 adalah 1 orang, dan di *Level* 5 adalah 2 orang. Maka *Level* yang terpilih adalah pada *Level* 3, karena

diartikan juga berarti 2 orang yang memilih di *Level* 5 tersebut juga merasa bahwa pada aktifitas ke 5 telah berada pada *Level* 3.

Berikut adalah hasil analisis hasil pada domain DSS01 – DSS06:

1. DSS01-01 Menjalankan Prosedur Operasional

Tabel 4. 3 Analisis DSS01-01

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Memelihara prosedur operasional kegiatan TI.	0	0	0	3	0	3	3
2. Menjadwalkan dan melaksanakan aktivitas sesuai jadwal.	0	0	1	3	1	1	3
3. Memverifikasi data pemrosesan diterima dan terproses secara utuh, akurat dan tepat waktu.	0	0	0	2	3	1	4
4. Memastikan standar keamanan sesuai dengan permintaan, pemrosesan, penyimpanan dan keluaran data.	0	0	0	2	4	0	4
5. Membuat *backup* untuk jadwal, pengambilan data, dan *log* data sesuai dengan prosedur yang dibuat.	0	0	1	1	1	3	5

Jadi berdasarkan tabel 4.3 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS01-01 pada aktifitas ke-1 dan ke-2 adalah 3, aktifitas ke-3 dan ke-4 adalah 4, dan aktifitas ke-5 adalah 5.

2. DSS01-02 Mengelola Layanan *Outsourced IT*

Tabel 4. 4 Analisis DSS01-02

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Memastikan bahwa kebutuhan institusi terhadap keamanan proses informasi sesuai SLA *(SERVICE LEVEL AGREEMENT) third party.*	0	0	0	2	3	1	4
2. Memastikan bahwa prioritas TI untuk pengiriman layanan ditaati	0	0	0	2	0	4	5

menurut SLA *third party.*							
3. Apakah proses manajemen internal TI terintegrasi dengan proses manajemen TI *provider* pihak luar.	0	0	0	2	1	3	5
4. Apakah dilakukan audit independen terhadap lingkungan operasional kerja *provider* pihak luar.	0	0	0	2	1	3	5

Jadi berdasarkan tabel 4.3 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS01-01 pada aktifitas ke-1 adalah 4 dan aktifitas ke-2, ke-3, ke-4, dan ke-5 adalah 5

3. DSS01-03 Memonitor Infrastruktur TI

Tabel 4. 5 Analisis DSS01-03

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi *Level* informasi yang dicatat berdasarkan risiko dan performansi.	0	0	1	1	1	3	5
2. Memelihara daftar aset infrastruktur yang perlu dimonitor berdasarkan tingkat kepentingan layanan.	0	0	0	1	2	3	5
3. Mengidentifikasi batasan pelanggaran dan *event conditions.*	0	0	1	2	2	1	3
4. Membuat *event log* dan memeliharanya dalam jangka waktu tertentu guna investigasi selanjutnya.	0	0	0	1	2	3	5
5. Membuat prosedur untuk memonitor *event log* yang telah dibuat.	0	0	1	3	1	1	3
6. Membuat *incident tickets* tepat ketika ada pelanggaran saat monitoring.	0	0	1	2	2	1	3

Jadi berdasarkan tabel 4.4 diperoleh nilai *capability* untuk aktifitas-aktifitas DSS01-03 pada aktifitas ke-1, ke-2, dan ke-4 adalah 5, aktifitas ke-3, ke-5, dan ke-6 adalah 3.

4. DSS01-04 Mengelola Lingkungan

Tabel 4. 6 Analisis DSS01-04

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi bencana alami atau bencana yang dikarenakan manusia yang mungkin terjadi.	0	0	1	2	2	1	3
2. Mengidentifikasi bagaimana peralatan TI terlindungi dari ancaman.	0	0	1	1	4	0	4
3. Membangun fasilitas TI pada lingkungan yang relatif aman dari ancaman.	0	0	1	1	4	0	4
4. Menjaga alat-alat yang dapat mendeteksi ancaman (air, api, asap).	0	0	1	1	1	3	5
5. Membuat prosedur, dokumentasi, dan pelatihan untuk respon peringatan bencana.	0	0	0	2	3	1	4
6. Membandingkan kemungkinan terjadinya bencana terhadap kebutuhan asuransi.	0	0	0	1	4	1	4
7. Membangun lokasi TI yang aman dari dampak bencana.	0	0	0	2	2	2	3
8. Membangun ruang server yang aman dan bersih.	0	0	0	0	3	3	4
9. Membangun fasilitas TI yang tahan terhadap fluktuasi tenaga listrik.	0	0	0	0	4	2	4

Jadi berdasarkan tabel 4.5 diperoleh nilai *capability* untuk aktifitas-aktifitas DSS01-04 pada aktifitas ke-1 dan ke-7 adalah 3, aktifitas ke-2, ke-3, ke-5, ke-6, ke-8, ke-9 adalah 4, dan aktifitas ke-4 adalah 5.

5. DSS01-05 Mengelola Fasilitas

Tabel 4. 7 Analisis DSS01-05

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat mekanisme pengelolaan fasilitas TI jika sumber tenaga putus.	0	0	1	1	1	3	5
2. Membuat fasilitas *housing system* TI yang mempunyai lebih dari satu sumber tenaga.	0	0	0	1	2	3	5
3. Memastikan sistem kabel untuk fasilitas TI mempunyai proteksi yang bagus.	0	0	0	2	1	3	5
4. Memastikan sistem kabel dengan alat-alatnya yang terhubung telah terstruktur dengan baik.	0	0	0	1	3	2	4
5. Menganalisis fasilitas yang memadai untuk penerapan high-*availability system.*	0	0	0	1	3	2	4
6. Menyesuaikan fasilitas TI yang ada dengan panduan kesehatan dan keamanan.	0	0	0	1	4	1	4
7. Mencatat, memonitor dan memperbaiki fasilitas TI 8. yang rusak.	0	0	0	0	4	2	4
9. Memberi pemahaman pada staf TI tentang *safety guidelines* dalam memanfaatkan fasilitas TI.	0	0	0	0	4	2	4
10. Memelihara fasilitas TI sesuai panduan layanan dan spesifikasi dari *supplier.*	0	0	0	0	3	3	4
11. Menganalisis terlebih dahulu jika ada penggantian lokasi TI.	0	0	0	2	3	1	4

Jadi berdasarkan tabel 4.6 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS01-05 pada aktifitas ke-1 sampai ke-3 adalah 5, dan pada aktifitas ke-4 sampai ke-11 adalah 4.

6. DSS-02.01 Mendefinisikan Skema Klasifikasi Insiden dan Permintaan Layanan

Tabel 4. 8 Analisis DSS02-01

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	1	2	3	4	5	
1. Membuat skema klasifikasi dan prioritas dari permintaan layanan.	0	0	0	3	3	0	3
2. Menentukan model kemungkinan insiden/dampak dari *known errors* (kesalahan yang terdiagnosis).	0	0	2	3	1	0	3
3. Membuat model permintaan layanan sesuai dengan jenis-jenisnya.	0	0	0	5	1	0	3
4. Menentukan Level-Level insiden terutama untuk insiden besar dan insiden tentang keamanan.	0	0	2	4	0	0	3
5. Membuat daftar insiden dan *knowledges sources* untuk menanganinya.	0	0	0	2	4	0	4

Jadi berdasarkan tabel 4.8 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-01 pada aktifitas ke-1 sampai ke-4 adalah 3 dan pada aktifitas ke-5 adalah 4.

7. DSS-02.02 Mengklasifikasikan dan memprioritaskan permintaan dan insiden

Tabel 4. 9 Analisis DSS02-02

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	1	2	3	4	5	
1. Membuat *log* untuk permintaan layanan dan insiden-insiden.	0	0	0	2	4	0	4
2. Mengklasifikasian jenis dan kategori *service request* dan	0	0	0	2	4	0	4

	insiden.							
3.	*Service request* dan insiden berdasarkan SLA pada poin pelayanan menjadi prioritas.	0	0	0	3	3	0	3

Jadi berdasarkan tabel 4.9 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-02 pada aktifitas ke-1 dan ke-2 adalah 4, dan pada aktifitas ke-3 adalah 3.

8. DSS-02.03 Memverifikasi, menyetujui dan memenuhi permintaan

Tabel 4. 10 Analisis DSS02-03

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Memverifikasi pemberian hak bagi pelaksana permintaan layanan.	0	0	0	0	2	4	5
2. Meminta persetujuan finansial dan fungsional ketika akan memenuhi permintaan layanan.	0	0	0	0	1	5	5
3. Memenuhi permintaan layanan sesuai prosedur yang dipilih.	0	0	0	0	1	5	5

Jadi berdasarkan tabel 4.8 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-03 pada aktifitas ke-1 sampai 3 adalah 5.

9. DSS-02.04 Mendiagnosis dan mengalokasikan insiden

Tabel 4. 11 Analisis DSS02-04

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi kemungkinan penyebab-penyebab insiden/masalah.	0	0	0	0	2	4	**5**
2. Membuat log masalah baru jika insiden yang terjadi belum ada di daftar *known*	0	0	0	0	1	5	**5**

errors.							
3. Mencari tenaga ahli jika diperlukan penanganan masalah yang lebih mendalam.	0	0	0	0	3	3	**4**

Jadi berdasarkan tabel 4.11 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-04 pada aktifitas ke-1 dan ke-2 adalah 5, dan pada aktifitas ke-3 adalah 4.

10. DSS02-05 Menyelesaikan dan memulihkan insiden

Tabel 4. 12 Analisis DSS02-05

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Memilih dan mengimplementasikan resolusi (pemecahan insiden) yang paling tepat.	0	0	0	1	2	3	5
2. Mencatat ada atau tidaknya implementasi solusi alternatif.	0	0	0	1	1	4	5
3. Menjalankan data *recovery* / pemulihan jika diperlukan.	0	0	0	2	1	3	5
4. Mendokumentasikan dan menilai resolusi insiden yang telah dilaksanakan.	0	0	0	0	1	5	3

Jadi berdasarkan tabel 4.12 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-05 pada aktifitas ke-1 sampai dengan ke-3 adalah 5, dan aktifitas ke-4 adalah 3.

11. DSS02-06 Menutup permintaan layanan dan insiden

Tabel 4. 13 Analisis DSS02-06

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Memverifikasi dengan *user* bahwa permintaan layanan telah terpenuhi secara memuaskan.	0	0	0	1	2	3	5

2. Menutup permintaan layanan yang telah terselesaikan.	0	0	1	2	3	0	4

Jadi berdasarkan tabel 4.13 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-06 pada aktifitas ke-1 adalah 5 dan aktifitas ke- 2 adalah 4.

12. DSS02.07 Melacak status dan membuat laporan

Tabel 4. 14 Analisis DSS02-07

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Melacak tingkatan/Level insiden dan resolusinya guna perbaikan dan ketuntasan penanganan insiden.	0	0	0	0	3	3	4
2. Mengidentifikasi informasi dan kebutuhan *stakeholders* terhadap laporan dan frekuensi pelaporannya.	0	0	0	1	2	3	5
3. Mengungkapkan tren insiden yang muncul dan pola permasalahannya.	0	0	0	2	1	3	5
4. Membuat laporan dan mendistribusikannya secara tepat waktu.	0	0	0	1	5	0	4

Jadi berdasarkan tabel 4.14 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-07 pada aktifitas ke-1 dan ke-4 adalah 4, dan pada aktifitas ke-2 dan ke-3 adalah 5.

13. DSS03-01 Mengidentifikasi dan mengklasifikasikan masalah

Tabel 4. 15 Analisis DSS03-01

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi masalah sesuai dengan korelasinya terhadap laporan insiden.	0	0	0	0	5	1	4
2. Melakukan penanganan masalah secara formal dengan akses ke semua data yang relevan.	0	0	0	0	1	5	5
3. Membuat *support group* untuk membantu identifikasi dan analisis akar masalah.	0	0	0	1	5	0	4

4. Mendefinisikan Level prioritas masalah melaui konsultasi dengan pihak manajemen bisnis.	0	0	0	1	5	0	4
5. Membuat report status dari masalah yang telah diidentifikasi.	0	0	0	1	5	0	4
6. Membuat katalog untuk semua *manajemen problems.*	0	0	0	1	5	0	4

Jadi berdasarkan tabel 4.15 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS02-07 pada aktifitas ke-1, 3, 4, 5 dan 6 adalah 4, dan aktifitas ke-2 adalah 5.

14. DSS03-02 Menginvestigasi dan mendiagnosis masalah

Tabel 4. 16 Analisis DSS03-02

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi problems yang bisa jadi adalah *known error.*	0	0	0	0	2	5	5
2. Mengasosiasi items yang terkena pengaruh *problems* ke dalam data/daftar *known errors*.	0	0	0	1	5	0	4
3. Membuat laporan progress ketika sedang menyelesaikan *problems.*	0	0	0	1	4	1	4

Jadi berdasarkan tabel 4.16 diperoleh nilai capability untuk aktifitas - aktifitas DSS03-02 pada aktifitas ke-1 adalah 5, aktifitas ke-2 dan ke-3 adalah 4.

15. DSS03-03 Mencatat *known error*

Tabel 4. 17 Analisis DSS03-03

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat *known error records* dan membangun solusi yang sesuai.	0	0	0	2	4	0	4
2. Mengidentifikasi dan menentukan prioritas dan pembuatan solusi terhadap *known errors.*	0	0	0	0	2	4	5

Jadi berdasarkan tabel 4.17 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS03-03 pada aktifitas ke-1 adalah 4, dan aktifitas ke-2 adalah 5.

16. DSS03-04 Menyelesaikan dan menutup masalah

Tabel 4. 18 Analisis DSS03-04

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Menutup *problems* yang telah selesai.	0	0	0	2	4	0	4
2. Menginformasikan penutupan *problems* ke *service desk.*	0	0	0	2	4	0	4
3. Mencatat penanganan yang berbeda dengan manajemen problems yang sebelumnya ditentukan.	0	0	2	4	0	0	3
4. Memonitor *impact* yang masih berlangsung.	0	0	0	2	4	0	4
5. Me-*review* dan mengkonfirmasi bahwa solusi masalah yang besar telah berhasil.	0	0	0	2	0	4	5
6. *Meeting* atau *sharing* pengetahuan yang diambil dari penanganan masalah dengan pihak *unit* lain.	0	0	0	2	4	0	4

Jadi berdasarkan tabel 4.18 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS03-04 pada aktifitas ke-1, 2, dan ke-4 adalah 4, aktifitas ke-3 adalah 3, dan aktifitas ke-5 adalah 5.

17. DSS-03.05 Menjalankan manajemen masalah secara proaktif

Tabel 4. 19 Analisis DSS03-05

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Mencatat informasi masalah yang berkaitan dengan insiden.	0	0	0	0	5	1	4
2. Melakukan diskusi tentang kemungkinan *known errors* dengan pihak –pihak yang menangani insiden, *problems*, dan perubahan TI dikarenakan insiden.	0	0	1	5	0	0	3

3. Memonitor *total cost* dari penanganan masalah-masalah.	0	0	0	0	3	3	4
4. Membuat laporan kesesuaian penanganan *problems* dengan kebutuhan dan SLA.	0	0	0	2	4	0	4
5. Mengoptimalkan penggunaan *resources* untuk penanganan masalah.	0	0	0	2	4	0	4
6. Menentukan *permanent fix* terhadap akar permasalahan.	0	0	0	4	0	2	3

Jadi berdasarkan tabel 4.19 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS03-05 pada aktifitas ke-1,3,4 dan 5 adalah 4, dan aktifitas ke-2 dan 6 adalah 3.

18. DSS04-01 Menjaga strategi keberlanjutan

Tabel 4. 20 Analisis DSS04-01

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi proses bisnis internal maupun *outsourced* yang kritikal bagi institusi.	0	0	1	2	3	0	4
2. Mengidentifikasi *key stakeholder* dan perannya untuk membuat kebijakan keberlanjutan bisnis/	0	0	2	3	1	0	3
3. Melakukan pendefinisian tujuan dan runag lingkup minimum yang harus dicapai untuk keberlangsungan bisnis.	0	0	2	3	1	0	3
4. Mengidentifikasi proses-proses pendukung bisnis dan layanan-layanan TI yang bersifat esensial.	0	0	3	4	0	0	3

Jadi berdasarkan tabel 4.20 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS03-05 pada aktifitas ke-1 adalah 4, dan aktifitas ke-2 sampai ke-4 adalah 3

.

19. DSS04-01 Menjaga strategi keberlanjutan

Tabel 4. 21 Analisis DSS04-02

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat skenario untuk kemungkinan *event* yang menyebabkan *incident* yang signifikan.	0	0	3	2	1	0	2
2. Menganalisis impact ke bisnis, sebagai evaluasi pengaruh gangguan atau insiden terhadap waktu.	0	0	2	3	0	1	3
3. Menentukan lama waktu minimum yang dibutuhkan untuk memulihkan proses bisnis dan dukungan TI.	0	0	3	1	1	1	3
4. Menilai kondisi ancaman seperti apa yang menyebabkan kehilangan *business continuity*.	0	0	2	3	1	0	3
5. Menganalisis *continuity requirements* untuk menghasilkan strategi bisnis dan strategi teknik yang baik.	0	0	2	3	0	1	3
6. Menentukan siapa yang memberi keputusan kunci agar rencana-rencana *continuity* dapat diajukan.	0	0	5	1	0	0	2
7. Mengidentifikasi *resource* dan *cost* untuk setiap strategi *continuity* dan rekomendasi yang dibuat.	0	0	2	2	2	0	2
8. Meminta *approval* terhadap strategi-strategi TI yang telah direncanakan kepada pihak eksekutif.	0	0	2	3	0	1	3

Jadi berdasarkan tabel 4.21 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-02 pada aktifitas ke-1,6 dan 7 adalah 2, dan aktifitas ke-2,3,4,5 dan ke-8 adalah 3.

20. DSS04-03 Mengembangkan dan mengimplementasikan respon dari keberlangsungan bisnis

Tabel 4. 22 Analisis DSS04-03

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Menentukan respon-respon dan komunikasinya terhadap gangguan yang muncul.	0	0	0	5	1	0	3
2. Mengembangkan dan menjaga *Business Continuity Plan (BCP)* yang mengandung prosedur-prosedur.	0	0	0	2	4	0	4
3. Menjamin *key suppliers* dan outsourced partners mempunyai continuity plan yang sesuai.	0	0	2	4	0	0	3
4. Mendefinisikan kondisi dan prosedur *recovery* yang mendukung keberlanjutan *business processing*.	0	0	2	4	0	0	2
5. Mendefinisikan *resources* yang dibutuhkan untuk mendukung *prosedur recovery*.	0	0	2	3	1	0	3
6. Mendefinisikan dan mencatatat informasi tentang *backup requirement* untuk mendukung rencana.	0	0	2	3	1	0	3
7. Menentukan skill individual yang dibutuhkan untuk mengimplementasikan rencana dan prosedur.	0	0	5	0	1	0	2
8. Mendistribusikan rencana dan *supporting documents* yang telah disusun ke pihak lain secara aman.	0	0	1	3	1	1	3

Jadi berdasarkan tabel 4.22 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-03 pada aktifitas ke-1,3,5,6 dan ke-8 adalah 3, aktifitas ke-2 adalah 4, dan aktifitas ke-4 dan 7 adalah 2.

21. DSS04-04 Latihan, tes, dan review dokumen *business continuity plan (BCP)*

Tabel 4. 23 Analisis DSS04-04

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Mendefinisikan tujuan dalam menguji proses bisnis, teknikal dan administratif yang ada di BCP.	0	0	1	4	1	0	3
2. Meminta persetujuan dengan *stakeholders* bahwa pengerjaan rencana bersifat realistik.	0	0	0	2	1	3	5
3. Membagi peran dan tanggung jawab dalam pelaksanaan pelatihan dan pengujian *continuiy plan*	0	0	0	2	0	4	5
4. Membuat jadwal pelatihan dan pengujian *continuity plan.*	0	0	1	5	0	0	3
5. Melakukan evaluasi dan analisis setelah pelatihan.	0	0	1	3	2	0	3
6. Membuat rekomendasi untuk mengembangkan *continuity plan* berdasarkan hasil pengujian dan review.	0	0	2	4	0	0	3

Jadi berdasarkan tabel 4.23 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-04 pada aktifitas ke-1, 4, 5, dan ke-6 adalah 3, aktifitas ke-2 dan ke-3 adalah 5

22. DSS04-05 *Review*, menjaga dan mengembangkan *continuity plan*

Tabel 4. 24 Analisis DSS04-05

Aktifitas	Frekuensi pilihan						*Level* yang dipilih
	0	**1**	**2**	**3**	**4**	**5**	
1. Me-*review* kapabilitas *continuity plan* terhadap operasional bisnis dan tujuan strategis	0	0	1	4	1	0	3
2. Merevisi *business impact assessment* jika diperlukan.	0	0	2	3	1	0	3

3. Memberi rekomendasi perubahan pada kebijakan, prosedur, infrastruktur yang ada di dalam BCP.	0	0	2	2	1	1	3
4. Me-*review continuity plan* secara teratur guna melihat ada atau tidak dampaknya terhadap bisnis.	0	0	0	2	4	0	4

Jadi berdasarkan tabel 4.24 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-05 pada aktifitas ke-1 sampai ke-3 adalah 3, dan aktifitas ke-4 adalah 4.

23. DSS04-06 Mengadakan training untuk continuity plan

Tabel 4. 25 Analisis DSS04-06

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mendefinisikan kebutuhan dan rencananya dalam mengadakan training *continuity plan.*	0	0	0	2	4	0	4
2. Pengembangan kompetensi/ skill ketika melakukan training.	0	0	1	4	0	1	3
3. Monitoring *skill* dan kompetensi berdasarkan hasil dari training dan pengujian.	0	0	1	4	0	1	3

Jadi berdasarkan tabel 4.25 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-05 pada aktifitas ke- 1 adalah 4, dan aktifitas ke-2 dan 3 adalah 3.

24. DSS04-07 Mengatur *backup*

Tabel 4. 26 Analisis DSS04-07

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Melakukan *backup* terhadap sistem, aplikasi, data dan dokumentasi sesuai dengan jadwal.	0	1	2	2	0	1	2
2. Memastikan bahwa *backup* yang dilakukan oleh *third parties* dilakukan dengan baik dan aman.	0	0	2	3	1	0	3
3. Mendefinisian *requirements* untuk *on-site* dan *off-site backup* sesuai dengan *business*	0	0	2	3	1	0	3

requirements.							
4. Membangun kesadaran *business continuity plan* pada staf-staf dan diadakan pelatihan.	0	0	1	4	0	1	3
5. Menguji dan me-refresh *archived* dan *backup* data secara periodik.	0	0	2	3	0	1	3

Jadi berdasarkan tabel 4.26 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS04-07 pada aktifitas ke-1 adalah 2 dan aktifitas ke-3 sampai ke-5 adalah 3.

25. DSS04-08 Melakukan *review* ulang

Tabel 4. 27 Analisis DSS04-08

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Menilai ketaatan terhadap pelaksanaan *business continuity plan.*	0	0	3	2	1	0	2
2. Menentukan keefektifan *business continuity plan.*	0	0	2	3	1	0	3
3. Mengidentifikasi kelemahan dan kelalaian dalam *continuity plan* dan dibuat rekomendasi perbaikan.	0	0	1	4	0	1	3
4. Meminta approval dari manajemen institusi jika dilakukan perubahan pada *continuity plan* .	0	0	1	3	2	0	3

Jadi berdasarkan tabel 4.27 diperoleh nilai capability untuk aktifitas - aktifitas DSS04-08 pada aktifitas ke-1 adalah 2 dan aktfitas ke-2 sampai ke-4 adalah 3.

26. DSS05-01 Perlindungan dari *malware*

Tabel 4. 28 Analisis DSS05-01

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengkomunikasikan kesadaran terhadap *malware* dan menerapkan prosedur	0	0	2	0	0	4	5

pencegahan.							
2. Menginstal dan aktivasi tools proteksi terhadap *malware* untuk semua fasilitas pemrosesan.	0	1	0	1	0	4	5
3. Mengkonfigurasi semua proteksi terhadap *software* berbahaya secara terpusat.	0	1	1	0	1	4	5
4. Melakukan *review* secara teratur dan evaluasi informasi terhadap potensi ancaman baru	0	0	1	0	1	4	5
5. Menerapkan filter terhadap *traffic* yang masuk seperti *email* dan *download*.	0	0	0	0	2	4	5
6. Mengadakan pelatihan pada staf-staf tentang *malware* pada *email* dan penggunaan internet.	0	0	0	0	2	4	5

Jadi berdasarkan tabel 4.28 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-01 pada aktifitas ke-1 sampai ke-5 adalah 5.

27. DSS05-02 Mengelola jaringan dan keamanan konektivitas

Tabel 4. 29 Analisis DSS05-02

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat kebijakan untuk keamanan konektivitas berdasarkan penilaian risiko.	0	0	1	1	3	1	4
2. Menentukan otorisasi terhadap *devices* yang boleh mengakses informasi institusi dan jaringan insitusi.	0	0	2	0	2	2	2
3. Membuat mekanisme *filtering* untuk jaringan seperti *firewalls* dan intrusion detection *software*.	0	0	1	1	2	2	4
4. Menerapkan enkripsi informasi saat pengiriman berdasarkan klasifikasinya.	0	0	2	0	2	2	2
5. Menerapkan protokol keamanan yang telah disetujui untuk	0	0	1	1	2	2	4

konektivitas jaringan.							
6. Melakukan konfigurasi peralatan jaringan dengan aman.	0	0	0	2	2	2	3
7. Membangun mekanisme yang terpercaya untuk mendukung transmisi yang aman.	0	0	1	1	2	2	4
8. Mengadakan *penetration test* atau simulasi untuk melihat kehandalan jaringan.	0	0	1	1	3	1	4
9. Menguji sistem keamanan secara berkala untuk menentukan kecukupan sistem perlindungan.	0	0	2	0	1	3	5

Jadi berdasarkan tabel 4.29 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-02 pada aktifitas ke-1, 5, 7, dan 8 adalah 4, dan aktifitas ke-2 dan ke-4 adalah 2, aktifitas ke-6 adalah 3.

28. DSS05-03 Mengelola keamanan *endpoint*

Tabel 4. 30 Analisis DSS05-03

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengkonfigurasi sistem operasi dengan cara yang aman.	0	0	1	1	0	4	5
2. Membuat mekanisme *lockdown* untuk perangkat-perangkat TI.	0	0	1	1	1	3	5
3. Mengenkripsi informasi pada penyimpanan/*storage* sesuai dengan klasifikasinya.	0	0	2	0	1	3	5
4. Mengatur remote access and control.	0	0	1	0	2	3	5
5. Mengkonfigurasi jaringan dengan cara aman.	0	0	2	0	1	3	5
6. Mengimplementasi *traffic filtering* pada jaringan di perangkat *endpoints.*	0	0	1	0	3	2	4
7. Melindungi dan menjaga integritas sistem.	0	0	1	0	3	2	4

8. Apakah dilakukan proteksi secara fisik untuk perangkat *endpoint*	0	0	1	0	2	3	5
9. Membuang *devices* yang tidak terpakai lagi dengan cara yang benar dan aman.	0	0	1	0	1	4	5

Jadi berdasarkan tabel 4.30 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-03 pada aktifitas ke-1 sampai ke-5 dan aktifitas ke-8 adalah 5, dan aktifitas ke-6 dan ke-7 adalah 4.

31. DSS05-04 Mengelola identitas *user* dan *logical access*

Tabel 4. 31 Analisis DSS05-04

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Menjaga hak-hak akses user sesuai dengan fungsi bisnis dan kebutuhan prosesnya..	0	0	1	1	1	3	5
2. Memastikan bahwa semua peran-peran telah terdefinisi dengan baik dan *unique* untuk tiap peran.	0	0	0	1	2	3	5
3. Melakukan *authentication* semua akses terhadap aset informasi berdasarkan klasifikasi keamanannya.	0	0	0	1	3	2	4
4. Mengatur siapa yang dapat melakukan perubahan terhadap hak-hak akses *(create, modification, delete).*	0	0	0	1	2	3	5
5. Memisahkan dan mengelola *privileged user account*	0	0	0	1	4	1	4
6. Melakukan *review* manajemen secara teratur/rutin mengenai semua akun dan hak-hak terkait.	0	0	0	1	3	2	4
7. Memastikan bahwa semua user dan aktivitasnya secara *unique* telah teridentifikasi.	0	0	1	0	1	4	5
8. Melakukan audit terhadap akses informasi-informasi yang	0	0	1	0	1	4	5

bersifat sangat sensitif.							

Jadi berdasarkan tabel 4.31 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-04 pada aktifitas ke-1, 2, 4, 7, dan 8 adalah 5, dan aktifitas ke-3,5 dan ke-6 adalah 4.

32. DSS05-05 Mengelola akses fisik ke aset TI

Tabel 4. 32 Analisis DSS05-05

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengelola permintaan dan pemberian akses ke fasilitas TI.	0	0	1	1	0	4	5
2. Memastikan bahwa profil akses tidak berubah-ubah.	0	0	1	1	1	3	5
3. Memastikan bahwa profil akses tidak berubah-ubah.	0	0	1	1	0	4	5
4. Menginstruksi kepada semua staf untuk memakai tanda pengenal yang terlihat.	0	0	1	0	2	3	5
5. Menemani pengunjung yang masuk ke IT sites dan tidak ditinggal sendirian.	0	0	1	0	2	3	5
6. Membangun pembatasan akses ke bagian lingkungan TI yang sensitif (pagar, dinding).	0	0	1	0	2	3	5
7. Mengadakan pelatihan / training tentang kesadaran keamanan fisik.	0	0	0	1	2	3	5

Jadi berdasarkan tabel 4.32 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-05 pada aktifitas ke-1 sampai ke-7 adalah 5.

33. DSS05-06 Mengelola dokumen yang sensitif dan perangkat output

Tabel 4. 33 Analisis DSS05-06

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	

1. Pengaturan penggunaan dan pembuangan form sensitif dan *output devices* baik di dalam/luar institusi.	0	0	1	1	1	3	5
2. Pengaturan hak untuk mengakses dokumen sensitif dan perangkat *output.*	0	0	1	1	0	4	5
3. Pembuatan inventarisasi dokumen yang sensitif dan perangkat *output.*	0	0	1	1	0	4	5
4. Pemberian perlindungan fisik secara tepat terhadap dokumen yang sensitif dan perangkat *output.*	0	0	1	0	3	2	4
5. Penghancuran informasi sensitif dan perangkat *output* dengan cara yang tepat.	0	0	1	1	1	3	5

Jadi berdasarkan tabel 4.33 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-05 pada aktifitas ke-1 sampai ke-3 dan 5 adalah 5, dan aktifitas ke-4 adalah 4.

34. DSS05-07 Memantau infrastruktur yang berhubungan dengan *security events*

Tabel 4. 34 Analisis DSS05-07

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mencatat *events* yang berkaitan dengan keamanan yang diperoleh dari alat-alat pemantau keamanan.	0	0	2	0	4	0	4
2. Menetapkan sifat dan karakteristik inisiden potensial yang berhubungan dengan keamanan.	0	0	1	1	3	1	4
3. Melakukan *review* secara rutin terhadap *event logs* untuk insiden-insiden yang potensial..	0	0	1	1	1	3	5
4. Memelihara prosedur dalam mengumpulkan bukti-bukti *security events.*	0	0	1	1	2	2	4

5. Memastikan *incident tickets* dibuat dengan tepat waktu.	0	0	1	1	1	3	3

Jadi berdasarkan tabel 4.34 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS05-07 pada aktifitas ke-1,2 dan ke-4 adalah 4, aktifitas ke-3 adalah 5, dan aktifitas ke 5 adalah 3.

35. DSS06-01 Menyelaraskan aktivitas-aktivitas kontrol yang ada di proses bisnis dengan sasaran institusi

Tabel 4. 35 Analisis DSS06-01

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengidentifikasi *control activities* yang berpengaruh terhadap proses-proses bisnis kunci.	0	0	1	0	5	0	4
2. Menetapkan prioritas *control activities* berdasarkan analisis risiko di proses bisnis.	0	0	2	0	3	1	4
3. Memastikan siapa yang memegang *control activities* utama	0	0	1	2	2	1	3
4. Memonitor *control activities* secara berkelanjutan pada *end-to-end.*	0	0	2	0	3	1	4
5. Mengembangkan pola dan operasional kontrol-kontrol proses bisnis.	0	0	2	1	0	3	5

Jadi berdasarkan tabel 4.35 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-01 pada aktifitas ke-1,2 dan 4 adalah 4, aktifitas ke-3 adalah 3, dan aktifitas ke-5 adalah 5.

36. DSS06-02 Mengontrol pemrosesan informasi

Tabel 4. 36 Analisis DSS06-02

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat transaksi yang dikerjakan oleh *authorised user* dengan mengikuti prosedur dan	0	0	1	0	3	2	4

tugasnya.							
2. Membuat otentikasi pemilik transaksi dan verifikasi bahwa dia mempunyai otoritas.	0	1	1	1	1	2	5
3. Mencatat transaksi yang dilakukan secara tepat waktu dan verifikasi serta validasi keakuratan.	0	0	1	1	2	2	4
4. Melakukan koreksi data yang salah ketika di-*input*-kan, tanpa mengganggu Level otorisasi yang asli..	0	1	1	1	2	2	4
5. Memelihara integritas dan validitas data melalui siklus pemrosesan.	0	0	1	1	2	2	4
6. Menjaga integritas data ketika ada gangguan yang tidak terduga.	0	0	1	0	1	4	5
7. Melakukan penanganan output yang dilakukan secara tepat waktu dan pengiriman ke user yang tepat..	0	1	0	0	4	1	4
8. Mengecek *addressing*, autentikasi dan integritas konten sebelum mengirimkan data transaksi.	0	0	1	2	1	2	3

Jadi berdasarkan tabel 4.36 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-02 pada aktifitas ke-1,3,4,5 dan ke-7 adalah 4, aktifitas ke-2 dan ke-6 adalah 5, dan aktifitas ke-8 adalah 3.

37. DSS06-03 Mengatur peran, tanggungjawab, hak akses dan Level otoritas

Tabel 4. 37 Analisis DSS06-03

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengalokasi peran dan tanggung jawab berdasarkan deskripsi	0	0	1	1	2	2	4

tugas yang telah disetujui.							
2. Mengalokasi Level otoritas untuk persetujuan transaksi.	0	0	2	1	0	3	5
3. Mengalokasi hak-hak akses dan *priviledges* sesuai dengan deskripsi tugas masing-masing	0	0	1	0	3	2	4
4. Menentukan peran untuk aktivitas yang bersifat sensitif sehingga terdapat perbedaan tugas yang jelas.	0	0	1	1	2	2	4
5. Melakukan training dan kesadaran terhadap tannggungjawab dan peran pada staf-staf TI.	0	0	1	1	3	1	4
6. Me-*review* secara rutin terhadap penentuan akses kontrol yang telah dibuat.	0	0	2	0	4	0	4

Jadi berdasarkan tabel 4.37 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-03 pada aktifitas ke-1,3,4,5 dan ke-6 adalah 4, dan aktifitas ke-2 adalah 5.

38. DSS06-04 Mengelola kesalahan dan exceptions

Tabel 4. 38 Analisis DSS06-04

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Mengatur *ownership*, perbaikan *error*, mengindahkan *error* dan penanganan kondisi yang tidak stabil.	0	0	2	0	4	0	4
2. Me-*review* kesalahan-kesalahan, *exceptions*, dan penyimpangan.	0	0	2	0	1	3	5
3. Melakukan *follow up*, koreksi, dan persetujuan kemudian *resubmit* dokumen dan transaksi.	0	0	0	3	2	1	3
4. Memelihara bukti-bukti tindakan perbaikan *error*.	0	0	2	0	2	2	2
5. Membuat laporan mengenai informasi-informasi *error* pada	0	0	1	1	1	3	5

proses bisnis secara tepat waktu.							

Jadi berdasarkan tabel 4.38 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-04 pada aktifitas ke-1 adalah 4, aktifitas ke-2 dan ke-5 adalah 5, dan aktifitas ke-3 adalah 3.

n

39. DSS06-05 Memastikan bahwa informasi dari event dapat ditelusuri dan pertanggung jawabannya

Tabel 4. 39 Analisis DSS06-05

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Menentukan *requirement* sistem penyimpanan *(retention)* yang dibuat berdasarkan kebutuhan bisnis.	0	0	1	1	3	1	4
2. Mencatat sumber informasi, bukti-bukti pendukung, dan rekaman transaksi.	0	0	1	0	3	2	4
3. Menghapus sumber informasi, bukti pendukung dan rekaman transaksi dengan cara yang tepat.	0	0	1	2	2	1	3

Jadi berdasarkan tabel 4.39 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-05 pada aktifitas ke-1 dan ke-2 adalah 4, dan aktifitas ke-3 adalah 3.

40. DSS06-06 Mengamankan aset-aset informasi

Tabel 4. 40 Analisis DSS06-06

Aktifitas	**Frekuensi pilihan**						***Level* yang dipilih**
	0	**1**	**2**	**3**	**4**	**5**	
1. Membuat prosedur keamanan untuk melindungi aset informasi.	0	0	2	0	1	3	5
2. Memberi kesadaran dan pelatihan terhadap suatu *acceptabel use* (cara-cara penggunaan yang benar).	0	0	2	0	1	3	5
3. Membatasi penggunaan, distribusi, dan akses fisik terhadap suatu penjagaan informasi sesuai klasifikasi	0	0	1	2	0	3	5

4. Mengimplementasi proses, alat-alat, teknik-teknik dalam memverifikasi kapatuhan pengamanan aset.	0	0	1	1	1	3	5
5. Membuat laporan kepada manajemen bisnis jika ada penyimpangan dan pelanggaran yang terjadi dalam penjagaan aset informasi.	0	0	1	1	0	4	5

Jadi berdasarkan tabel 4.40 diperoleh nilai *capability* untuk aktifitas - aktifitas DSS06-06 pada aktifitas ke-1 sampai 5 adalah 5.

4.3.3 Rekapitulasi Nilai *Capability*

Setelah dilakukan analisis hasil kuisoner maka di dapatkanlah hasil nilai – nilai pada tiap aktifitas yang ada pada domain DSS (*Deliver, service, and Support*) dan di masukan ke dalam form kerja audit. Tindakan selanjutnya yang dilakukan adalah mencari rata – rata nilai pada tiap proses untuk mengetahui bagaimana kondisi tiap proses yang ada dengan cara menjumlahkan seluruh level yang dipilih lalu dibagi dengan jumlah item pertanyaan di tiap domain.

Berikut adalah hasil rekapitulasi nilai proses pada domain DSS (*Deliver, Service, and Support*):

Tabel 4. 41 Rekapitulasi *Capability*

Proses Domain	*Level* rata - rata	Pembulatan Level
DSS-01 Mengelola Operasi	4,118	4
DSS-02 Mengelola Permintaan Layanan dan Mengelola Insiden	4,208	4
DSS-03 Mengelola Masalah	4,045	4
DSS-04 Mengelola Keberlanjutan	3,024	3
DSS-05 Mengelola Layanan Keamanan	4,510	4
DSS-06 Mengelola Kontrol-kontrol Proses Bisnis	4,156	4

Dari *Capability Level* yang didapat dilakukan pembulatan untuk memudahkan mencari kondisi terkini berdasarkan kriteria *capability Level* yang telah ditetapkan. Dalam melakaukan pembulatan tersebut menggunakan konsep penentuan *capability process* tertentu, yaitu suatu proses akan mencapai *Level* k jika semua atribut sebelum *Level* k terpenuhi secara *fully achieved* dan semua atribut di Level k telah terpenuhi secara *largely* (>50% hingga 85%) atau *fully achieved* (>85%) [21]. Disini penulis menggunakan pilihan yang terpenuhi secara *fully achieved* atau *Level* terpenuhi dengan nilai >85%, yang di rasa akan lebih akurat dalam menilai atau menggambarkan kondisi yang *existing* yang ada.

4.4 Pengumpulan *Evidence* dan Kondisi *Existing*

4.4.1 Pengumpulan dan daskripsi *Evidence*

Dalam penentuan suatu kondisi yang di dapat sudah valid akan diperkuat lagi, dalam audit ini dilakukan dengan pengumpulan bukti – bukti yang sudah ditetapkan pada COBIT 5 Domain DSS (*Deliver, Service, and Support*). Hasil bukti yang di dapat diperiksa dengan kesesuaiaan kondisi *existing* yang telah dapat dan menjadi alat ukur tersendiri.

Berikut adalah hasil pengumpulan bukti yang di dapat

Tabel 4. 42 Pengumpulan Bukti

DSS01 – *Manage Operations*				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS01.01 Perform Operational Procedures	*Operational schedule*	Dokumen Jadwal Operasional	Ada	Dilakukan selama 24 jam. Menerapkan sistem piket
	Backup log	Rekaman aktivitas atau transaksi	Ada	Dilakukan selama 24 jam, ada CCTV, terdapat akses log door, juga terdapat report per 2 jam jikalau terdapat gangguan dari piket
DSS01.02 Manage Outsourced IT Service	*Independent assurance plans*	Dokumen rencana penilaian *assurance* yang dilakukan secara independen terkait *outsourced IT*	Ada	Terdapat di dokumen / Kontrak SLA
DSS01.03 Monitor IT Infrastructure	*Asset monitoring rules and event condition*	Dokumen monitoring atau pengawasan terhadap aset dan insiden	Ada	Menggunakan *tools managed engine*
	Event log	Rekaman dari kegiatan atau insiden yang terjadi	Ada	Menggunakan *tools event management*
	Incident tickets	Bisa berupa form ataupun tabel yang diisi berdasarkan suatu insiden atau peristiwa	Ada	Menggunakan *tools remedy*
DSS01.04 Manage the	*Environmental Policies*	Dokumen mengenai aturan lingkungan	Ada	Perangkat mengikuti standar

Environment		kerja		internasional (TIA 942). Aturan kepegawaian mengikuti aturan SDM PT Telkom
	Insurance policy reports	Bisa berupa dokumen ataupun laporan yang berisi mengenai kebijakan insurance (asuransi/jaminan)	Ada	Tidak menggunakan asuransi pada perangkat, tetapi menggunakan kontrak maintenance (jikalau rusak maka diperbaiki / *corrective maintenance*), yang memperbaiki adalah perusahaan ke 3 (pihak ke-3). Terdapat dokumen antara Telkom Sigma dengan pihak ke 3.
DSS01.05 Manage Facilities	*Facilites assessment reports*	Bisa berupa dokumen ataupun laporan yang berisi mengenai pengukuran kualitas dari fasilitas yang digunakan	Ada	*Preventive mainteance* (per 3 bulan). Perusahaan pihak ke-3 yang datang ke Telkom Sigma
	Health and safety awareness	Bisa berupa daftar awareness terhadap kesehatan dan keamanan	Ada	Kondisi keamanan perangkat sudah diatur melalui *Standar Operating Procedure (SOP)* dan *Standar Maintenace Prosedure (SMP).* Kemanan ruangan sudah menggunakan *log door,* kemanan dari manusia menggunakan *finger print,* keamanan sistem sudah menggunakan *security procedure.*

DSS02 *Manage Service Requests and Incidents*				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS02.01 Define incident and service request classification schemes	*Operational scheduleIncidents and service request classification schemes and models*	Skema dan model klasifikasi permintaan layanan dan insiden	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Rules for incident escalation	Atau transaksi Aturan peLevelan insiden	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Criteria for problem registration	Kriteria problem registration	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS02.02 Record, classify and prioritise requests and incidents	*Incident and service request log*	Rekaman permintaan layanan dan insiden	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Classified and prioritised incidents and service requests	Bisa berupa dokumen ataupun laporan yang berisi mengenai permintaan layanan dan insiden yang telah diklasifikasikan dan prioritasnya	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS02.03 Verify, approve and fulfil service requests	*Approved service request*	Bisa berupa dokumen ataupun laporan yang berisi mengenai permintaan layanan yang disetujui	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Fulfilled service request	Bisa berupa dokumen ataupun laporan yang	Ada	Menggunakan tools bmc remedy *(Tools incident service) :*

		berisi mengenai permintaan layanan yang telah dipenuhi		*Problem management dan request management*
DSS02.04 Investigate, diagnose and allocate incidents	*Incident symptoms*	Daftar atau rekaman terhadap gejala-gejala dari insiden yang terjadi	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Problem log	Rekaman akan permasalahan yang dihadapi	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS02.05 Resolve and recover from incidentss	*Incident resolution*	Daftar pemecahan atau resolusi dari insiden atau peristiwa yang terjadi	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS02.06 Close service requests and incidents	*Closed service requests and incidents*	Daftar pelayanan dan insiden yang telah selesairmintaan	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	User confirmation of satisfactory fulfillment or resolution	Konfirmasi user terhadap kepuasan akan pemenuhn tau pemecahan permintaan layanan dan insiden	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS02.07 Track status and produce reports	*Incident status and trends report*	Laporan status dari insiden dan tren insiden	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Request fulfillment status and trends report	Laporan dari status pemenuhan permintaan layanan	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*

DSS03 Manage Problems				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS03.01 Identify and classify problems	Problem classification scheme	Skema klasifikasi masalah	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Problem status reports	Laporan status masalah	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Problem register	Daftar permasalahan	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS03.02 Investigate and diagnose problems	Root causes of problems	Bisa berupa dokumen ataupun laporan dari akar penyebab permasalahan yang terjadi	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Problem resolution reports	Laporan pemecahan masalah	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS03.03 Raise known errors	Known-error records	Rekaman dari kesalahan-kesalahan yang terdeteksi	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Proposed solution to known errors	Bisa berupa dokumen ataupun laporan dari solusi-solusi terhadap kesalahan-kesalahan	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS03.04 Resolve and	Closed problem records	Rekaman dari masalah yang telah	Ada	Menggunakan tools bmc remedy *(Tools*

close problems		terselesaikan		*incident service) : Problem management dan request management*
	Communication of knowledge learned	Dilakukannya komunikasi terhadap masalah yang ada dan penanganannya	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
DSS03.05 Perform proactive and close problems	Problem resolution monitoring reports	Laporan pemantauan terhadap resolusi masalah	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*
	Identified sustainable solution	Bisa berupa laporan atau daftar dari solusi-solusi yang handal	Ada	Menggunakan tools bmc remedy *(Tools incident service) : Problem management dan request management*

DSS04 *Manage Continuity*				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS04.01 Define the business continuity policy, objectives and scope	*Policy and objectives for business continuity*	Kebijakan dan tujuan dari keberlangsungan proses bisnis	Ada	Turunan tujuan perusahaan dari Direksi (dengan Keputusan Direksi), Lalu melalui SGM CDC, lalu diturunkan kepada SM Bina Lingkungan yang berikutnya menjadi Probis
	Disruptive incident scenarios	Gangguan dari Skenario insiden yang terjadi	Ada	Gangguan yang terjadi di user (Bina Lingkungan) yang berikutnya akan dilaporkan ke bagian PRANDAL

				kemudian akan dianalisa dan pengambilan tindakan
	Assessments of current continuity capabilities and gaps	Penilaian kapabilitas dan kesenjangan proses bisnis saat ini	Ada	kewenangan dilakukan oleh Manager Perencanaan dan Pengembangan Bagian PRANDAL
DSS04.02 Maintain a continuity strategy	*Business impact analyses*	Analisis impact terhadap proses bisnis	Ada	Dilakukan analisis ooleh Bagian PRANDAL per triwulan dan tahunan
	Continuity requirements	Kebutuhan terhadap kontinuitas proses bisnis	Ada	Kebutuhan terhadap proses bisnis berdasarkan kebutuhan user yang telah disetujui oleh SM Bina Lingkungan agar compliance. Selanjutnya disampaikan kepada SM PRANDAL
	Approved strategic options	Option-option strategis yang telah disepakati dalam rangka kontinuitas proses bisnis	Ada	Proses Bisnis Bina Lingkungan dianalisa oleh PRANDAL kemudian diketahui dan disetujui oleh SM Bina Lingkungan dan SGM CDC
DSS04.03 Develop and implement a business continuity response	*Incident response actions and communication*	Tindakan respon terhadap insiden dan komunikasinya terhadap pihak-pihak terkait	Ada	Dari user (Bagian Bina Lingkungan) kepada Bagian PRANDAL dengan menggunakan nota dinas yang berisi insiden dan permintaan perbaikan. SIM belum

				mengakomodir pelaporan insiden dari Bagian Bina Lingkungan kepada Bagian PRANDAL, penggunaan online hanya sebatas pengiriman laporan dan nota dinas saja (belum terakomodir langsung didalam SIM)
	BCP	*Business Continuity Plan* merupakan dokumen yang menjelaskan mengenai rencana-rencana strategis yang akan dalam rangka mempertahankan kontinuitas proses bisnis	Ada	Blue print 5 tahunan (2013-2017)
DSS04.04 Exercise, test and review the BCP	*Test objectives*	Daftar tujuan pengujian	Ada	Dilakukan aktivitas *Rolling Business Plan (pengujian business plan / update business plan),* dilakukan per tahun
	Test exercises	Rekaman pengujian	Ada	Dilakukan aktivitas *Rolling Business Plan (pengujian business plan / update business plan),* dilakukan per tahun
	Test results and recomendations	Hasil dan rekomndasi berdasarkan pengujian	Ada	Dilakukan aktivitas *Rolling Business Plan (pengujian business plan / update business*

				plan), dilakukan per tahun
DSS04.05 Review, maintain and improve the continuity plan	*Results of reviews of plans*	Hasil dari *review* terhadap rencana-rencana strategis yang terdapat pada BCP	Ada	Dari *user* (Bagian Bina Lingkungan) kepada Bagian PRANDAL dengan menggunakan nota dinas yang berisi insiden dan permintaan perbaikan. SIM belum mengakomodir pelaporan insiden dari Bagian Bina Lingkungan kepada Bagian PRANDAL, penggunaan online hanya sebatas pengiriman laporan dan nota dinas saja (belum terakomodir langsung didalam SIM)
	Recommended changes to plans	Daftar perubahan-perubahan yang diperlukan	Ada	Dari user (Bagian Bina Lingkungan) kepada Bagian PRANDAL dengan menggunakan nota dinas yang berisi insiden dan permintaan perbaikan. SIM belum mengakomodir pelaporan insiden dari Bagian Bina Lingkungan kepada Bagian PRANDAL, penggunaan online hanya sebatas

				pengiriman laporan dan nota dinas saja (belum terakomodir langsung didalam SIM)
DSS04.06 Conduct continuity plan training	*Training requirements*	Daftar kebutuhan terhadap pelatihan/training yang akan dilakukan	Tidak Ada	*Training* hanya berupa training user administrasi bagi karyawan yang baru bergabung
	Monitoring results of skills and competencies	Bisa berupa dokumen ataupun laporan yang berisi mengenai hasil dari pengawasan terhadap keterampilan dan kompetensi yang diperoleh dari pelatihan/training	Tidak Ada	Untuk monitoring *result of skill* mengikuti Bina Lingkungan SGM PT Telkom
DSS04.07 Manage backup arrangements	*Test results of backup data*	Bisa berupa dokumen ataupun laporan yang berisi mengenai hasil pengujian dari backup data	Ada	*Back up* data sudah tercover di SIM
DSS04.08 Conduct postresumption review	*Post-resumption review report*	Laporan tinjauan paska-penerusan/kelanjutan	Ada	Review report dilaporkan saat rapat *budget committee* CDC (evaluasi kinerja dan rencana ke depan) seharusnya dilaksanakan per 3 bulan, namun terkadang dilaksanakan dan terkadang tidak.
	Approved changes to the plans	Daftar perubahan terhadap rencana-rencana yang sebelumnya telah disusun	Ada	Review report dilaporkan saat rapat *budget committee* CDC (evaluasi kinerja dan rencana ke depan) seharusnya

				dilaksanakan per 3 bulan, namun terkadang dilaksanakan dan terkadang tidak.

DSS05 Manage Security Services				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS05.01 Protect against malware	*Malicious software prevention policy*	Daftar kebijakan pencegahan terhadap *malware software*	Ada	Di PC sudah terdapat anti virus yang legal. Terdapat *firewall* sebelum masuk ke data centre. Terdapat IPS (*Intruction Prevention System* : Tingkatan *firewall* yang lebih tinggi). Dilakukan *review* security per 3 bulan.
	Evaluations of potential threats	Daftar evaluasi terhadap ancaman-ancaman yang potensial	Ada	Dilakukan *review* security per 3 bulan.
DSS05.02 Manage network and connectivity security	*Connectivity security policy*	Daftar kebijakan keamanan konektivitas	Ada	Dibatasi oleh *firewall*. Hanya dibuka *port-port* tertentu *(normally close).* Secara proses harus ada surat izin tertulis (nota dinas) dari yang berwenang. Sebelum bisa diakses menggunakan internet, sistem harus lulus *furiabirity test*.
	Results of penetration tests	Laporan dari hasil tes *penetration*	Ada	Pernah ada (pernah dilakukan). Hanya tidak periodik.
	Security policies for	Daftar kebijakan keamanan untuk	Ada	Menggunakan anti virus. Jikalau tidak

	endpoint devices	perangkat e*ndpoint*		ada di *software catalog,* maka program tidak akan berjalan.
DSS05.03 Manage endpoint security	*Approved user access rights*	Daftar hak-hak akses *user* yang telah disepakati	Ada	Termasuk ke dalam *review* akses *user* per 3 bulan.
DSS05.04 Manage user identity and logical access	*Results of reviews of users Accounts and privileges*	Laporan hasil tinjauan dari akun dan hak-hak akses *user*	Ada	Termasuk ke dalam review akses *user* per 3 bulan.
	Approved access requests	Daftar permintaan akses yang disetujui	Ada	Termasuk ke dalam review akses *user* per 3 bulan.
DSS05.05 Manage physical access to IT assets	*Access logs*	Rekaman dari aktivitas pengaksesan pada Aset-aset informasi, prosedur pengamanan yang jelas, serta penanggungjawab	Ada	Termasuk ke dalam review akses *user* per 3 bulan.
	Inventory of sensitive documents and devices	Daftar inventarisasi dokumen dn perangkat yang sensitive	Ada	Inventarisasi perangkat terdapat di Bagian Logistik PT Telkom
DSS05.06 Manage sensitive documents and output devices	*Access privileges*	Daftar hak akses istimewa	Ada	Hak akses untuk bisa mengakses perangkat sudah screening sejak masuk ke dalam ruangan, menggunakan finger screen, setelah itu untuk masuk ke perangkat pun membutuhkan input user name dan *password account* pegawai
	Security event logs	Rekaman kejadian terkait keamanan sistempengujian dari *backup* data	Ada	*Review log* dilakukan per 3 bulan. Untuk *back up data inputan*, sudah secara otomatis *terback up* di sistem

DSS05.07 Monitor the infrastructure for security related events	*Security incident characteristics*	Karakteristik keamanan	Ada	Untuk keamanan sistem menggunakan *log firewall* dan *log antivirus* yang berikutnya akan diketahui *security*nya, juga *review log* per 3 bulan.
	Security incident tickets	Dapat berupa form pengamanan	Ada	Pengelolaan insiden menggunakan *helpdesk* aplikasi *bmc remedy*

DSS06 Manage Business Process Controls				
Sub Proses	**Output/Bukti**	**Deskripsi**	**Keberadaan output (Ada/Tidak)**	**Keterangan**
DSS06.01 Align control acitivites embedded in business processes with enterprise objective	*Results of processing effectiveness reviews*	Laporan dari hasil peninjauan terhadap keefektifan pemrosesn bisnis	Ada	User melaporkan kepada Bagian PRANDAL yang kemudian dilakukan perbaikan proses sesuai kebutuhan user
	Root cause analyses and recommendation.	Dokumen analisis terhadap akar permasalahan yang timbul	Ada	Terdapat di Bagian PRANDAL
DSS06.02 Contol the processing of information	*Processing control reports*	Laporan dari kontrol pemrosesan	Ada	Terdapat di Bagian PRANDAL
DSS06.03 Manage roles, responsibilities, access privileges and Level of authority	*Allocated roles and responsibilities*	Daftar alokasi peran dan tanggungjawab	Ada	Terdapat pada dokumen *User Akses Matriks (UAM)*
	Allocated Levels of authority	Daftar alokasi hak akses	Ada	Terdapat pada dokumen *User Akses Matriks (UAM)*
	Allocated access rights	Daftar autoritas *Level*	Ada	Terdapat pada dokumen *User Akses Matriks (UAM)*

DSS06.04 Manage errors and exceptions	*Evidence of error connection and remediation*	Lembaran koreksi terhadap ketidaksesuaian	Ada	Koreksi diusulkan oleh *user* kemudian dilakukan analisis oleh Bagian PRANDAL dan disetujui oleh *user* (SM BL) dan SGM CDC)
	Error reports and root cause analysis	Laporan mengenai kerusakan dan analisis terhadap penanggulangan kerusakan yang terjadi	Ada	Terdapat kerusakan ketika Bina Lingkungan menemukan kendala dalam SIM kemudian dilaporkan kepada PRANDAL, dari PRANDAL diteruskan kepada Bagian ITSS dan Telkom Sigma untuk pembenahan kendala *Technical* IT
DSS06.05 Ensure traceability of information events and accountabilities.	*Retention requirements*	Daftar kebutuhan untuk sistem penyimpanan	Ada	Terdapat di SIM BL secara otomatis,
	Record of transactions	Laporan atau rekaman transaksi	ada	Terdapat di SIM BL secara otomatis,
DSS06.06 Secure information assets	*Reports of violations*	Laporan yang berisi daftar pelanggaran-pelanggaran yang dilakukan di dalam system	Ada	Analisis yang dilakukan ada, namun daftar pelanggran tidak dilaporkan, di *komlac* terdapat pada problem manajemen

Dari tabel-tabel tersebut dapat dilihat beberapa bukti yang telah diambil. Dari tabel tersebut terdapat beberapa bukti yang diperoleh dan ada yang tidak diperoleh dan juga pendeskripsian yang menerangkan kondisi dari bukti yang dicari, hal tersebut dapat dijadikan sebagai evaluasi terhadap *capability Level* yang di dapat. Dalam pengambilan bukti ini ada beberapa objek bukti yang dapat untuk didokumentasikan dan ada yang tidak dikarenakan objek tersebut bersifat *private*.

4.4.2 Penilaian kondisi *existing*

4.4.2.1 Kondisi *Existing DSS01*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS01 :

1) Menjalankan absensi dan rekap aktivitas dilakukan dengan baik dengan Dilakukan selama 24 jam. Menerapkan sistem piket dalam mengelola *ticket* insiden
2) Pengelolaan penilaian *assurance* IT telah diatur melalui *SLA (Service Level Agreement)*
3) Monitoring atau pengawasan terhadap aset dan insiden menggunakan tools managed engine yang dikelola oleh masing-masing PIC pengelola aplikasi Sistem Informasi
4) Rekaman dari kegiatan atau insiden yang terjadi menggunakan tools event management yang dikelola oleh masing-masing PIC pengelola aplikasi Sistem Informasi
5) Mengelola insiden ticket menggunakan tools bmc remedy yang dikelola oleh masing-masing PIC pengelola aplikasi Sistem Informasi
6) Mengelola environtment IT diatur dalam *System Operating Procedure (SOP)* dan *System Maintenance Prosedure (SMP)*
7) Mengelola Fasilitas IT diatur dalam System Operating Procedure (SOP) dan Systmen Maintenance Prosedure (SMP)
8) Perangkat mengikuti standar internasional (TIA 942). Aturan kepegawaian mengikuti aturan SDM PT Telkom
9) Tidak menggunakan asuransi pada perangkat, tetapi menggunakan kontrak maintenance (jikalau rusak maka diperbaiki / corrective maintenance) dan preventive mainteance (per 3 bulan). Perusahaan pihak ke-3 yang datang ke Telkom Sigma
10) Kemanan ruangan sudah menggunakan log door, kemanan dari manusia menggunakan *finger print*, keamanan sistem sudah menggunakan *security procedure.*

4.4.2.2 Kondisi *Existing DSS02*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS02 :

1) Dalam menjalankan layanan insiden dan permintaan layanan telah dibuatkan skema layanan/ SOP tentang *request insiden.*
2) Terdapat aturan – aturan mengenai penanganan insiden, dan telah di dokumentasikan dalam bentuk SLA.
3) Pengelolaan *service* dan insiden dikelola dengan menggunakan *tools bmc remedy* (*Tools incident service*) : *Problem management* dan *request management*
4) Insiden yang terjadi dialami oleh bagian Bina Lingkungan yang kemudian diteruskan kepada bagian PRANDAL dalam bentuk nota dinas pada SIM-BL, lalu oleh bagian PRANDAL dilaporkan kepada divisi ITSS .

5) *Tools remedy* mengelola insiden dengan memperoleh *request* dari PRANDAL CDC Telkom dalam bentuk per *ticket request* sehingga dapat dilakukan penanganan secara satu persatu dan aktual.
6) Pada aplikasi tersebut insiden yang diterima dan dibenahi oleh PIC dari SIM-BL pada unit ITSS

4.4.2.3 Kondisi *Existing DSS03*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS03 :

1) PIC SIM-BL dari Divisi ITSS melakukan pengklasifikasian terhadap permasalahan yang muncul, dan tertulis dalam SLA
2) Permasalah yang ada di rekap dan dibenahi langsung oleh divisi PIC SIM-BL dari ITSS
3) Melakukan investigasi dan mendiagnosa masalah – masalah yang timbul, dan terdokumentasikan secara langsung pada *tools bmc remedy*
4) Masalah yang timbul dikelola dan langsung dibenahi dengan menggunakan *tools remedy* oleh PIC SIM-BL dari Divisi ITSS
5) Jika terjadi *error* pada SIM-BL maka terdapat 2 kemungkinan *report* terjadinya *error* tersebut : bisa dari PRANDAL kepada ITSS, atau dari ITSS kepada PRANDAL, yang kemudian tindakan pembenahan dilakukan.

4.4.2.4 Kondisi *Existing DSS04*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS04 :

1) Turunan tujuan perusahaan dari Direksi (dengan Keputusan Direksi), Lalu melalui SGM CDC, lalu diturunkan kepada SM Bina Lingkungan yang berikutnya menjadi Proses bisnis
2) Gangguan yang terjadi di user (Bina Lingkungan) yang berikutnya akan dilaporkan ke bagian PRANDAL kemudian akan dianalisis dan pengambilan tindakan
3) Penilaian kapabilitas dan kesenjangan proses bisnis saat ini menjadi kewenangan dari Manager Bagian Perencanaan dan Pengembangan Bagian PRANDAL
4) Kebutuhan terhadap proses bisnis berdasarkan kebutuhan *user* yang telah disetujui oleh SM Bina Lingkungan agar *compliance*. Selanjutnya disampaikan kepada SM PRANDAL
5) Untuk menjaga keberlangsungan strategi dalam proses bisnis terlebih dahulu dilakukan *review* terhadap proses bisnis per triwulan dan tahunan yang kemudian melahirkan analisis pengaruh/dampak yang terjadi dengan kesiapan di Bagian Bina Lingkungan dan pilihan strategi yang ada di komunikasikan dengan pihak SM Bina Lingkungan dan disetujui SGM CDC. Namun review terhadap proses bisnis per 3 bulan terkadang dilaksanakan dan terkadang tidak dilaksanakan
6) Untuk merespon indisen, *user* (Bagian Bina Lingkungan) melaporkan kepada Bagian PRANDAL dengan menggunakan nota dinas yang

berisi insiden dan permintaan perbaikan. SIM belum mengakomodir pelaporan insiden dari Bagian Bina Lingkungan kepada Bagian PRANDAL, penggunaan online hanya sebatas pengiriman laporan dan nota dinas saja (belum terakomodir langsung didalam SIM)

7) Hasil analisis dari proses *guidance* yang dilakukan Bagian PRANDAL mengenai aspek performansi dan dampak resiko
8) List Change Request dari PRANDAL hasil analiss dari nota dinas Bina Lingkungan
9) Dokumen ataupun laporan yang berisi mengenai hasil pengujian dari backup data dilakukan otomatis pada SIM-BL, *operation* dan *development technical IT* pada ITSS dan Telkom Sigma
10) Bina Lingkungan memiliki *Bussines Plan Continuity* 5 Tahunan Terdapat target-target yang harus dicapai oleh Bina Lingkungan (Bantuan, dll) sesuai dengan Permen-BUMN, KD, dan Visi CDC
11) Tidak adanya pelatihan yang dilakukan terhadap pegawai, *Training* hanya berupa training user administrasi bagi karyawan yang baru bergabung
12) Review report dilaporkan saat rapat *budget committee* CDC (evaluasi kinerja dan rencana ke depan) seharusnya dilaksanakan per 3 bulan, namun terkadang dilaksanakan dan terkadang tidak.
13) Proses bisnis dalam penyaluran bantuan dari aktivitas survey lokasi objek bantuan memiliki beberapa kendala, yaitu tidak adanya tim khusus survey dan juga belum ada standarisasi verifikasi survey berdasarkan nominal objek bantuan untuk mengefektif efisiensikan waktu
14) Lembar internal control masih menggunakan manual yaitu *microsoft word*

4.4.2.5 Kondisi *existing DSS05*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS05 :

1) Di PC sudah terdapat anti virus yang legal. Terdapat *firewall* sebelum masuk ke data centre. Terdapat IPS (*Intruction Prevention System* : Tingkatan *firewall* yang lebih tinggi). Dilakukan *review security* per 3 bulan
2) Konektivitas Dibatasi oleh *firewall*. Hanya dibuka *port-port* tertentu (*normally close*). Secara proses harus ada surat izin tertulis (nota dinas) dari yang berwenang. Sebelum bisa diakses menggunakan internet, sistem harus lulus *furiabirity test*.
3) *Penetration Test* Pernah ada (pernah dilakukan). Hanya tidak periodik.
4) *Software* menggunakan lisensi original. Jikalau *software* tidak ada di *software catalog*, maka program tidak akan berjalan.
5) Dilakukan *review* akses user per 3 bulan.
6) Inventarisasi perangkat terdapat di Bagian Logistik PT Telkom
7) Hak akses untuk bisa mengakses perangkat sudah *screening* sejak masuk ke dalam ruangan, menggunakan *finger screen*, setelah itu

untuk masuk ke perangkat pun membutuhkan input *user* name dan *password account* pegawai

8) *Review log* dilakukan per 3 bulan. Untuk *back up* data inputan, sudah secara otomatis *terback up* di sistem
9) Untuk keamanan sistem menggunakan *log firewall* dan *log antivirus* yang berikutnya akan diketahui *securitynya*, juga *review log* per 3 bulan.
10) Pengelolaan insiden menggunakan helpdesk aplikasi *bmc remedy*

4.4.2.6 Kondisi *Existing DSS06*

Berdasarkan audit yang dilakukan pada lingkung domain DSS, maka didapatlah kondisi *existing* dari DSS06 :

1) Penyelarasan aktivitas kontrol yang ada di proses bisnis dengan mengacu kepada target Bina Lingkungan sudah berlangsung baik. Dilengkapi laporan tinjuan dan juga analisis terhadap akar permasalahan yang muncul
2) Laporan dari hasil peninjauan terhadap keefektifan pemrosesn bisnis dilakukan oleh PRANDAL yang kemudian hasil dan koreksinya dilaporkan pada rapat koordinasi antara SM Bina Lingkungan dengan SM PRANDAL per triwulan dan per tahunan
3) Pemantauan dilakukan terus – menerus, dokumentasi insiden dan pelaporan error pada berdasarkan nota dinas dari user SIM-BL
4) Peran, tanggungjawab, hak akses dan Level otoritas telah didefinisikan pada dokumen dokumen *User Akses Matriks* (*UAM*)
5) Terdapat rekaman di sistem informasi secara langsung di SIM BL yang dapat digunakan untuk memastikan jejak kegiatan informasi dan pertanggung jawabannya.

4.5 Analisis *Gap*

Analisis *Gap* ini dlakukan untuk mencari selisih dari *Level capability* yang didapat dengan Level target yang ingin dicapai. Dalam penentuan Level target, ditentukan dengan Level yang sedang dituju dari Level rata – rata yang didapat. Contoh untuk DSS01 di peroleh Level rata –b rata 4,029 maka DSS01 sedang dalam tahap menuju Level capability 5 dan masih mencapai 0,029 atau 2,9% di atas Level 4 atau kurang dari 0,971 atau 97% menuju Level capabilty 5. Sehingga ditetapkan Level targetnya adalah Level 5.

4.5.1 Analisis *Gap* DSS01

Berdasarkan analisi hasil dan ditetapkannya *Level capability* pada DSS01, telah diperoleh bahwan nilai *Level capability* DSS01 berada pada Level 4 yaitu bahwa DSS01 dalam *Predictabel Process* yang berarti DSS01 dilakukan, aktifitas – aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Level target yang ingin dicapai adalah Level 5 yaitu *Optimizing Process*.

Tabel 4. 43 Analisis Gap DSS01

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS01 Manage Operations	4	5	1

Untuk menuju pada Level 5 maka yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

4.5.2 Analisis *Gap* DSS02

Berdasarkan analisi hasil dan ditetapkannya *Level capability* pada DSS02, telah diperoleh bahwan nilai *Level capability* DSS02 berada pada Level 4 yaitu bahwa DSS02 dalam *Predictabel Process* yang berarti DSS02 dilakukan, aktifitas – aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Level target yang ingin dicapai adalah Level 5 yaitu *Optimizing Process*.

Tabel 4. 44 Analisis *Gap* DSS02

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS02 Manage Service Requests and Incidents	4	5	1

Untuk menuju pada Level 5 maka yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

4.5.3 Analisis *Gap* DSS03

Berdasarkan analisi hasil dan ditetapkannya *Level capability* pada DSS03, telah diperoleh bahwan nilai *Level capability* DSS03 berada pada Level 4 yaitu bahwa DSS03 dalam *Predictabel Process* yang berarti DSS03 dilakukan, aktifitas-aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Level target yang ingin dicapai adalah Level 5 yaitu *Optimizing Process*.

Tabel 4. 45 Analisis *Gap* DSS03

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS03 Manage Problems	4	5	1

Untuk menuju pada Level 5 maka yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

4.5.4 Analisis *Gap* DSS04

Berdasarkan analisi hasil dan ditetapkannya *Level capability* pada DSS04, telah diperoleh bahwan nilai *Level capability* DSS04 berada pada Level 3 yaitu bahwa DSS04 dalam *Established Process* yang berarti DSS04 telah dilakukan, ada standar penerapan dalam melakukan proses tersebut, terdokumentasi dan komunikasi berjalan dengan baik. Level target yang ingin dicapai adalah Level 4 yaitu *Predictabel Process*.

Tabel 4. 46 Analisis *Gap* DSS04

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS04 Manage Continuity	3	4	1

Untuk menuju pada Level 4 maka yang harus dilakukan yaitu menetapkan ukuran layanan atau informasi yang ingin dihasilkan dan memastikan ukuran layanan tersebut tercapai, kemudian memantau dan menganalisisnya.

4.5.5 Analisis *Gap* DSS05

Berdasarkan analisi hasil dan ditetapkannya *Level capability* pada DSS05, telah diperoleh bahwan nilai *Level capability* DSS05 berada pada Level 4 yaitu bahwa DSS05 dalam *Predictabel Process* yang berarti DSS05 dilakukan, aktifitas-aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Level target yang ingin dicapai adalah Level 5 yaitu *Optimizing Process*.

Tabel 4. 47 Analisis Gap DSS05

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS05 Manage Security Services	4	5	1

Untuk menuju pada Level 5 maka yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

4.5.6 Analisis *Gap* DSS06

Berdasarkan analisis hasil dan ditetapkannya *Level capability* pada DSS06, telah diperoleh bahwan nilai *Level capability* DSS06 berada pada Level 4 yaitu bahwa DSS06 dalam *Predictabel Process* yang berarti DSS06 dilakukan, aktifitas-aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Level target yang ingin dicapai adalah Level 5 yaitu *Optimizing Process*.

Tabel 4. 48 Analisis Gap DSS06

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS06 Manage Bussiness Process Controls	4	5	1

Untuk menuju pada Level 5 maka yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

.

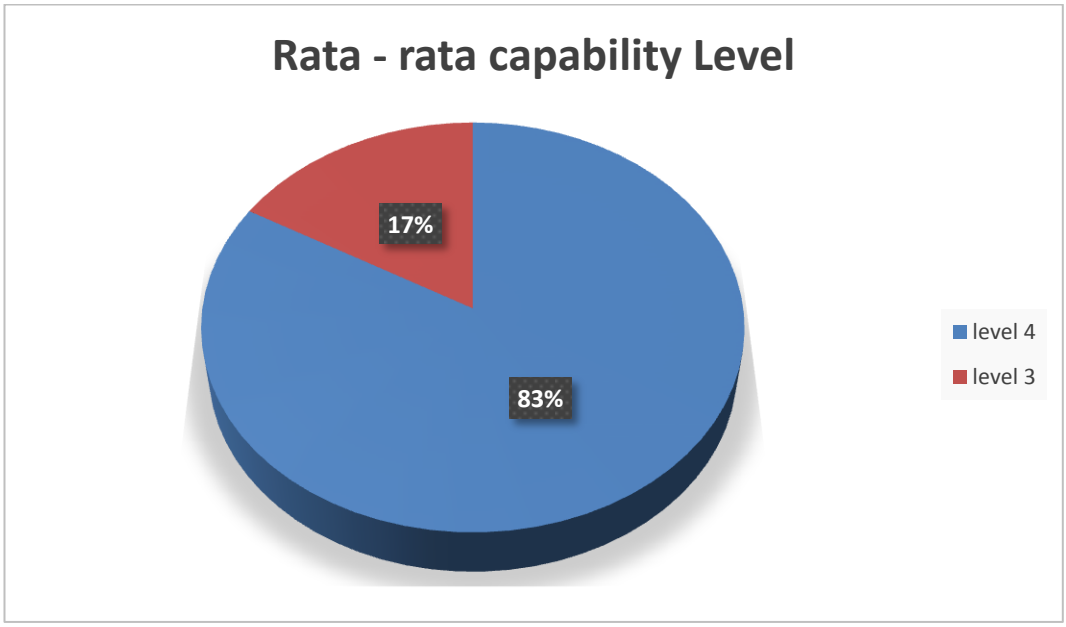
4.5.7 Analisis Keseluruhan *Gap*

Berikut ini adalah hasil dari pelaksanaan audit, diperolehnya hasil *capability Level* untuk keseluruhan proses adalah sebagai berikut :

Tabel 4. 49 Analisis Keseluruhan *Gap*

Nama Proses	***Level Existing***	***Level Target***	***Gap***
DSS01 Manage Operations	4	5	1
DSS02 Manage Service Requests and Incidents	4	5	1
DSS03 Manage Problems	4	5	1
DSS04 Manage Continuity	3	4	1
DSS05 Manage Security Services	4	5	1

DSS06 Manage Bussiness Process Controls	4	5	1



Gambar 4. 2 Diagram Rata – rata Capability

Dari Tabel 4.44 diperoleh *capability Level* tiap-tiap proses domain DSS COBIT 5, dari gambar 4.2 dapat diketahui bahwa rata-rata *capability Level* yang diperoleh berada pada Level 4 yaitu *Predictabel Process*. Artinya aktifitas – aktifitas, kebijakan dan aturan terdokumentasi dan menghasilkan layanan/ informasi optimal yang telah dimonitor dan dianalisis. Serta untuk mencapai Level 5 yaitu *Optimizing Process* yang harus dilakukan yaitu membuat inovasi dan strategi untuk pengembangan aktivitas sesuai hasil analisis dari aktifitas yang telah terstandardisasi sebelumnya juga memaksimalkan aktivitas yang sudah berjalan cukup baik.

4.6 Rekomendasi

Dalam rekomendasi, dapat dituliskan point rekomendasi untuk 1 sub bab atau lebih, tergantung dari keterkaitan rekomendasi dengn sub bab terkait

4.6.1 Rekomendasi DSS01

Berdasarkan analisis *Gap* yang di dapat dengan Level target yang ingin dicapai pada DSS01, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS 01-03 Mengelola Infrastruktur dan DSS 01-05 Mengelola Fasilitas :

1. Pembangunan kesadaran dan pemahaman untuk menjaga perangkat dan infrastruktur IT kepada staff melalui :
   - *Training* / pelatihan

- Imbauan melalui gambar dan tulisan di sudut-sudut ruangan dan ketika *log-in* computer

Meskipun terdapat kontrak *maintenance* namun kerusakan membuat hambatan bagi jalannya operasional (minimal hambatannya adalah terdapatnya *space* waktu produktif yang terbuang)

2. Diperlukan adanya pengawasan *monitoring* ruangan secara 24 jam dengan menggunakan kamera CCTV, karena didalam ruangan belum menggunakan monitoring yang memiliki fungsional melihat sudut-sudut ruangan.

DSS 01-01 Menjalankan Prosedur Operasional dan DSS 01-04 Mengelola Lingkungan Kerja :

1. Perlu adanya sistem pengawasan piket atau yang bertugas dengan cara memastikan di waktu awal mulai piket, waktu pertengahan piket, serta waktu akhir piket.
2. Perlu diadakannya rapat evaluasi mingguan untuk membuat evaluasi dan proyeksi mengenai jalannya *operation* (performansi) yang berikutnya dapat dihasilkan list *point* evaluasi mingguan dan *list point* proyeksi seminggu kedepan dalam menjalankan *operation IT* (seperti : evaluasi pembagian tugas, evaluasi pemrosesan data, dsb)

4.6.2 Rekomendasi DSS02

Berdasarkan analisis *Gap* yang di dapat dan dengan *Level* target yang ingin dicapai pada DSS02, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS02 - 01.Mendifinisikan skema klasifikasi insiden dan permintaan layanan, DSS02- 03.Memverifikasi, menyetujui dan memenuhi permintaan layanan , DSS02-04. Mendiagnosis dan mengalokasikan insiden, DSS02-05. Menyelesaikan dan Memenuhi insiden, DSS02-06. Menutup permintaan layanan dan insiden, DSS02-07. melacak status & membuat laporan :

1. Perlu dibuat fungsi *Helpdesk* dari *user* (Bina Lingkungan) kepada Manager Sistem Informasi Perencanaan dan Pengendalian (PRANDAL) untuk mengefisiensikan waktu dalam pelaporan insiden
2. Setiap perubahan terhadap aplikasi didokumentasikan dalam *Log Book* yang merecord aktivitas sebagai berikut :
   - *Change request* oleh *user*
   - *Manager* pengelolaan sistem informasi CDC melakukan *review change request* kemudian diteruskan ke ITSS
   - Manager pengelolaan sistem informasi CDC melakukan transport ke production

   Logbook tersebut digunakan untuk memitigasi resiko perubahan yang tidak terotorisasi, akses yang tidak terotorisasi dan ketidaktersediaan data finansial.

DSS02 - 02.Mengklarifikasi & memproriataskan permintaan & insiden :

1. Membuat skema klasifikasi dan prioritas dari permintaan layanan yang diperoleh dari *user* (Bina Lingkungan) sebelum diteruskan kepada ITSS agar proses perbaikan dan pembaharuan dilakukan berdasarkan urutan prioritas
2. Menentukan *Level-Level* insiden terutama untuk insiden besar dan insiden tentang keamanan yang terjadi dari pelaporan *user* agar dapat dibuat mitigasi pola pencegahan terhadap potensi insiden yang akan terjadi

4.6.3 Rekomendasi DSS03

Berdasarkan analisis *Gap* yang di dapat dan dengan *Level* target yang ingin dicapai pada DSS03, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS03-01. Mengidentifikasi dan mengklasifikasikan masalah dan DSS03-02. Menginvestigasi & diagnosis masalah :

1. Membuat fungsi *troubleshooter* untuk dapat mengetahui *problem* yang terjadi secara cepat dan tepat sasaran
2. Menentukan *permanent fix* terhadap akar permasalahan yang telah dianalisis

4.6.4 Rekomendasi DSS04

Berdasarkan analisis *Gap* yang di dapat dan dengan *Level* target yang ingin dicapai pada DSS04, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS04-02. Menjaga strategi keberlanjutan, DSS04-04. Latihan, tes, dan review dokumen *business continuity plan (BCP)*, DSS04-07. Mengatur *backup*, dan DSS04-08. Melakukan *review* ulang :

1. Bagian Perencanaan dan Pengendalian CDC PT Telkom melakukan *monitoring* dan memastikan proses *backup/restore* yang dilakukan oleh ITS *reliability* dan *availibility* data terpenuhi.
2. Dilakukannya tindak lanjut dari proses *monitoring backup/restore* tersebut untuk memitigasi resiko data aplikasi keuangan yang hilang karena ketidaklengkapan atau ketidak cukupan *backup* dan *restore*
3. Rapat *budget commitee* per 3 bulan dalam mengontrol, mengevaluasi, dan membuat proyeksi kedepan perlu dilaksanakan secara konsisten, agar pelaksanaan dapat selalu dilakukan perbaikan demi target *blue print* 5 tahun dapat tercapai.

DSS04-03. Mengembangkan & Mengimplementasikan Respon Dari Keberlangsungan Bisnis dan DSS04-05. *Review*, menjaga dan mengembangkan *continuity plan* :

1. Perlu membuat tim khusus untuk *survey* lokasi bantuan, khususnya objek penerima bantuan yang jarak lokasinya jauh, agar proporsional dalam pembagian tugas karyawan sehingga tidak ada pekerjaan yang tertunda
2. Untuk verifikasi data penerima bantuan yang tidak dalam jumlah besar (missal : dibawah Rp 10.000.000,00) cukup menggunakan *Voice Processing Recording* (VPR) sehingga langsung terekam data yang dibutuhkan melalui wawancara dan tidak perlu dilakukan *survey* ke tempat lokasi

3. Perlu menggunakan lembar *internal control* secara otomatis dari SIM, tidak perlu menggunakan *Microsoft Word* untuk membuat lembar *internal control*, sudah langsung otomatiasi dengan SIM.

DSS04-06. Mengadakan *Training* untuk *continuity plan:*

1. Perlu diadakannya pelatihan mengenai proses bisnis Bina Lingkungan bagi karyawan, diadakan rutin 1 tahun 1 kali, untuk membekali atau meng-*upgrade* pengetahuan mengenai persoalan sosial dan bina lingkungan, juga menambah kepekaan rasa peduli sosial bagi setiap karyawan

4.6.5 Rekomendasi DSS05

Berdasarkan analisis *Gap* yang di dapat dan dengan Level target yang ingin dicapai pada DSS05, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS05-02. Mengelola jaringan dan keamanan konektifvitas

1. Melakukan *penetration test* secara periodik, yaitu 3 bulan 1 kali

DSS05-05. Mengelola akses fisik ke aset TI dan DSS05-07. Memantau infrastruktur yang berhubungan dengan *security events* :

1. Menentukan otorisasi terhadap devices yang boleh mengakses informasi institusi dan jaringan insitusi, artinya *screening* terhadap kode *device* (pencatatan kodefikasi dan pembuatan sistem *screening*)

DSS05-04. Mengelola identitas *user & logical access*:

1. Menerapkan enkripsi informasi saat pengiriman berdasarkan klasifikasinya agar informasi tersebut aman

4.6.6 Rekomendasi DSS06

Berdasarkan analisis *Gap* yang di dapat dan dengan *Level* target yang ingin dicapai pada DSS06, maka berikut adalah beberapa rekomendasi yang dapat penulis berikat untuk meningkatkan kualitas Bagian Bina Lingkungan Unit CDC PT Telkom:

DSS06-01. Menyelaraskan aktivitas kontrol yang ada di proses bisnis dengan sasaran intitusi

1. Melakukan inovasi proses bisnis dalam bantuan sosial setiap 2 tahun 1 kali merujuk kepada evaluasi *blue print* 1 tahun 1 kali.

DSS06-06. Mengamankan aset - aset informasi :

1. Memantau dan mengevaluasi prosedur keamanan untuk melindungi aset informasi.
2. Menyimpan dengan baik atau mengarsipkan data seperti sumber informasi, rekaman transaksi untuk dijadikan bukti dalam pengukuran penilaian keberlangsungan proses bisnis dan dapat sebagai rekomendasi.
3. Mengidentifikasi jenis – jenis data yang bersifat rahasia, membuat prosedur penyimpanan dan penghapusan yang tepat.

DSS06-03. Mengatur peran, tanggungjawab, hak akses dan Level otoritas

1. Membuat kebijakan dalam penentuan peran yang berwenang untuk mengakses aktivitas atau data yang bersifat sensitif, dijelaskan secara rinci dan didokumentasikan.

DSS06-04. Mengelola kesalahan dan *exceptions:*

1. Membuat kebijakan terhadap pemberian hukuman kepada pegawai yang melakukan pelanggaran – pelanggaran dalam pemantauan kegiatan proses bisnis.

4.6.7 Rekomendasi umum keseluruhan proses

Sebelumnya telah dituliskan beberapa rekomendasi yang berdasar pada tiap proses yang ada pada domain DSS (*Deliver, Service, and Support*). Berikut ini beberapa tambahan rekomendasi secara umum berdasar kondisi Bagian Bina Lingkungan Unit CDC PT Telkom dalam ruang lingkup Sistem Informasi Bina Lingkungan.

Capability Level yang didapat secara keseluhan adalah Level 4 *Predictable Process*, Level target yang ingin dicapai adalah 5 *Optimizing process*, sehingga rekomendasi yang disusun adalah sebagai berikut :

1. Memperketat kontrol terhadap proses yang berlangsung untuk mempertahankan proses yang sudah berjalan cukup baik
2. Membuat inovasi-inovasi terhadap proses bisnis agar berjalan variatif kea rah yang lebih baik
3. Berdasarkan prioritas, maka Domain yang masih tertinggal adalah DSS04 yaitu *manage continuity*, maka perlu dilaksanakan terlebih dahulu rekomendasinya untuk meningkatkan performansi dalam berlangsungnya bisnis proses
4. Meningkatkan dan konsisten dalam mengontrol dan mengevaluasi pencapaian terhadap *blue print* 5 tahunan, khususnya kontrol dan evaluasi per 3 bulan dan per tahun.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan audit yang dilakukan pada Bina Lngkungan SGM CDC PT Telkom dalam studi kasuss. COBIT 5 Domain DSS (*Deliver, Service and Support*) maka kesimpulan dari tugas akhir ini adalah:

1. Pada tahap pra audit teah diperoleh proses domain DSS COBIT 5 yang dimana merupakan keseluruhan proses dari domain DSS yang sesuai dengan kondisi tata kelola Bina Lingkungan SGM CDC PT Telkom dan digunakan sebagai ruang lingkup dan digunakan sebagai ruang lingkup dan standar audit yaitu DSS01, DSS02, DSS03, DSS04, DSS05, DSS06.
2. Dari hasil audit, diketahui ada 1 proses yang mempunyai *Level* kapabilitas 3 yaitu DSS04, ada 5 proses yang mempunyai *Level* kapabilitas 4 yaitu DSS01, DSS02, DSS03, DSS05 dan DSS06.
3. Menurut *Level* kapabilitas masing-masing proses, ditentukan *Level* target masing-masing proses yaitu berupa 1 *Level* di atas *Level* kapabilitas, yang ditentukan berdasar analisis dan juga persetujuan dengan *stakeholder*, sehingga didapat *Level* target untuk DSS01, DSS02, DSS03, DSS05 dan DSS06 adalah Level 5, untuk DSS04 adalah *Level* 4
4. *Level* capability keseluruhan yang diperoleh berdasarkan keseluruhan rata-rata adalah 4, yang berarti sebagian besar aktifitas pada domain DSS untuk Bina Lngkungan SGM CDC PT Telkom telah dilakukan, ada standar penerapan dalam melakukan proses tersebut, telah termonitor, terukur, dan telah dilakukan perencanaan prediksi kedepan sudah berjalan dengan baik.
5. Level target yang ingin dicapai adalah 5 *Optimizing process*, sehingga rekomendasi yang disusun adalah sebagai berikut :

    a. Memperketat kontrol terhadap proses yang berlangsung untuk mempertahankan proses yang sudah berjalan cukup baik
    b. Membuat inovasi-inovasi terhadap proses bisnis agar berjalan variatif kea rah yang lebih baik
    c. Berdasarkan prioritas, maka Domain yang masih tertinggal adalah DSS04 yaitu *manage continuity*, maka perlu dilaksanakan terlebih dahulu rekomendasinya untuk meningkatkan performansi dalam berlangsungnya bisnis proses
    d. Meningkatkan dan konsisten dalam mengontrol dan mengevaluasi pencapaian terhadap *blue print* 5 tahunan, khususnya kontrol dan evaluasi per 3 bulan dan per tahun.

5.2 Saran

Berikut adalah saran yang dapat disampaikan dalam tugas akhir ini adalah :

1. Penilaian tingkat kapabilitas terkait Bina Lingkungan SGM CDC PT Telkom dalam tugas akhir ini dapat dilanjutkan lagi pada modul-modul lain menggunakan COBIT 5.
2. Dapat ditambahkan *scoring/*pembobotan dalam terkait pengumpulan bukti/*evidence* yang dicari, Untuk memperjelas pemberian rekomendasi.
3. Metode dalam penghitungan validasi dan penentuan *Level capability* tiap aktifitas dapat dilakukan dengan metode yang berbeda.

DAFTAR PUSTAKA

[1] Anonym. 2010. *Modul Kupas Tuntas*. –

[2] Arisanti, Dian. 2011. *Audit Sistem Informasi Ditinjau Dari Perspektif Keuangan Menggunakan Standar COBIT 4.1 pada Direktorat Keuangan Pelabuhan Indonesia III*. STMKI Surabaya.

[3] Budiyono. 2007. *Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT Dalam Mendukung Layanan Teknologi Informasi Studi Kasus : PT PLN (PERSERO) Distribusi Jawa Barat dan Banten*. Bandung : Institut Teknologi Bandung

[4] Fransiskus Adikara, S.Kom, MM Ari Pambudi, S.Kom, M.KomTeknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul Jl. Terusan Arjuna, Tomang Tol *ANALISIS KEBUTUHAN STAKEHOLDER DALAM RANGKAMENGEMBANGKAN MODEL TATA KELOLA TEKNOLOGIINFORMASI DENGAN KERANGKA KERJA COBIT 5 PADAPERGURUAN TINGGI*

[5] Gondodiyoto, Sanyoto. 2007. *Audit Sistem Informasi + Pendekatan CobIT*. Jakarta : Mitra Wacana Media.

[6**]** Ken Vander Wal, John Lainhard, and Peter Tessin. *A COBIT 5 Overview*. ISACA, 2012.

[7] Gultom, Manorang. 2012. *Audit Tata Kelola Teknologi Informasi Pada PTPN 13 Pontianak Menggunakan Framework COBIT*. AMIK Panca Bhakti.

[8] Hines, Greg. 2004. *ITIL and COBIT - Similarities, Differences and Interrelationship*. Pepperweed Consulting.

[9] http://sharingvision.com/2013/07/5-prisnsip-cobit-5/

[10] Putri Ramadhani, Dina. 2013. *Analisis Tata Kelola Teknologi Informasi Dengan Menggunakan Penerapan Framework COBIT 4.1 (Studi Kasus : Rumah Sakit Hasan Sadikin Bandung.* Bandung : IT Telkom

[11] ISACA. 2012. *COBIT 5: A Business Framework for Governance & Management IT.*

[12] ISACA. 2012. *COBIT 5 : Enabling Processes.*

[13] Omari, Al, dkk. 2012. *Optimising COBIT 5 for IT Governance.* Queensland University of Technology.

[14] Susilo, Willy. *Audit SDM.*

[15] Svata, Vlasta. 2011. *IS Audit Considerations in Respect of Current Economic Environment.* University of Economics in Prague.

[16] Ron Webber. 1999. *Information Systems Control and Audit*. Prentice Hall.

[17] Ramadiansyah, R. E. S., Martonno, H. Y., Asmana, R. 2011. *Aplikasi Tata Kelola dan Audit Sistem Informasi Menggunakan Framework COBIT Pada Domain PO dan AI*. Surabaya : ITS.

[18] Iskandar, Y. 2012. *Analisis Penerapan Framework COBIT 4.1 Dalam Perencanaan dan Implementasi Tata Kelola Teknologi Informasi Sebagai Usulan Pada PT Total E&P Indonesie*. Bandung : Institut Teknologi Telkom.

[19] Kusumasindra, F. (2013). *Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 pada Domain Delivery, Service dan Support di Institute Manajemen Telkom.* Institute Teknologi Telkom.
[20] ISACA. (2013). Self-assesment Guide-Using COBIT 5.
[21] Jung, Ho-Won, Robin Hunter. 2001. *The Relationship Between ISO/IEC 15504 Process Capability Levels, ISO 9001 Certification and Organization Size : An Empirical Study.* Elsevier.
[22] Rahmawati, Diana. 2010. *Audit Sistem Informasi Berbasis Komputer.* Yogyakarta : UNY.