

BAB 3

IDENTIFIKASI OBJEK PENELITIAN

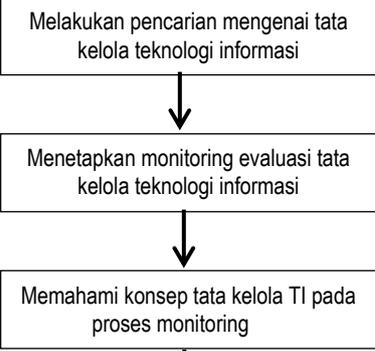
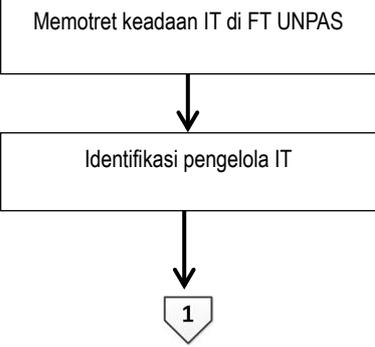
Bab ini menjelaskan mengenai kebutuhan yang berhubungan dengan topik permasalahan yang diangkat, yaitu melakukan identifikasi kondisi tata kelola TI pada saat ini

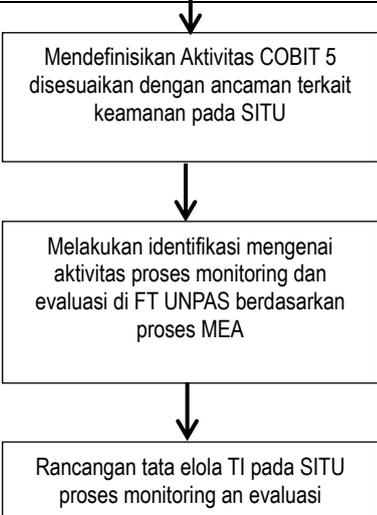
3.1 Kerangka Tugas Akhir

Kerangka Tugas Akhir bertujuan untuk menggambarkan konsep dan pemikiran utama dalam penyelesaian tugas akhir yang dibuat, penyelesaian tugas akhir dilandasi oleh tiga komponen, yaitu:

1. Tahap dan Hasil adalah komponen yang berisi mengenai gambaran yang akan dikerjakan mulai dari tahapan yang dilakukan, hasil yang akan didapatkan berdasarkan tahapan yang dilakukan dan kontribusi untuk tahapan selanjutnya.
2. Langkah Penelitian adalah komponen yang berisi hal-hal yang akan dikerjakan berdasarkan tahapan yang telah dijelaskan sebelumnya.
3. Literatur dan Referensi adalah komponen yang berisi sumber pengetahuan yang dijadikan landasan dalam mengerjakan tugas akhir.

Adapun penjelasan mengenai penyelesaian tugas akhir pada perancangan digambarkan pada gambar 3.1.

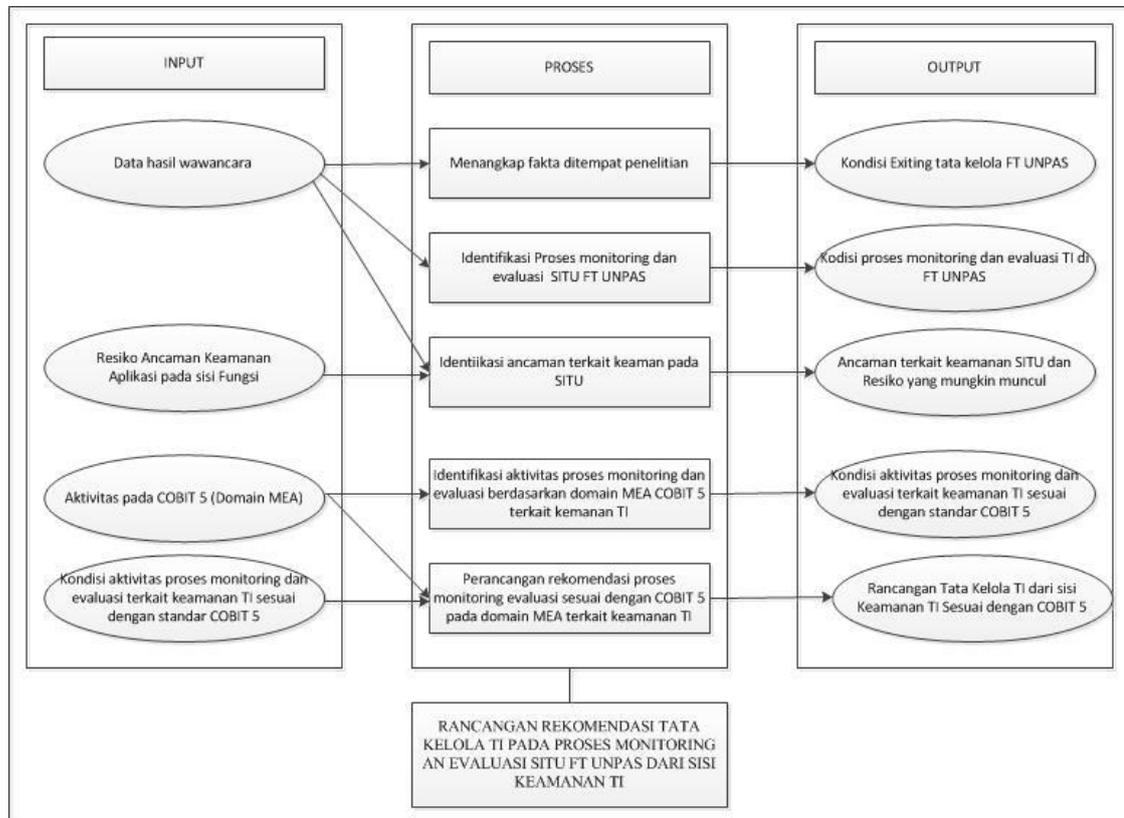
Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
<p>Tahap 1: Pendahuluan (Memahami dan menetapkan konsep tata kelola)</p> <p>Hasil : Konsep tata kelola TI Kontribusi: Pengumpulan Data</p>	 <pre> graph TD A[Melakukan pencarian mengenai tata kelola teknologi informasi] --> B[Menetapkan monitoring evaluasi tata kelola teknologi informasi] B --> C[Memahami konsep tata kelola TI pada proses monitoring] </pre>	<ol style="list-style-type: none"> 1. Tata Kelola[ADI 13] 2. Teknologi Informasi[KAD14] 3. Tata Kelola TI [SUR09] 4. Tata Kelola [ISA12A] 5. Elemen Tata Kelola[HAE05] 6. COBIT[HAK14] 7. <i>Monitoring Evaluate Assess</i>[ISA12B]
<p>Tahap 2: Pengumpulan Data (memotret keadaan tata kelola TI di FT UNPAS)</p>	 <pre> graph TD D[Memotret keadaan IT di FT UNPAS] --> E[Identifikasi pengelola IT] E --> F{1} </pre>	<ol style="list-style-type: none"> 8. Hasil Wawancara 9. Mengenai PUSDATIN[PUS13] 10. Proses MEA[ISA13] 11. Risiko keamanan aplikasi WEB [OWA10] 12. Permasalahan Insitut [PUT10]

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
<p>Hasil : Informasi mengenai gambaran umum TI Kontribusi: Perancangan Tata Kelola TI</p>	 <pre> graph TD 1[1] --> A[Menentukan proses MEA yang akan dipilih berdasarkan masalah] </pre>	
<p>Tahap 3: Perancangan Tata Kelola TI</p> <p>Hasil : Rancangan tata kelola TI proses monitoring dan evaluasi Kontribusi: Kesimpulan TA</p>	 <pre> graph TD B[Mendefinisikan Aktivitas COBIT 5 disesuaikan dengan ancaman terkait keamanan pada SITU] --> C[Melakukan identifikasi mengenai aktivitas proses monitoring dan evaluasi di FT UNPAS berdasarkan proses MEA] C --> D[Rancangan tata elola TI pada SITU proses monitoring an evaluasi] </pre>	<p>13. Risiko keamanan aplikasi WEB [OWA10] 14. Aktivitas yang ada pada Domain MEA COBIT 5 [ISA12B] 15. Proses MEA[ISA13] 16. Berdasarkan hasil wawancara dengan pengelola TI</p>
<p>Tahap 6: Kesimpulan TA (Penetapan Kesimpulan Akhir)</p> <p>Hasil : Kesimpulan dan Hasil TA, Rekomendasi Prosepek TA Kontribusi: -</p>	 <pre> graph TD E[Kesimpulan TA dan Temuan-temuan] --> F[Prospek dan rekomedasi TA] </pre>	

Gambar 3.1. Kerangka Tugas Akhir

3.2 Skema Analisis

Skema analisis bertujuan untuk membantu memudahkan dan memahami bagaimana alur dari analisis yang dilakukan untuk melakukan perancangan rekomendasi tata kelola TI dari sisi ancaman terkait keamanan pada SITU di FT UNPAS. Analisis meliputi input, proses dan output yang ditunjukkan pada gambar 3.2.



Gambar 3.2. Skema Analisis

Deskripsi lengkap mengenai langkah-langkah analisis yang digambarkan pada Gambar 3.2 diuraikan pada tabel 3.1.

Tabel 3.1. Deskripsi Skema Analisis

No.	Langkah Analisis	Objek Analisis	Hasil Analisis	Maksud Analisis
1.	Menangkap fakta ditempat penelitian	Data hasil wawancara Tata kelola TI FT UNPAS	Kondisi existing tata kelola TI	Memahami bagaimana pengelolaan SITU FT UNPAS sehingga dapat memilih proses yang akan digunakan untuk penelitian.
2.	Identifikasi proses monitoring dan evaluasi SITU FT UNPAS	Data hasil wawancara	Kondisi proses monitoring dan evaluasi TI di FT UNPAS	Memahami bagaimana alur proses monitoring dan evaluasi SITU FT UNPAS pada saat ini.
3.	Identifikasi ancaman terkait keamanan pada SITU	Risiko Ancaman Keamanan Aplikasi pada sisi Fungsi	Ancaman terkait keamanan SITU dan Risiko yang mungkin muncul	Mengetahui masalah yang pernah terjadi yang diakibatkan dari ancaman keamanan SITU dan mengetahui risiko yang mungkin terjadi terhadap keamanan SITU.
4.	Identifikasi aktivitas proses monitoring dan evaluasi berdasarkan domain MEA COBIT 5 terkait keamanan TI	Aktivitas pada COBIT 5 (Domain MEA)	Kondisi aktivitas proses monitoring dan evaluasi terkait keamanan TI sesuai dengan standar COBIT 5	Mengetahui kondisi aktivitas proses monitoring dan evaluasi dimana aktivitas yang diidentifikasi disesuaikan dengan aktivitas yang ada pada domain MEA terkait keamanan TI.

No.	Langkah Analisis	Objek Analisis	Hasil Analisis	Maksud Analisis
5.	Perancangan rekomendasi proses monitoring evaluasi sesuai dengan COBIT 5 pada domain MEA terkait keamanan TI	<ol style="list-style-type: none"> 1. Aktivitas pada COBIT 5 (Domain MEA) 2. Kondisi aktivitas proses monitoring dan evaluasi terkait keamanan TI sesuai dengan standar COBIT 5 	Rancangan Tata Kelola TI dari sisi Keamanan TI Sesuai dengan COBIT 5	Membuat rancangan rekomendasi tata kelola SITU pada proses monitoring dan evaluasi terkait kaeamanan SITU, rancangan berupa rancangan perbaikan aktivitas proses monitoring dan evaluasi.

3.3 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.

3.4 Profil Institut

Fakultas Teknik UNPAS merupakan oragnisasi penyelenggara pendidikan dimana mempunyai visi, misi dan tujuan untuk mendukung berjalannya proses bisnis.

3.4.1 Visi dan Misi

Adapun Visi dan Misi FT UNPAS yang tertera pada RENSTRA RENOP 2012-2016[UNP12] yaitu:

Visi

Visi Fakultas Teknik adalah menjadi penyelenggara pendidikan tinggi teknik terkemuka menuju komunitas akademik peringkat internasional yang mengusung nilai kesundaan dan keislaman ditahun 2021.

Misi

Menyelenggarakan pendidikan tinggi teknik yang berkualitas dalam melaksanakan Tridharma Perguruan Tinggi, berkontribusi dalam pembangunan serta mengusung nilai Kesundaan dan Keislaman.

3.4.2 Tujuan Institut

Berdasarkan visi dan misi maka tujuan dimasa mendatang tujuan FT UNPAS yang tertera pada RENSTRA RENOP 2012-2016[UNP12] yaitu:

1. Menjadi fakultas yang mandiri dan bertatakelola baik (*Good Faculty Governance*)
2. Menghasilkan lulusan yang:
 - a. Bertaqwa kepada Allah SWT, berkontribusi dalam peningkatan mutu kehidupan bermasyarakat berdasarkan pancasila, menunjang tinggi nilai kemanusiaan, memiliki kepekaan sosial terhadap masyarakat dan menunjukkan sikap bertanggungjawab terhadap pekerjaan pada bidang keahliannya secara mandiri.

- b. Tanggap terhadap kemajuan ilmu teknologi serta dinamika perubahan sosial dan masyarakat, khususnya yang berkaitan dengan bidang keahliannya.
 - c. Menguasai dasar-dasar ilmiah serta pengetahuan metodologi sehingga mampu menemukan, memahami, menjelaskan dan merumuskan penyelesaian masalah yang ada didalam kawasan keahliannya.
3. Menghasilkan penelitian yang dapat memperkaya khasanah keilmuan dengan menemukan konsep, model, dan pradigma baru dibidang teknik yang berbasis pada moral dan etika dalam rangka memecahkan masalah dimasyarakat.
 4. Mejadi fakultas yang mengedepankan kesejahteraan dengan mengembangkan professional.

3.4.3 Tujuan Spesifik Institut

Adapun tujuan spesifik FT UNPAS yang tercantum pada RENSTRA RENOP 2012-2016 FT UNAPAS[UNP12] yaitu:

1. Meningkatkan pengalaman nilai-nilai luhur agama islam dan kesundaan untuk mendukung pengembangan Insan Fakultas Teknik yang memiliki keunggulan dalam IPTEKS, religius dan berbudi luhur serta berbunya (luhung elmuna, pengkuh agamana, jembar budayana).
2. Meningkatkan citra Fakultas Teknik baik sekala nasional maupun dikawasan global.
3. Meningkatkan mutu penyelenggaraan proses pembelajaran untuk mendukung pencapaian kompetensi lulusan yang sesuai dengan tuntutan segenap pemangku kepentingan.
4. Meningkatkan kuantitas dan kualitas penelitian serta karya ilmiah untuk mendukung pengembangan IPTEKS serta berkontribusi dalam penyelesaian masalah-masalah nasional.
5. Meningkatkan mutu lembaga kemahasiswaan untuk mendukung pengembangan kreativitas dan prestasi mahasiswa sesuai minat dan bakatnya.
6. Meningkatkan sistem pengelolaan sumber daya manusia untuk mendukung penyelenggaraan pendidikan, penelitian dan pengabdian kepada masyarakat yang bermutu.
7. Meningkatkan jejaring kerjasama dalam dan luar negri.

3.5 Gambaran Umum TI di FT UNPAS

Gambaran umum TI FT UNPAS menjelaskan mengenai satuan kerja pengelola TI, program strategi TI serta Layanan TI

3.5.1 Satuan Kerja Pengelola TI

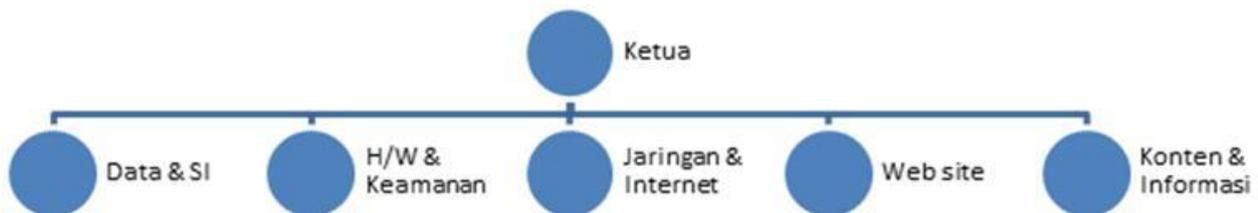
FT Unpas telah menetapkan optimalisasi penggunaan TIK dalam mendukung operasional sehari-hari ke dalam salah satu rencana strategis fakultas. Hal ini harus dibarengi organisasi yang bertanggung jawab terhadap Pengelolaan TI, adapun Pengelola TI dilingkungan FT UNPAS yaitu Pusat Data dan Teknologi Informasi (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 3.3 :



Gambar 3.3. Struktur Organisasi PUSDATIN[PUS13]

Deskripsi tugas dari tiap-tiap bagian yang ada pada Gambar 3.3 Struktur Organisasi PUSDATIN ditunjukkan pada Tabel 3.2.

Tabel 3.2.Deskripsi Tugas Struktur Organisasi PUSDATIN

No.	Bagian	Tugas
1.	Ketua PUSDATIN	<ol style="list-style-type: none"> 1. Menjamin seluruh perencanaan, realisasi, operasional dan perawatan TIK sejalan dengan visi dan misi FT Unpas. 2. Berkordinasi dengan komite TIK untuk menjamin perencanaan, realisasi, operasional, dan perawatan TIK sesuai dengan kebutuhan seluruh unit kerja yang dilayani.
3.	Data dan Sistem Informasi	<ol style="list-style-type: none"> 1. Membantu tugas Ketua PUSDATIN. 2. Menjalankan tugas dengan berpihak kepada kebijakan dan rencana yang telah dirumuskan. 3. Bertanggung jawab terhadap realisasi, operasional, dan perawatan Sistem informasi akademik dan sistem informasi dilingkungan FT UNPAS.
4.	Hardware dan Keamanan	<ol style="list-style-type: none"> 1. Menyusun rencana pengembangan hardware sesuai kebutuhan PUSDATIN. 2. Memberikan rekomendasi spesifikasi dan harga hardware yang diajukan seluruh unit kepada pimpinan FT UNPAS. 3. Bersama-sama pimpinan FT UNPAS dan pengelola TIK melalui unit yang ditunjuk untuk melakukan negosiasi harga hardware yang akan dibeli. 4. Melakukan perawatan hardware dan sistem operasi komputer dan multimedia di lingkungan FT UNPAS. 5. Menjamin keamanan layanan TI di FT UNPAS dalam rangka menjaga integritas dari

No.	Bagian	Tugas
		informasi dan melindungi aset TI.
6.	Jaringan dan Internet	<ol style="list-style-type: none"> 1. Menyusun rencana pengembangan sistem jaringan di lingkungan FT UNPAS. 2. Mengendalikan langsung operasionalisasi sistem jaringan di lingkungan FT UNPAS dan seluruh unit yang ada, yaitu: intranet, internet dan hotspot. 3. Menata dan merawat sistem cabling dan switching. 4. Mengelola bandwidth, routing dan firewall.
5.	Website	Mengembangkan dan mengelola website FT UNPAS sebagai sarana penyebar informasi bagi khalayak umum.
6.	Konten dan Informasi	<ol style="list-style-type: none"> 1. Mengawasi penyampaian informasi. 2. Mengawasi konten dari informasi.

(Sumber : Hasil wawancara pada tanggal 23 April 2015 pada Tabel B.2 Lampiran B)

3.5.2 Strategi

Adapun strategis pengelolaan TI yang tercantum dalam Buku Design Teknologi Informasi Fakultas Teknik Unpas[PUS13] yaitu:

1. Menggunakan kombinasi teknologi dengan platform terbuka (*open source*) maupun *proprietary*.
2. Memanfaatkan sumber daya informasi dengan kerjasama lembaga lain baik setingkat fakultas maupun universitas (SPTIK) sehingga tidak terjadi duplikasi pekerjaan atau data.
3. Mengembangkan *IT leadership* di lingkungan Fakultas Teknik.
4. Mengadakan pendidikan dan pelatihan TI untuk memberdayakan sumber daya manusia di Fakultas Teknik.

3.5.3 Program Strategis Pengelolaan TI

Adapun program strategis pengelolaan TI yang tercantum dalam Buku Design Teknologi Informasi Fakultas Teknik Unpas[PUS13] yaitu:

1. Mengembangkan rancangan arsitektur sistem informasi pendukung administrasi Fakultas Teknik berbasis jaringan dengan struktur modular sehingga dapat diimplementasikan secara bertahap secara bottom-up sesuai dengan jadwal ketersediaan sumber daya.
2. Mengembangkan kerangka acuan (*framework*), yang menjadi standar, serta norma-norma petunjuk (*guidelines*) untuk pengembangan sistem otomasi penyelenggaraan akademik yang dapat menjadi sumber data untuk kebutuhan pelaporan internal maupun eksternal.
3. Melengkapi peralatan teknologi yang dibutuhkan Fakultas Teknik maupun unit kerja dan personil.
4. Membangun sistem teknologi informasi yang sesuai kebutuhan *stakeholder* Fakultas Teknik.

3.5.4 Layanan TI

Pada saat ini Fakultas Teknik Unpas telah menyadari kebutuhan akan Tekonlogi Informasi dan Komunikasi (TIK). Dari sisi strategis, FT Unpas telah menetapkan optimalisasi penggunaan TIK dalam mendukung operasional sehari-hari ke dalam salah satu rencana strategis fakultas. Hal ini terealisasi dengan adanya layanan TI pada lingkungan FT UNPAS. Adapun layanan TI yang digunakan salah satunya adalah SITU, yang dimana menjadi objek penelitian pada tugas akhir ini.

3.6 Keamanan Teknologi Informasi

Berdasarkan Sistem yang akan dikembangkan di Fakultas Teknik Unpas merupakan sistem yang beberapa diantaranya memiliki 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 keamanan yang diterapkan pada SITU pada penelitian ini fokuskan pada *application Security* berdasarkan sisi Fungsi.

3.7 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.

3.7.1 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*.

3.7.2 SITU Sebagai Teknologi Informasi

Definisi yang telah diuraikan mengenai teknologi informasi pada bab 2 sub 2.2 dapat disimpulkan bahwa SITU sebagai teknologi informasi adalah suatu teknologi yang berhubungan dengan pengolahan data yang meliputi data dari mahasiswa, dosen, jadwal kuliah menjadi informasi yang diperlukan oleh pengguna teknologi yaitu civitas akademik dan proses penyaluran data menjadi informasi dan proses penyaluran data/ informasi tersebut dalam batas-batas ruang dan waktu seperti halnya jadwal perkuliahan.

3.7.3 Strategi Bisnis SITU

Peran SITU terhadap aktivitas FT UNPAS dibagi menjadi dua bagian yaitu aktivitas utama dan pendukung, adapun peran SITU terhadap aktivitas FT UNPAS yang telah dijelaskan pada bab 3 sub bab 3.7.1 salah satu tujuan penggunaan SITU yaitu Mengintegrasikan data dari fakta operasional mengenai akademik, SDM, Sarana dan Prasarana, serta keuangan. Berikut dijelaskan pada tabel 3.3.

Tabel 3.3. Peran SITU Terhadap Aktivitas Bisnis

No	Aktivitas Bisnis	Sistem / Aplikasi	Deskripsi	Status	Keterlibatan Aplikasi
1.	Akademik	Sistem Informasi Akademik	Sistem Informasi Akademik merupakan sistem informasi tingkat operasional yang mendukung kegiatan operasional bidang akademik dengan merekam aktivitas dan transaksi paling dasar dari kegiatan akademik	Sudah berjalan	<ul style="list-style-type: none"> – Pengelolaam data master – Manajemen program – Manajemen kurikulum – Integrasi – Perwalian – Penanganan mahasiswa pindahan – Penjadwalan dan penugasan dosen – Pengelolaan SAP – Monitoring PBM – Evaluasi PBM – Pengelolaan ujian – Pengelolaan nilai – Pengelolaanm Tugas Akhir – Pengelolaan kelulusan – Tracing wisuda – Tracing Alumni – Pencetakan kartu ujian
2.	Sumber Daya Manusia	Sistem Informasi Sumber Daya Manusia	Sistem Informasi Sumber Daya Manusia merupakan sistem informasi tingkat operasional yang mendukung kegiatan operasional bidang kepegawaian dengan merekam aktivitas dan transaksi paling dasar dari kegiatan kepegawaian	Belum di implementasikan	<ul style="list-style-type: none"> – Pengelolaan data master pegawai – Pengelolaan kenaikan gaji berkala – Pengelolaan transaksi pegawai – Pengelolaan transaksi khusus dosen
3.	Keuangan	Sistem Informasi Keuangan	Sistem Informasi Keuangan merupakan sistem informasi tingkat operasional yang mendukung kegiatan operasional bidang keuangan dengan merekam aktivitas dan transaksi paling dasar dari kegiatan keuangan	Sudah berjalan	<ul style="list-style-type: none"> – Pengeloalaan master biaya dan potongan – Pengelolaan penerimaan pembayaran DP dan DPP dari mahasiswa – Pencatatan pencarian DP dan DPP mahasiswa

No	Aktivitas Bisnis	Sistem / Aplikasi	Deskripsi	Status	Keterlibatan Aplikasi
4.	Sarana dan Prasarana	Sistem Informasi Sarana dan Prasarana	Sistem Informasi Sarana dan Prasarana merupakan Sistem Pengelolaan dan memberikan informasi tentang inventory dan pemanfaatan aset dan fasilitas lingkungan FT UNPAS	Belum di implementasikan	– Pengelolaan Investasi sarana prasarana

(Sumber : Hasil wawancara tanggal 22 oktober 2014 pada Tabel B.3 Lampiran B)

Dari tabel diatas terlihat keterlibatan aktivitas FT UNPAS dengan SITU, terlihat SITU memberikan kontribusi untuk mengelola fitur aktivitas secara sistem terlihat dari fitur yang ada pada SITU pada setiap sub sistemnya. Adapun berdasarkan hasil wawancara kepada pihak pengelola TI yang optimal digunakan adalah SITU Akademik sedangkan SITU keuangan sudah mulai digunakan dan untuk SITU SDM dan sarana dan prasarana sudah ada namun belum dijalankan.

3.7.4 Identifikasi Kondisi Sumber Daya SITU

Identifikasi kondisi sumber daya SITU disesuaikan dengan *resource* yang ada pada COBIT . Berdasarkan hasil observasi dan wawancara pihak terkait kondisi sumber daya SITU dijelaskan pada pada tabel 3.4.

Tabel 3.4. Kondisi Sumber Daya TI

No	Sumber Daya TI	Kondisi
1.	Manusia, keterampilan dan Kompetensi	<ol style="list-style-type: none"> 1. Belum adanya pelatihan bagi pengguna TI. 2. Belum terdefinisinya atau terdokumentasinya struktur pengelola TI sehingga Akibatnya layanan diberikan dengan penugasan ad hoc sehingga tidak ada penjaminan kualitas layanan secara terstruktur dan berkesinambungan. 3. FT UNPAS memiliki banyak potensi SDM yang memiliki pemahaman TIK dengan baik.
2.	Informasi	<ol style="list-style-type: none"> 1. Informasi sesuai dengan kebutuhan pengguna. 2. Isi informasi SITU kadang sering tidak terupdate
3.	Layanan, Infrastruktur dan Aplikasi	<ol style="list-style-type: none"> 1. Belum adanya kebijakan atau panduan khusus untuk layanan TIK. 2. Tidak ada tim khusus yang diberi tugas merumuskan Layanan TIK ad hoc. Akibatnya layanan diberikan dengan penugasan ad hoc sehingga tidak ada penjaminan kualitas layanan secara terstruktur dan berkesinambungan. 3. Bentuk-bentuk layanan ad hoc kurang terdokumentasikan dengan baik. Akibatnya setiap kali ada permintaan baik yang sifatnya baru maupun serupa dengan layanan yang pernah diberikan sebelumnya selalu dilayani tanpa acuan. 4. SITU FT UNPAS masih terus dikembangkan dan masing-masing bagian dituntut untuk melakukan penyesuaian dengan cepat agar integrasi seluruh data semakin cepat terwujud.

3.8 Permasalahan yang Terjadi di FT UNPAS

Permasalahan yang terjadi di FT UNPAS menjadi masukan untuk dibuatnya suatu rancangan pada penyelesaian tugas akhir ini, adapun faktornya tidak ada pengelolaan risiko dan belum adanya dokumen ceklis.

1. Tidak Ada Pengelolaan Risiko

Pengelolaan risiko harusnya menjadi suatu perhatian bagi FT UNPAS, ketika terjadi permasalahan dapat diatasi dengan baik. sehingga tingkat risiko seperti *hacker*, kerusakan tidak terduga dapat diminimalkan.

2. Belum adanya proses *ceklis* monitoring kegiatan teknologi informasi

Belum adanya bukti *checklist* TI yang dapat memberikan nilai bagi FT UNPAS, sehingga hal ini menjadi suatu permasalahan yang menyebabkan tata kelola TI pada FT UNPAS belum dapat diukur sudah sejauh mana tata kelola TI telah dilakukan.

Permasalahan yang terjadi pada FT UNPAS dijelaskan pada gambar dengan mengadopsi dari peneliti sebelumnya yaitu Risma Bayu[PUT10] terlihat pada gambar 3.4.



Gambar 3.4. Permasalahan FT UNPAS

3.9 Masalah SITU

Permasalahan SITU menjadi hal yang perlu diperhatikan, jika terjadi permasalahan terhadap SITU maka mungkin membuat proses bisnis yang ada akan terganggu sehingga akan mengurangi kenyamanan kepada penggunanya. Adapun beberapa permasalahan yang pernah dialami SITU dan solusi yang ditawarkan oleh pengelola untuk menjaga ketersediaan SITU berdasarkan hasil wawancara yaitu diuraikan pada tabel 3.5:

Tabel 3.5. Permasalahan SITU

No	Permasalahan	Solusi
1.	Load tinggi melakukan <i>checking</i> terus menerus sehingga menyebabkan korup database.	Dilakukan pengembangan terhadap SITU, dan perbaikan algoritma aplikasi agar tidak melakukan <i>checking</i> terus menerus saat melakukan transaksi.
2.	Sering terjadinya mati listrik dan hal ini diperburuk karena belum adanya ketersediaan genset sehingga hardisk menjadi crash dan layanan SITU sendiri menjadi terhambat.	Dilakukan Upgrading dan Backup
3.	Performa server menurun dikarenakan pengguna semakin banyak permasalahan ini sangat terlihat jelas pada saat pada masa perwalian mahasiswa.	Upgrading
4.	Banyaknya intruder, intruder adalah orang yang menyusup ke dalam suatu system ,Intruder (atau lebih dikenal dengan cracker, hacker, carder dan lain sebagainya), intruder bermaksud untuk menyusup terhadap SITU maupun untuk mengakses dan kemungkinan besar berniat untuk mengubah dan menghapus data penting.	Dialkukan pengembangan terhadap SITU terutama pada sisi kewanaman
5.	Permasalahan dengan ISP	Mengkomunikasikan kepada pihak ISP untuk melakukan perbaikan sehingga konektivitas dapat terjaga.

(Sumber: Hasil wawancara pada tanggal 22 Oktober 2014 pada Tabel B.1 Lampiran B)

3.10 Identifikasi Masalah Ancaman Keamanan SITU

Identifikasi ancaman keamanan SITU bertujuan untuk memunculkan masalah yang pernah terjadi pada SITU dan sekaligus mendefinisikan risiko yang mungkin terjadi pada ancaman keamanan pada SITU. Adapun yang ancaman keaman pada SITU yang diuraikan berdasarkan pada kewanaman pada sisi fungsi. Masalah yang pernah terjadi pada SITU FT UNPAS diuraikan pada tabel 3.6.

Tabel 3.6 Masalah terhadap ancaman terkait keamanan pada SITU

No	Masalah	Deskripsi	Penyebab
1.	Pengubahan nilai	Perubahan nilai dilakukan oleh mahasiswa/ penyerang dengan kepezingan untuk mengubah nilai yang awalnya kurang memuaskan menjadi nilai yang diharapkan oleh mahasiswa/ penyerang tersebut, jika masalah ini tidak segera diselesaikan mungkin akan terjadi dampak yang lebih serius yaitu mengubah nilai dan matakulia dapat dikatakan lulus walaupun belum mengambil mata kuliah bersangkutan.	Penyebab dari perubahan nilai yang telah ditelusuri oleh pengelola yaitu kegagalan untuk membatasi Akses URL, karena mahasiswa/ penyerang tidak berhak melakukan perubahan nilai, yang seharusnya dilakukan oleh pihak administrasi nilai. Mungkin hal ini juga disebabkan oleh scripting yang kurang baik.
2.	Pencetakan kartu ujian dengan status belum membayar uang administrasi 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 dari perubahan status yang telah ditelusuri oleh pengelola yaitu kegagalan untuk membatasi Akses URL, karena seharusnya pencetakan kartu nilai harus dengan status sudah melakukan administrasi.
3.	Penghapusan data	Pernah terjadinya penghapusan data pada SITU, sehingga dampaknya mengganggu kegiatan administrasi SITU.	Kegagalan untuk membatasi Akses URL, sehingga penyerang dapat melakukan penghapusan data tanpa hak akses.

(Sumber: Hasil wawancara pada tanggal 09 Juni 2015)

Risiko ancaman terkait keamanan yang mungkin terjadi pada SITU FT UNPAS perlu diuraikan untuk mengetahui dampak dari risiko itu sendiri. Adapun risiko yang diuraikan berdasarkan *The Ten Most Critical Web Application Security Risks*[OWA10] dengan dampak yang disesuaikan dengan FT UNPAS, risiko diuraikan pada tabel 3.7.

Tabel 3.7. Risiko yang mungkin terjadi

No	Risiko	Dampak Teknikal
1.	SQL Injeksi	Injeksi dapat menyebabkan hilang atau rusaknya data yang penting pada SITU sehingga terganggunya layanan pemberian informasi. Sehingga hal ini dapat mengurangi akuntabilitas, atau penolakan akses.
2.	Cross-site scripting	Penyerang dapat mengeksekusi <i>script</i> dalam browser dari pengguna SITU dengan tujuan untuk membajak sesi pengguna, mengubah situs, memasukan konten berbahaya, mengerahkan pengguna, membajak <i>browser</i> pengguna menggunakan <i>malware</i> , dsb.
3.	Otentikasi dan pengelolaan Sesi yang Buruk	Otentikasi dan pengelolaan sesi yang buruk memungkinkan beberapa atau bahkan semua akun pengguna SITU diserang. Setelah berhasil, penyerang dapat melakukan segala hal yang dapat dilakukan oleh pengguna TI yang diserang. Akun yang memiliki hak istimewa seringkali menjadi target seperti administrasi, pengelola TI, terutama master pengelola.
4.	Referensi objek langsung yang tidak aman	Referensi objek langsung yang tidak aman hal ini dapat mengkompromikan seluruh data yang dapat diacu oleh parameter yang ada di SITU. Sehingga penyerang dapat mengakses seluruh data.
5.	Cross-site request Forgery	Penyerang dapat menyebabkan pengguna SITU merubah sembarang data yang

No	Reiko	Dampak Teknikal
		dibolehkan atau melakukan tindakan yang terorisasi untuk pengguna.
6.	Kesalahan konfigurasi Kemanan	Kesalahan konfigurasi kemanan ini dapat menyebabkan penyerang mudah untuk mencari celah keamanan yang nantinya akan berakibat pada akses ke data atau fungsionalitas pada SITU, jadi dapat dikatakan berakibat penyalahgunaan data secara utuh oleh penyerang.
7.	Penyimpanan kriptografi yang tidak aman	Penyimpanan kriptografi yang tidak aman sehingga hal ini menyebabkan data rahasia terenkripsi oleh pihak penyerang.
8.	Kegagalan membatasi akses URL	Kegagalan membatasi akses URL memungkinkan penyerang mengakses fungsionalitas yang tidak terorisasi. dan yang menjadi target adalah Fungsi-fungsi administrative seperti pada permasalahan yang telah diuraikan pada tabel 3.5.
9.	Perlindungan yang tidak cukup pada layer transfort	Perlindungan yang tidak cukup pada layer transfort sehingga dapat mengekspos data pengguna perorangan dan dapat mengarah pada pencurian akun SITU. Sehingga seluruh situs dapat terekspos. Setup SSL yang buruk juga dapat memfasilitasi serangan <i>phising</i> .
10.	Ridect dan forward yang tidak divalidasi	Ridect dan forward yang tidak divalidasi hal ini dapat menyebabkan penyerang berusaha menginstalasi <i>malware</i> atau mengalabui pengguna SITU untuk menyingkap <i>password</i> atau informasi sensitive lainnya.

3.11 Identifikasi Proses Monitoring dan Evaluasi di FT UNPAS

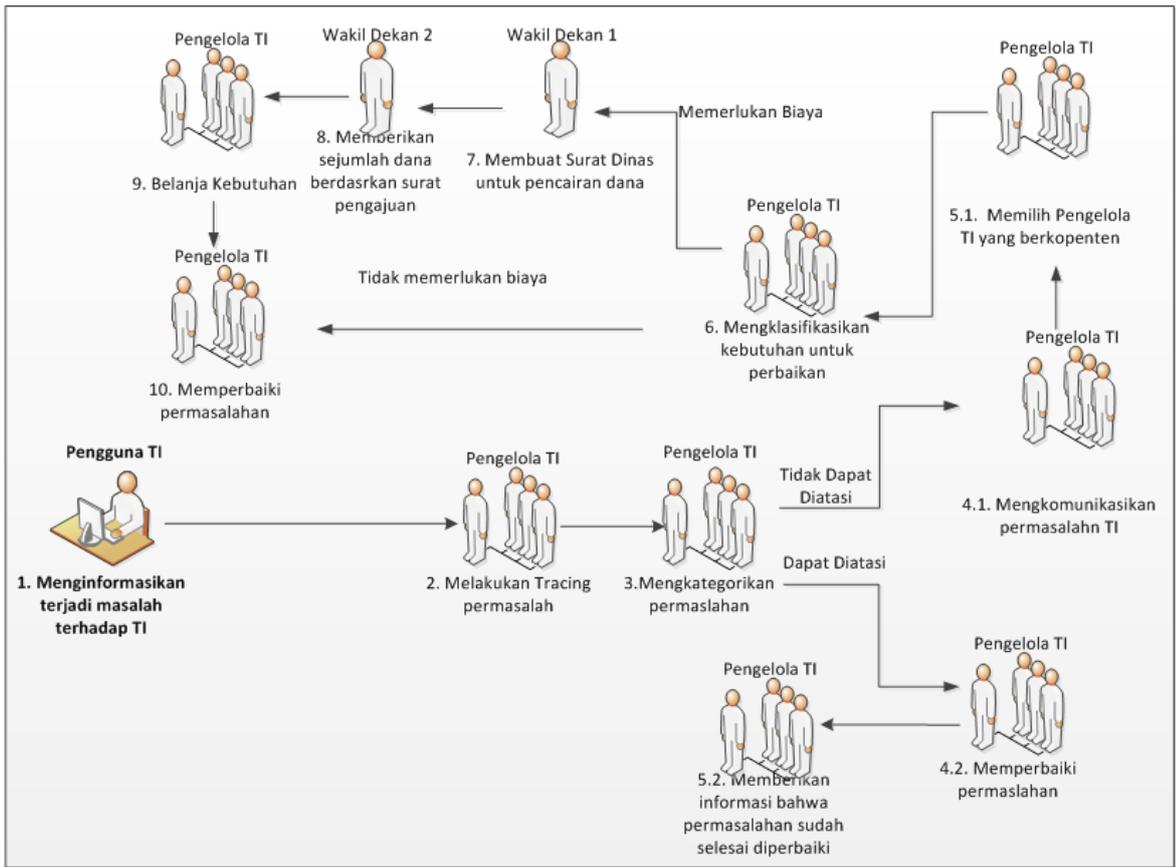
Pada dasarnya proses monitoring dan evaluasi atau disebut pengawasan yang dilakukan di FT UNPAS yaitu berdasarkan terbentuknya peraturan pemerintahan Nomor 19 tahun 2005 tentang standar Nasional Pendidikan (SNP) telah memberikan arahan tentang pentingnya peningkatan mutu yang berkelanjutan yang saat ini dinamakan Satuan Penjamin Mutu Internal (SPMI). Dimana hal ini penjaminan mutu setidaknya meliputi semua proses dalam pendidikan. Berjalannya proses ini yaitu berlandaskan Tim Pengembangan SPMI-PT, “Sistem Penjamin Mutu Internal Perguruan Tinggi” Bahan Pelatihan, Dirjen Dikti 2010.

Lingkup Universitas mendefinisikan standar Satuan Pengawas Internal (SPI) sebagai pengawas standar. Periode pengawasan dilakukan tahunan atau satu tahun sekali. Berdasarkan hasil wawancara kepada ketua SPI yang menjadikan syarat pengawasan adalah suatu standar yang dibentuk oleh SPMI dan pihak yang bertanggung jawab untuk memenuhi isi standar. Adapun pihak yang bertanggung jawab yaitu:

1. Rektor sebagai pimpinan universitas
2. Dekan sebagai pimpinan fakultas
3. Ketua program studi sebagai pimpinan program studi

3.12 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 direpresntasikan dengan diagram *workflow* seperti pada yang terlihat pada gambar 3.5.



Gambar 3.5. Alur Proses Evaluasi TI

(Sumber: Hasil wawancara pada tanggal 22 Oktober 2014 pertanyaan 3 Lampiran B-3)

3.13 Identifikasi Aktivitas Proses Monitoring dan Evaluasi dan Penilaian

Identifikasi aktivitas proses monitoring dan evaluasi dan penilaian 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 tabel 3.8.

Tabel 3.8. Identifikasi Aktivitas

No	Kode	Proses	Aktivitas	Eksistensi		Keterangan
				Ada	Tidak Ada	
1.	MEA01.03	Mengumpulkan kinerja proses dan kesesuaian data	Menetapkan <i>requirement</i> monitoring, indikator, pengumpulan data dan metode pengumpulan untuk monitoring keamanan TI;	✓		Setiap <i>requirement</i> monitoring, indikator, pengumpulan data dan metode pengumpulan untuk monitoring keamanan TI dilakukan namun hal ini tidak dibarengi dengan dokumentasi, aktivitas ini dilakukan dengan pola dan pengetahuan dari pengelola TI.
			Menentukan metode analisis yang tepat.		✓	Tidak ada metode analisis terhadap kinerja dan proses kesesuaian data terkait dengan keamanan TI.
2.	MEA01.05	Memastikan pelaksanaan	Menentukan tindakan korektif yang berkaitan dengan serangan/	✓		Setiap terjadi serangan/ pelanggaran/ insiden ada tindakan

No	Kode	Proses	Aktivitas	Eksistensi		Keterangan
				Ada	Tidak Ada	
		tindakan korektif	pelanggaran/ insiden			yang dilakukan oleh pengelola namun tidak didokumentasikan
			Menanamkan tindakan korektif dan perencanaan terkait dalam keamanan TI.	✓		Adanya upaya untuk tindakan korektif terjadi serangan/ pelanggaran/ insiden dan perencanaan terkait dalam keamanan TI keseluruhan namun tidak didokumentasikan.
3.	MEA02.04	Mengidentifikasi dan melaporkan kekurangan kontrol	Mengidentifikasi kelemahan kontrol keamanan TI dari perspektif berbasis risiko.		✓	Tidak dilakukannya identifikasi kelemahan kontrol keamanan dari perspektif berbasis risiko, pada saat ini risiko terlihat berdasarkan permasalahan yang muncul.
			Menyoroti adanya efek yang mengalir dalam dinamika sistem		✓	Tidak adanya aktivitas yang melakukan pendefinisian mengenai efek yang akan terjadi dalam sistem yang berjalan saat ini.
4.	MEA03.01	Mengidentifikasi <i>requirement</i> kepatuhan eksternal	Mengidentifikasi hukum atau peraturan yang berdampak terhadap keamanan TI.		✓	Tidak adanya identifikasi hukum atau peraturan yang berdampak terhadap keamanan TI, yang terjadi pada saat ini ketika terjadi masalah terkait ancaman keamanan tidak ditindak lanjuti.
			Termasuk ketentuan-ketentuan khusus di bawah hak prerogatif keamanan nasional.		✓	Tidak adanya ketentuan-ketentuan khusus di bawah hak prerogatif keamanan nasional. Sehingga pada saat ini untuk pelaku yang melakukan serangan terhadap SITU tidak ditindak lanjuti.