PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5 PADA PROSES MONITORING DAN EVALUASI TERKAIT KEAMANAN SITU

(Studi Kasus : Fakultas Teknik Universitas Pasundan)

Rama Fitriani[1], Edwar J. Ramdon[2], Rita Rijayanti[3]

[1,2,3] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pasundan Bandung
[1,2,3] Universitas Pasundan Bandung, Jalan Setiabudi no. 193 Bandung 40153

[1]rama.fitriani@mail.unpas.ac.id , [2] edounpas@gmail.com, [3] rita.rijayanti@unpas.ac.id

Abstrak

Teknologi Informasi pada era ini sudah menjadi kebutuhan yang sangat penting untuk menunjang berjalannya proses bisnis secara efektif dan efisien pada perusahaan maupun institut. Universitas Pasundan (UNPAS) Bandung terutama Fakultas Teknik (FT) menerapkan teknologi informasi untuk mendukung layanan akademik. Layanan Teknologi Informasi (TI) tersebut diterapkan dalam bentuk aplikasi berbasis web dengan nama Sistem Informasi Terpadu (SITU). Namun, permasalahannya penerapan TI tersebut tidak disertai dengan proses monitoring dan pengevaluasian sehingga tidak ada kontrol dalam penerapannya terutama pada ketersediaan data dan keamanan.

Penelitian ini dilakukan untuk mengetahui kondisi tata kelola TI pada proses monitoring dan evaluasi terkait dengan keamanan TI pada SITU di FT UNPAS yang mengacu pada COBIT 5 domain Monitoring Evaluate Assess (MEA). Tahapan dalam pengerjaan Tugas Akhir ini dimulai dengan identifikasi masalah, study literature, menetukan teknik pengumpulan data, analisis objek penelitian, dan perancanagan tata kelola TI pada proses monitoring dan evaluasi.

Hasil akhir dari penelitian ini adalah berupa kesimpulan dan rancanagan mengenai perbaikan aktivitas tata kelola TI pada proses monitoring dan evaluasi pada sisi ancaman terkait keamanan TI pada SITU di Fakultas Teknik Universitas Pasundan Bandung dengan memanfaatkan COBIT 5 sebagai acuan.

Kata Kunci : *Tata Kelola Teknologi Informasi, Teknologi Informasi, COBIT 5, Domain Monitoring Evaluate Assess (MEA), Fakultas Teknik Universitas Pasundan*

1 Pendahuluan

1.1 Latar Belakang

Teknologi Informasi pada era ini sudah menjadi kebutuhan yang sangat penting untuk menunjang berjalannya proses bisnis secara efektifitas dan efisiensi pada perusahaan, untuk mencapai hal tersebut diperlukan adanya pengelolaan TI atau yang disebut dengan Tata Kelola Teknologi Informasi (*IT Governance*).

Tata Kelola Teknologi Informasi (*IT Governance*) adalah pertanggungjawaban dewan direksi dan manajemen eksekutif. Hal ini, merupakan bagian yang terintegrasi dengan tata kelola perusahaan dan berisi kepemimpinan dan struktur serta proses organisasi yang menjamin bahwa organisasi teknologi informasi mengandung dan mendukung strategi serta tujuan bisnis[14].

Universitas Pasundan Bandung terutama Fakultas Teknik (FT) sebagai penyelenggara pendidikan, dimana Fakultas Teknik UNPAS harus memberikan layanan akademik. Dalam pelaksanaannya Fakultas Teknik UNPAS dirasa perlu untuk memanfaatkan peranan teknologi informasi, layanan Teknologi Informasi (TI) tersebut diterapkan dalam bentuk aplikasi berbasis web dengan nama Sistem Informasi Terpadu (SITU), Tidak dapat disangkal lagi bahwa informasi harus didapatkan dan diproses secara cepat. Disinilah peranan SITU sebagai komponen utama dalam menunjang akademik untuk Fakultas Teknik UNPAS. Adapun tujuan SITU yaitu mempermudah sivitas akdemik untuk mendapatkan informasi dan mempermudah karyawan untuk melakukan tugasnya. Adapun penerapan SITU ini harus dibarengi dengan pengelolaan TI yang baik dan benar agar keberadaan TI mampu untuk menunjang kesuksesan Fakultas Teknik UNPAS dalam pencapaian tujuannya.

Maka dapat dikatakan pihak pengelola dari SITU harus menjamin ketersediaan Informasi bagi Sivitas Akademik berupa sebuah layanan yang baik. Salah satu proses untuk menjamin ketersediaan informasi adalah adanya proses monitoring dan evaluasi, namun pada saat ini belum adanya proses proses monitoring dan evaluasi terhadap tata kelola

teknologi informasi secara terstruktur terutama pada sisi kemanan. Jika proses monitoring dan evaluasi dilakukan maka perananan SITU akan lebih optimal. Melihat pentingnya melakukan monitoring dan evaluasi terhadap tata kelola SITU maka penulis tertarik untuk mengusulkan adanya kegiatan monitoring dan evaluasi terhadap tata kelola SITU dengan menerapkan sebuah standar yaitu *Control Objectives for Information and related Technology* (COBIT). Dimana hal ini dapat menghindari risiko kegagalan teknologi informasi yang digunakan oleh FT UNPAS sehingga menjaga dan meningkatkan kualitas dan mutu peranan teknologi informasi yang digunakan yaitu SITU.

1.2 Identifikasi Masalah

Dari uraian latar belakang yang telah dikemukakan, maka dapat ditarik identifikasi masalah yaitu belum adanya tata kelola TI pada proses monitoring dan evaluasi terkait keamanan TI pada SITU FT UNPAS.

1.3 Tujuan Tugas Akhir

Adapun tujuan dalam penelitian Tugas Akhir ini adalah membuat rancangan tata kelola TI pada proses monitoring dan evaluasi SITU dengan kerangka kerja COBIT 5 domain *Monitoring Evaluate Assess* (MEA) SITU FT UNPAS terkait keamanan SITU FT UNPAS. Fokus rancancanagan dikhususkan untuk perbaikan aktivitas pada proses monitoring dan evaluasi.

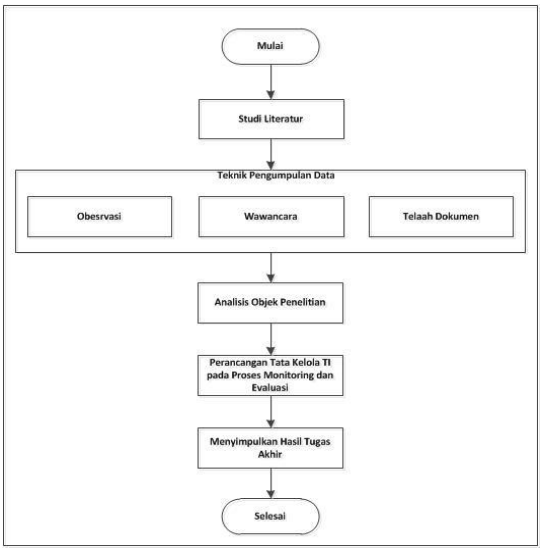
1.4 Lingkup Tugas Akhir

Adapun pada penelitian Tugas Akhir ini dibatasi yaitu:

1. Objek yang diteliti adalah Sistem Informasi Terpadu UNPAS (SITU) terkait keamanan.
2. Tugas akhir ini melakukan perancangan tata kelola pada SITU di Fakultas Teknik UNPAS dengan menggunakan kerangka kerja COBIT 5 pada domain *Monitoring Evaluate Assess* (MEA) pada proses yang berhubungan dengan keamanan TI yang meliputi *base practice* MEA01.03 *Collect and process performance and conformance data*, MEA01.05 *Ensure the implementation of corrective actions*, MEA02.04 *Identify and report control deficiencies*, MEA03.01 *Identify external compliance requirement,* perancangan ini yang terkait dengan aktivitas proses.

1.5 Metodologi Tugas Akhir

Adapun langkah-langkah penelitian yang dikerjakan dalam menyelesaikan Tugas Akhir terlihat pada gambar 1.



Gambar 1

Keterangan :

1. Studi literatur

Mencari dan mempelajari buku-buku referensi di beberapa perpustakaan mengenai teori dan hal-hal lainnya yang dibutuhkan untuk menyelesaikan tugas akhir yang akan dibuat.

2. Teknik Pengumpulan Data

Teknik pengumpulan data merupakan tahap untuk pengumpulan data-data yang sesuai dengan objek penelitian, tahap ini bertujuan untuk memahami kondisi FT UNPAS. Pengumpulan data dilakukan dengan observasi, wawancara dan kajian dokumen. Penjelasan mengenai ketiga teknik pengumpulan data dijelaskan dibawah ini:

a. Observasi

Observasi merupakan teknik pengumpulan data yang dilakukan dengan cara melakukan pengamatan secara langsung pada FT UNPAS. Observasi ini bertujuan untuk mendapatkan informasi mengenai kondisi nyata yang terjadi pada pengelolaan TI di FT UNPAS.

b. Wawancara

Pengumpulan data melalui wawancara dilakukan tidak terstruktur dimana penulis mengajukan pertanyaan, pertanyaan dapat berkembang seiring dari jawaban responden. Wawancara tersebut dilakukan dengan tujuan untuk mendapatkan informasi yang terkait dengan visi-misi, proses bisnis dan untuk mengetahui kebutuhan perancangan tata kelola TI proses monitoring dan evaluasi penanggulangan ancaman terkait keamanan pada SITU FT UNPAS.

c. Telaah Dokumen

Selanjutnya metode yang ketiga adalah melakukan kajian terhadap dokumen-dokumen terkait pengelolaan TI yang ada pada Fakultas Teknik Universitas Pasundan terutama pada proses monitoring dan evaluasi.

3. Analisis Objek Penelitian

Melakukan analisis berdasarkan objek penelitian sehingga dapat menjadi acuan untuk melakukan perancangan proses monitoring.

4. Perancangan Tata Kelola TI

Selanjutya melakukan perancangan tata kelola TI pada proses monitoring dan evaluasi, perancangan disesuaikan dengan kerangka kerja COBIT 5 pada domain MEA.

5. Menyimplukan Hasil Tugas Akhir

Pada tahap ini dilakukan untuk menyimpulkan tugas akhir yang telah dibuat, serta memberikan usulan untuk pengembangan selanjutnya.

2 Landasan Teori

2.1 Teknologi Informasi

Teknologi informasi telah didefinisikan oleh banyak para ahli yang telah dijelaskan dalam buku Abdul Kadir yang berjudul Pengenalan Sistem Informasi Edisi Revisi, teknologi informasi yaitu [8]:

1. Menurut kamus Oxford (1995), teknologi informasi adalah studi atau penggunaan alat elektronika, terutama computer, untuk menyimpan, menganalisis, dan mendistribusikan informasi apa saja, termasuk kata-kata, bilangan, dan gambar.
2. Menurut Alter(1992), teknologi informasi mencakup perangkat keras dan perangkat lunak untuk melaksanakan satu atau sejumlah tugas pemrosesan data seperti menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, atau menampilkan data.
3. Martin (1999) mendefinisikan teknologi informasi tidak hanya terbatas pada teknologi computer (perangkat keras dan perangkat lunak) yang digunkan untuk memproses dan menyimpan informasi, melainkan mencakup teknologi komunikasi untuk mengirimkan informasi..

2.2 Tata Kelola Teknologi Informasi

Tata kelola Teknologi Informasi telah didefinisikan oleh beberapa ahli seperti yang telah dijelaskan dalam buku Kridanto Surendro, Definisi Tata Kelola Teknologi Informasi yaitu[14]:

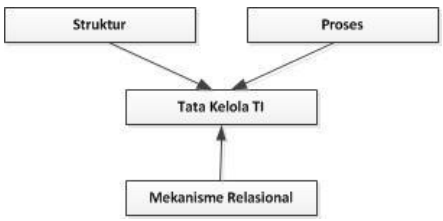
1. Menurut IT Governance Institute (ITGI), Tata kelola teknologi informasi adalah pertanggung jawaban direksi dan manajemen eksekutif . hal ini, merupakan bagian yang terintegrasi dengan tata kelola perusahaan dan berisi kepemimpinan dan struktur serta proses organisasi yang menjamin bahwa organisasi teknologi informasi mengandung dan mendukung strategi serta tujuan bisnis.
2. Menurut Van Grembergen 2002, Tata kelola teknologi informasi adalah penilaian kapasitas organisasi oleh dewan direksi, manajemen eksekutif, manajemen teknologi informasi untuk mengendalikan formulasi dan implementasi strategi teknologi informasi dalam rangka mendukung bisnisnya.[14].

Dari definisi Kridanto Surendro menyimpulkan bahwa yang dimaksud dengan tata kelola teknologi informasi adalah upaya untuk menjamin pengelolaan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis suatu *enterprise* yang dilakukan oleh dewan direksi, manajemen eksekutif dan juga manajemen teknologi informasi[14].

2.3 Elemen Tata Kelola TI

Tata kelola TI dapat dikembangkan dengan menggunakan panduan struktur, proses, dan mekanisme[2]. Setiap organisasi pasti akan berbeda satu dengan yang lain dalam penerapan struktur, proses dan mekanisme hubungannya, tergantung dari kondisi, situasi dan tantangan yang dihadapi masing-masing organisasi.

Suatu kerangka kerja untuk implementasi tata kelola TI yang terdiri dari panduan struktur, proses, dan mekanisme hubungan seperti yang terlihat pada gambar 2.



Gambar 2. Kerangka Kerja Elemen Tata Kelola TI[2]

Adapun Struktur melibatkan adanya fungsi-fungsi yang bertanggung jawab seperti eksekutif TI dan komite TI. Proses mengacu pada pembuatan keputusan strategis dan monitoring misalnya melalui *IT Balanced Scorecard.* Mekanisme hubungan termasuk partisipasi pihak bisnis dan TI, dialog strategis, pembelajaran bersama, dan komunikasi yang baik[2].

2.4 Cyber Security

Definisi *cybersecurity*, mengacu pada ITU-T X.1205 cybersecurity adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna termasuk terhubung perangkat komputasi, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang disampaikan dan / atau disimpan dalam lingkungan cyber. *Cybersecurity* berusaha untuk memastikan

pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber* [7]. Tujuan keamanan umum terdiri dari [7]:

1. Integrity.
2. Confidentilality.
3. Availability.

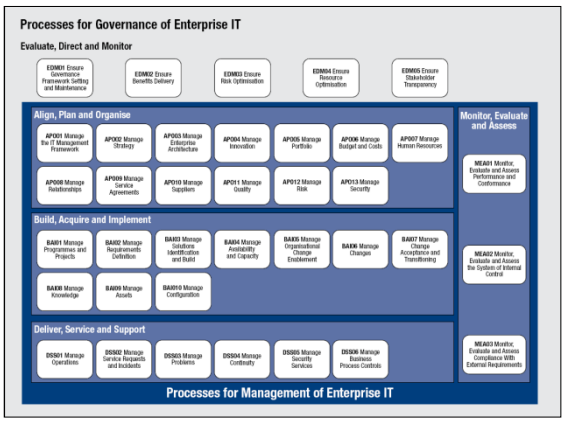
2.5 COBIT(*Control Objectives for Information and related Technology*)

COBIT dikembangkan oleh *IT Governance Institute* (ITGI), yang merupakan seperangkat pedoman umum untuk manajemen IT yang dibuat oleh *Information System Audit and Control Association* (ISACA).

COBIT adalah sekumpulan dokumentasi *best practices* untuk tata kelola teknologi informasi yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani *gap* antara risiko bisnis, kebutuhan control dan masalah-masalah teknis IT. COBIT bermanfaat bagi auditor karena merupakan teknik yang dapat membantu dalam identifikasi *IT controls issues*. COBIT berguna bagi IT *user* karena memperoleh keyakinan atas kehandalan sistem aplikasi yang dipergunakan. Sedangkan para manajer memperoleh manfaat dalam keputusan investasi di bidang IT serta infrastrukturnya, menyusun *strategic IT Plan*, menentukan *information architecture*, dan keputusan atas *procurement* (pengadaan / pembelian) asset[3].

2.6 Dimensi Proses

Dimensi Proses menggunakan COBIT 5 merupakan Acuan untuk model proses. COBIT 5 menyediakan suatu acuan model proses yang digambarkan dengan suatu arsitektur, dimana arsitektur tersebut menggambarkan hubungan setiap proses, didalamnya terdapat 37 proses. COBIT 5 membagi proses IT kedalam dua area yaitu Governance dan Management. Proses tersebut ditunjukan pada gambar 3.



Gambar 3

2.7 Domain Monitor, Evaluate and Assess

Fokus domain MEA pada COBIT 5 yaitu pada area manajemen yaitu proses penilaian dan kebutuhan perusahaan dan sistem yang sedang berjalan masih memenuhi atau tidak, memastikan desain control mematuhi regulasi, serta monitoring berkaitan dengan penilaian indipenden berkaitan efektivitas serta kemampuan untuk memenuhi bisnis objektive oleh penilaian indipenden. Domain MEA terdiri dari 3 kontrol *objective*[5].

2.8 MEA untuk Keamanan TI

Proses manajemen untuk cybersecurity didistribusikan di seluruh COBIT 5 Proses Reference Model. Dimana kegiatan keamanan informasi umum yang diperlukan untuk suatu proses, kegiatan cybersecurity juga akan dibutuhkan. Namun demikian tidak semua tugas-tugas keamanan informasi tingkat tinggi dan kegiatan harus dicerminkan atau berulang-ulang untuk kepentingan cybersecurity; dalam beberapa kasus, hal itu akan cukup untuk terhubung ke pengaturan keamanan yang ada[6].

Pada penelitian ini menggunakan fokus pada domain MEA yaitu MEA01 (*Monitor, Evaluate and Assess Performance and Conformance*), MEA02 (*Monitor, Evaluate and Assess the System of Internal Control dan Monitor*) *dan* MEA03 (*Evaluate and Assess Compliance with External Requirements*) dengan pilihan proses yang berkaitan dengan keamanan TI. Adapun penjelasasan proses MEA terkait kemanan TI diuraikan pada gambar .

No	Kode	Proses	Keamanan TI
1.	MEA01	*Monitor, Evaluate and Assess Performance and Conformance*	Proses pendukung untuk monitorng cybersecurity (dalam batas-batas hokum dan peraturan)
2.	MEA02	*Monitor, Evaluate and Assess the System of Internal Control*	Proses pendukung untuk kontrol penilaian di cybersecurity, termasuk pelaporan serangan/ pelanggaran dan aktivitas yang mencurigakan lainnya
3.	MEA03	*Monitor, Evaluate and Assess Compliance with External Requirements*	Proses untuk mengidentifikasi dan menafsirkan persyaratan kepatuhan eksternal dan *cybersecurity*

Gambar 4. Proses MEA Keamanan TI[6]

Adapun hubungan MEA yang kaitannya erat dengan terkait kemanan TI yaitu pada *base practice* MEA01.03, MEA01.05, MEA02.04, MEA03.01. *Base Practice* yang berkaitan dengan keamanan TI diuraikan pada tabel pada gambar 5.

No	Kode	*Base Practice*	Deskripsi
1.	MEA01.03	Mengumpulkan kinerja proses dan kesesuaian data	Mengumpulkan dan mengolah data tepat waktu dan akurat sesuai dengan pendekatan perusahaan.
2.	MEA01.05	Memastikan pelaksanaan tindakan korektif	Membantu para pemangku kepentingan dalam mengidentifikasi, memulai dan pelacakan tindakan korektif untuk mengatasi anomali.
3.	MEA02.04	Mengidentifikasi dan melapokan kekurangan kontrol	Mengidentifikasi kekurangan kontrol dan menganalisis dan mengidentifikassi akar penyebab yang mendasarinya. Tingkatkan kekurangan kontrol dan melaporkan kepada stakeholder.
4.	MEA03.01	Mengidentifikasi requirement kepatuhan eksternal	Secara terus menerus, mengidentifikasi dan memonitor perubahan dalam undang-undang local dan internasional, peraturan dan persyaratan eksternal lainnya yang harus dipenuhi dan perspektif TI.

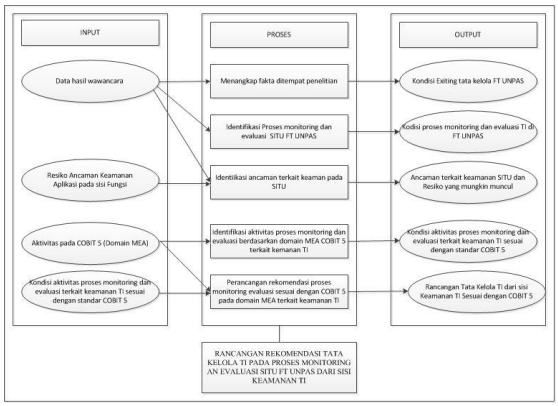
Gambar 5. Tabel *Base Practice* Terkait Keamanan TI

3 Identifikasi Objek Penelitian

3.1 Skema Analisis

Skema analisis bertujuan untuk membantu memudahkan dan memahami bagaimana alur dari analisis yang dilakukan untuk melaukan

perancangan rekomendasi tata kelola TI dari sisi ancaman terkait keamanan pada SITU di FT UNPAS. Analisis meliputi input, proses dan output yang ditunjukan pada gambar 6 .



Gambar 6. Skema Analiasis

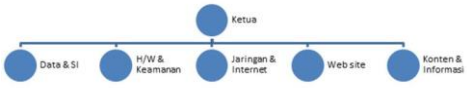
FT Unpas telah menetapkan optimalisasi penggunaan TIK dalam mendukung operasional sehari-hari ke dalam salah satu rencana strategis fakultas. Hal ini harus dibarengi organisasi yang bertanggunga jawab terhadap Pengelolaan TI, adapun Pengelola TI dilingkungan FT UNPAS yaitu Pusat Data dan Teknologi Informasi (PUSDATIN) FT UNPAS, dengan visi dari PUSDATIN yaitu:

Mendukung pencapaian visi fakultas teknik dalam hal dukungan informasi dan teknologi informasi.

Adapun Tugas Pokok dari PUSDATIN yaitu:

1. Mengelola infrastruktur TIK yang ada pada lingkungan FT UNPAS.
2. Mendukung kebutuhan TIK, dari mulai Mengatur pengadaan TIK dilingkungan FT UNPAS.
3. Memastikan kegiatan operasional TIK di lingkungan Fakultas Teknik UNPAS berjalan dengan baik.

Adapun Struktur Organisasi PUSDATIN tergambar pada gambar 7 :



Gambar 7. Struktur Organisasi PUSDATIN[PUS13]

3.2 Objek Penelitian

Objek penelitian merupakan topik atau sesuatu yang diteliti. Pada penelitian ini objek yang diteliti adalah tata kelola TI pada proses monitoring dan evaluasi terkait keamanan pada SITU FT UNPAS.

3.3 Keamanan Teknologi Informasi

Berdasarkan Sistem yang akan dikembangkan di Fakultas Teknik Unpas merupakan sistem yang beberapa diantaranya memilki data yang sangat sensitif seperti data akademik dan keuangan. Untuk itu aspek keamanan menjadi salah satu aspek yang harus disiapkan dalam implementasi sistem informasi.

Fitur keamanan yang diterapkan pada Sistem Informasi Terpadu Fakultas Teknik Unpas, terbagi menjadi 3 (tiga) kelompok yaitu :

1. *Network Security*, fokus pada keamanan media pembawa informasi/data atau jalur komunikasi data.
2. *Computer Security*, fokus kepada komputer yang digunakan (server, workstation) termasuk didalamnya masalah yang berhubungan dengan sistem operasi.
3. *Application Security*, fokus kepada aplikasi dan basisdata.

Terdapat 3 kelompok fitur kemananan yang diterapkan pada SITU pada penelitian ini fokuskan pada *application Security* berdasarkan sisi Fungsi.

3.4 SITU

Sistem informasi terpadu unpas (SITU) adalah sebuah sistem yang dibangun dan dikelola oleh Satuan Pengelola Teknologi Informasi dan Komunikasi (SPTIK) UNPAS. Terbentuknya SITU dilatarbelakangi oleh kebutuhan adanya sistem informasi yang mengintegrasikan data dan proses bisnis semua unit kerja dilingkungan UNPAS dan hal ini didukung program Hibah Kompetisi Institusi dari DIKTI tahun 2007.

Tujuan SITU

SITU terbagi menjadi beberapa sub Sistem Informasi yaitu Sistem Informasi Akademik, Sistem Informasi Kepegawaian dan Keuangan, Sistem Informasi Sarana dan Prasarana, Sistem Informasi Kemahasiswaan, dari bagian sub sistem tersebut sesuai dengan tujuan dari penggunaan SITU. Adapun tujuannya yaitu:

1. Secara umum meningkatkan tata kelola Organisasi
2. Secara Khusus:

a. Mengintegrasikan data dari fakta operasional mengenai akademik, SDM, Sarana dan Prasarana, serta keuangan.
b. Meningkatkan akses informasi maupun layanan bagi para stakeholder.
c. Meningkatkan brand-image UNPAS sebagai intitusi pendidikan

Pengelolaan SITU seperti halnya pada FT UNPAS mempunyai pengelola sendiri dengan tujuan penyesuaian kebutuhan stakeholder yang ada di FT UNPAS. SITU merupakan sebuah sistem yang berbentuk aplikasi berbasis web/ *web-based software.*

3.5 Identifikasi Masalah Ancaman Keamanan SITU

Identifikasi ancaman keamanan SITU bertujuan untuk memunculkan masalah yang pernah terjadi pada SITU dan sekaligus mendefinisikan resiko yang mungkin terjadi pada ancaman keamanan pada SITU. Adapun yang ancaman keaman pada SITU yang diuraikan berdasarkan pada kemanan pada sisi fungsi. Masalah yang pernah terjadi pada SITU FT UNPAS diuraikan pada tabel 8.

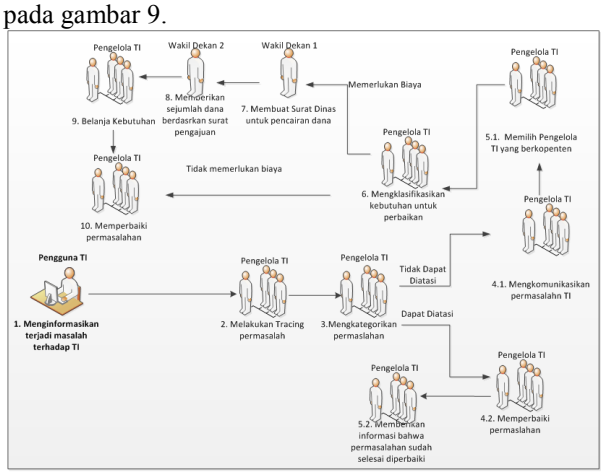
No	Masalah	Deskripsi	Penyebab
1.	Pengubahan nilai	Perubahan nilai dilakukan oleh mahasiswa/ penyerang dengan kepetingan untuk mengubah nilai yang awalnya kurang memuaskan menjadi nilai yan diharapkan oleh mahasiswa/ penyerang tersebut, jika masalah ini tidak segera diselesaikan mungkin akan terjadi dampak yang lebih serius yaitu mengubah nilai dan matakulia dapat dikatatakn lulus walaupun belum mengambil mata kuliah bersangkutan.	Penyebab dan pengubahan nilai yang telah ditelusu oleh pengelola yatu kegagalan untuk membatasi Akse URL, karena mahasiswa/ penyerang tidak berhal melakukan perubahan nilai, yang seharusnya dilakuka oleh pihak administrasi nilai. Mungkin hal ini jug disebabkan oleh scripting yang kuarang baik.
2.	Pencetakan kartu ujian dengan status belum membayar uang administasi ujian	Pencetakan kartu ujian seharusnya dapat dilakukan ketika status keuangan/ administrasi keuangan, pada hal ini mahasiswa dapat mencetak kartu ujian, dampak bisnisnya sendiri berdampak pada keuangan.	Penyebab dan pengubahan status yang telah ditelusu oleh pengelola yatu kegagalan untuk membatas Akses URL, karena seharusnya pencetakan kartu nila harus dengan status sudah melakukan administrasi
3.	Penghapusan data	Pernah terjadinya penghapusan data pada SITU, sehingga dampaknya mengganggu kegiatan administarasi SITU.	Kegagalan untuk membatasi Akses URL, sehingg penyerang dapat melakukan penghapusan data tanp hak akses.

(*Sumber: Hasil wawancara pada tanggal 09 Juni 2015*)

Gambar 8.Tabel Masalah Terhadap Ancaman Terkait Keamanan Pada SITU

3.6 Identifikasi Alur Proses Monitoring dan Evaluasi TI

Proses monitoring dan evaluasi TI yang terjadi pada saat ini adalah hanya jika terjadi permasalahan atau perintah melakukan perbaikan atau perkembangan yang diperintahkan oleh pimpinan atau WADEK II, adapun proses monitoring dan evaluasi dilakukan tidak secara terstruktur pelaksanaan TI sendiri belum dilandaskan prosedur dan tidak adanya dokumen yang mendukung akan pengelolaan TI. Adapun proses evaluasi jika terjadi masalah berdasarkan hasil wawancara direpresesntasikan dengan diagram *Workflow* seperti pada yang terlihat pada gambar 9.



Gambar 9. Alur Proses Evaluasi TI
(*Sumber: Hasil wawancara pada tanggal 22 Oktober 2014*)

3.7 Identifikasi Aktivitas Proses Monitoring dan Evaluasi dan Penilaiaan

Identifikasi aktivitas proses monitoring dan evaluasi dan penilaiaan bertujuan untuk mengetahui aktivitas pada FT UNPAS yang disesuaikan dengan aktivitas yang ada pada COBIT 5 pada domain *Monitoring, Evaluate Assess* yang berkaitan dengan keamanan TI. Adapun aktivitas yang telah diidentifikasi dijelaskan pada gambar 10.

No	Kode	Proses	Aktivitas	Eksistensi	
				Ada	Tidak Ada
1.	MEA01.03	Mengumpulkan kinerja proses dan kesesuaian data	Menetapkan *requirement* monitoring, indikator pengumpulan data dan metode pengumpulan untuk monitoring keamanan TI;	✓	
			Menentukan metode analisis yang tepat.		✓
2.	MEA01.05	Memastikan pelaksanaan tindakan korektif	Menetukan tindakan korektif yang berkaitan dengan serangan/ pelanggaran/ insiden	✓	
			Menanamkan tindakan korektif dan perencanaan terkait dalam keamanan TI.	✓	
3.	MEA02.04	Mengidentifikasi dan melapokan kekurangan kontrol	Mengidentifikasi kelemahan kontrol keamanan TI dari perspektif berbasis risiko.		✓
			Menyoroti adanya efek yang mengalir dalam dinamika sistem		✓
4.	MEA03.01	Mengidentifikasi *requirement* kepatuhan eksternal	Mengidentifikasi hukum atau peraturan yang berdampak terhadap kemanan TI.		✓
			Termasuk ketentuan-ketentuan khusus di bawah hak preorogatif kemanan nasional.		✓

Gambar 10. Tabel Identifikasi Aktivitas

4 Perancangan Tata Kelola Teknologi Informasi

4.1 MEA01 *Monitor, Evaluate and Assess Performance and Conformance*

Proses MEA01 yang proses praktik yang meliputi kemanan TI yaitu MEA01.03 dan MEA01.05. Adapun Berdasarkan hasil identifikasi aktivitas sesuai dengan COBIT 5 pada proses MEA01 di FT UNPAS yaitu ada beberapa aktivitas yang dilakukan namun belum terdokumentasi.

Adapun untuk perbaikan tata kelola TI pada proses MEA01 harus adanya *work* product, *work product* pada proses MEA01 yaitu:

1. MEA01.03 Proses monitoring data
2. MEA01.05 Proses pelacakan untuk tindakan perbaikan pada masalah keamanan informasi

4.2 MEA02 Monitor, Evaluate and Assess the System of Internal Control

Proses MEA02 yang proses praktik yang meliputi kemanan TI yaitu MEA02.04. Adapun Berdasarkan hasil identifikasi aktivitas sesuai dengan COBIT 5 pada proses MEA02 di FT UNPAS yaitu belum ada aktivitas yang dilakukan.

Adapun untuk perbaikan tata kelola TI pada proses MEA01 harus adanya *work* product, *work product* pada proses MEA01 yaitu MEA02.04 Hasil penilaian tindakan perbaikan.

4.3 MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

Proses MEA03 yang proses praktik yang meliputi kemanan TI yaitu MEA03.05. Adapun Berdasarkan hasil identifikasi aktivitas sesuai dengan COBIT 5 pada proses MEA03 di FT UNPAS yaitu belum ada aktivitas yang dilakukan.

Adapun untuk perbaikan tata kelola TI pada proses MEA03 harus adanya *work* product, *work product* pada proses MEA03 yaitu MEA03.01 Persyaratan kepatuhan keamanan informasi eksternal.

4.4 Rekomendasi Aktivitas Perbaikan

Rekomendasi perbaikan aktivitas bertujuan untuk memberikan rekomendasi dari rancangan aktivitas perbaikan dari proses pengarahan yang lebih detail. Adapun rekomendasi aktivitas perbaikan diuraikan pada tabel 1 .

Tabel 1. Rekomendasi Aktivitas Perbaikan

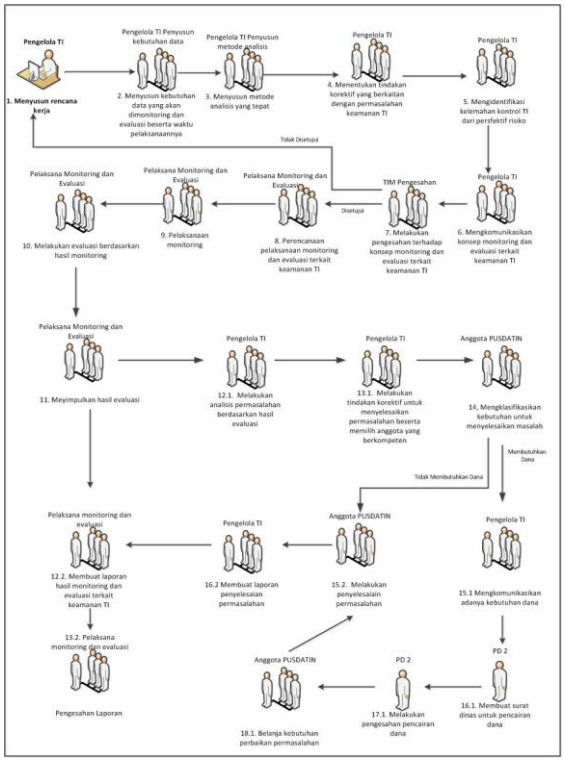
Kode Proses	Kode Aktivitas	Rancangan Aktivitas Perbaikan di FT UNPAS	Keterangan
ME01.03	MEA1.3.1	Melakukan penetapan requirement monitoring, indikator, pengumpulan data dan metode pengumpulan untuk monitoring keamanan pada SITU.	1. Mengumpulkan data dari requirement 2. Menilai efisiensi (usaha dalam kaitannya dengan wawasan yang disediakan) dan kesesuaian (kegunaan dan maknanya) dan memvalidasi integritas (akurasi dan kelengkapan) dari data yang dikumpulkan mengenai kemanan SITU.
	MEA1.3.2	Membuat suatu metode analisis untuk keamanan SITU sesuai dengan kebutuhan FT UNPAS.	Analisis yang tepat adalah dengan cara melakukan monitoring infrastruktur untuk kejadian yang berhubungan dengan kemanan dimana hal yang perlu dilakukan Mengidentifikasi dan mengelompokkan kontrol yang ada di atas intrusi, termasuk deteksi teknis, pengenalan pola oleh staf, pelaporan dan eskalasi. Sehingga yang menjadikan acuan analisis yaitu: 1. Adanya tuntunan insiden kemanan 2. Mengetahui karakteristik insiden kemanan 3. log peristiwa kemanan.
MEA01.05	MEA1.5.1	Membuat suatu prosedur standar operasional untuk tindakan yang akan dilakukan ketika terjadi serang/ pelanggaran/ insiden sesuai dengan tugas dan tanggung jawab dari pengelola TI. Disertai membuat pilihan dan rekomendasi untuk mengatasi masalah	1. Menetapkan tindakan korektif yang akan dilakukan untuk menyelesaikan masalah melakkan identifikasi kondisi terjadi serangan/ pelanggran/ insiden, menetapkan penyebab terjadinya serangan/ pelanggran/ insiden, melakukan evaluasi kebuthan akan tindakan yang akan dilakakukan untuk memastikan bahwa serangan/ pelanggran/ insiden tidak terulang kembali, Menetapkan dan menerapkan hasil tindakan yang diperlukan, Mengkaji tindakan korektif yang dilambil 2. Tanggapan ulasan manajemen, pilihan dan rekomendasi untuk mengatasi masalah dan penyimpangan yang besar. 3. Pastikan bahwa tugas tanggung jawab untuk tindakan korektif dipertahankan. 4. Melacak hasil tindakan yang dilakukan.
	MEA1.5.2	Membuat laporan berkala mengenai tanggung jawab dari pengelola TI terkait dengan penyelesaian masalah keamanan TI pada SITU	1. Megkomunikasikan tindakan korektif yang harus dilakukan untuk menyelesaikan masalah tertkait dengan kemanan SITU. 2. Melakukan pengawasan terhadap tindakan yang dialakukan untuk mengatasi masalah terkait kemanan 3. Membuat laporan berkala kepada pemangku kepentingan mengenaik tanggung jawab dari

Kode Proses	Kode Aktivitas	Rancangan Aktivitas Perbaikan di FT UNPAS	Keterangan
			para pengelola TI untuk tindakan yang dilakukan untuk mengatasi masalah
MEA02.04	MEA2.4.1	Memberikan definisi dan tanggung jawab kepada pengelola TI untuk menyelesaikan dan melaporkan status kontrol keamanan TI yang berkaitan dengan risiko kemanan TI. Serta definisikan juga risiko-risiko yang mungkin terjadi terkait dengan keamanan TI yaitu SITU.	1. Definisikan risiko keamananan dari seperti ancaman, kerentanan dan kategorikan dari *Low* sampai *Hight.* 2. Mengidentifikasi, laporan dan log pengecualian kontrol, dan menetapkan tanggung jawab untuk menyelesaikan dan melaporkan status. 3. Pertimbangkan risiko perusahaan terkait untuk menetapkan ambang untuk eskalasi pengecualian kontrol dan kerusakan. 4. Berkomunikasi prosedur eskalasi pengecualian kontrol, analisis akar penyebab, dan pelaporan untuk memproses pemilik dan stakeholder TI. 5. Tentukan mengontrol pengecualian harus dikomunikasikan kepada individu yang bertanggung jawab untuk fungsi dan yang pengecualian harus meningkat. Menginformasikan pemilik proses yang terkena dampak akan kemanan SITU dan para pemangku kepentingan.
	MEA2.4.2	Pertimbangkan risiko kemanan SITU terhadap FT UNPAS untuk menetapkan kerentanan atas dampak yang terjadi.	1. Pertimbangkan risiko kemanan SITU terhadap FT UNPAS dampak yang mempengaruhi seperti risko organisasi, risiko sosial 2. Tentukan mengontrol pengecualian harus dikomunikasikan kepada individu yang bertanggung jawab untuk fungsi dan yang pengecualian harus meningkat. Menginformasikan pemilik proses yang terkena dampak dan para pemangku kepentingan. 3. Menindaklanjuti semua pengecualian untuk memastikan bahwa yang disepakati-tindakan telah ditangani.
MEA03.01	MEA3.3.1	Membuat suatu peraturan yang relevan dengan penggunaan sumber daya TI dan pengolahan informasi dalam bisnis dan operasi TI perusahaan yang memiliki dampak terhadap keaman SITU.	1. Menetapkan tanggung jawab untuk mengidentifikasi dan memonitor perubahan persyaratan kontrak eksternal hukum, peraturan dan lainnya yang relevan dengan penggunaan sumber daya TI dan pengolahan informasi dalam bisnis dan operasi TI perusahaan. 2. Mengidentifikasi dan menilai semua persyaratan kepatuhan potensial dan dampaknya terhadap aktivitas kemanan SITU. 3. Menilai dampak dari persyaratan hukum dan peraturan yang berhubungan dengan TI kontrak pihak ketiga yang terkait dengan operasional TI terkait kemanan SITU. 4. Mendapatkan kuasa independen, jika sesuai, perubahan undang-undang yang berlaku, peraturan dan standar. 5. Menjaga log up-to-date dari semua persyaratan hukum, peraturan dan kontrak yang relevan, dampaknya dan tindakan yang

Kode Proses	Kode Aktivitas	Rancangan Aktivitas Perbaikan di FT UNPAS	Keterangan
			diperlukan. 6. Menjaga mendaftar secara keseluruhan harmonis dan terintegrasi persyaratan kepatuhan eksternal untuk perusahaan.
	MEA3.3.2	Tentukan ketentuan-ketentuan khusus yang sesuai dengan FT UNPAS berdasarkan ketentuan nasiaonal	Perhatikan Landasan hukum yang diperlukan untuk pelaksanaanya.

4.5 Perancangan Alur Proses Monitoring dan Evaluasi

Perancangan alur proses monitoring dan evaluasi bertujuan untuk membuat rancangan alur proses monitoring dan evaluasi terkait kemanan SITU disesuiakan dengan COBIT 5. Adapun rancangan berupa alur yang direfresentasikan dengan diagram *workflow* yang digambarkan secara gelobal seperti yang digambarkan pada gambar .



Gambar 11. Alur Proses Monitoring dan Evlauasi

5 Kesimpulan dan Saran

5.1 Kesimpulan

Dalam penelitian Tugas akhir ini dilakukan identifikasi kondisi tata kelola TI pada proses monitoring dan evaluasi dan penyusunan rancangan rekomendasi serangkaian aktivitas pada proses monitoring dan evaluasi mengacu pada kerangka kerja COBIT 5. Penelitian ini diawali dengan melakukan identifikasi permasalahan dalam tata kelola TI pada proses monitoring dan evaluasi sehingga dapat diperoleh 3 proses dan dipilih 4 *base practice COBIT 5 yang* relevan yang berkaitan dengan kemanan TI. Selanjutnya melakukan identifikasi aktivitas proses monitoring dan evaluasi di FT UNPAS yang mengacu pada aktivitas COBIT 5. Hasil identifikasi menunjukan bahwa bahwa tata kelola teknologi informasi pada proses monitoring dan evaluasi terkait keamanan TI yaitu MEA01 di FT UNPAS yaitu ada beberapa aktivitas yang dilakukan namun belum terdokumentasi, MEA02 di FT UNPAS yaitu belum ada aktivitas yang dilakukan dan MEA03 di FT UNPAS yaitu belum ada aktivitas yang dilakukan. Maka secara umum ada pada proses beberapa yang dilakukan tetapi tidak ada bukti. Kemudian untuk mencapai tata kelola TI yang diharapkan maka perlu adanya suatu rancangan tata kelola TI dalam rangka meningkatkan tata kelolanya. Rancangan yang dibuat berupa rancangan perbaikan aktivitas pada proses monitoring dan evaluasi yang mengacu pada COBIT 5.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan dapat diberikan saran yaitu memperbaiki tata kelola teknologi informasi pada proses monitoring dan evaluasi terkait dengan keamanan SITU dengan memanfaatkan rancanagan perbaikan aktivitas yang disususn oleh penulis.

6 Daftar Pustaka

[1] Adikara Fransiskus., 2013, "*Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan COBIT 5 pada Labolatorium Rekayasa Perangkat Lunak Universitas Esa Unggul*", Universitas Esa Unggul.

[2] Haes, S., Wim, V. G., 2005, "*IT Governance Structures, Processes, and Relational Mechanisme : Achieving IT Business Aligment In Major Belgian Financial group*", Jurnal System Scient.

[3] Hakim, A., Hoga, S., Agus, S., Oktober 2014 , "*Evaluasi Tata Kelola Teknologi Informasi dengan Framework COBIT 5 dikementrian ESDM (Studi Kasus pada PUSDATIN ESDM)*", Journal Of Information, Volume 10, Nomor 2.

[4] ISACA, 2012, "*A Business Framework for the Governance and Management of Interprise IT : Using COBIT 5*" , USA.
[5] ISACA, 2012 "*Enabling Processes*", USA.
[6] ISACA, 2013, "Transforming Cybersecurity: Using COBIT 5", USA.
[7] ITU, 2015, "*Definition Of Cybersecurity*", tersedia : April 2015 http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.
[8] Kadir Abdul., 2014, "*Pengenalan Sistem Informasi Edisi Revisi*", Andi, Yogyakarta.
[9] Kusumaningputri, D. C., Imam, R., Rahmat, M., 2013, "*Penilaian Penetapan Teknologi Informasi Menggunakan Framework COBIT 5 di Institut Teknologi Telkom*", Institut Teknologi Telkom.
[10] OWASP, 2010, "*The Ten Most Crtical Web Application Security Risks*", Creative Commons (CC) Attribution Share-Alike.
[11] PUSDATIN., 2013, "*Grand Design Teknologi Informasi Fakultas Teknik Unpas*", Tidak di Terbitkan, Bandung.
[12] Putra, Risma, Bayu., 2010, Dana, Indra, S., "*Rancangan Tata Kelola TI untuk Institusi Pemerintah Studi Kasus Bappenas*" , Sistem Informasi MTI-UI, Volume 4, Nomor .
[13] Sakam R., Djunaedy., Melia Liyanthy., 2007 , "*Audit sistem informasi akademik Universitas Pasundan Dengan Metode COBIT*",Infomatek, Volume 9, Nomor 2.
[14] Surendro, Kridanto., 2009 , "*Implementasi Tata Kelola Teknologi Informasi*", Informatika Bandung, Bandung.
[15] UNPAS., 2012, "*Rencana Strategis dan Rencana Operasional FT-UNPAS 2012-2016*", Tidak di Terbitkan, Bandung.