BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang identifikasi kendali dan memperkirakan resiko, mengumpulkan bukti, mengevaluasi temuan, sampai dengan membuat rekomendasi audit sistem informasi.

4.1 Evaluasi Hasil Pengujian & Laporan Audit

Mengidentifikasi kendali dan memperkirakan resiko, mengumpulkan bukti, memaparkan temuan-temuan hasil audit yang dibagi menurut masing-masing domain menurut audit framework yang digunakan. Penilaian yang dilakukan dihasilkan dari wawancara dengan pihak-pihak yang berkepentingan. Pihak-pihak yang berkepentingan tersebut telah ditentukan pada RACI *Chart*. RACI *Chart* menjelaskan siapa yang Bertanggung Jawab (*Responsible*), *Accountable*, *Consulted* dan/atau *Informed*.

Audit dengan COBIT

COBIT adalah standar pengendalian yang umum terhadap teknologi informasi, dengan memberikan kerangka kerja dan pengendalian terhadap teknologi informasi yang dapat diterapkan dan diterima secara internasional. Selain itu, COBIT dipilih karena dikembangkan dengan memperhatikan keterkaitan tujuan bisnis dengan tidak melupakan fokusnya pada teknologi informasi. Kerangka kerja COBIT bersifat umum, oleh sebab itu harus disesuaikan dengan melihat proses bisnis dan tanggung jawab proses teknologi informasi terhadap aktivitas perguruan tinggi. Keberadaan COBIT dapat dipakai sebagai metode dalam proses audit sistem informasi. Dalam proses audit

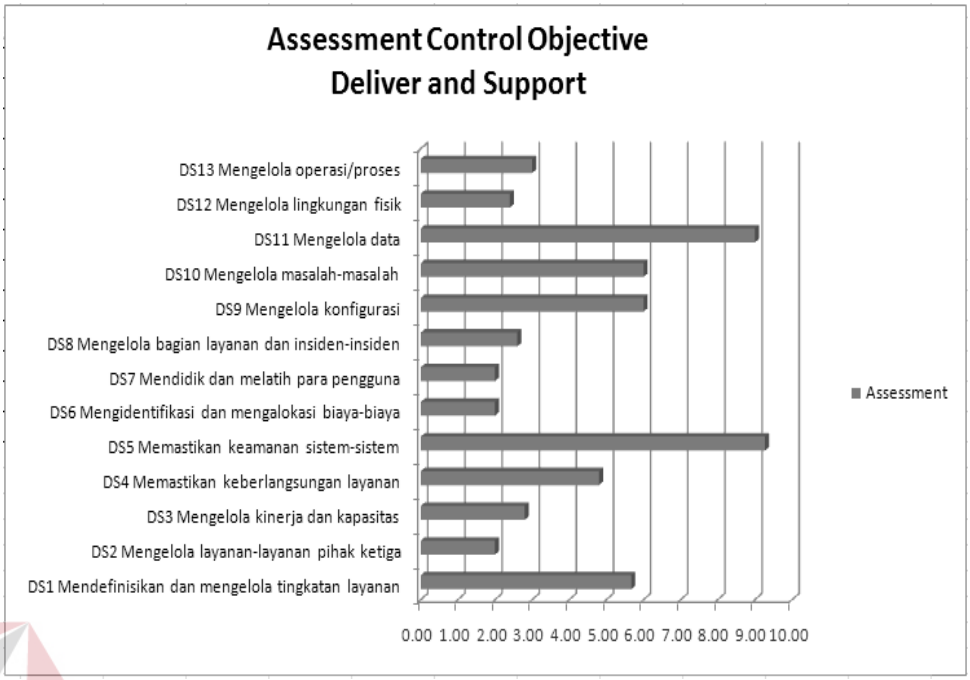
menggunakan COBIT, pada tahapan awal dilakukan penetapan *Management Guidelines*. *Management Guidelines* merupakan tool untuk membantu penugasan tanggungjawab, mengukur kinerja, dan melakukan benchmark serta mengetahui gap dalam kemampuan. Keterangan di bawah ini dapat menjawab pertanyaan seperti: Sejauh mana IT harus dikontrol, dan apakah cost ditentukan berdasarkan benefit? Apakah indicator dari kinerja yang baik? Apakah yang harus dilakukan untuk mencapai kinerja yang baik? Serta, Bagaimana melakukan pengukuran dan perbandingan.

Berdasarkan COBIT penilaian dilakukan menggunakan 3 pengukuran, yaitu: *Control Objective*, *Maturity Level*, dan tingkat resiko yang diukur dengan KPI, PKGI, serta ITKGI.

4.1.1 *Control Objective*

Tolok ukur untuk mencapai *business goal* yang diinginkan yang berupa statement yang berisi tentang hasil atau fungsi yang diinginkan. Dilakukan dengan mengimplementasikan *control procedures* dalam IT proses tertentu. Merupakan karakteristik dari proses yang terkelola dengan baik. Merupakan *best practice management objectives* umum untuk semua aktifitas IT.

Pada penelitian ini, dilakukan penilaian atau perkiraan *Control Objective* pada domain *Deliver & Support* yang dilakukan pada Bagian Akademik STIKOMP Surabaya (dapat dilihat pada Lampiran 1). Berikut ini adalah hasil pengukuran *control objective* yang dilakukan di Bagian Administrasi Akademik STIKOMP Surabaya. Gambar 4.1 Menunjukkan grafik penilaian dari perhitungan *Control Objective*. Sedangkan Tabel 4.1 Menunjukkan secara detil nilai dari *Control Objective* tiap sub domain yang telah ditunjukkan pada gambar 4.1.



Gambar 4.1 Grafik Penilaian *Control Objective*

Domain *Deliver* & *Support*

Tabel 4.1 Nilai *Control Objective* Domain *Deliver* & *Support*

Domain	Assessment	Importance
DS1 Mendefinisikan dan mengelola tingkatan layanan	5.67	Medium
DS2 Mengelola layanan-layanan pihak ketiga	2.00	Rendah
DS3 Mengelola kinerja dan kapasitas	2.80	Rendah
DS4 Memastikan keberlangsungan layanan	4.80	Medium
DS5 Memastikan keamanan sistem-sistem	9.27	Tinggi
DS6 Mengidentifikasi dan mengalokasi biaya-biaya	2.00	Rendah
DS7 Mendidik dan melatih para pengguna	2.00	Rendah
DS8 Mengelola bagian layanan dan insiden-insiden	2.60	Rendah
DS9 Mengelola konfigurasi	6.00	Medium
DS10 Mengelola masalah-masalah	6.00	Medium
DS11 Mengelola data	9.00	Tinggi
DS12 Mengelola lingkungan fisik	2.40	Rendah
DS13 Mengelola operasi/proses	3.00	Rendah

Pada tabel 4.1 terlihat bahwa DS5 dan DS11 memiliki tingkat kepentingan tertinggi di antara domain lainnya yaitu mempunyai nilai berkisar antara 9 – 12, sehingga perlu untuk diperhatikan dan terus dimonitor proses-proses yang berkaitan dengan domain tersebut. Untuk DS1, DS4, DS9 dan DS10 memiliki tingkat kepentingan medium yaitu mempunyai nilai berkisar antara 4 – 8. Sedangkan DS2, DS3, DS6, DS7, DS8, DS12 dan DS13 memiliki tingkat kepentingan rendah yaitu mempunyai nilai berkisar antara 0 – 3.

Dari nilai tersebut dapat ditarik kesimpulan sebagai berikut:

1. **DS1 Mendefinisikan dan mengelola tingkatan layanan**

   Framework manajemen tingkat layanan sudah memiliki pengendalian yang bagus namun dokumentasi masih bersifat informal. Sudah ada definisi mengenai layanan-layanan. Pihak pengelola telah mendefinisikan dengan jelas mengenai layanan minimum yang akan dihasilkan oleh sistem informasi akademik dan sudah didokumentasikan. Pada saat mendefinisikan atau memodifikasi tingkat layanan user ikut dilibatkan. Tanggung jawab user Sistem Informasi Akademik telah didefinisikan dengan jelas. Layanan yang disediakan bagi user Sistem Informasi Akademik kurang didefinisikan dengan jelas. Pemantauan dalam pencapaian keberhasilan layanan Sistem Informasi Akademik belum tentu dilakukan secara berkala namun dilakukan jika terdapat usulan/tambahan sistem sehingga performance Sistem Informasi Akademik semakin baik dari waktu ke waktu. Sangat diperlukan petugas yang bertanggung jawab memonitor dan melaporkan kinerja yang dihasilkan dalam penerapan Sistem Informasi Akademik.

2. DS2 Mengelola layanan-layanan pihak ketiga

Pihak ketiga yang dimaksud di sini yaitu bagian PPTI sendiri. Identifikasi supplier sudah dilakukan dengan baik. Sudah ada dokumentasi formal akan hubungan teknik dan organisasi yang mencakup tugas dan tanggungjawab, tujuan, penyampaian yang diharapkan. Pengawasan terhadap kinerja pihak ketiga dilakukan secara informal, belum ada dokumentasi tentang hal itu.

3. DS3 Mengelola kinerja dan kapasitas

Pemonitoran dan pelaporan kinerja yang dihasilkan dalam penerapan Sistem Informasi Akademik belum didokumentasikan. Belum menggunakan tools tertentu untuk membantu memodelkan/memprediksi kebutuhan, kinerja dan keandalan konfigurasi pada masa yang akan datang. Sumberdaya (fasilitas, aplikasi) secara berkala disesuaikan dengan kebutuhan dan perkembangan teknologi. Pihak pengelola kurang membuat perencanaan untuk meninjau ulang kinerja hardware yang tersedia dalam memenuhi kualitas layanan yang diharapkan. Fasilitas yang tersedia sangat mendukung Sistem Informasi Akademik supaya dapat diakses dengan baik dari local (intranet) STIKOMP. Fasilitas Sistem Informasi Akademik yang tersedia memiliki kecepatan akses yang cukup memadai. Fasilitas yang tersedia sangat mendukung Sistem Informasi Akademik agar dapat diakses dengan baik dari internet. Terdapat fasilitas pesan/email yang sangat membantu sebagai sarana komunikasi bagi user untuk dapat melaporkan kinerja sistem kepada pihak pengelola Sistem Informasi Akademik, sehingga kinerja dapat selalu dimonitoring secara kontinyu. Perlu

menyediakan fasilitas yang mendukung user dalam menjalankan kegiatan operasionalnya. Perlu menyediakan sumberdaya yang sesuai dengan kebutuhan. Sudah ada dokumentasi mengenai fasilitas-fasilitas yang mendukung sistem informasi akademik. Tapi belum ada dokumentasi mengenai kinerja hardware yang digunakan guna mendukung sistem informasi akademik.

4. DS4 Memastikan keberlangsungan layanan

Sudah ada penanggung jawab dalam mengimplementasikan kerangka kerja sebagai solusi alternative jika terjadi gangguan layanan Sistem Informasi Akademik (meliputi aplikasi, file-file data serta kebutuhan hardware). Rencana kerja Sistem Informasi Akademik dibuat dengan memperhatikan keselarasannya dengan tujuan institusi. Belum ada suatu kerangka kerja formal yang akan dijadikan solusi alternative jika terjadi gangguan layanan Sistem Informasi Akademik (meliputi aplikasi, file-file data serta kebutuhan hardware). Belum tersedia prosedur formal untuk mengimplementasikan rencana kerja tersebut. Prosedur untuk mengimplementasikan rencana kerja tersebut , cukup disosialisasikan kepada pihak terkait. Pelatihan diberikan kepada pihak terkait mengenai cara mengimplementasikan prosedur tersebut. Perlu membuat kerangka kerja sebagai solusi alternative jika terjadi gangguan layanan Sistem Informasi Akademik (meliputi aplikasi, file-file data serta kebutuhan hardware). Tidak ada dokumentasi mengenai solusi jika terjadi gangguan layanan sistem informasi akademik dan prosedur yang berkaitan dengan sistem informasi akademik.

5. DS5 Memastikan keamanan sistem-sistem

Monitoring dan evaluasi terhadap keamanan data dan fasilitas fisik yang berkaitan dengan Sistem Informasi Akademik cukup baik dilakukan. Belum ada definisi yang tertulis mengenai hal-hal yang menyebabkan terganggunya layanan Sistem Informasi Akademik beserta langkah antisipasinya. Sistem Informasi Akademik sudah dilengkapi dengan pendeteksi virus. Indikasi pelanggaran terhadap keamanan system dapat dideteksi dalam waktu singkat. Sudah dilakukan pengelompokan data-data Sistem Informasi Akademik berdasarkan kriteria tertentu. Sudah tersedia prosedur dalam memberikan dan memutuskan hak akses user. Pelanggaran keamanan sistem yang terjadi, secara berkala belum tentu dicatat, dilaporkan dan ditinjau untuk menghasilkan solusinya. Pihak pengelola sudah membuat perencanaan menangani masalah keamanan (data dan fasilitas hardware) implementasi Sistem Informasi Akademik. Pihak pengelola akan meninjau ulang system keamanan yang telah diimplementasikan jika terjadi gangguan terhadap sistem atau ada perubahan mengenai prosedur keamanan dan belum tentu dilakukan review secara berkala. User perlu diberikan hak akses yang sesuai dengan fungsi pekerjaannya. Tidak diperlukan suatu prosedure dalam memberikan dan memutuskan hak akses user. Tidak perlu dilakukan peninjauan secara berkala terhadap hak akses yang diberikan kepada user. Perlu dilakukan pendeteksian terhadap indikasi pelanggaran keamanan system dalam waktu singkat. Tidak ada dokumentasi mengenai fasilitas untuk mengubah password, catatan/laporan pelanggaran keamanan sistem yang terjadi. Namun sudah ada dokumentasi mengenai prosedur manajemen hak akses user dan prosedur keamanan.

6. **DS6 Mengidentifikasi dan mengalokasi biaya-biaya**

   Analisis terhadap cost-benefit (biaya yang dikeluarkan dan manfaat yang diperoleh) pada implementasi Sistem Informasi Akademik belum tentu dilakukan secara berkala. Tidak ada dokumentasi mengenai analisis cost benefit.

7. **DS7 Mendidik dan melatih para pengguna**

   Pelaksana pelatihan belum tentu mengacu pada kurikulum dan program kerja yang telah didefinisikan. Penetapan pelatih disesuaikan dengan kebutuhan materi pelatihan. Sudah ada pelatihan untuk staff IT dan staff Akademik mengenai prosedur pengoperasian SI akademik, penyusunan kurikulum dan penyusunan modul untuk pelatihan staff IT dan staff akademik. Terdapat pelatihan untuk staff IT dan staff Akademik mengenai setiap perubahan sistem kerja, diimbangi dengan adanya pengarahan, sosialisasi atau pendidikan dan pelatihan SDM. Dukungan alokasi biaya, sumber daya, fasilitas dan infrastruktur yang sudah disediakan untuk program pendidikan dan pelatihan. Adanya pengaruh pendidikan dan pelatihan yang telah diberikan untuk perbaikan kinerja SDM. Sudah ada pelatihan mengenai keamanan SI akademik berkaitan dengan penanganan terhadap kegagalan sistem yang berdampak pada integritas, kerahasiaan dan ketersediaan data akademik. Adanya keterlibatan staff akademik, staff IT, maupun peserta pelatihan dari unit kerja lain dalam penyusunan kurikulum maupun kebutuhan akan program pelatihan pendidikan yang akan diberikan. Materi pelatihan yang diberikan sudah sesuai dengan pengerjaan tugas kerja di masing-masing unit kerja yang mengikuti

pelatihan. Tidak ada dokumentasi mengenai pelatihan baik itu materi pelatihan atau pelaksana pelatihan.

8. DS8 Mengelola bagian layanan dan insiden-insiden

Analisa terhadap permasalahan yang diajukan oleh user belum dilakukan secara periodik. Dilakukan pemeriksaan secara berkala terhadap asset TI yang dimiliki. Tersedia media komunikasi yang memadai yang berfungsi menampung pertanyaan dan keluhan user. Respon dari pihak pengelola terhadap permasalahan dan pertanyaan user telah diberikan dengan cukup memadai (dari segi kapasitas solusi dan ketepatan waktu). Rekapitulasi terhadap permasalahan dilakukan secara periodik untuk selanjutnya dilakukan analisis terhadap penyebab masalah tersebut supaya tidak terulang masalah yang sama pada masa yang akan datang. Pihak pengelola sangat perlu memberikan tanggapan terhadap permasalahan dan pertanyaan dari user. Ada dokumentasi mengenai pertanyaan dan keluhan dari user serta aset IT. Sedangkan analisa terhadap permasalahan yang diajukan oleh user belum terdokumentasikan.

9. DS9 Mengelola konfigurasi

Pemeriksaan secara berkala terhadap asset TI yang dimiliki belum dilakukan secara periodic. Selalu dipastikan bahwa Sistem Informasi Akademik menggunakan software yang berlisensi. Ada petugas yang bertanggung jawab mengelola perubahan konfigurasi asset TI yang dimiliki (software, hardware dan fasilitas lain). Semua software dan hardware yang digunakan selalu diinventarisir secara lengkap. Sumber daya(fasilitas, aplikasi, data) Sistem Informasi Akademik yang kritis

(sangat penting) didefinisikan dan dipelihara secara khusus. Kesalahan dan permasalahan yang timbul dalam penerapan Sistem Informasi Akademik diinventarisir, diteliti, dan dipecahkan dengan cara dan waktu yang efisien. Kesalahan dan permasalahan yang timbul dalam penerapan sistem informasi akademik, petunjuk/prosedur pengoperasian sistem informasi akademik bagi user, konfigurasi aset IT (baik itu software, hardware dan fasilitas lain) sudah didokumentasikan.

10. **DS10 Mengelola masalah-masalah**

Rekapitulasi terhadap permasalahan yang untuk selanjutnya dilakukan analisis terhadap penyebab masalah tersebut supaya tidak terulang masalah yang sama pada masa yang akan datang belum dilakukan secara periodik. Kesalahan dan permasalahan yang timbul dalam penerapan Sistem Informasi Akademik diteliti dan dipecahkan dengan cara dan waktu yang efisien. Belum tersedia prosedur dan kriteria yang baku untuk penanganan masalah perbaikan masih dilakukan dengan sifat yang reaksional serta tidak ada prosedur untuk penanganannya.

11. **DS11 Mengelola data**

Adanya petunjuk (prosedur) yang perlu diketahui oleh user sebelum menginput data, ada pesan peringatan apabila user melakukan kesalahan dalam menginputkan data, ada batasan terhadap pengaksesan data oleh user hanya untuk data yang terkait dengan aktifitasnya saja yang bisa diakses. Adanya validasi/pengesahan terhadap dokumen yang dihasilkan Sistem Informasi Akademik oleh pihak berwenang. Evaluasi mengenai kemampuan system

dalam menghasilkan informasi yang akurat tidak dilakukan secara berkala. Back-up data dosen, mata kuliah, absensi, nilai mahasiswa dilakukan secara lengkap. Media penyimpanan data yang digunakan saat ini dianggap cukup memadai (baik dari segi efektifitas dan keamanan). Ada petugas yang bertanggung jawab mengelola data library (koleksi data) Sistem Informasi Akademik. Letak server backup data dan database/aplikasi lain berada pada satu gedung. Standard perawatan, membuat data cadangan (backup) dan recovery data telah didefinisikan dan diterapkan. Cukup tersedia petunjuk (prosedur) bagi user sehingga user mampu mengoperasikan Sistem Informasi Akademik. Fasilitas menu Sistem Informasi Akademik lengkap dan disertai pesan peringatan jika user melakukan kesalahan menginputkan data. Sebelum data disimpan system mengkonfirmasi terlebih dahulu kebenaran data yang diinputkan. Tidak dapat dipastikan bahwa data yang dapat diakses oleh user hanya data yang terkait dengan aktifitasnya. Secara berkala dilakukan evaluasi terhadap kemampuan system menghasilkan informasi yang akurat. Perubahan data nilai oleh dosen yang menangani nilai tetang kesalahan penghitungan/penginputan selalu dikonfirmasikan terlebih dahulu. Back-up data dosen, mata kuliah, absensi, nilai mahasiswa dilakukan secara lengkap. Proses penyiapan data akademik meliputi data dosen yang akan mengajar setiap semesternya berdasarkan program studi, pengumpulan Kartu Rencana Studi (KRS) mahasiswa berdasarkan semesternya, pengumpulan nilai mahasiswa dari dosen berdasarkan semesternya, pengumpulan data absensi mahasiswa berdasarkan mata kuliah dibuat untuk diikuti oleh user di semua jurusan yang ada di STIKOMP. Dokumen-dokumen sumber akademik sudah

dipersiapkan secara tepat oleh masing-masing Bagian akademik di tingkat jurusan. Adanya penanganan kesalahan selama pengolahan data akademik memungkinkan adanya pendeteksian, pelaporan, dan perbaikan terhadap kesalahan-kesalahan tersebut. Adanya prosedur-prosedur input data akademik dibuat dengan tujuan proses input hanya dilakukan oleh staf yang berwenang. Adanya pengontrolan yang memeriksa akurasi, kelengkapan, dan keabsahan data akademik untuk pemrosesan. Adanya validasi pemrosesan data, otentikasi, dan penyuntingan data akademik dilakukan di pusat pengolahan data. Pertukaran informasi akademik antar unit kerja yang ada di STIKOMP melalui jaringan. Tata cara untuk pendistribusian output dari proses yang dilakukan SI akademik yang disosialisasikan ke unit kerja di Institusi meliputi pencetakan Kartu Hasil Studi dilakukan jika semua nilai sudah masuk, pencetakan data kehadiran mahasiswa dilakukan setiap akhir perkuliahan. Pemeriksaan tingkat akurasi laporan output SI akademik oleh penyedia dan pengguna yang tepat. Adanya perlindungan yang memadai terhadap informasi yang sensitif selama berlangsungnya akses tanpa ijin, modifikasi, dan kesalahan pengiriman data. Adanya pencegah akses terhadap informasi yang sensitif dari komputer, disk, dan peralatan lainnya saat digunakan untuk penggunaan yang lainnya. Proses penyimpanan data memperhatikan kebutuhan-kebutuhan pengambilan, dan keefektifan, serta kebijakan keamanan. Implementasi strategi untuk back-up dan pengembalian data. Waktu yang digunakan untuk pemeriksaan back-up untuk menjamin pencadangan dilaksanakan sesuai dengan strategi dan kemampuan penggunaan pencadangan (back-up). Back-up data disimpan dengan aman dan tempat penyimpanan secara periodik diperiksa, sehubungan

dengan keamanan akses fisik dan keamanan file data, dan item-item lainnya. Otentifikasi dan integritas informasi yang didapat dari luar organisasi diperiksa secara ketat sebelum diambilnya tindakan yang kritis. Sudah ada dokumentasi mengenai pengelolaan data.

12. **DS12 Mengelola lingkungan fisik**

    Adanya pengendalian akses terhadap fasilitas TI. Keamanan fisik dan pengendalian akses terhadap fasilitas TI yang ada dianggap cukup memadai (terkait lokasi, peralatan pelindung keamanan fisik lainnya). Pemeriksaan cukup dilakukan secara berkala terhadap hasil dari setiap aktifitas layanan pendukung Sistem Informasi Akademik. Ada dokumentasi mengenai fasilitas IT.

13. **DS13 Mengelola operasi/proses**

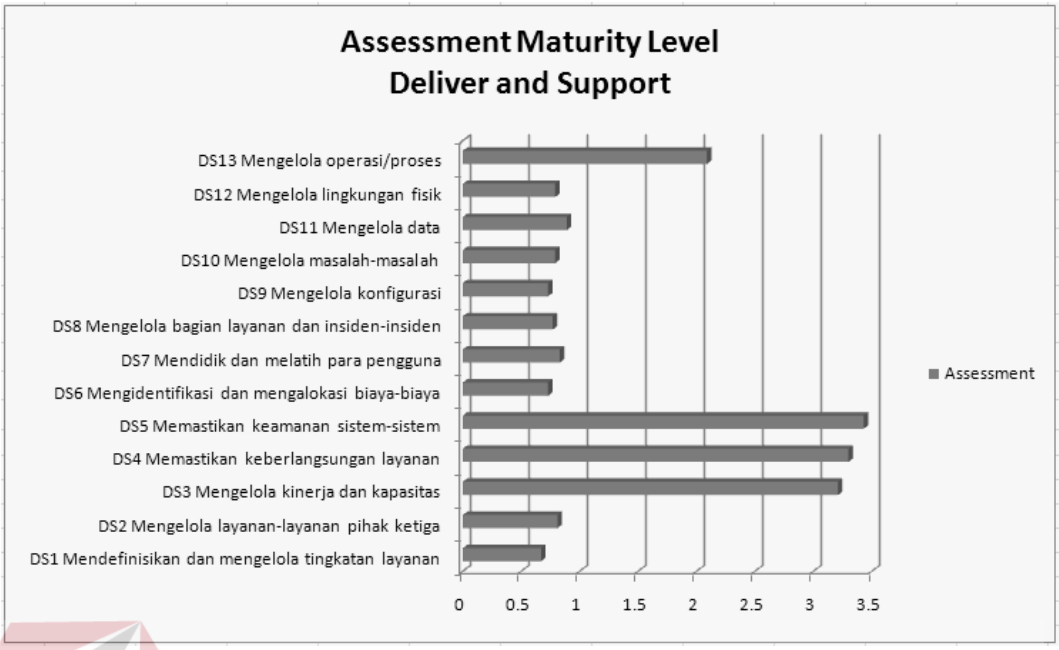
    Pemeriksaan secara berkala terhadap hasil dari setiap aktifitas layanan pendukung Sistem Informasi Akademik tidak dilakukan secara berkala. Proses akademik sudah dilaksanakan sesuai jadwal yang direncanakan. Pengisian KRS yang terjadwal pada Sistem Informasi Akademik sangat membantu mempercepat dan memperlancar akses Sistem Informasi Akademik. Dosen yang menangani masalah perwalian melakukan validasi KRS tepat waktu sesuai jadwal yang direncanakan. Dosen yang menangani masalah penilaian telah melakukan pengisian nilai belum tentu tepat waktu sesuai jadwal yang direncanakan. Tidak ada dokumentasi mengenai aktifitas/proses yang berkaitan dengan sistem. Tapi ada dokumentasi mengenai hasil output dari sistem informasi akademik.

4.1.2 Maturity Level

Maturity Level atau tingkat kematangan membahas pilihan strategis dan perbandingan (*benchmarking*). Untuk kendali terhadap proses IT, sehingga manajemen dapat memetakan di mana organisasi berada, di mana organisasi tersebut berdiri dibandingkan dengan organisasi lain yang terbaik di dalam industri, serta terhadap standar internasional di mana organisasi tersebut ingin berada. Tingkat kematangan inilah yang menjadi tolak ukur dalam menilai efektifitas manajemen IT dalam Sistem Informasi Akademik di STIKOMP Surabaya.

Maturity Model menunjukkan tingkat seberapa baik aktifitas untuk manajemen proses IT yang dilakukan. Terdiri dari 6 level yang berisi statement-statement. Statement menyatakan kondisi yang harus dipenuhi untuk mencapai level tersebut. Statement tersebut memiliki referensi kepada *activity* yang ada dalam RACI *Chart*. Dari statement dibuat pertanyaan-pertanyaan kepada pihak yang berkaitan dengan mereferensi pada RACI *Chart* yang nantinya dilakukan penilaian yang menghasilkan nilai maturity.

Pada penelitian ini, dilakukan penilaian atau perkiraan *Maturity Level* pada domain *Deliver & Support* yang dilakukan pada Bagian Akademik STIKOMP Surabaya (dapat dilihat pada Lampiran 2). Berikut ini adalah hasil pengukuran penilaian *Maturity Level* yang dilakukan di Bagian Administrasi Akademik STIKOMP Surabaya. Gambar 4.2 menunjukkan grafik penilaian dari perhitungan *Maturity Level*. Sedangkan Tabel 4.2 menunjukkan secara detil nilai dari *Maturity* tiap sub domain yang telah ditunjukkan pada gambar 4.2.

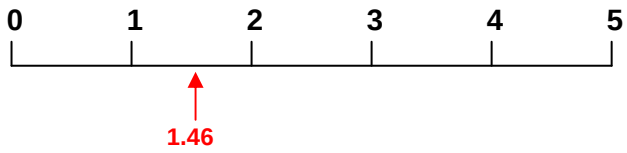


Gambar 4.2 Grafik Penilaian Maturity Level Domain *Deliver* & *Support*

Tabel 4.2 Nilai Maturity tiap Sub Domain *Deliver* & *Support*

Domain	Nilai Maturity Level
DS1 Mendefinisikan dan mengelola tingkatan layanan	0.67
DS2 Mengelola layanan-layanan pihak ketiga	0.81
DS3 Mengelola kinerja dan kapasitas	3.21
DS4 Memastikan keberlangsungan layanan	3.3
DS5 Memastikan keamanan sistem-sistem	3.43
DS6 Mengidentifikasi dan mengalokasi biaya-biaya	0.73
DS7 Mendidik dan melatih para pengguna	0.83
DS8 Mengelola bagian layanan dan insiden-insiden	0.77
DS9 Mengelola konfigurasi	0.73
DS10 Mengelola masalah-masalah	0.79
DS11 Mengelola data	0.89
DS12 Mengelola lingkungan fisik	0.79
DS13 Mengelola operasi/proses	2.09
Rata-rata	**1.46**

MATURITY LEVEL:



Gambar 4.3 Posisi Maturity Level Domain *Deliver & Support* pada Bagian AAK STIKOMP Surabaya

Pada tabel 4.2 terlihat bahwa DS1, DS2, DS6, DS7, DS8, DS9, DS10, DS11, DS12 memiliki tingkat kematangan di bawah standar internasional (standar nilai-nilai proses IT di ISACA) yaitu berada di bawah 2 padahal standar internasional mempunyai nilai *maturity level* antara 2-3 sehingga perlu untuk ditingkatkan dalam setiap sub domain yang ada supaya minimal sesuai dengan standar internasional. Untuk DS13 sudah sesuai dengan standar namun masih perlu ditingkatkan. Sedangkan DS3, DS4, DS5 memiliki tingkat kematangan di atas standar internasional, hal ini perlu dipertahankan sebaik-sebaiknya. Dari hasil perhitungan didapatkan nilai rata-rata dari domain ini adalah **1.46 (**ditunjukkan pada gambar 4.3**)** yang berarti tingkat kematangan (*Maturity Level*) manajemen IT Sistem Informasi Akademik STIKOMP Surabaya berdasarkan COBIT 4.0 adalah **Mendekati *Repeatable but intuitive*.**

Dari nilai tersebut dapat ditarik kesimpulan sebagai berikut:

1. **DS1 Mendefinisikan dan mengelola tingkatan layanan.**

   Terdapat persetujuan tingkat layanan yang disetujui, namun sifatnya informal dan belum lengkap. Koordinator tingkat layanan diberi penugasan dengan jelas namun dengan otoritas yang terbatas.

2. **DS2 Mengelola layanan-layanan pihak ketiga.**

   Proses untuk mengawasi/mengatur penyedia layanan pihak ketiga, berhubungan resiko dan penyampaian dari pelayanan masih bersifat informal. Kontrak yang dilakukan masih bersifat standar berdasarkan *terms & conditions* vendor yang dipilih. Pengukuran dilakukan namun tidak relevan.

3. **DS3 Mengelola kinerja dan kapasitas.**

   Manajemen sadar akan akibat yang mungkin timbul dari tidak diaturnya kinerja dan kapasitas dengan baik. Kebutuhan kinerja biasanya berdasar pada penilaian sistem secara individual dan pengetahuan tim pendukung dan tim proyek. Beberapa alat-alat individu mungkin dapat digunakan untuk mengenali masalah kinerja dan kapasitas, tapi konsistensi dari hasil tergantung pada keahlian individu utama. Namun belum ada penilaian secara menyeluruh dari kemampuan kinerja IT atau pertimbangan situasi beban puncak dan rencana terburuk. Sebuah pengukuran kinerja yang terutama tergantung pada kebutuhan IT dan bukan pada kebutuhan customer.

4. **DS4 Memastikan keberlangsungan layanan.**

   Terdapat penugasan untuk menjamin keberlangsungan service. Pencapaian untuk menjamin kelangsungan service dipisah-pisahkan pelaksanaannya/tdk terpadu. Pelaporan terhadap ketersediaan sistem bersifat sporadis/tersebar, tidak lengkap dan tidak mencantumkan akibat terhadap bisnis. Prakteknya terdapat keberlangsungan service, namun kesuksesannya berdasarkan pada individu masing-masing/operator yang melaksanakannya.

5. **DS5 Memastikan keamanan sistem-sistem.**

   Tanggung jawab dan akuntabilitas akan keamanan IT ditugaskan kepada seorang koordinator keamanan IT, tetapi kekuasaan manajemen dari koordinator tersebut terbatas. Kesadaran akan kebutuhan keamanan, terfragmentasi dan terbatas. Meskipun informasi yang relevan terhadap keamanan dihasilkan oleh sistem, tapi kurang dianalisis. Kebijakan keamanan tengah dibangun, tetapi keahlian dan peralatan kurang mencukupi. Pelatihan keamanan telah tersedia tetapi pelaksanaannya tergantung pada masing-masing orang.

6. **DS6 Mengidentifikasi dan mengalokasi biaya-biaya.**

   Sudah ada kesadaran secara keseluruhan akan kebutuhan untuk mengenali dan mengalokasikan biaya-biaya. Namun didasari oleh asumsi yang informal. Pembagian biaya berdasar pada perkiraan biaya, contoh : biaya-biaya hardware, dan sebenarnya tidak berhubungan dengan penggerak

nilai. Belum ada pelatihan formal atau komunikasi dalam prosedur standar alokasi dan identifikasi biaya.

7. **DS7 Mendidik dan melatih para pengguna.**

   Ada kesadaran dari kebutuhan sebuah program pelatihan dan pendidikan dan menghubungkan proses-proses keluar organisasi. Permulaan pelatihan dikenali dalam rencana kinerja individu pegawai. Proses-proses dikembangkan ke tahap dimana kelas pelatihan dan pendidikan informal diajar oleh instruktur yang berbeda, selama mencakup persoalan subjek yang sama dengan pendekatan yang berbeda. Beberapa dari kelas menunjukkan persoalan mengenai kelakuan yang layak dan kesadaran dan latihan keamanan sistem. Terdapat kepercayaan yang tinggi pada pengetahuan individu. Bagaimanapun, ada komunikasi yang tetap pada keseluruhan persoalan dan kebutuhan untuk menunjukkannya.

8. **DS8 Mengelola bagian layanan dan insiden-insiden.**

   Terdapat kesadaran organisasional akan perlunya fungsi help desk internal yang menangani permasalahan sistem. Layanan help desk telah disediakan secara informal berdasarkan jaringan pengetahuan yang dipunyai individual. Individu ini mempunyai beberapa alat-alat umum tersedia untuk membantu dalam pemecahan kejadian.

9. **DS9 Mengelola konfigurasi.**

   Management tahu akan kebutuhan untuk mengendalikan konfigurasi IT dan memahami manfaat konfigurasi informasi yang akurat dan lengkap.

Alat konfigurasi manajemen digunakan pada tingkat tertentu namun menggunakan platform yang berbeda-beda.

10. **DS10 Mengelola masalah-masalah.**

Terdapat pengetahuan yang luas tentang kebutuhan dan keuntungan me-manage masalah berkaitan dengan IT antara unit bisnis dan fungsi layanan informasi. Proses pemecahan masalah telah disusun sampai pada titik dimana beberapa individu kunci bertanggungjawab untuk mengidentifikasi dan menyelesaikan masalah. Informasi dibagi secara informal dan reaktif diantara staf. Service level untuk komunitas pengguna bervariasi dan dihambat oleh ketidakcukupan struktur pengetahuan untuk manager problem.

11. **DS11 Mengelola data.**

Terdapat kesadaran akan kebutuhan keakuratan manajemen data dalam organisasi. Kepemilikan data mulai muncul pada level atas. Kebutuhan keamanan untuk manajemen data didokumentasikan oleh individual tertentu dan belum konsisten serta aturan dan definisi data dikendalikan oleh kebutuhan IT. Beberapa monitoring didalam IT dilakukan pada aktivitas utama manajemen data (backup, pengembalian, penyelesaian). Tanggung jawab untuk manajemen data secara informal ditugaskan pada staff IT utama.

12. **DS12 Mengelola lingkungan fisik.**

    Telah terdapat kesadaran akan perlunya perlindungan dan pengaturan lingkungan komputerisasi secara fisik. Hal ini terlihat dari alokasi dana dan sumber daya, namun sifatnya masih informal dan terpecah-pecah. Belum terdapat dokumentasi yang baik mengenai hal ini. Pengendalian lingkungan diterapkan dan dimonitor oleh personil operasi.

13. **DS13 Mengelola operasi/proses.**

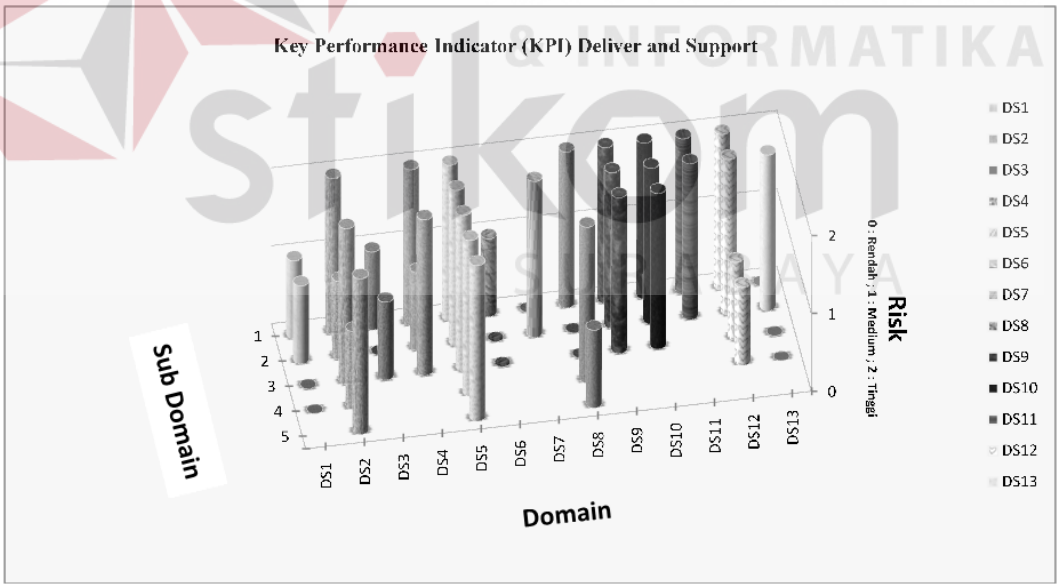
    Organisasi telah sadar sepenuhnya kebutuhan akan melakukan strukturisasi fungsi dukungan IT (*support*). Namun belum ada prosedur standar yang dicapai dan aktivitas prosesnya masih bersifat reaktif. Dana untuk peralatan dialokasikan kasus per kasus. Masih terdapat ketergantungan terhadap keahlian dan kemampuan seseorang. Belum ada standar prosedur dan dokumentasi.

4.1.3 Key Performance Indicator (KPI), Process Key Goal Indicator (PKGI), Information Technology Key Goal Indicator (ITKGI)

Pengukuran KPI, PKGI, dan ITKGI memungkinkan manajemen organisasi untuk secara efektif menangani kebutuhan dan tuntutan pengembangan teknologi informasi yang efektif dan efisien. KPI, PKGI, dan ITKGI memberikan gambaran kepada organisasi mengenai posisi dan arah mereka dalam mencapai tujuan-tujuan yang diharapkan dalam pengembangan teknologi informasi. KPI, PKGI, dan ITKGI digunakan untuk menunjukan bagaimana hubungan antara proses dengan bisnis dan *IT Goal*.

Key Performance Indicators (KPI) digunakan untuk memantau kinerja setiap proses TI, yang merupakan indikasi utama yang mendefinisikan ukuran dari seberapa baiknya kinerja proses TI dalam memungkinkan tujuan yang akan dicapai (untuk mengukur sejauh mana proses berjalan sesuai dengan goal yang telah ditentukan).

Pada penelitian tugas akhir ini, dilakukan penilaian atau perkiraan resiko yang berkaitan dengan KPI pada domain *Deliver & Support* yang dilakukan pada Bagian Akademik STIKOMP Surabaya. Berikut ini adalah hasil pengukuran penilaian resiko KPI yang dilakukan di Bagian Administrasi Akademik STIKOMP Surabaya. Gambar 4.4 menunjukkan grafik penilaian resiko KPI. Sedangkan Tabel 4.3 menunjukkan secara detil nilai resiko KPI tiap sub domain yang telah ditunjukkan pada gambar 4.4.



Gambar 4.4 Grafik Penilaian Resiko KPI Domain *Deliver* & *Support*

Tabel 4.3 Penilaian Resiko KPI tiap Sub Domain *Deliver* & *Support*

Domain	Sub Domain	Risk
D1	1	1
	2	1
	3	0
	4	0
D2	1	2
	2	1
	3	2
	4	1
	5	2
D3	1	1
	2	0
	3	1
D4	1	2
	2	1
	3	2
D5	1	2
	2	2
	3	2
	4	2
	5	2
D6	1	1
	2	0
	3	0

Domain	Sub Domain	Risk
D7	1	0
	2	2
D8	1	2
	2	0
	3	0
	4	2
	5	1
D9	1	2
	2	2
	3	2
D10	1	2
	2	2
	3	2
D11	1	2
	2	2
D12	1	2
	2	2
	3	1
	4	1
D13	1	0
	2	2
	3	0
	4	0

Keterangan : Risk 0 = Rendah, Risk 1 = Medium, Risk 2 = Tinggi

Pada tabel 4.3 terlihat bahwa beberapa sub domain ada yang memiliki tingkat resiko yang tinggi, medium maupun rendah. Proses-proses yang mempunyai resiko tinggi berarti jika aktifitas tersebut tidak terpenuhi, maka proses bisnis yang lain akan terganggu. Sebaiknya aktivitas yang beresiko tinggi ataupun medium diupayakan agar mempunyai resiko yang rendah. Sedangkan aktivitas yang beresiko rendah selayaknya dipertahankan. Untuk penjelasan lebih lengkap ada pada lampiran 3.

Dari nilai tersebut dapat ditarik kesimpulan sebagai berikut:

1. **DS1 Mendefinisikan dan mengelola tingkatan layanan**

   Review SLA formal yang bersesuaian dengan bisnis pertahun belum dilakukan secara berkala dan mempunyai tingkat resiko medium. Layanan-layanan biasanya didefinisikan/dirumuskan terlebih dahulu sesuai dengan kebutuhan user. Pelaporan mengenai tingkat layanan tidak selalu didokumentasikan tergantung dari kasusnya.

2. **DS2 Mengelola layanan-layanan pihak ketiga**

   Supplier sudah mendefinisikan kebutuhan dan tingkat layanan secara jelas dengan adanya komunikasi yang efektif antara supplier dengan user. Layanan supplier sudah diidentifikasi dan dikategorikan sesuai dengan kebutuhan. Resiko yang terkait dengan supplier diidentifikasi dan diusahakan untuk dikurangi. Kinerja supplier dimonitor tidak secara berkala melainkan tergantung dari kebutuhan user. Kesalahan dari supplier pada suatu waktu dikomplain oleh user tergantung dari jenis kesalahannya.

3. **DS3 Mengelola kinerja dan kapasitas**

   Belum ada peramalan mengenai kapasitas dan performansi. Kapasitas dan ketersediaan sistem memang direncanakan terlebih dahulu dan disediakan sesuai dengan kebutuhan user. Kinerja sistem belum terdokumentasi dengan baik. Apabila terjadi gangguan atau kekurangan dari sistem, user akan melakukan konfirmasi kepada pihak penyedia layanan untuk mengubah atau menambahkan kekurangan ke dalam sistem tersebut

dengan mempertimbangkan kelayakannya. Tidak semua aset dimonitor melalui tool yang tersentralisasi.

4. **DS4 Memastikan keberlangsungan layanan**

   Rencana kemungkinan IT tidak dilakukan secara formal hanya melalui pemikiran beberapa orang dan belum ada dokumentasi mengenai hal tersebut, namun sudah ada kesadaran untuk mengembangkan dan memperbaiki rencana kemungkinan IT tersebut. Belum ada pengujian dan pelatihan mengenai rencana kemungkinan IT. Ada komponen-komponen dalam infrastruktur yang bersifat kritis dan sudah dilakukan pengendalian terhadap resiko yang mungkin terjadi.

5. **DS5 Memastikan keamanan sistem-sistem**

   Manajemen telah menyadari dan memahami kebutuhan keamanan, vulnerabilities (kemampuan mudah diserang) dan ancaman. Keamanan dan adanya ancaman telah diperkirakan. Pengelolaan identitas user telah dilakukan dan disahkan dengan cara yang sesuai dengan standar. Pengendalian terhadap keamanan telah dilakukan namun belum dimonitor secara periodik. Pengujian keamanan tidak dilakukan secara teratur. Biasanya pengujian tersebut secara tidak langsung terjadi dikarenakan memang ada gangguan dalam keamanan.

6. **DS6 Mengidentifikasi dan mengalokasi biaya-biaya**

   Biaya-biaya direview dan dialokasikan oleh manajemen bisnis sesuai dengan rencana anggaran yang telah ditentukan sebelumnya. Ongkos disesuaikan dengan kualitas dari layanan yang disediakan dan

dilaksanakan sesuai dengan kebijakan yang disetujui. Biaya-biaya disusun berdasarkan kebutuhan dan dialokasikan sesuai dengan kebijakan yang disetujui.

7. DS7 Mendidik dan melatih para pengguna

Kurikulum pelatihan disusun dan disesuaikan dengan kebutuhan. Sudah ada pengelolaan yang cukup mengenai pelatihan mulai dari kurikulum pelatihan sampai personil yang bertanggungjawab dalam memberikan pelatihan. Namun belum dimonitor dan dilaporkan secara formal (belum terdokumentasi).

8. DS8 Mengelola bagian layanan dan insiden-insiden

Sudah ada personil yang bertanggungjawab dalam hal instalasi sebuah bagian layanan. Pemecahan kejadian didasarkan pada prioritas kebutuhan dan tingkat kepentingannya. Sudah ada definisi kriteria dan prosedur peningkatan yang jelas namun belum terdokumentasi dengan baik. Kejadian dan permintaan layanan kadang dicatat dan dilaporkan sesuai dengan kasusnya. Pelatihan setiap staf bagian layanan dilakukan jika ada perubahan mengenai layanan. Terkadang ada kejadian yang membutuhkan bantuan lokal/setempat (bantuan lapangan, kunjungan pribadi) tapi terkadang ada kejadian/pertanyaan-pertanyaan yang tidak dapat dipecahkan pada saat itu. Pertanyaan/kejadian yang ada diprioritaskan berdasarkan tingkat kebutuhan dan kebutuhan yang bersifat kritis akan diselesaikan terlebih dahulu.

9. **DS9 Mengelola konfigurasi**

   Sudah ada tempat penyimpanan pusat dari semua susunan item yang ada. Susunan item/data dikenali pada saat awal pendefinisian dan tahap perencanaan serta secara berkala dipelihara. Adanya pemeriksaan integritas dari susunan data. Jika ada ketidaksesuaian konfigurasi, akan dilakukan pengecekan dan penelusuran terlebih dahulu apakah perlu dilakukan perubahan atau perbaikan konfigurasi. Sudah ada pengendalian jika terjadi ketidaksesuaian yang berhubungan dengan bentuk informasi yang tidak lengkap atau yang hilang. Bentuk item dikonfigurasi sesuai dengan tingkat layanan untuk kinerja, keamanan dan ketersediaan.

10. **DS10 Mengelola masalah-masalah**

    Adanya wewenang kepada pengelola masalah untuk melakukan analisa penyebab sumber dari masalah dan mencari pemecahannya. Masalah yang ada serta pemecahannya belum didokumentasikan.

11. **DS11 Mengelola data**

    Backup sudah dilakukan. Sudah ada pengendalian mengenai pengelolaan data dan rencana pemulihan. Tingkat keamanan data dan perlengkapan sudah ditentukan.

12. **DS12 Mengelola lingkungan fisik**

    Sudah ada manajemen terhadap pengelolaan fasilitas (keamanan fisik). Sudah ada personil yang diberi wewenang dan tanggungjawab mengelola lingkungan fisik. Adanya pelatihan dari personil dalam ukuran

keselamatan, keamanan dan fasilitas/kesempatan. Sudah ada pengendalian terhadap resiko yang mungkin terjadi.

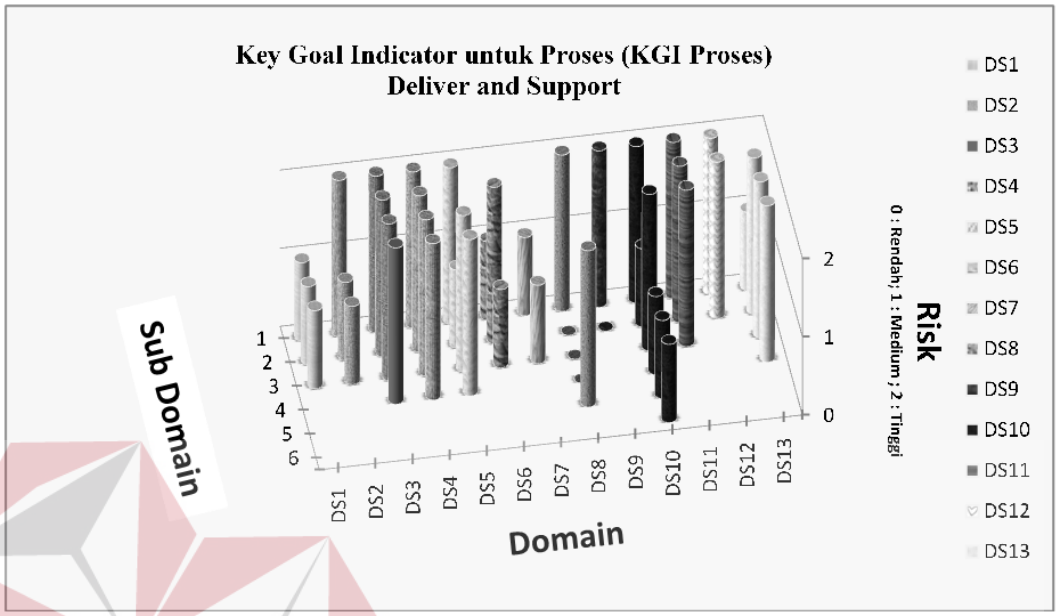
13. DS13 Mengelola operasi/proses

Lingkungan IT memang dirancang sesuai dengan tingkat layanan yang telah disetujui. Adanya pemeliharaan dan pengawasan terhadap infrastruktur IT. Jadwal pemeliharaan aset hardware dilakukan dan dijalankan sesuai dengan program kerja.

Key Goal Indicators (KGI) digunakan untuk memantau perolehan dari tujuan proses TI, di mana didefinisikan ukuran yang memberitahu pihak manajemen apakah suatu proses IT telah mencapai kebutuhan bisnisnya. KGI digunakan untuk memantau seberapa jauh IT mencapai kebutuhan bisnisnya. KGI dibagi menjadi dua yaitu: KGI untuk Proses dan KGI untuk TI. KGI untuk proses atau Process Key Goal Indicators (PKGI) mendefinisikan bagaimana seharusnya TI mendukung "Tujuan TI". KGI untuk TI atau Information Technology Key Goal Indicator (ITKGI) mendefinisikan apa yang diharapkan bisnis dari TI (bagaimana bisnis mengukur kinerja TI).

Pada penelitian tugas akhir ini, dilakukan penilaian atau perkiraan resiko yang berkaitan dengan KGI untuk proses pada domain *Deliver & Support* yang dilakukan pada Bagian Akademik STIKOMP Surabaya. Berikut ini adalah hasil pengukuran penilaian resiko KGI untuk proses yang dilakukan di Bagian Administrasi Akademik STIKOMP Surabaya. Gambar 4.5 menunjukkan grafik penilaian resiko KGI untuk proses. Sedangkan Tabel 4.4 menunjukkan secara

detil nilai resiko KGI untuk proses tiap sub domain yang telah ditunjukkan pada gambar 4.5.



Gambar 4.5 Grafik Penilaian Resiko KGI untuk Proses Domain *Deliver* & *Support*

Tabel 4.4 Penilaian Resiko KGI untuk Proses tiap Sub Domain *Deliver* & *Support*

Domain	Sub Domain	Risk
DS1	1	1
	2	1
	3	1
DS2	1	2
	2	1
	3	1
DS3	1	2
	2	2
	3	2
	4	2
DS4	1	2
	2	2
	3	2
	4	2
DS5	1	2
	2	1
	3	2
	4	2
DS6	1	1
	2	2
	3	1
DS7	1	1

Domain	Sub Domain	Risk
DS7	2	0
	3	1
DS8	1	2
	2	0
	3	0
	4	0
	5	2
DS9	1	2
	2	0
DS10	1	2
	2	1
	3	2
	4	1
	5	1
	6	1
DS11	1	2
	2	2
	3	2
DS12	1	2
	2	2
DS13	1	2
	2	2
	3	2

Keterangan : Risk 0 = Rendah, Risk 1 = Medium, Risk 2 = Tinggi

Pada tabel 4.4 terlihat bahwa beberapa sub domain ada yang memiliki tingkat resiko yang tinggi, medium maupun rendah. Proses-proses yang mempunyai resiko tinggi berarti jika aktifitas tersebut tidak terpenuhi, maka proses bisnis yang lain akan terganggu. Sebaiknya aktivitas yang beresiko tinggi ataupun medium diupayakan agar mempunyai resiko yang rendah. Sedangkan aktivitas yang beresiko rendah selayaknya dipertahankan. Untuk penjelasan lebih lengkap ada pada lampiran 3.

Dari nilai tersebut dapat ditarik kesimpulan sebagai berikut:

1. **DS1 Mendefinisikan dan mengelola tingkatan layanan**

   Tidak semua layanan berada dalam katalog, hanya layanan-layanan yang diperlukan saja yang ada. Tapi tidak menutup kemungkinan untuk menambahkan layanan-layanan lainnya sesuai dengan kebutuhan dan permintaan user. Layanan-layanan yang dibuat telah sesuai dengan tingkat layanan yang dibutuhkan atau sesuai dengan permintaan user.

2. **DS2 Mengelola layanan-layanan pihak ketiga**

   Adanya pengelolaan hubungan dan tanggungjawab kedua belah pihak dengan penyedia layanan yang berkualitas. Supplier mendapatkan kebutuhan dan tingkat layanan yang jelas. Perselisihan formal dengan supplier kadang-kadang terjadi jika kebutuhan atau permintaan dari user belum sesuai dengan tingkat layanan yang disetujui. Hal-hal yang berkaitan dengan tingkat layanan memiliki resiko yang tinggi sehingga harus diperhatikan dan sebisa mungkin memperkecil resiko tersebut.

3. **DS3 Mengelola kinerja dan kapasitas**

   Sudah ada pengawasan dan pengukuran mengenai beban maksimum dan waktu respon suatu proses dengan tetap mengacu SLA, namun belum dimonitor secara berkala. Penggunaan akan sumber daya IT telah diusahakan seoptimal mungkin. Sudah ada pengendalian dan manajemen resiko jika terjadi kegagalan dalam proses baik itu mengenai keterlambatan maupun mengenai kecepatan akses.

4. **DS4 Memastikan keberlangsungan layanan**

   Sebenarnya telah ada rencana kelancaran IT yang mendukung rencana kelancaran bisnis tapi hal itu masih bersifat informal dan belum ada dokumentasi mengenai hal tersebut. Rencana keberlanjutan IT sebagian besar telah dijalankan tapi tidak secara berkala dilakukan pemeliharaan. Memang hal itu dapat memperkecil kemungkinan terjadinya gangguan layanan IT. SLA disusun sesuai dengan kebutuhan. Terkadang rencana keberlanjutan IT tidak dapat memenuhi/hanya mengisi sebagian kebutuhan bisnis.

5. **DS5 Memastikan keamanan sistem-sistem**

   Sudah ada manajemen hak akses user mengenai akses data yang bersifat kritis dan juga akses ke informasi, aplikasi dan infrastruktur. Keamanan sudah diidentifikasi dan dimonitor namun belum ada pelaporan mengenai hal itu. Sudah ada pengendalian dari keamanan yang mudah diserang dan kejadian.

6. **DS6 Mengidentifikasi dan mengalokasi biaya-biaya**

   Terkadang memang terdapat perbedaan antara anggaran belanja, ramalan dan biaya yang sebenarnya, hal itu dikarenakan biaya-biaya yang sebenarnya berubah sesuai dengan pasar. Tapi keseluruhan biaya IT telah dialokasikan sesuai dengan model biaya yang telah disetujui.

7. **DS7 Mendidik dan melatih para pengguna**

   Sudah ada program pelatihan untuk user mengenai aplikasi dan solusi teknologi. Adanya layanan untuk pelatihan dan menjawab pertanyaan-

pertanyaan dari user. Stakeholder merasa cukup puas dengan adanya pelatihan yang disediakan.

8. **DS8 Mengelola bagian layanan dan insiden-insiden**

   Kejadian atau pertanyaan yang ada diusahakan selesai tepat pada waktunya dan terkadang dokumentasi mengenai hal tersebut akan dilakukan menyusul.

9. **DS9 Mengelola konfigurasi**

   Sudah ada tempat penyimpanan pusat dari semua aset yang ada. Adanya pemeliharaan keutuhan dari susunan tempat penyimpanan dan terkadang ada tinjauan mengenai susunan aset yang sebenarnya untuk pemenuhan basis dalam tempat penyimpanan.

10. **DS10 Mengelola masalah-masalah**

    Pencatatan terhadap masalah yang terjadi tidak semuanya didokumentasikan walaupun semua masalah yang ada telah terpecahkan. Masalah-masalah yang ada diselidiki sumber penyebabnya dan mencari penyelesaiannya secepat mungkin, namun terkadang ada masalah yang membutuhkan waktu lama dalam pemecahannya.

11. **DS11 Mengelola data**

    Sudah ada pemeliharaan mengenai backup data. Hal itu akan mempermudah dalam perbaikan data jika terjadi kerusakan. Pengelolaan data meliputi pemeliharaan kelengkapan, ketepatan, kebenaran, kemudahan pencapaian dari data yang tersimpan.

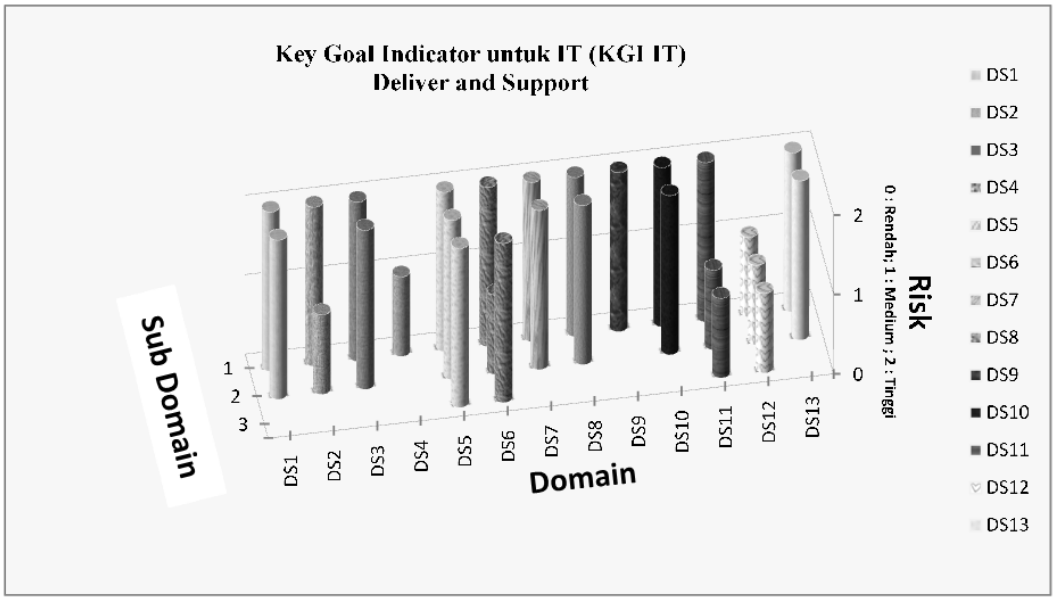
12. **DS12 Mengelola lingkungan fisik**

    Sudah ada otorisasi terhadap siapa saja yang boleh menggunakan fasilitas komputer. Lingkungan fisik disediakan dan dikelola sesuai dengan infrastruktur dan sumber daya IT. Sudah ada penendalian terhadap pelanggaran keamanan fisik atau kegagalan.

13. **DS13 Mengelola operasi/proses**

    Belum ada prosedur operasional formal yang berkaitan dengan tingkat layanan yang telah disetujui sehingga dapat menyebabkan hilangnya waktu atau keterlambatan yang merupakan akibat penyimpangan dari prosedur operasi. Adanya penyusunan jadwal dan pengolahan permintaan khusus dalam tingkat layanan yang disetujui walaupun terkadang pemenuhan tingkat layanan tersebut ada beberapa yang tidak sesuai dengan jadwal yang telah ditentukan. Usaha perlindungan fisik untuk informasi yang bersifat sensitif telah diupayakan untuk dilakukan.

Pada penelitian tugas akhir ini, dilakukan penilaian atau perkiraan resiko yang berkaitan dengan KGI untuk IT pada domain *Deliver & Support* yang dilakukan pada Bagian Akademik STIKOMP Surabaya. Berikut ini adalah hasil pengukuran penilaian resiko KGI untuk IT yang dilakukan di Bagian Administrasi Akademik STIKOMP Surabaya. Gambar 4.6 menunjukkan grafik penilaian resiko KGI untuk IT. Sedangkan Tabel 4.5 menunjukkan secara detil nilai resiko KGI untuk IT tiap sub domain yang telah ditunjukkan pada gambar 4.6.



Gambar 4.6 Grafik Penilaian Resiko KGI untuk IT Domain *Deliver* & *Support*

Tabel 4.5 Penilaian Resiko KGI untuk IT tiap Sub Domain *Deliver* & *Support*

Domain	Sub Domain	Risk
DS1	1	2
	2	2
DS2	1	2
	2	1
DS3	1	2
	2	2
DS4	1	1
DS5	1	2
	2	2
	3	2
DS6	1	2
	2	1
	3	2
DS7	1	2

Domain	Sub Domain	Risk
DS7	2	2
DS8	1	2
	2	2
DS9	1	2
DS10	1	2
	2	2
DS11	1	2
	2	1
	3	1
DS12	1	1
	2	1
	3	1
DS13	1	2
	2	2

Keterangan : Risk 0 = Rendah, Risk 1 = Medium, Risk 2 = Tinggi

Pada tabel 4.5 terlihat bahwa beberapa sub domain ada yang memiliki tingkat resiko yang tinggi, medium maupun rendah. Proses-proses yang

mempunyai resiko tinggi berarti jika aktifitas tersebut tidak terpenuhi, maka proses bisnis yang lain akan terganggu. Sebaiknya aktivitas yang beresiko tinggi ataupun medium diupayakan agar mempunyai resiko yang rendah. Sedangkan aktivitas yang beresiko rendah selayaknya dipertahankan. Untuk penjelasan lebih lengkap ada pada lampiran 3.

Dari nilai tersebut dapat ditarik kesimpulan sebagai berikut:

1. **DS1 Mendefinisikan dan mengelola tingkatan layanan**

   Pengguna dan stakeholder merasa puas terhadap kesesuaian layanan dengan tingkat layanan yang disetujui atau yang sesuai dengan kebutuhan bisnis. Adanya pengertian akan biaya IT, manfaat, strategi, kebijakan dan tingkat layanan.

2. **DS2 Mengelola layanan-layanan pihak ketiga**

   Komplain user terjadi jika layanan tidak sesuai dengan permintaan kebutuhan dari user. Hal ini memiliki tingkat resiko yang tinggi dalam menghambat aktifitas user, sehingga harus diperhatikan dan sebisa mungkin memperkecil resiko tersebut. Kepuasan user tercapai jika kebutuhannya telah terpenuhi berdasarkan tingkat layanan yang telah disetujui.

3. **DS3 Mengelola kinerja dan kapasitas**

   Sebelum penerapan sistem, sumber daya IT telah disesuaikan dengan kebutuhan sistem sehingga dapat dipastikan bahwa layanan IT telah

tersedia sesuai dengan yang dibutuhkan. Infrastruktur IT, sumber daya dan kemampuan telah diusahakan seoptimal mungkin.

4. **DS4 Memastikan keberlangsungan layanan**

   Layanan IT yang tersedia sudah sesuai dengan yang dibutuhkan, apabila belum sesuai akan dilakukan perbaikan atau penambahan sampai sesuai dengan kebutuhan. Pengaruh bisnis terkecil dalam kejadian sebuah gangguan atau perubahan layanan IT telah diperkirakan. Sudah ada pengendalian mengenai layanan IT dan infrastuktur apabila terjadi eror, serangan yang disengaja atau bencana dapat menahan dan pulih dari kegagalan.

5. **DS5 Memastikan keamanan sistem-sistem**

   Sudah ada otorisasi terhadap segala hal yang berhubungan dengan informasi yang bersifat kritis dan rahasia serta terhadap semua aset IT. Adanya pemeliharaan integritas/keutuhan informasi dan pengolahan infrastruktur. Semua aset IT sudah ada perlindungan namun belum dilakukan pencatatan secara berkala. Sudah ada pengendalian terhadap layanan IT dan infrastruktur apabila sewaktu-waktu ada kegagalan selama terjadi eror, serangan yang disengaja atau bencana agar dapat bertahan dan pulih.

6. **DS6 Mengidentifikasi dan mengalokasi biaya-biaya**

   Terdapat usaha perbaikan biaya IT agar efisien dan ada kontribusi yang menguntungkan kepada bisnis. IT diusahakan menunjukan kualitas

layanan dalam hal biaya efisien, kemajuan yang terus-menerus dan kesiapan bagi perubahan masa depan.

7. **DS7 Mendidik dan melatih para pengguna**

   User cukup puas dengan penawaran layanan dan tingkat layanan yang ada (sistem atau teknologi baru). Sudah ada personil yang membantu user dalam memahami penggunaan aplikasi dan solusi teknologi. Infrastruktur IT, sumber daya dan kemampuan diusahakan seoptimal mungkin. Belum ada pengukuran kemajuan produktifitas pegawai secara formal sebagai hasil dari pemahaman sistem yang lebih baik.

8. **DS8 Mengelola bagian layanan dan insiden-insiden**

   User merasa puas dengan adanya bagian pelayanan yang bisa menyelesaikan kejadian atau masalah yang ada dan juga dengan adanya penawaran layanan serta tingkat layanan. Sudah ada personil yang membantu user dalam memahami penggunaan yang tepat dan kinerja dari aplikasi dan solusi teknologi.

9. **DS9 Mengelola konfigurasi**

   Pokok persoalan yang ada terkadang juga dikarenakan susunan dari aset yang tidak tepat untuk itu diperlukan manajemen aset yang bagus dan dilakukan secara berkala. Infrastruktur IT, sumber daya dan kemampuan diusahakan seoptimal mungkin. Semua aset-aset IT dijaga namun belum ada dokumentasi secara periodik.

10. **DS10 Mengelola masalah-masalah**

    Memang terkadang dari masalah operasional bisa berakibat kepada bisnis. Untuk itu perlu diusahakan agar semua masalah yang timbul dapat segera terselesaikan dengan baik dan memastikan user puas dengan adanya penawaran layanan dan tingkat layanan.

11. **DS11 Mengelola data**

    Informasi yang bersifat kritikal dan rahasia telah diberi otorisasi hanya kepada pihak yang mempunyai hak untuk mengaksesnya. Pemenuhan IT dipastikan sesuai dengan hukum dan peraturan yang ada. Sudah ada pengendalian untuk memulihkan data yang bersifat kritikal karena hal itu nantinya berpengaruh terhadap kepuasan user dengan tersedianya data yang akurat dan tepat waktu.

12. **DS12 Mengelola lingkungan fisik**

    Sudah ada manajemen hak akses terhadap penggunaan infrastruktur IT, informasi yang bersifat kritikal dan rahasia. Sudah ada pengendalian terhadap layanan IT dan infrastruktur agar dapat secara tepat menahan dan pulih dari kegagalan/gangguan/kerusakan yang disebabkan oleh kesalahan, serangan yang disengaja atau bencana. Masih terus berusaha untuk menjaga dan melindungi semua aset-aset IT. Sudah ada pengendalian lingkungan fisik.

13. **DS13 Mengelola operasi/proses**

    Kecelakaan operasional memang terkadang berpengaruh terhadap tingkat layanan namun hal itu telah diupayakan seminimal mungkin dapat

dihindari dan telah ada upaya pengendalian akan adanya kecelakaan operasional. Sudah ada kendali terhadap layanan IT dan infrastruktur agar dapat secara tepat menahan dan pulih dari kegagalan/gangguan/kerusakan yang disebabkan oleh kesalahan, serangan yang disengaja atau bencana. Adanya kepuasan dari end user atas adanya penawaran layanan dan tingkat layanan. Layanan IT yang dibutuhkan dapat disediakan sesuai dengan permintaan user.

4.2 Temuan – Rekomendasi

Proses audit sistem informasi yang dilakukan di Bagian Akademik STIKOMP Surabaya didapatkan bahwa kebanyakan aktivitas TI yang dilakukan sudah mempunyai pengendalian yang baik. Berdasarkan analisa *maturity level* sub domain DS3 mengelola kinerja dan kapasitas, DS4 memastikan keberlangsungan layanan, dan DS5 memastikan keamanan sistem-sistem sudah sesuai dengan standar sehingga harus dipertahankan dan tetap dilaksanakan. Namun selain ditemukan keberhasilan yang telah dilaksanakan, masih terdapat beberapa temuan yang masih perlu diperbaiki. Temuan tersebut diadakan analisa sebab dan akibat, serta diberikan rekomendasi untuk dilaksanakan agar proses TI yang lain bisa lebih baik dan sesuai standar COBIT 4.0. Daftar temuan dan rekomendasi pada tabel 4.6.