AUDIT PENERAPAN TEKNOLOGI INFORMASI BERBASIS RISIKO DENGAN *FRAMEWORK* COBIT VERSI 4.1 DI PERGURUAN TINGGI XYZ

[1]Murahartawaty, [2]Candra Widya Iswara, [3]Ibnu Asror
[1,2,3]Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
[1]murahartawaty@gmail.com, [3]asror_182@yahoo.co.id

***Abstrak*—Perguruan Tinggi XYZ merupakan Perguruan Tinggi yang menerapkan Teknologi Informasi (TI) dalam menunjang kegiatan operasionalnya. "Penguatan Sistem Penjaminan Mutu Melalui Implementasi Tata Kelola Sesuai Prinsip *Good University Governance*" merupakan salah satu strategi Perguruan Tinggi XYZ ke depan, untuk itu tata kelola TI (*IT Governance*) harus segera diwujudkan. Masalah mendasar terkait *IT Governance* di Perguruan Tinggi XYZ saat ini adalah belum adanya pemahaman yang jelas terkait manajemen risiko TI dan pengukuran terhadap kinerja proses TI belum dilakukan. Berdasarkan kondisi tersebut perlu dilakukannya audit penerapan TI untuk mengevaluasi kontrol–kontrol TI serta mengetahui *maturity* level TI. Audit didukung dengan *Control Objective for Information and Related Technology* (COBIT) versi 4.1 dan *Risk IT Framework*. Proses–proses TI yang akan diaudit yakni PO2, PO3, PO7, PO8, PO9, AI1, AI2, AI4, AI6, AI7, DS1, DS3, DS4, DS5, DS8, DS11, DS12, ME2. Audit ini terdiri dari 3 proses yakni pre audit, *field work*, dan *reporting*. Hasil audit menunjukkan bahwa *maturity* level penerapan TI di Perguruan Tinggi XYZ adalah 11% level *Non Existent*, 17% level *Initial* / Ad hoc, 33% level *Repeatable but Intuitive*, 39% level *Defined*, 0% level *Managed* and *Measurable* dan 0% level 5 *Optimized*. Rekomendasi perbaikan disusun berdasarkan periode yakni periode I (2014 – 2015) dan periode II (2015 – 2017) dan periode III (2017 – 2018).**

Kata kunci*—Audit Teknologi Informasi, COBIT, IT *Risk*, IT *Governance

I. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) yang sangat pesat dewasa ini telah menjadi bagian penting dari organisasi. Keuntungan yang dapat dirasakan dengan jelas adalah penurunan biaya usaha dengan tingkat pelayanan membaik, kepuasan meningkat, dan omset meningkat tinggi. Hal ini menyatakan bahwa penerapan TI sangat mendukung kinerja suatu organisasi, di mana inovasi TI sebagai faktor penting[1]. Oleh karena itu, TI mulai dikembangkan untuk pendidikan Perguruan Tinggi (PT) untuk mendukung kegiatan operasional seperti administrasi, belajar mengajar, melakukan riset, mengembangkan TI dengan menghasilkan *software* dan *hardware*, dan menghasilkan Sumber Daya Manusia (SDM) yang menguasai TI[9]. TI di Perguruan Tinggi bertujuan untuk menyampaian informasi yang cepat dan mudah sehingga mutu layanan akademik berbasis TI meningkat dan para pengguna merasa puas.

Direktorat Jenderal Pendidikan Tinggi, Kementerian Pendidikan dan Kebudayaan (Kemdikbud) terus berupaya meningkatkan tata kelola perguruan tinggi demi ketertiban dan keteraturan PT tersebut. Rencana strategis perguruan tinggi harus dalam bentuk dokumen tertulis, sehingga dapat memenuhi prinsip transparansi.

Budaya dokumen tertulis dari setiap aktivitas, standar operasional prosedur, dan tata kelola perguruan tinggi sangat penting dalam perkembangan dan kemajuan perguruan tinggi ke depan[6]. Demikian halnya dengan TI, agar TI dapat dimanfaatkan seoptimal mungkin untuk kepentingan strategi bisnis, maka tata kelola TI harus diperhatikan dengan baik[14]. Tata kelola TI (IT *Governance*) merupakan bagian yang terintegrasi dengan tata kelola perusahaan dan berisi kepemimpinan dan struktur serta proses organisasi yang menjamin bahwa organisasi TI mengandung dan mendukung strategi dan tujuan bisnis.

Perguruan Tinggi XYZ merupakan salah satu PT swasta di Indonesia yang menerapkan TI. Segenap civitas akademika memerlukan informasi yang memadai untuk menunjang aktifitasnya. Terdapat bagian Sistem Informasi (SISFO) yang memiliki peran untuk pemenuhan kebutuhan akan informasi dengan pengembangan dan pelayanan TI untuk pengolahan data, sehingga SISFO merupakan hal yang vital bagi Perguruan Tinggi XYZ[11]. Salah satu strategi Perguruan Tinggi XYZ ke depan adalah "*Penguatan Sistem Penjaminan Mutu Melalui Implementasi Tata Kelola Sesuai Prinsip Good University Governance*"[3], untuk itu IT *Governance* harus segera diwujudkan. Namun berdasarkan observasi awal terkait IT *Governanace* yakni belum adanya pemahaman yang jelas terkait risiko TI, transparansi akan risiko signifikan terhadap proses bisnis SISFO, dan tanggung jawab pengelolaan risiko TI. Selain itu, pengukuran terhadap kinerja proses TI belum dilakukan karena fokus perhatian masih terpusat pada pengembangan aplikasi / sistem informasi dan infrastruktur akibatnya pengukuran terhadap penerapan TI kurang mendapatkan perhatian. Oleh karena itu, perlu dilakukan evaluasi terhadap implementasi tata kelola TI yakni audit penerapan TI.

Audit memiliki peranan penting dalam pengimplementasian IT *Governance* organisasi. Besarnya risiko yang mungkin muncul akibat penerapan TI membuat audit ini menjadi sangat penting dilakukan[10]. Tidak hanya itu,

hasil dari audit tersebut dapat digunakan untuk mengukur tingkat kematangan TI di Perguruan Tinggi XYZ dan rekomendasi untuk mencapai *World Class University*. Audit yang dilakukan akan menggunakan *control practices* yang terdapat pada *framework* COBIT (*Control Objective for Information and Related Technology)* Versi 4.1. Tabel 1 berikut merupakan perbandingan *framework* yang telah diimplementasikan oleh ribuan organisasi dengan berbagai ukuran bisnis.

TABEL 1
PERBANDINGAN COBIT, ITIL, ISO 27001[8]

Area	COBIT	ITIL	ISO 27001
Fungsi	Mapping Proses TI	Mapping Manajemen *Service* Level TI	*Framework* Keamanan Informasi
Tujuan	Menyediakan kerangka kerja control internal TI untuk mendukung tata kelola TI	Meningkat-kan efisiensi operasional TI dan kualitas layanan pelanggan	Mendukung realisasi dan implementasi sistem manajemen keamanan informasi perusahaan
Area	4 Proses dan 34 Domain	9 Proses	10 Domain
Issuer	ISACA	OGC	ISO Board
Implementation	Audit Sistem Informasi	Mengelola *Service* Level	Kepatuhan kepada standar keamanan

ITIL (*Information Technology Infrastructure Library)* bertujuan peningkatan efisiensi operasional TI dan kualitas layanan pelanggan[10]. ITIL tidak menyediakan panduan pengeloolaan TI yang memenuhi kebutuhan di tingkat yang lebih tinggi. ISO 27001 merupakan dokumen standar sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha penerapan konsep-konsep keamanan informasi di organisasi[10]. Sedangkan COBIT berfokus pada definisi, implementasi, audit, pengukuran dan peningkatan kontrol pada proses tertentu IT yang mencakup seluruh siklus hidup TI[7]. COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja yang memastikan bahwa TI selaras dengan kebutuhan bisnis, TI yang mendukung bisnis dengan lebih baik dan mampu memaksimalkan manfaat, pengunaan sumber saya TI yang bertanggung jawab serta risiko TI dikelola dengan tepat. PT perlu mengelola dan mengontrol IT *resources* dengan menggunakan kumpulan proses untuk menyampaikan informasi yang diperlukan. Sebagian besar, TI yang diterapkan di PT merupakan aset yang berharga karena dapat mendukung kinerja PT. Dengan demikian PT dapat memahami dan mengelola risiko-risiko yang berhubungan, seperti peningkatan pemenuhan pengaturan dengan banyaknya proses bisnis yang secara kritikal bergantung terhadap TI[11]. Oleh karena itu, sesuai dengan tujuan audit yang dilakukan adalah untuk mengukur kematangan TI dan karaktristik COBIT maka *framework* COBIT adalah pilihan yang efektif untuk membantu dalam proses audit ini.

Setiap proses bisnis memiliki risiko, demikian halnya dengan proses TI. Risiko yang terkait dengan TI yakni IT *Risk* (risiko TI) adalah risiko bisnis yang terkait dengan penggunaan, kepemilikan, pengoperasian, keterlibatan, pengaruh dan penerapan TI dalam suatu organisasi. Risiko TI menjadi bahan pertimbangan prioritas proses TI yang akan diaudit. Oleh karena itu, digunakan audit berbasis risiko yakni audit yang dilakukan berdasarkan proses-proses yang memiliki potensi risiko yang tinggi atau pada proses kritikal yang berdampak negatif jika terjadi masalah. Dalam melakukan analisis risiko didukung oleh *Risk* IT *Framework* yang menyediakan *framework* untuk mengidentifikasi, mengendalikan, dan mengelola risiko TI. Domain yang digunakan adalah domain *Risk Evaluation*. Kombinasi dari COBIT Versi 4.1 dan *Risk* IT sangat cocok digunakan dalam audit penerapan TI di Perguruan Tinggi XYZ karena audit akan lebih terfokus pada proses kritikal dan tidak terjebak pada proses yang kurang berisiko.

Untuk itu, rumusan masalah dalam penelitian ini adalah bagaimana tingkat kematangan TI di Perguruan Tinggi XYZ dari hasil audit TI berbasis risiko dengan *framework* COBIT Versi 4.1 dan bagaimana rekomendasi dari hasil audit TI untuk meningkatkan performansi TIdi Perguruan Tinggi XYZ. Manfaat yang akan diperoleh dari penelitian ini adalah memperoleh hasil evaluasi yang dapat digunakan untuk menyelaraskan TI dengan tujuan Perguruan Tinggi XYZ, membangun kesadaran dan tanggung jawab atas risiko TI, meningkatkan performansi IT untuk menuju *World Class University*, dan persiapan menghadapi audit eksternal.

II. TINJAUAN PUSTAKA

A. Audit Berbasis Risiko

Audit Berbasis Risiko adalah metodologi pemeriksaan yang dipergunakan untuk memberikan jaminan bahwa risiko telah dikelola di dalam batasan risiko yang telah ditetapkan manajemen pada tingkatan korporasi[2]. Ada 2 hal utama yang harus dipahami oleh internal auditor yakni aspek pengendalian dari setiap proses bisnis yang terkait, dan risiko serta faktor-faktor pengendalian guna mendukung pencapaian sasaran perusahaan.

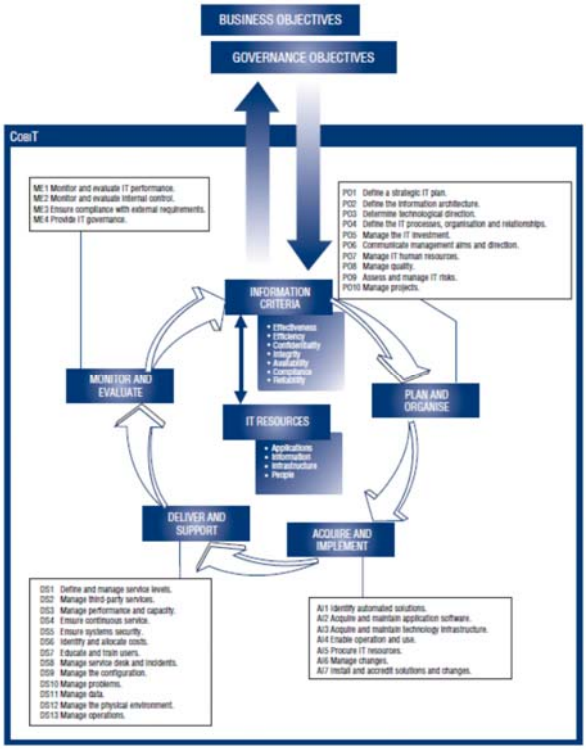
1. COBIT Versi 4.1

Control Objective for Information and Related Technology, disingkat *COBIT*, adalah suatu panduan standar praktik manajemen teknologi informasi. Secara umun *COBIT* dirancang sebagai alat *IT Governance* yang dapat membantu dalam pemahaman dan manajemen risiko dan *benefit* sehubungan dengan informasi dan TI terkait. Seperti Gambar 1 digambarkan bahwa *COBIT* memiliki 4 cakupan domain yakni sebagai berikut:

1. *Plan and Organise (PO),* domain ini mencakup level strategis dan taktis, dan konsennya pada identifikasi cara TI yang dapat menambah pencapaian terbaik tujuan-tujuan bisnis.
2. *Acquire and Implement(AI)***,** untuk merealisasikan strategi TI, solusi TI yang perlu diidentifikasikan, dikembangkan atau diperlukan, juga diimplementasikan dan

diintegrasikan dalam proses bisnis.

3. *Deliver and Support (DS)* domain ini menyangkut penyampaian aktual dari layanan yang diperlukan, dengan menyusun operasi tradisional terhadap keamanan dan aspek kontinuitas sampai pada pelatihan, domain ini termasuk proses data aktual melalui sistem aplikasi, yang sering diklasifikasikan dalam pengendalian aplikasi.
4. *Monitor and Evaluate (ME)*, semua proses TI perlu dinilai secara teratur atas suatu waktu untuk kualitas dan pemenuhan kebutuhan pengendalian. Domain ini mengarahkan kesalahan manajemen pada proses pengendalian organisasi dan penjaminan independen yang disediakan oleh audit internal dan eksternal atau diperolah dari sumber alternatif.



Gambar 1 *Framework* COBIT versi 4.1

1. *Maturity Model*

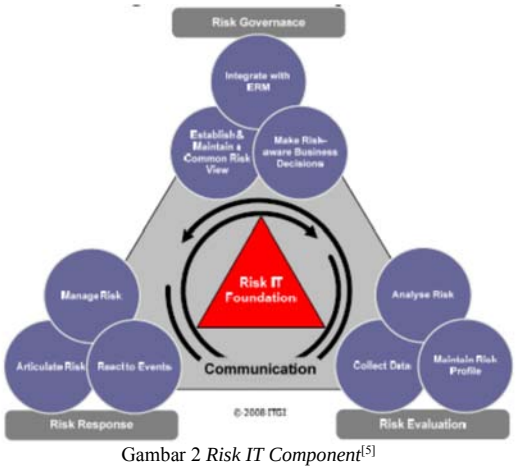
Dalam ISAC Foundation (2007), untuk memetakan status kematangan proses - proses TI, berikut adalah penjelasan lebih rinci mengenai skala 0 – 5:

- Skala 0 (*Non-Existent*)
  Sama sekali tidak ada proses TI yang diidentifikasi. Perusahaan belum menyadari adanya isu yang harus dibahas.
- Skala 1 (*Initial*)
  Perusahaan sudah mulai mengenali proses TI di perusahaannya, belum ada standarisasi, dilakukan secara individual, dan tidak terorganisasi. Tidak ada proses yang baku, sebagai gantinya ada pendekatan khusus yang cenderung diterapkan per kasus. Pendekatan manajemen secara keseluruhan masih belum terorganisasi.
- Skala 2 (*Repeatable but Intuitive)*
  Perusahaan sudah mulai memilliki prosedur dalam proses TI tetapi tidak ada pelatihan dan komunikasi formal tentang prosedur standar tersebut. Tanggung jawab terhadap proses tersebut masih dibebankan pada individu dan tingkat ketergantungan pada kemampuan individu sangat besar sehingga terjadi kesalahan.
- Skala 3 (*Defined Process*)
  Prosedur di perusahaan sudah distandarisasi, terdokumentasi, dan dikomunikasikan melalui pelatihan tetapi implementasi masih tergantung pada individu apakah mau mengikuti prosedur tersebut atau tidak. Prosedur yang dibuat tersebut tidak rumit, hanya merupakan formalisasi kegiatan yang sudah ada.
- Skala 4 (*Managed and Measurable*)
  Perusahaan dapat mengukur dan memonitor prosedur yang ada sehingga mudah ditanggulangi jika terjadi penyimpangan. Proses yang ada sudah berjalan dengan baik dan konstan. Otomasi dan perangkat TI yang digunakan terbatas.
- Skala 5 (*Optimized*)
  Proses yang ada sudah mencapai *best practice* melalui proses perbaikan yang terus menerus. TI sudah digunakan terintegrasi untuk otomatisasi proses kerja dalam perusahaan, meningkatkan kualitas, efektivitas, serta kemampuan beradaptasi terhadap perusahaan.

Dengan menggunakan *maturity model* di atas untuk tiap-tiap proses dari 34 proses TI, manajemen dapat memetakan : (1) Status organisasi saat ini, (2) Status *best in class* di industri sekarang sebagai perbandingan, (3) Strategi organisasi untuk peningkatan posisi yang ingin dicapai organisasi.

2. *Risk IT Framework*

Risk IT *Framework* melengkapi COBIT dalam menyediakan *framework* yang komprehensif untuk mendukung TI yang berkualitas tinggi. *Risk* IT merupakan suatu set praktik terbaik untuk meningkatkan manajemen risiko dengan menyediakan *framework* untuk mengidentifikasi, mengendalikan dan mengelola risiko TI. Gambar 2 berikut adalah gambar *Risk* IT *Framework*.



Gambar 2 *Risk IT Component*[5]

B. *IT Balanced Scorecard*

Berikut adalah penjelasan mengenai empat prespektif *IT BSC* yakni[16]:

1. Perspektif kontribusi organisasi (*corporate contribution*) adalah perspektif yang mengevaluasi kinerja TI berdasarkan pandangan dari manajemen eksekutif, para direktur dan *shareholder*.
2. Perspektif orientasi pengguna *(user orientation)* adalah perspektif yang mengevaluasi kinerja IT berdasarkan cara pandang pengguna bisnis dan lebih jauh lagi adalah pelanggan dari unit bisnis yang ada. Dalam perspektif ini organisasi melakukan identifikasi pelanggan dan segmen pasar yang akan dimasuki.
3. Perspektif keunggulan operasional *(operational excellence)* adalah perspektif yang menilai kinerja IT berdasarkan cara pandang manajemen IT itu sendiri dan lebih jauh lagi adalah pihak yang berkaitan dengan audit dan pihak yang menetapkan aturan-aturan yang digunakan.
4. Perspektif orientasi dimasa depan (*future orientation*) adalah perspektif yang menilai kinerja IT berdasarkan cara pandang dari departemen itu sendiri, yaitu :pelaksanaan, para praktisi, dan profesional yang ada. Kemampuan organisasi untuk dapat menghasilkan produk atau jasa di masa mendatang dengan kemampuan layanan yang memuaskan harus dipersiapkan mulai dari saat ini.

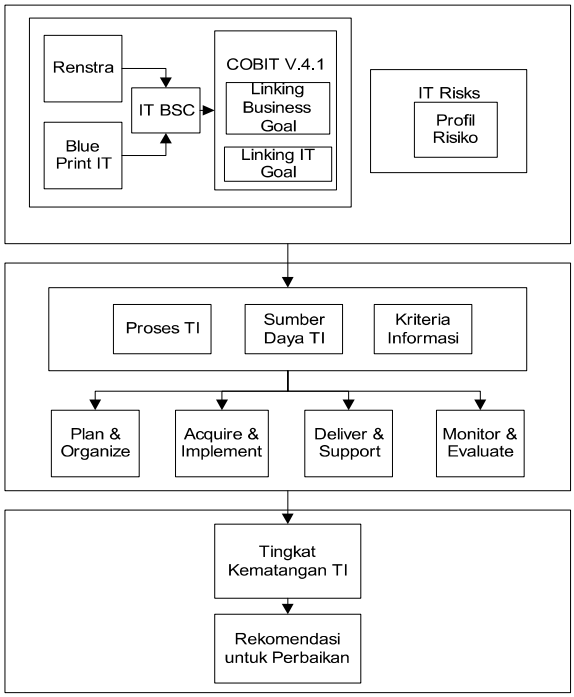
III. METODE PENELITIAN

Rencana strategis dan *Blueprint IT* digunakan sebagai landasan untuk penentuan tujuan bisnis dalam setiap prespektif *IT BSC* yakni prespektif kontribusi bisnis, orientasi pengguna, keunggulan operasional dan orientasi masa depan. Tujuan bisnis ini dihubungkan dengan tujuan TI yang ada di *COBIT*. Setiap proses dari TI memiliki risiko–risiko yang berpotensi menghambat kelancaran proses tersebut atau bahkan dapat mempengaruhi tercapainya tujuan dari penggunaan TI maupun tujuan bisnis Perguruan Tinggi XYZ. Sehingga dilakukan analisis risiko dengan dukungan *Risk IT Framework* yakni domain *Risk Evaluation (RE)* yang menghasilkan profil risiko.

Tujuan bisnis Perguruan Tinggi XYZ yang sesuai dengan hasil pemetaan *COBIT* dikombinasikan dengan hasil analisis risiko sehingga diperoleh komponen yang akan diaudit yakni domain *Plan and Organise*, *Acquire and Implement*, *Deliver and Support*, dan *Monitor and Evaluate*. Pada setiap domain memiliki proses TI , kriteria informasi, dan sumber daya TI yang meliputi aplikasi, informasi, manusia, dan infrastruktur masing-masing. Dari penilaian setiap domain inilah akan dihasilkan skor untuk kematangan TI. Skor ini digunakan untuk mengetahui tingkat kematangan TI saat ini sehingga dapat digunakan dalam menentukan rekomendasi untuk perbaikan (*Opportunities For Improvement*).

Gambar 3 sebagai berikut menunjukkan model konseptual dalam penelitian seseuai dengan penjelasan di atas. Berikut adalah langkah-langkah pelaksanaan audit dalam penelitian ini.

1. Pre audit yang meliputi penentuan tujuan, analisis risiko, *mapping* renstra dan *blueprint* IT ke COBIT versi 4.1, identifikasi proses yang akan diaudit, perancangan program audit yang meliputi prosedur audit dan *form* wawancara serta *checklist maturity level.*
2. *Field work* yakni pelaksanaan audit dengan wawancara dan observasi, melakukan penilai*an maturity level* proses TI, mengidentifikasi temuan.
3. Reporting yakni proses pelaporan hasil audit meliputi penentuan rekomendasi serta penyusunan Laporan Hasil Audit (LHA).



Gambar 3 Model Konseptual

IV. PELAKSANAAN DAN HASIL

A. *Identifikasi Proses yang Diaudit*

Pelaksanaan audit dimulai dengan tahap pre audit yakni perencanaan proses yang diawali dengan analisis risiko dengan dukungan *Risk IT Framework* dengan domain *Risk Evaluation.* Berdasarkan profil risiko yang diperoleh diketahui bahwa proses bisnis kritikal adalah registrasi, proses terkait infrastruktur dan layanan. Aset kritikal meliputi perangkat jaringan, dan aplikasi akademik di Perguruan Tinggi XYZ. Hasil *mapping* renstra dan *blueprint* IT ke dalam setiap prespektif BSC pada COBIT sebagian besar terdapat pada prespektif internal. Kemudian akan dilakukan *mapping* terkait tujuan bisnis dan tujuan TI.

Profil risiko akan dikombinasikan dengan hasil *mapping* untuk diperoleh proses yang akan diaudit yakni sebagai berikut:

a) Me-*review* pengelolaan risiko bisnis yang terkait dengan TI yang meliputi proses PO9, AI6, AI7, DS4, DS5, DS11, DS12, ME2.
b) Me-*review* peningkatan pelayanan terhadap *user* yang meliputi PO8, DS1, DS3, DS4, DS8.
c) Pembangunan ketersediaan dan kontinuitas layanan TI yang

meliputi DS3, DS4, DS, DS8, AI6.

d) Me-*review* peningkatan dan pemeliharaan fungsionalitas proses bisnis yakni pengembangan TI yang efektif dan efisien untuk meningkatkan kualitas operasional yang didukung oleh infrastruktur dan lingkungan yang memadai yang meliputi PO2, PO3, AI1, AI2, AI4.

e) Me-*review* perolehan dan pemeliharaan *skill* dan SDM yang termotivasi agar tercipta SDM yang berkualitas dan kuantitas yang sesuai untuk menghasilkan riset–riset unggul yakni proses PO7.

V. PELAKSANAAN AUDIT DAN PENILAIAN *MATURITY LEVEL*

Pelaksanaan audit dilakukan dengan melakukan wawancara, observasi, mengisi form *checklist maturity level* proses TI. Pemeriksaan dilakukan disetiap *control* pada proses TI dengan melihat bukti-bukti yang ada seperti dokumen SOP, kebijakan dan lain-lain. Gambar 4 berikut adalah contoh *form checklist maturity level.*

PO9 Asses and Manage IT Risk

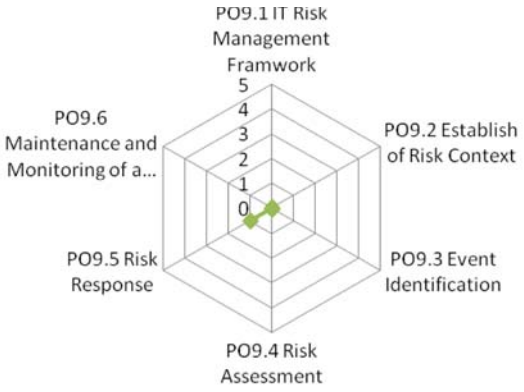
No	Statement	Cobit Ref.	Assessment						Responsibility			
			Non Existent	Initial / Ad hoc	Repeatable but Intuitive	Defined	Managed and Measurable	Optimized	Head of SISFO	SIDNAI	SIDA	BANGSI
			0	1	2	3	4	5				
1	Membangun *framework* manajemen risiko TI yang selaras dengan manajemen risiko organisasi.	PO9.1	√						X			
2	Membangun ruang lingkup untuk penilaian risiko untuk memastikan hasil yang tepat.	PO9.2	√						X			
3	Mengidentifikasi kejadian yang memiliki potensi berdampak negative pada organisasi.	PO9.3	√						X			
4	Melakukan penilaian risiko secara regular terhadap proses – proses TI yang berisiko operasional.	PO9.4	√						X			
5	Mengembangkan dan memelihara respon risiko yang mengidentifikasi strategi risiko.	PO9.5		√					X			

Gambar 4 Form *Checklist Maturity Level*

Dari hasil checklist akan dilakukan perhitungan *maturity level* proses TI, Tabel 2 berikut ini merupakan contoh perhitungannya dan Gambar 5 adalah representasi dari hasil penilaian *Maturity* Level.

TABEL 2
PERHITUNGAN *MATURITY LEVEL*

PO9 Assess and Manage IT Risks	***Maturity Level***
PO9.1 IT Risk Management Framwork	0
PO9.2 Establish of Risk Context	0
PO9.3 Event Identification	0
PO9.4 Risk Assessment	0
PO9.5 Risk Response	1
PO9.6 Maintenance and Monitoring of a Risk Action Plan	0
Average	**0.17**



Gambar 5 Diagram Radar Maturity Level

VI. IDENTIFIKASI TEMUAN

Bersamaan dengan pelaksanaan audit dilakukan identifikasi temuan baik yang sesuai dan tidak sesuai berdasarkan *maturity level* proses tersebut serta melihat *maturity model* di setiap proses pada COBIT versi 4.1, sehingga proses yang berada pada level 0 hingga 2 akan dikelompokkan menjadi temuan tidak sesuai dan level 3 hingga 5 menjadi temuan sesuai.

Berikut adalah temuan sesuai :

a) Terdapat arsitektur informasi yang tercantum dalam *Blueprint* TI.

b) Terdapat perencanaan arah teknologi yang akan digunakan sesuai dengan strategi TI dan arsitektur sistem

c) Sesuai dengan peran unit dalam proses rekruitasi, sudah dijalankan dengan baik dan sudah terdapat *training* personil untuk memelihara *skill*, kemampuan, *internal control.*

d) Proses pengembangan dan pemeliharaan sistem informasi sudah berjalan dengan baik. Pengelolaan perubahan sistem informasi telah diterapkan dengan baik. Dokumentasi terkait pengembangan sistem informasi sudah tersedia.

e) Semua sistem informasi / aplikasi telah memiliki user manual.

f) Sudah terdapat proses dalam memastikan kecukupan *acceptance testing*. Sudah terdapat pendokumentasian dalam *acceptance testing*. Sudah dilakukan *monitoring* terhadap operasional sistem

g) Sudah terdapat pengelolaan *sevice desk* dan insiden yang terstandarisasi dengan adanya prosedur yang terdokumentasi.

Berikut adalah temuan tidak sesuai:

a) Tidak terdapat *Quality Management System* terkait dengan TI, serta tidak terdapat panduan formal untuk melakukan penilaian kualitas TI

b) Tidak terdapat proses manajemen risiko meliputi perencanaan risiko, penilaian risiko, mitigasi risiko dan sosialiasasi penanganan risiko di seluruh aktivitas proses TI. Belum terdapat panduan untuk manajemen risiko. Belum tersedianya dokumentasi terkait proses manajemen risiko.

c) Tidak terdapat analisis risiko dalam proses penentuan solusi.
d) Tidak terdapat manajemen perubahan yang terdokumentasi untuk infrastruktur TI.
e) Tidak terdapat pengelolaan terkait *Service Level Management (SLM).*
f) Tidak terdapat perencanaan performansi dan kapasitas TI, serta tidak terdapat panduan untuk pengelolaan performansi dan kapasitas TI.
g) Tidak terdapat *Business Continuity Plan (BCP)* yang terdokumentasi dan tidak terdapat *IT Service recovery* and *resumption plan* yang terdokumentasi.
h) Tidak terdapat *IT Security Police* yang terdokumentasi dan tidak terdapat sosialisasi kebijakan TI secara formal.
i) Tidak terdapat prosedur terdokumentasi terkait *backup* dan restorasi data dan aplikasi.
j) Tidak terdapat prosedur terdokumentasi terkait pengelolaan lingkungan fisik.
k) Tidak terdapat prosedur terdokumentasi pelaksanaan monitoring secara kontinyu untuk meningkatkan kontrol TI.

VII. PENYUSUNAN REKOMENDASI PERBAIKAN

Sebelum menyusun rekomendasi dilakukan identifikasi SWOT (*Strength, Weakness, Opportunity* dan *Threat)* di setiap tujuan bisnis kemudian dilakukan analisis SWOT untuk menyusun strategi rekomendasi. Dalam penyusunan rekomendasi mempertimbangkan juga urutan prioritas rekomendasi yakni ditunjukkan pada Tabel 3 sebagai berikut.

TABEL 3
URUTAN REKOMENDASI

Tujuan Bisnis	*Maturity Level*	Ranking
Pengelolaan risiko bisnis terkait TI	1.75	2
Peningkatan pelayanan terhadap user	1.4	1
Pembangunan ketersediaan dan kontinuitas layanan TI	2	3
Peningkatan dan Pemeliharaan Fungsionalitas Proses Bisnis	2.8	4
Perolehan dan Pemeliharaan Skill dan SDM	2.86	5

Berdasarkan urutan tersebut maka tujuan bisnis yang paling rendah *maturity level* nya akan diprioritaskan untuk dilakukan perbaikan dengan mengimplementasikan rekomendasi yang telah disusun. Rekomendasi yang disusun diharapkan untuk dapat memperbaiki proses dalam mencapai level 3 hingga 5 yakni sebagai berikut.

A. Periode I (2014 – 2015)

Periode I dikatakan sebagai jangka pendek yakni jangka waktu 1 tahun ke depan. Pada periode ini diharapkan semua proses TI dapat mencapai *maturity level* 3 (*defined)* terlebih untuk proses yang masih berada pada *maturity level* 0 hingga *maturity level* 2. Beberapa rekomendasi yang harus dicapai pada periode I adalah sebagai berikut:

1. Melengkapi semua prosedur yang belum terdokumentasi terutama terkait pengembangan infrastruktur TI sesuai dengan target unit SISFO hingga akhir tahun 2012.
2. Menyusun *Quality Management System* (QMS)
   Berisi definisi, kriteria, perencanaan, prosedur kualitas yang sejalan dengan kebutuhan bisnis. *QMS* ini harus dipelihara, didokumentasikan dan dikomunikasikan secara reguler.
3. Menyusun *Service Level Management* (SLM) *Framework*
   Framework ini mencakup proses untuk menciptakan kebutuhan layanan, definisi layanan, SLA dan OLAs dan sumber pendanaan. Mendefinisikan struktur organisasi untuk manajemen tingkat layanan yang meliputi peran, tugas dan tanggung jawab internal dan eksternal penyedia layanan dan customer. Dalam hal ini penyedia layanan TI adalah SISFO dan customer adalah user/ unit.
4. Menyusun *Business Continuity Plan* (BCP)
   BCP disusun berdasarkan pemahaman risiko dari dampak bisnis yang potensial dan persyaratan untuk ketahanan, alternatif proses dan kemampuan pemulihan dari semua layanan TI yang kritikal. *BCP* harus mencakup panduan, peran dan tanggung jawab, prosedur, proses komunikasi dan pendekatan pengujian. Salah satu proses penting dalam *BCP* adalah penyediaan sistem *backup* dan *mirroring* yang telah menjadi Rencana Kerja Manajemen tahun 2012 unit SISFO.
5. Menyusun *IT Risk Management Framework*
   Panduan dalam mengelola risiko TI meliputi identifikasi, dampak dan kecenderungan risiko, beserta mitigasi risikonya, dan sebagai panduan untuk melakukan perencanaan, eksekusi, pelaporan penilaian risiko berdasarkan metode kualitatif dan kuantitatif. *Framework* ini harus selalu dipelihara dan dikomunikasikan.
6. Menyusun *IT Security Police*
   Berisi kebijakan-kebijakan keamanan sistem dengan melibatkan prosedur-prosedur terkait layanan, personil, *software,* dan *hardware* agar tindakan keamanan TI sejalan dengan kebutuhan bisnis. Kebijakan ini mendukung pembangunan data center yang sudah menjadi Rencana Kerja Manajemen tahun 2012 unit SISFO.
7. Menyusun *Monitoring of Internal Control Framework*
   Berisi definisi, kriteria, dan aksi-aksi untuk melakukan monitoring serta *self assessment* terhadap kontrol.
8. Mewujudkan *ERP-University* dengan mengintegrasikan sistem informasi akademik, non akademik dan pendukung.

B. Periode II (2015 - 2017)

Periode II merupakan periode jangka menengah, rekomendasi yang diberikan adalah bagaimana melakukan pengelolaan dan pengukuran proses TI yang telah berjalan dengan baik serta telah memiliki panduan dalam menjalankan proses tersebut. Pencapaian di periode II ini diharapkan dapat

meraih *maturity level* 4 *(Managed and Measurable*). Berikut adalah rekomendasi untuk periode II:

1. Mendefinisikan proses TI di Perguruan Tinggi XYZ yang bersifat kritikal secara reguler dengan dukungan penuh *stakeholder* dan kesepakatan dari pemilik proses bisnis yang relevan.
2. Melakukan penilaian atas kebutuhan kontrol berdasarkan kebijakan, panduan dan kematangan proses saat ini, melalui analisis pengukuran yang melibatkan *stakeholder* kunci.
3. Dalam setiap proses penilaian akuntabilitas harus jelas dan ditegakkan.
4. Menyusun strategi perbaikan yang sesuai dengan kasus bisnis yang dialami berdasarkan hasil penilaian.
5. Melakukan monitoring terhadap performansi dalam pencapaian hasil yang diinginkan secara konsisten sebagai bahan persiapan untuk memperoleh sertifikasi ISO 20000 dan 27001.

C. Periode III (2017 - 2018)

Periode III merupakan periode jangka panjang, rekomendasi lebih terarah pada optimasi proses – proses TI hingga mencapai *best practice* atau mencapai *maturity level* 5 *(Optimized)* dengan perbaikan terus menerus. Rekomendasi bersifat makro dan selaras dengan visi Perguruan Tinggi XYZ serta menyempurnakan pencapaian pada periode I dan II. Berikut adalah rekomendasi untuk periode III:

1. Dalam melakukan perubahan bisnis harus berdasarkan kritikalitas proses TI yang telah didefinisikan pada level 4 dan mencakup semua kebutuhan untuk menilai kembali kemampuan proses kontrol.
2. Pemilik proses TI secara reguler melakukan *self assessment* dengan metode *fishbone* dan SWOT untuk menegaskan bahwa kontrol berada pada tingkat kematangan yang tepat untuk memenuhi kebutuhan bisnis serta menemukan cara membuat kontrol tersebut lebih efektif dan efisien.
3. Perguruan Tinggi XYZ melakukan *benchmarking* pada *best practice* eksternal dan meminta saran dari pihak eksternal untuk efektifitas internal kontrol.

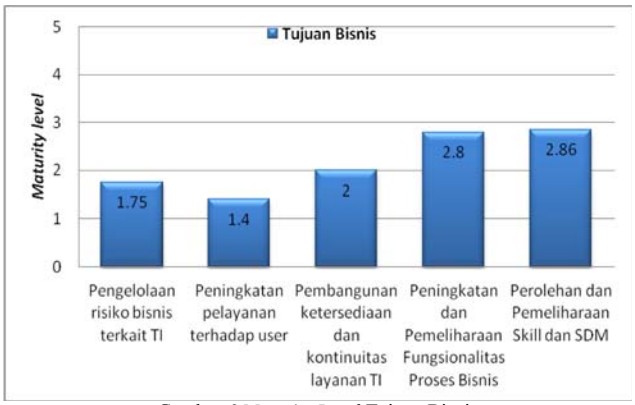
VIII. PENUTUP

A. Kesimpulan

Hasil audit penerapan TI berbasis risiko dan *framework COBIT* Versi 4.1 di Perguruan Tinggi XYZ menunjukkan bahwa tingkat kematangan proses TI terdiri dari:

1. Dua proses berada pada level 0 yakni PO9, DS1 dengan prosentase sebesar 11%.
2. Tiga proses berada pada level 1 yakni PO8, DS3, ME2 dengan prosentase sebesar 17%.
3. Enam proses berada pada level 2 yakni AI1, AI6, DS4, DS5, DS11, DS12 dengan prosentase sebesar 33%.
4. Tujuh proses berada pada level 3 yakni PO2, PO3, PO7, AI2, AI4, AI7, DS8 dengan prosentase sebesar 39%.

Sedangkan pencapaian *maturity level* di setiap tujuan bisnis digambarkan dalam Gambar 6 sebagai berikut.



Gambar 6 *Maturity Level* Tujuan Bisnis

Berdasarkan hasil audit disusun rekomendasi yang berupa rencana strategis TI berdasarkan jangka waktu tertentu yakni Periode I (2014 – 2015), Periode II (2015 - 2017), Periode III (2017 – 2018).

B. Saran

1. Bagi Perguruan Tinggi XYZ

a. Mengimplementasikan rekomendasi perbaikan dengan dukungan penuh dari semua pihak di Perguruan Tinggi XYZ sabagai persiapan audit eksternal.
b. Menyadari pentingnya perbaikan terus-menerus, dengan melakukan penilaian dan evaluasi, dapat diketahui kekurangan-kekurangannya sehingga dapat dilakukan perbaikan-perbaikan control untuk mencapai *IT Governance* yang baik pada khususnya dan *Good University Governance* pada umumnya.
c. Menambahkan bagian Audit TI di Sistem Penjaminan Mutu (SPM) Perguruan Tinggi XYZ sehingga review terkait TI dapat dilakukan secara reguler.
d. Menentukan metode dan target waktu untuk mencapai *maturity level* yang diharapkan.

2) Bagi penelitian selanjutnya:

a) Penelitan mengenai audit penerapan TI selanjutnya menggunakan COBIT Versi 5 atau kombinasi dari *framework* lain seperti ISO dan ITIL.
b) Pelaksanaan audit bekerja sama dengan pihak SPM Perguruan Tinggi XYZ untuk memudahkan proses audit.

DAFTAR PUSTAKA

[1] Anasthasia, Komang Isabella. "Teknologi Informasi Dalam Organisasi." Jimbaran, 2011.

[2] Christina, Diane. "Pemahaman Dasar Praktik Internal Audit ." Oktober 22, 2010. http://dianechristina.wordpress.com/2010/10/22/pemahaman- (accessed Juni 11, 2011).

[3] *Institut Teknologi Telkom.* Desember 6, 2010. http://www.ittelkom.ac.id/index.php?categoryid=12

(accessed Juni 8, 2011).
[4] ISACA. *ISACA.* http://www.isaca.org. (accessed 2011 - 2012).
[5] IT Governance Institute. "Risk IT Framework." Exposure Draft, United State of America, 2009.
[6] Kemendikbud. "Tata Kelola Perguruan Tinggi Terus Ditingkatkan." *Workshop Pemberdayaan Kelembagaan dan Peningkatan Tata Kelola Perguruan Tinggi Regional II.* Yogyakarta, 2012.
[7] Morency, John. *COBIT VS ITIL.* 2005.
[8] Priandono, Anjar. *Comparison between COBIT, ITIL and ISO27001.*
[9] Raharjo, Budi. "Pemanfaatan Teknologi Informasi di Perguruan Tinggi." *Sosialisasi Mengenai Implementasi Penerapan UU No. 19 Tahun 2002 Tentang Hak Cipta; Pemerintah Sebagai Panutan Dalam Ketaatan Lisensi Peranti Lunak.* Bandung, 2004.
[10] Sarno, Riyanarto. *Audit Sistem dan Teknologi Informasi.* Surabaya: ITS Press, 2009.
[11] Setiawan, Alexander. *Pengaruh Kematangan, Kinerja Dan Perkembangan Teknologi Informasi Di Perguruan Tinggi Swasta* . Surabaya: Universitas Kristen Petra.
[12] Setiawan, Erwin Budi. "Perancangan Strategis Sistem Informasi Perguruan Tinggi XYZ untuk Menuju World Class University." *Seminar Nasional Aplikasi Teknologi Informasi*, 2009: A-97.
[13] Setyobudi, Yayon Wahyu. "PEMODELAN 0DALAM PERENCANAAN AUDIT UMUM PADA DIVISI AUDIT INTERN (Studi Kasus pada PT Bank ABC Kantor Cabang Jakarta)." Tesis, 2006.
[14] Surendro, Kridanto. *Implementasi Tata Kelola Teknologi Informasi.* Bandung: Informatika, 2009.
[15] UPT SISFO. "Cetak Biru TIK." 2011.
[16] Wijaya, Rahmadi. "Analisis Model IT menggunakan Balanced ."
[17] Yayasan Pendidikan Telkom. "Struktur Organisasi dan Tata Kerja (SOTK) Institut Teknologi Telkom." Bandung,2010