Audit Teknologi Informasi menggunakan *Framework* COBIT 5 Pada Domain DSS (*Delivery, Service, and Support*) (Studi Kasus : iGracias Telkom University)

Rio Kurnia Candra[1], Imelda Atastina[2], Yanuar Firdaus[3]

Program Studi Teknik Informatika Telkom University, Bandung

[1]rioinkurnia@gmail.com, [2]imelda@telkomuniversity.ac.id, [3]yanuar@telkomuniversity.ac.id

Abstraksi

Teknologi informasi (TI) merupakan suatu bagian yang sangat penting bagi perusahaan atau lembaga dan merupakan suatu nilai investasi untuk menjadikan perusahaan atau lembaga tersebut menjadi lebih baik. Perusahaan atau lembaga menempatkan teknologi informasi sebagi suatu hal yang dapat mendukung pencapaian rencana strategis perusahaan untuk mencapai sasaran visi, misi dan tujuan perusahaan atau lembaga tersebut, begitu halnya dengan Telkom University. Teknologi Informasi yang diterapkan perlu diatur agar dapat dimanfaatkan dengan baik. Untuk mengatur teknologi informasi itu sendiri memerlukan audit yang bertujuan untuk mengevaluasi dan memastikan pemenuhannya ditinjau dari pendekatan objektif dari suatu standar. Teknologi Informasi di Telkom University memerlukan audit untuk mengevaluasi, menilai kapabilitas, dan menyusun rekomendasi terhadap teknologi informasi yang dipakai. *Framework* audit yang digunakan adalah COBIT 5 domain DSS (*Deliver, Service*, dan *Support*) yang fokus pada penilaian pengiriman dan layanan teknologi informasi serta dukungannya termasuk pengelolaan masalah agar keberlanjutan layanan tetap terjaga.

Kata Kunci : audit, COBIT 5, domain DSS, Teknologi Informasi, Telkom University.

Abstract

Information technology (IT) is very important part for the company or institution and an investment to make the value of the company or institution to be better. Company or institution placing information technology as a sign of things to support the achievement of the company's strategic plan to achieve the goals of vision, mission and objectives of the company or institution, well as with Telkom University. Information Technology applied should be regulated in order to put to good use. To manage information technology requires audit aimed to evaluate and ensure compliance in terms of the objective of a standard approach. Information Technology at Telkom University require audits to evaluate, assess capabilities, and make a recommendation on the use of information technology. Audit framework used is COBIT 5 domain DSS (Deliver, Service, and Support) which focus on the assessment and delivery of information technology services and support for sustainability issues including the management of the service is maintained.

Key Word : audit, COBIT 5, domain DSS, Information Technology, Telkom University.

1. Pendahuluan

Saat ini Teknologi informasi (TI) menjadi suatu bagian yang sangat penting bagi perusahaan atau lembaga – lembaga yang bersekala *enterpirse*. Perusahaan atau lembaga menempatkan teknologi sebagi suatu hal yang dapat mendukung pencapaian rencana strategis perusahaan untuk mencapai sasaran visi, misi dan tujuan perusahaan atau lembaga tersebut. Perusahaan atau lembaga tersebut berupaya untuk menerapkan suatu sistem informasi yang dapat memenuhi kebutuhan perusahaan dalam mencapai tujuannya misalnya untuk meningkatkan kegiatan operasional kerja. Fungsi teknologi informasi tidak hanya untuk meningkatkan operasional kerja tetapi juga memberi nilai tambah dan keuntungan kompetitif [19].

Dengan berbagai keuntungan dan pentingnya Teknologi informasi, Perguruan Tinggi (PT) mengimplementasikan ke dalam proses operasionalnya. Perguruan tinggi dapat memanfaatkan Teknologi informasi untuk pelayanan administrasi, mendukung Kegiatan Belajar Mengajar (KBM), sebagai media berkomunikasi, dan membantu untuk pengambilan keputusan. Dengan diimplimentasikan teknologi informasi yang baik pada PT maka akan meningkatkan kualitas layanan di PT tersebut. Telkom University merupakan salah satu Perguruan Tinggi swasta di Indonesia, yang bernaung dibawah Yayasan Pendidikan Telkom (YPT). Telkom University memiliki visi yaitu menjadi perguruan tinggi berkelas dunia (*A World Class University*) yang berperan aktif dalam pengembangan ilmu pengetahuan dan seni berbasis teknologi informasi. Telkom University telah menerapkan penggunaan teknologi informasi sebagai penunjang dalam hal pelayanan akademik yang diperuntukan bagi seluruh civitas akademika, salah satu sistem informasi yang dimilki oleh Telkom University adalah iGracias (Integrated Academic Information System) yang ditangani oleh Direktorat Sistem Informasi Telkom University.

iGracias merupakan sistem informasi yang digunakan untuk keperluan akademik di lingkungan Telkom University yang dapat diakses oleh mahasiswa, dosen, dan juga orangtua mahasiswa tersebut. Banyak fiture yang terdapat pada sistem tersebut misalnya untuk keperluan registrasi, input mata kuliah, perwalian dan lain – lain. iGracias yang telah diimplimentasikan pada Telkom Univrsitay tentu perlu untuk diukur dan dievaluasi untuk mengetahui apakah teknologi informasi yang diimplementasikan sudah sesuai dengan yang diharapkan dan mampu memudahkan proses bisnis dari Telkom University. Untuk itu perlu dilakukannya Audit teknologi informasi. Dengan dilakukannya audit maka dapat diketahui tingkat keamanan asset, pemeliharaan integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara effisien [20], dan juga dapat diketahui tingkat kematangan teknologi informasi di Telkom University dan menghasilkan rekomendasi untuk mencapai tingkat kematangan yang optimal sehingga dapat membantu merealisasikan visi , misi, dan tujuan di Telkom University.

Audit teknologi informasi memiliki beberapa standar yang digunakan untuk peneletian. Contoh standar tersebut adalah ITIL dan COBIT 5. ITIL memiliki fokus pada layanan untuk pelanggan dan tidak memberikan proses penyelarasan strategi perusahaan terhadap strategi teknologi informasi yang dikembangkan [10]. 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 teknologi informasi secara *holistic* sehingga nilai yang diberikan oleh teknologi informasi 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]. COBIT 5 menyediakan kerangka kerja yang lengkap. Terdapat 5 domain dan 37 proses pada COBIT 5 yang dapat digunakan untuk melakukan audit. Maka dari itu COBIT 5 dianggap sesuai dan dapat membantu dalam proses audit teknologi informasi karena mencakup semua elemen pada teknologi informasi yang dipakai.

Domain DSS dipilih karena dianggap sesuai dengan kondisi teknologi informasi yang ada pada Telkom University saat ini. Dengan kondisi teknologi informasi di Telkom University yang sedang berlangsung dan kebutuhan untuk mengirimkan layanan, melayani, dan mendukung layanan teknologi informasi, maka Domain DSS yang dianggap sesuai dengan hal tersebut. Domain lain seperti APO (*Align, Plan, and Organize*) akan dirasa sesuai diterapkan pada tata kelola teknologi informasi yang belum dijalankan atau akan dijalankan, domain BAI (*Build, Acquire, and Implement*) akan dirasa sesuai diterapkan pada unit khusus yang berperan sebagai pembangun (*developer*) atau memperbaiki tata kelola teknologi informasi yang sudah ada, domain MEA (*Monitor, Evaluate, and Asses*) akan dirasa sesuai diterapkan untuk kondisi yang telah dibangun dan berlangsung, dan pelaksanaan *monitoring* dilakukan oleh pihak internal, karena *monitoring* dengan audit memiliki intensitas dan jangka waktu yang berbeda [16].

2. Tinjauan Pustaka

2.1 Sistem

Menurut Andri Kristanto (2008:1), "Sistem merupakan jaringan kerja dari prosedur – prosedur yang saling berhubungan, berkumpul bersama – sama untuk melakukan suatu kegiatan atau menyelesaikan suatu sasaran tertentu" [2].

Menurut Gordon B.Davis (1974;81), "Sistem dapat berupa abstrak atau fisis. Sistem yang abstrak adalah susunan yang teratur dari gagasan-gagasan atau konsepsi-konsepsi yang saling bergantung" [2].

Azhar Susanto (2000:3), "Sistem adalah kumpulan /group dari sub sistem / bagian / komponen apapun baik phisik maupun non phisik yang saling berhubungan satu sama lain dan bekerja sama secara harmonis untuk mencapai satu tujuan tertentu" [2].

Dari pengertian diatas, dapat disimpulkan bahwa sistem adalah kumpulan dari komponen – komponen yang saling berhubungan dan bergantung untuk mencapai suatu tujuan tertentu.

2.2 Informasi

Menurut Jogiyanto HM. (1999: 692), "Informasi dapat didefinisikan sebagai hasil dari pengolahan data dalam suatu bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian – kejadian (event) yang nyata (fact) yang digunakan untuk pengambilan keputusan" [5].

Menurut Anton M. Meliono. (1990: 331), "Informasi adalah data yang telah diproses untuk suatu tujuan tertentu. Tujuan tersebut adalah untuk menghasilkan sebuah keputusan" [5].

Menurut Gordon B. Davis (1991: 28), "Informasi adalah data yang telah diolah menjadi sebuah bentuk yang berarti bagi penerimanya dan bermanfaat bagi

pengambilan keputusan saat ini atau mendatang" [5].

Dari pengertian diatas, dapat disimpulkan bahwa informasi adalah data yang telah diolah menjadi data yang berguna untuk suatu tujuan tertentu, yang dapat bermanfaat bagi pengambilan keputusan saat ini atau mendatang.

2.3 Sistem Informasi

Menurut Laudon, Kenneth , Jane (2007:42), "Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan" [8].

Menurut Budi Sutedjo Dharma Oetomo (2006: 36), "Sistem Informasi adalah kumpulan elemen yang saling berhubungan satu sama lain untuk membentuk suatu kesatuan untuk mengintegrasi data, memproses dan menyimpan serta mendistribusikan informasi tersebut" [8].

Menurut Gondodiyoto (2007), "Sistem informasi dapat didefinisikan sebagai kumpulan elemen – elemen atau sumber daya dan jaringan prosedur yang saling berkaitan secara terpadu, terintegrasi dalam suatu hubungan hierarki tertentu, dan bertujuan mengolah data menjadi informasi" [8].

Menurut O'Brien (2005, P5), "Sistem informasi adalah suatu kombinasi terartur apapun dari people (orang), hardware (perangkat keras), software (piranti lunak), computer networks and data communications (jaringan komunikasi), dan database (basis data) yang mengumpulkan, mengubah dan menyebarkan informasi di dalam suatu bentuk organisasi" [8].

Dari pengertian diatas, dapat disimpulkan bahwa sistem informasi adalah kumpulan dari elemen – elemen atau sumber daya dan jaringan yang saling berkaitan satu sama lain membentuk suatu kesatuan untuk mengintegrasi data, dan bertujuan mengolah data menjadi informasi.

2.4 Teknologi Informasi

Teknologi Informasi adalah studi atau peralatan elektronika, terutama komputer, untuk menyimpan, menganalisa, dan mendistribusikan informasi apa saja, termasuk kata-kata, bilangan, dan gambar (kamus Oxford, 1995) [6].

Menurut Haag & Keen (1996), "Teknologi Informasi adalah seperangkat alat yang membantu anda bekerja dengan informasi dan melaksanakan tugas-tugas yang berhubungan dengan pemrosesan informasi" [6].

Menurut martin (1999), "Teknologi Informasi tidak hanya terbatas pada teknologi komputer (software & hardware) yang digunakan untuk memproses atau menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi" [6].

2.5 Audit

Menurut Sukrisno Agoes (2004), "Suatu pemeriksaan yang dilakukan secara kritis dan sistematis oleh pihak yang independen, terhadap laporan keuangan yang telah disusun oleh manajemen beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut" [3].

Menurut Arens dan Loebbecke (2003), "Suatu proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan. Auditing seharusnya dilakukan oleh seorang yang independen dan kompeten" [3].

Menurut Mulyadi (2002), "Auditing merupakan suatu proses sistematik untuk

memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan" [3].

Dari pengertian diatas, dapat disimpulkan bahwa audit adalah proses pengumpulan dan evaluasi bukti dengan tujuan untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria – kriteria yang telah di tetapkan.

Tujuan audit adalah mendapatkan informasi faktual dan signifikan berupa data hasil analisa, penilaian, rekomendasi auditor yang dapat digunakan oleh *auditee* atau menejemen untuk berbagai keperluan misalnya untuk dasar pengambilan keputusan , pengendalian manajemen, perbaikan atau perubahan dalam berbagai aspek dalam upaya mengamankan kebijakan dan mencapai tujuan organisasi secara keseluruhan [18].

2.6 Audit Sistem Informasi/Teknologi Informasi

Menurut Weber (1999, p.10), "Audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem komputer dapat melindungi aset, memelihara integritas data, memungkinkan tujuan organisasi untuk dicapai secara efektif dan menggunakan sumber daya secara efisien" [7].

Menurut Gondodiyoto (2003, p.151), "Audit sistem informasi merupakan suatu pengevaluasian untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis, memiliki mekanisme pengamanan aset yang memadai, serta menjamin integritas data yang memadai" [7].

Dari pengertian diatas, dapat disimpulkan bahwa audit sistem informasi adalah proses pengumpulan bukti dan evaluasi untuk mengetahui tingkat kesesuaian sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah sistem informasi telah didesain dan diimplementasikan secara efektif, efisien dan ekonimis, memiliki mekanisme pengamanan asset yang memadai dan menjamin integritas data.

2.7 COBIT

Menurut Sasongko (2009), "Control Objective for Information & Related Technology(COBIT) adalah sekumpulan dokumentasi best practice untuk IT Governance yang dapat membantu auditor, pengguna (user), dan manajemen, untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis IT" [4] .

Menurut Tanuwijaya dan Sarno (2010), "COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengatur keselarasan TI dengan bisnis. Selain itu, kerangka kerja juga memastikan bahwa TI memungkinkan bisnis, memaksimalkan keuntungan, resiko TI dikelola secara tepat, dan sumber daya TI digunakan secara bertanggung jawab" [4].

COBIT adalah salah satu framework yang digunakan untuk standar audit, COBIT merupakan standar yang dinilai lengkap dan cakupan yang menyeluruh sebagai framework audit. COBIT dikembangkan secara berkala oleh ISACA. Didalam COBIT ini terdapat beberapa Domain yang digunakan untuk proses audit.

2.8 Pemetaan Hubungan Enterprise Goals, IT – Related Goals, dan Proses control

Pemetaan hubungan ini digunakan utnuk melakukan penilaian tingkat kapabilitas,

beberapa tahap hubungan pemetaan terseut diantaranya antara adalah :

1. Pemetaan Enterprise Goals dengan tujuan perusahaan.

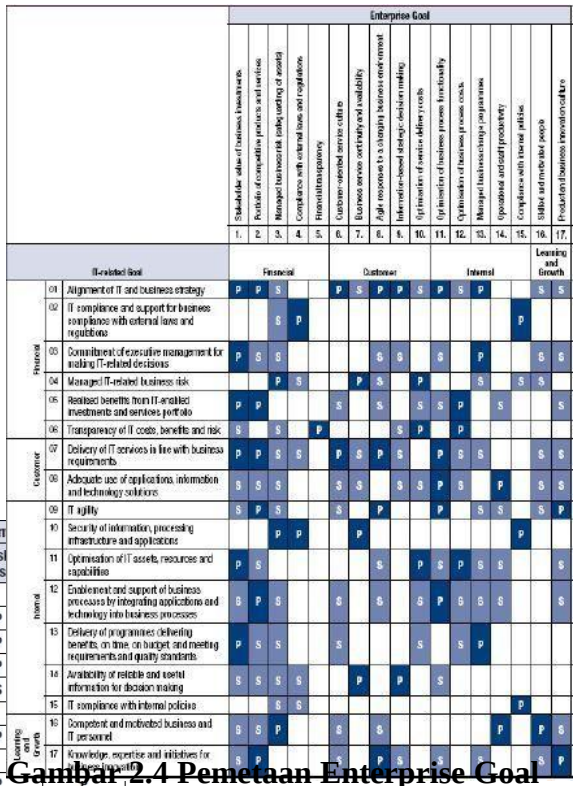
Pemetaan dilakukan ke dalam perspektif *IT Balanced Scorecard* (*IT BSC*). Jika hubungan keterkaitan antara tujuan perusahaan yang menjadi objek dengan Enterprise Goals pada COBIT 5 sangat kuat, maka diberi tanda "P" yang berarti *primary*. Jika terdapat hubungan yang tidak dominan, maka diberi tanda "S" yang berarti *secondary*. Jika tidak ada hubungan sama sekali maka dikosongkan.

BSC Dimension	Enterprise Goal	Relation to Gover	
		Benefits Realisation	Risk Optimis
Financial	1. Stakeholder value of business investments	P	
	2. Portfolio of competitive products and services	P	P
	3. Managed business risk (safeguarding of assets)		P
	4. Compliance with external laws and regulations		P
	5. Financial transparency	P	S
Customer	6. Customer-oriented service culture	P	
	7. Business service continuity and availability		P
	8. Agile responses to a changing business environment	P	
	9. Information-based strategic decision making	P	P
	10. Optimisation of service delivery costs	P	
Internal	11. Optimisation of business process functionality	P	
	12. Optimisation of business process costs	P	
	13. Managed business change programmes	P	P
	14. Operational and staff productivity	P	
	15. Compliance with internal policies		P
Learning and Growth	16. Skilled and motivated people	S	P
	17. Product and business innovation culture	P	

Gambar 2.3 Pemetaan Enterprise Goal dengan Tujuan Perusahaan

2. Pemetaan Enterprise Goals dengan IT – Related Goals.

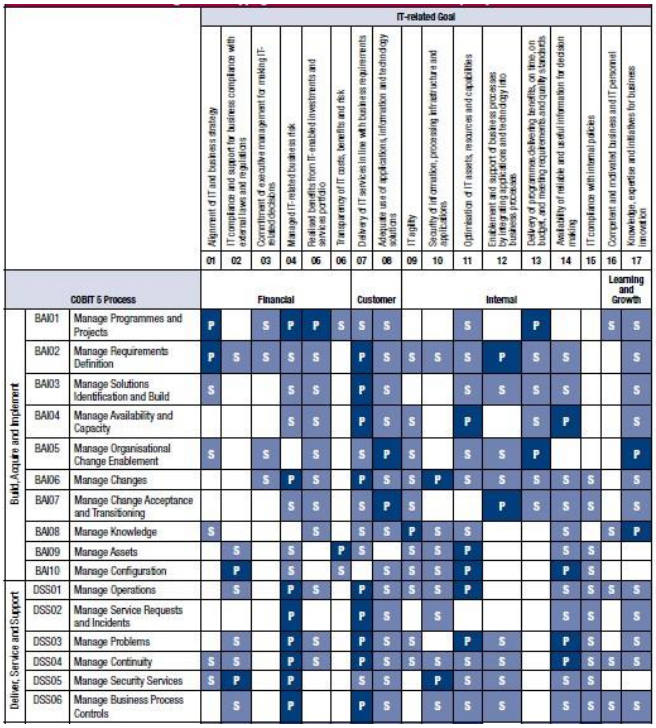
   Pemetaan yang dilakukan pada hubungan sama dengan yang dilakukan pada hubungan Enterprise Goals dengan Tujuan perusahaan. Jika hubungan keterkaitan antara IT – Related Goals yang menjadi objek dengan Enterprise Goals yang terpilih pada COBIT 5 sangat kuat, maka diberi tanda "P" yang berarti *primary*. Jika terdapat hubungan yang tidak dominan, maka diberi tanda "S" yang berarti *secondary*. Jika tidak ada hubungan sama sekali maka dikosongkan.



Gambar 2.4 Pemetaan Enterprise Goal dengan IT-Related Goal

3. Pemetaan IT – Related Goalsd dengan Proses domain DSS

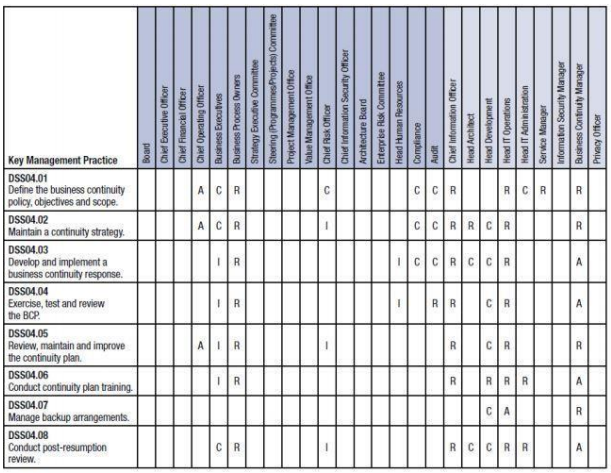
   Pemetaan ini dilakukan untuk mendapat proses – proses domain DSS mana sajakah yang masuk dalam ruang kegiatan audit. Setiap tujuan TI memiliki masing-masing proses TI yang relevan. Setelah dilakukan mapping terhadap tujuan bisnis perusahaan dengan tujuan TI, selanjutnya dilakukan mapping tujuan TI dengan proses TI [12].



Gambar 2.5 Pemetaan IT-Related Goal dengan Proses Domain DSS

2.9 Diagram RACI

Diagram RACI adalah bagian dari *Responsibility Assignment Matrix* (RAM), yaitu bentuk pemetaan antara sumberdaya dengan aktivitas dalam setiap prosedur. RACI merupakan singkatan dari R (*Responsible*), A (*Accountable*), C (*Consulted*), dan I (*Informed*). Untuk melakukan penilaian dengan domain DSS, maka dilakukan mapping antara *sub control objectives* dan sumber daya manusia yang ada pada pelaksaan sistem informasi. Berikut contoh dari diagram RACI pada DSS04 [12] :



Gambar 2.6 Diagram RACI

Mapping tersebut dilakukan untuk seluruh control objective yang ada pada domain DSS. Dalam mapping tersebut diberi suatu nilai berupa R/A/C/I, yang memiliki arti [12] :

- R (*Responsible*), berarti bahwa bagian tersebut merupakan pihak pelaksana yang harus bertanggung jswab melaksanakan dan menyelesaikan aktivitas yang menjadi tanggung jawabnya.
- A (*Accountable*) berarti bahwa bagian tersebut merupakan pihak yang harus mengarahkan jalannya pelaksanaan aktivitas.
- C (*Consulted*) berarti bahwa bagian tersebut merupakan pihak yang akan menjadi tempat konsultasi selama pelaksanaan aktivitas.
- I (*Informed*) berarti bahwa bagian tersebut merupakan pihak yang diberikan infromasi mengenai pelaksanaan aktivitas.

2.10 Proses Capability Model

ISO/IEC 15505 mendefinisikan pengukuran untuk penilaian kemampuan proses dari framework COBIT. *Process capability* didefinisikan pada 6 level poin dari 0 sampai 5, yang mempresentasikan peningkatan capability dari proses yang diimplementasikan.

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 2.7 Level Capability

Berikut adalah penjelasan level dari *process capability* [14] :

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.

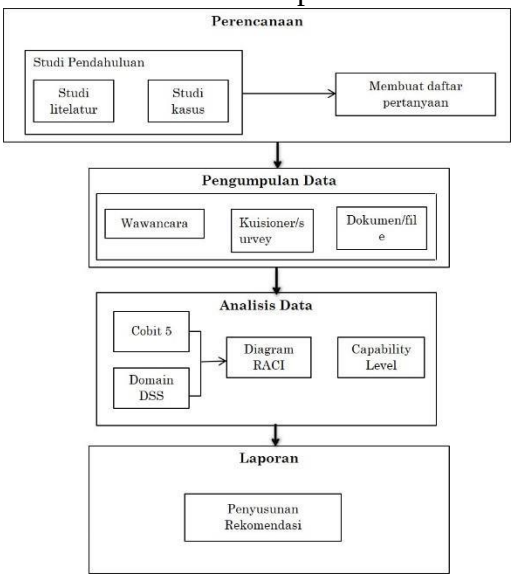
Setiap proses yang dinilai akan menghasilkan 4 level rating point, yaitu :

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%

3. Metodologi

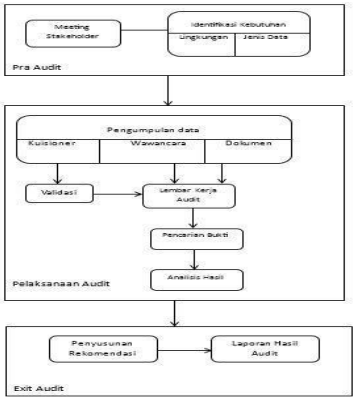
3.1 Metode Konseptual

Penelitian yang akan dilakukan akan terdiri dari beberapa fase-fase audit yang terdiri dari perencanaan, pengumpulan data, analisis data, dan laporan. Audit akan dijalankan mulai studi pendahuluan terhadap studi pustaka dan studi kasus, kemudian fase terakhir akan diakhiri dengan pembuatan laporan yang didalamnya terdapat hasil rekomendasi, yang menunjukkan kegiatan audit selesai dan ditutup.



Gambar 3.1 Meteode Konseptual

3.2 Prosedur Audit



Gambar 3.2 Prosedur Audit

4. 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 Direktorat SISFO terhadap audit yang dilakukan. Pengumpulan data dilakukan melalui kuisioner, wawancara, dan survey lapangan.
Dalam pengumpulan data melalui kuisioner dan wawancara ini dilakukan berdasarkan tabel Raci Chart yang sudah dipetakan dengan struktur organisasi di Telkom University. Table Raci Chart sendiri dapat di lihat pada lampiran A

4.1.1 Kuisioner

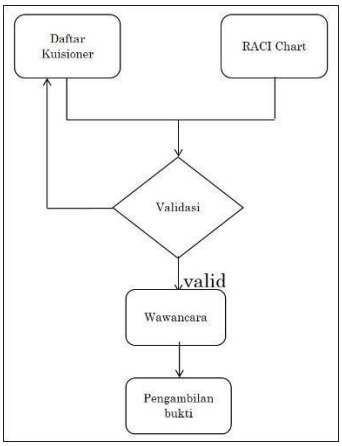
Pada tahap ini, dilakukannya kuisioner untuk mencari tanggapan – tanggapan dari para responden mengenai kondisi terkini yang ada pada Direktorat SISFO terkait dengan domain DSS (*Deliver, Service and Support*). Kuisioner ini berisikan pertanyaan – pertanyaan yang sesuai dengan proses – proses yang ada pada Domain DSS (*Deliver, Service and Support*).

4.1.2 Wawancara

Pada tahap wawancara ini, dilakukan untuk mengkroscek/mencari kebenaran dari tanggapan – tanggapan pada kuisioner yang telah di dapat, dan juga untuk memperoleh bukti – bukti yang terkait dengan domain DSS (Deliver, Service and Support). Wawancara dilakukan secara *face to face* dengan responden, dan juga didokumentasikan dengan rekaman wawancara.

4.1.3 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 kuisioner, kemudian di sesuai atau di petakan dengan hasil diagram RACI supaya daftar kuisoner tepat dengan sasaran. Setelah itu melakukan validasi hasil kuisioner, apabila data kuisioner ada yang tidak valid maka kuisioner yang tidak valid diulang kembali sampai menghasilkan hasil valid. Kemudin setelah semua data valid maka dilakukan kroscek dengan melakukan wawancara ke pihak yang memiliki jabatan tinggi di Direktorat SISFO, kemudian disertai dengan pengambilan bukti.

4.2 Teknik Pengukuran Data

Pengukuran data digunakan untuk menilai apakah hasil dari kuisioner 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. Nilai r-kritis yang ditetapkan adalah sebesar 0,30 [17]. 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 Direktorat SISFO dalam domain DSS (Deliver, Service and Support) menghasilkan data yang valid/dapat dipercaya.

Hasil nilai perhitungan validasi tiap item dapat dilihat pada lampiran C.

4.3 Analisis Hasil

4.3.1 Analisis Hasil Kuisioner

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 kuisioner. 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 DSS01-01 pada aktifitas ke 3 terdapat 9 responden, kemudian dari 9 responden yang memilih di level 2 adalah 4 orang, di level 4 adalah 4 orang, dan di level 5 adalah 1 orang. Maka level yang terpilih adalah pada level 3, karena diartikan juga berarti 4 orang yang memilih di level 4 tersbut juga merasa bahwa pada aktifitas ke 3 telah berada pada level 3.

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

Tabel 4.36

Proses Domain	Level rata - rata	Pembulatan level
DSS-01 Mengelola Operasi	3,82	3
DSS-02 Mengelola Permintaan Layanan dan Mengelola Insiden	4,29	4
DSS-03 Mengelola Masalah	3,69	3
DSS-04 Mengelola Keberlanjutan	3,4	3
DSS-05 Mengelola Layanan Keamanan	3,4	3
DSS-06 Mengelola Kontrol-kontrol Proses Bisnis	3,06	3

Dari Capability level yang didapat 4.36 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%) [15]. 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 atau belum, 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.

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 dilakukan dengan baik.

2) Dalam menjalankan prosedur operasional telah dilakukan dengan baik, dan ada beberapa aktivitas-aktivitas tertulis di *Standard Operating Procedure* (SOP) dan roadmap yang berdasarkan kalender akademik.
3) Tidak asuransi independent terhadap manajemen *outsourced IT service*.
4) Pelaksanaan monitoring infrastruktur IT terlaksana dengan baik.
5) Dalam manage *environtmen* Direktorat SISFO menjalankan kehendak sesuai dengan yang di tetapkan oleh SDM.
6) Dalam menjaga fasilitas yang dimiliki, tidak ada penilaian terhadap fasilitas yang ada. Dalam pengawasan fasilitas disak ada yang mengawasi, terdapat CCTV tapi tidak ada orang yang menjaganya.

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) Direktorat SISFO memiliki aplikasi sistem informasi tersendiri dalam pelayanan yang berkaitan dengan sistem informasi di Telkom University.
4) Aplikasi sistem informasi yang dimiliki Direktorat SISFO dapat digunakan dalam merekap insiden – insiden yang terjadi, laporan insiden yang terjadi, laporan status insiden yang sedang dikerjakan, dan laporan insiden yang sudah selesai.
5) Pada aplikasi tersebut insiden yang diterima di alokasikan ke bagian yang sesuai untuk menanganinya.
6) Ada yang memonitoring bagaimana tindakan terhadap insiden yang ada dari *helpdesk* Direktorat SISFO.
7) Dilakukannya pelaporan saat rapat besar Direktorat SISFO tiap 3 bulan terhadap insiden – insiden yang ada.

4.4.2.3 Kondisi *Existing* DSS03

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

1) Direktorat SISFO melakukan pengklasifikasian terhadap permasalahan yang muncul, dan tertulis dalam SLA
2) Permasalah yang ada di rekap dan dilaporkan dalam rapat besar tiap 3 bulan Direktorat SISFO
3) Melakukan investigasi dan mendiagnosa masalah – masalah yang timbung, namun pendokumentasiannya tidak dijaga, jadi hanya terdokumentasi dalam notulensi RTM (Rapat Tinjauan Manajemen).
4) Terdapat pencatatan dari kejadian error terhadap iGracias, dan juga dilaporkan saat rapat besar 3 bulan Direktorat SISFO
5) Dalam menyelesaikan masalah dan menutup masalah dikomunikasikan dalam RTM dan dilakukan dengan baik, direkap dan dijaga dengan baik.

4.4.2.4 Kondisi *Existing* DSS04

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

1) Direktur Direktorat SISFO membuat kebijakan terhadap keberlangsungan proses bisnis dengan melakukan kesepakatan terhadap unit SPM dan kemudian disetujui oleh Warek I Telkom University
2) Direktorat SISFO membuat antisipasi terhadap ganguan dari skenario insiden yang ada dengan meresolusi gangguan secara teknis dan menyelesaikan gangguan non teknis dengan kebijakan.

3) Dilakukanya pemantauan/penilaian terdahap proses bisinis yang berlangsung oleh SPM dan SAI.
4) Untuk menjaga keberlangsungan strategi dalam proses bisnis terlebih dahulu dilakukan analisis pengaruh/dampak yang terjadi dengan kesiapan dan ketetapan di Direktorat SISFO dan pilihan strategi yang ada di komunikasikan dengan pihak SPM.
5) Tidak dilakukannya *Bussines Plan Continuity* untuk pengembangan implementasi proses bisnis di Direktorat SISFO, hal ini sedang dalam tahap perencanaan, belum berlangsung. Rencana ini akan berlangsung setelah berlangsungnya sertifikasi.
6) Adanya pelatihan yang dilakukan terhadap pegawai untuk pengembangan skill setiap 1 tahun sekali. Hasil pelatihan dilaporkan dalam bentuk laporan kegiatan.
7) Dalam menejemen *backup* dilakukannya test terlebih dahulu, kemudian hasil dilaporkan setelah itu baru digunakan secara tetap.
8) Melakukan review terhadap kegiatan proses bisnis dan membuat daftar – daftar perubahan terhadap perencanaan yang telah disusun dalam RTM.

4.4.2.5 Kondisi existing DSS05

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

1) Ada aturan tertulis dalam aktivitas-aktivitas untuk melindungi fasilitas dari *maleware*, namun dokumen tidak dijaga.
2) Melakaukan riset terhadap ancaman – ancaman yang potensial.
3) Dibuatnya kebijakan mengenai keamanan konektifitas dan perangkat endpoint yang terdapat pada SKPL.
4) Dalam manjemen hak akses dilakukannya pembuatan hak akses pada SKPL, kemudian dimonitorng. Apabila ada permintaan hak akses maka permintaan harus di disposisi.
5) Terdapat pemantauan dari aktifitas pengaksesan padasistem iGracias
6) Setiap perangkat sensitive dan perangkat – perangkat yang ada di inventariskan dengan baik kebagian logistic.
7) Dibuatkannya daftar hask akses yang istimewa berdasarkan structural
8) Terdapat penentuan karakteristik keamanan dalam memonitoring keamanan infrastruktur yang di tentukan dalam rapat dan terdapat security incident ticket dalam sistem informasi helpdesk.

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 tujuan Direktorat SISFO sudah berlangsung baik. Dilengkapi laporan tinjuan dan juga analisis terhadap akar permasalahan yang muncul
2) Pemantauan dilakukan terus – menerus namun tidak terdapat dokumentasinya.
3) Peran, tanggungjawab, hak akses dan level otoritas telah didefinisikan dan terdokumentasi dalam sistem *dashboard* yang bersifat *private*.
4) Telah dilakukannya koreksi yang dilakukan oleh pihak SPM untuk mengetahui kesalahan – kesalahan kemudian dianalisis dan dilaporkan saat RTM.
5) Terdapat rekaman di sistem informasi *helpdesk* yang dapat digunakan untuk memastikan jejak kegiatan informasi dan pertanggung jawabannya.
6) Tidak adanya laporan mengenai daftar – daftar pelangaran terhadap sistem yang padahal dilakukan analisisnya.

4.5 Analisis *Gap*

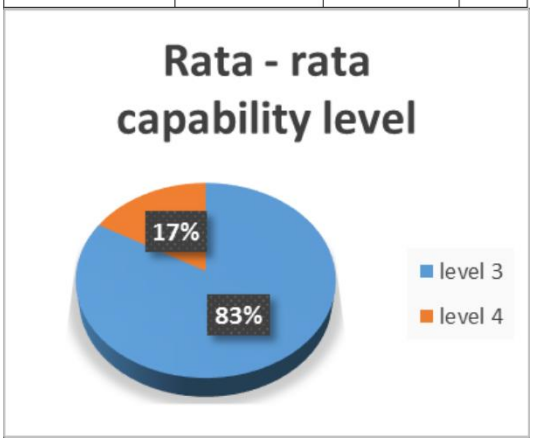
Analisis *Gap* ini dlakukan untuk mencari selisih dari *level capability* yang didapat dengan level target yang ingin dicapai. Dalam penentuan level target, ditentukan dengan level yang sedang dituju dari level rata – rata yang didapat. Contoh untuk DSS01 di peroleh level rata – rata 3,82 maka DSS01 sedang dalam tahap menuju level capability 4 dan masih mencapai 0,82 atau 82% di atas level 3 atau kurang dari 0,18 atau 18% menuju level capabilty 4. Sehingga ditetapkan level targetnya adalah level 4.

4.5.7 Analisis keseluruhan *Gap*

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

Tabel 4.44

Nama Proses	Level Existing	Level Target	Gap
DSS01 Manage Operations	3	4	1
DSS02 Manage Service Requests and Incidents	4	5	1
DSS03 Manage Problems	3	4	1
DSS04 Manage Continuity	3	4	1
DSS05 Manage Security Services	3	4	1
DSS06 Manage Bussiness Process Controls	3	4	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 3 yaitu *Establsh Process*. Artinya aktivitas-aktivitas telah dilakukan, ada standar penerapan dalam melakukan proses tersebut, terdokumentasi dan komunikasi berjalan dengan baik.

4.6 Rekomendasi

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 Direktorat SISFO :

1) Menindak lanjuti hasil audit independent terhadap kualitas layanan, lingkungan dan dengan pihak luar yang menjalin kerjasama, apabila dari audit independent tidak ada maka ditambahkan sendiri.
2) Melakukan analisis perangkat IT untuk mencegah ancaman yang timbul dari tindakan manusia seperti pencurian, dan juga terlindung dari ancaman dari hal – hal lain misalkan kebocoran, akan hujan, bahaya kebakaran karena konsleting dll.
3) Melakukan penilaian terhadap infrastruktur yang dimilki dan dibuat dokumentasinya untuk bahan evaluasi kedepan.
4) Menjaga dan memonitoring infrastruktur dengan baik, karena telah disediakan CCTV namun tidak ada yang menoperasikannya, lebih baik disediakan pegawai yang bertugas untuk memonitoringnya, misalkan satpam.

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 Direktorat SISFO :

1) Membuat klasifikasi terhadap jenis – jenis layanan dan insiden yang dilayani, sehingga mudah untuk dipetakan ke

bagian atau divisi yang akan langsung menyelesaikan layanan atau insiden tersebut.
2) Membuat strategi – strategi dalam permintaan layanan dan pemecahan insiden baik dalam bentuk kebijakan ataupun tindakan penanganan langsung seperti sistem.
3) Melakukan review terhadap SLA yang dibuat minimal tiap satu tahun untuk mengetahui ketidaksesuaian yang terjadi dan melukan inovasi terhadap SLA yang sudah ada.
4) Memberikan wadah untuk kritik dan saran kepada konsumen untuk menilai pelayanan, kepuasan konsumen dan pengembangannya.
5) Membuat inovasi strategi terhadap insiden yang belum terselesaikan, menganalisis dan mengevaluasi kembali inovasi strategi yang dibuat.
6) Membuat dokumentasi terhadap resolusi atau solusi alternative terhadap pemecahan insiden dan mengevaluasinya.
7) Mengembangkan sistem yang dapat melaporkan kecenderungan masalah atau insiden yang dihadapi sehingga pihak Direktorat SISFO dapat mengetahui kesalahan – kesalahan yang didapatkan.
8) Mendefinisikan batas waktu pemecahan dalam klasifikasi insiden dan mengevaluasi minimal tiap bulan sekali.

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 Direktorat SISFO :

1) Melakukan pemantauan terhadap kinerja penyelesaian masalah yang telah ditentukan.
2) Mendokumentasikan dan mengalisa kembali laporan masalah yang ada baik yang sudah terselesaikan maupun yang belum terselesaikan.
3) Menganalisa akar – akar permasalahan yang muncul dan pemecahan masalah, kemudian mendokumentasikannya supaya tidak terjadi masalah yang sama.
4) Membuat sistem/skema yang dapat mengetahui jalannya penyelesaian pemecahan masalah yang ada agar dapat dipantau oleh pihak atasan.
5) Membuat dokumentasi terkait solusi – solusi dalam pemecahan masalah.
6) Melakukan analisa pembiayan untuk menyelesaikan masalah, melakukan pemantauan dan didokumentasikan.
7) Memebuat analisa pengalokasian sumberdaya yang akan digunakan untuk mengoptimalkan resource yang dimiliki.

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 Direktorat SISFO :

1) Melakukan pengukuran keberlangsungan proses bisnis untuk mengetahui tingkat kematangannya dan kesenjangan proses bisnis, didokumentasikan dan dievaluasi.
2) Mengukur kesesuaian kebijakan yang dibuat dalam keberlangsungan proses bisnis.
3) Menganalisis dan membuat skema atau SOP tentang terjadinya gangguan dalam sekenario proses bisnis yang ditetapkan.
4) Melakukan evaluasi terhadap kebutuhan keberlanjutan proses bisnis yang berlangsung.

5) Menetapkan ukuran – ukuran terhadap ancaman – ancaman yang dapat menggangu jalannya proses bisnis.
6) Membuat skema atau sistem yang berisi respon terhadap insiden dan kominukasinya, mendokumentasikan dan dievaluasi.
7) Membuat *business continuity plan* (BCP) untuk pengembangan proses bisnis dan dokumentasikan.
8) Melakukan pengukuran dan evaluasi terhadap tujuan pelatihan.
9) Melakukan penjaminan keamanan terhadap distribusi data yang bersifat rahasia.
10) Membuat ketetapan ukuran – ukuran untuk pengambangan latihan sumberdaya manusia yang dimiliki, dan dipantau keberlangsungannya.

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 Direktorat SISFO :

1) Membuat kebijakan terkait dengan maleware software, didokumentasikan dan dievaluasi. (mis: menginstall antivirus yang diwajibkan)
2) Menetapkan sistem yang digunakan untuk mengevaluasi ancaman – ancaman yang akan timbul, didokumentasikan dan dimonitoring.
3) Melakukan evaluasi yang dilakukan rutin, minimal tiap semester terhadap sistem informasi yang dikhawatirkan dapat timbul potensi ancaman baru.
4) Memberikan peringatan kepada semua pegawai akan kedasarannya terhadap keamanan sistem dan perangkat yang dimiliki.
5) Membuat laporan mengenai ujicoba sistem keamanan yang diterapkan dan dievaluasi.
6) Mengukur kualitas sistem keamanan dan hak akses yang diberikan.
7) Mengevaluasi atau memantau hak akses yang diberikan untuk terjaga dari ancaman – ancaman yang potensial.

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 Direktorat SISFO :

1) Menetapkan ukuran – ukuran goal dari proses bisnis, mendokumentasikan dan dievaluasi.
2) Membuat laporan dari kontrol pemrosesan agar mudah diketahui gejala – gejala yang timbul.
3) Memantau dan mengevaluasi prosedur keamanan untuk melindungi aset informasi.
4) Membuat kebijakan dalam penentuan peran yang berwenang untuk mengakses aktivitas atau data yang bersifat sensitive, dijelaskan secara rinci dan didokumentasikan.
5) Mereview penyimpangan – penyimpangan yang terjadi dalam keberlangsungan prose bisnis, mendokumentasikan dan dievaluasi
6) Membuat kebijakan terhadap pemberian hukuman kepada pegawai yang melakukan pelanggaran – pelanggaran dalam pemantauan kegiatan proses bisnis.
7) Menyimpang dengan baik atau mengarsipkan data seperti sumber informasi, rekaman transaksi untuk dijadikan bukti dalam pengukuran penilaian keberlangsungan proses bisnis dan dapat sebagai rekomendasi.
8) Mengidentifikasi jenis – jenis data yang bersifat rahasia, membuat prosedur penyimpanan dan penghapusan yang tepat.

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 Direktorat SISFO dalam ruang lingkup iGracias.

Capability level yang didapat secara keseluhan adalah level 3 *Established Process*, level target yang ingin dicapai adalah 4 *Predictable process*, sehingga rekomendasi yang disusun adalah sebagai berikut:

1) Membuat penerapan pengukuran layanan yang harus dipenuhi dalam tiap proses bisnis untuk terjaminnya sistem iGracias berjalan dengan baik.
2) Membuat sistem monitoring dan evaluasi yang tepat terhadap proses bisnis untuk mengoptimalkan keberlangusngan iGracias.
3) Membuat dokumentasi atau laporan mengenai keseluruhan hasil proses yang berlangsung, dan juga pelanggaran yang terjadi sebagai bahan evaluasi dan pengembangan keberlanjutannya.
4) Membuat dan menjaga dengan baik pendokumentasian informasi yang dapat meningkatkan/menjaga keberlangsungan jalannya sistem iGracias.

5. Kesimplan dan Saran

5.1 Kesimpulan

Berdasarkan audit yang dilakukan pada Direktorat SISFO Telkom University dalam study kasus iGracias dengan *framework* COBIT 5 Domain DSS (*Deliver, Service, and Support*) maka kesimpulan dari tugas akhir ini adalah :

1) Pada tahap Pra audit telah diperoleh 6 proses domain DSS COBIT 5 yang dimana merupakan keseluruhan proses dari domain DSS yang sesuai dengan kondisi tata kelola Direktorat SISFO Telkom University dan digunakan sebagai ruang lingkup dan standar audit yaitu DSS01, DSS02, DSS03, DSS04, DSS05, dan DSS06.
2) Dari hasil audit, diketahui ada 1 proses yang mempunyai level kapabilitas 4 yaitu DSS02, ada 5 proses yang mempunyai level kapabilitas 3 yaitu DSS01, DSS03, DSS04, 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, DSS03, DSS04, DSS05 dan DSS06 adalah level 4, untuk DSS02 adalah level 5.
4) Level *capability* keseluruhan yang diperoleh berdasarkan keseluruhan rata – rata adalah 3, yang berarti sebagian besar aktifitas pada domain DSS untuk Direktorat SISFO Telkom University telah dilakukan, ada standar penerapan dalam melakukan proses tersebut, terdokumentasi dan komunikasi berjalan dengan baik.

5.2 Saran

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

1) Penilaian tingkat kapabilitas terkait Direktorat SISFO Telkom University 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.