AUDIT TATA KELOLA TEKNOLOGI INFORMASI DENGAN KERANGKA COBIT STUDI KASUS : PENERAPAN AUDIT TATA KELOLA TI PADA BANK XYZ OLEH DIVISI AUDIT INTERN

TESIS

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Magister Akuntansi

DWI PRIHATINI
0606148765

UNIVERSITAS INDONESIA
FAKULTAS EKONOMI
PROGRAM STUDI MAGISTER AKUNTANSI
JAKARTA
DESEMBER 2009

AUDIT TATA KELOLA TEKNOLOGI INFORMASI DENGAN KERANGKA COBIT STUDI KASUS : PENERAPAN AUDIT TATA KELOLA TI PADA BANK XYZ OLEH DIVISI AUDIT INTERN

TESIS

DWI PRIHATINI
0606148765

UNIVERSITAS INDONESIA
FAKULTAS EKONOMI
PROGRAM STUDI MAGISTER AKUNTANSI
JAKARTA
DESEMBER 2009

HALAMAN PERNYATAAN ORISINALITAS

Karya Akhir ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	:	Dwi Prihatini
NPM	:	0606148765
Tanda Tangan	:	
Tanggal	:	

HALAMAN PENGESAHAN

Tesis ini diajukan oleh

Nama	: Dwi Prihatini
NPM	: 0606148765
Program Studi	: Magister Akuntansi
Judul Tesis	: Audit Tata Kelola Teknologi Informasi dengan Kerangka COBIT Studi Kasus : Penerapan Audit Tata Kelola TI pada PT Bank XYZ oleh Divisi Audit Intern

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Akuntansi pada Program Studi Magister Akuntansi, Fakultas Ekonomi, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	: Novy G. A. Pelenkahu, MBA	( )
Penguji	: Dr. Yudho Giri Sucahyo	( )
Penguji	: Dr. Setyo Hari Wijanto	( )

Ditetapkan di : Jakarta
Tanggal : 1 Desember 2009

Mengetahui,
Ketua Program

Dr. Lindawati Gani
NIP. 196205041987012001

KATA PENGANTAR

Bismillahirrahmanirrahim.

Alhamdulillahirrabbil 'alamin. Puji dan syukur kehadirat Allah SWT, karena atas berkah, rahmat, pertolongan dan hidayah-Nya, saya dapat menyelesaikan Karya Akhir yang berjudul :

AUDIT TATA KELOLA TEKNOLOGI INFORMASI DENGAN KERANGKA COBIT

STUDI KASUS :
PENERAPAN AUDIT TATA KELOLA TI
PADA PT BANK XYZ OLEH DIVISI AUDIT INTERN

Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai penyusunan Karya Akhir ini, sangatlah sulit bagi saya untuk menyelesaikannya.

Pertama-tama rasa hormat dam ucapan terima kasih penulis sampaikan kepada Bapak Novy G.A Pelenkahu, MBA, selaku Dosen Pembimbing yang telah bersedia meluangkan waktu dan pikiran di tengah-tengah kesibukannya untuk memberikan bimbingan, pengarahan dan saran penulisan.

Penulis juga menghaturkan terima kasih kepada :

1. Pimpinan dan seluruh staf pengajar serta karyawan akademik, perpustakaan dan laboratorium komputer Program Magister Akuntansi UI yang semuanya telah memberikan arahan, dukungan dan semangat untuk terus giat belajar
2. Pimpinan dan Staf PT Bank XYZ yang tidak dapat saya sebutkan, yang sangat telah membantu memberikan pengumpulan data dan dukungannya
3. Mba Risna, untuk support dan bantuannya pada saat-saat genting
4. Teman kelompok belajar, Mba Kiki, Ica, Galih, Mba Debbi
5. Semua rekan-rekan mahasiswa Program Maksi FEUI, terutama teman-teman kelas F dan G Sore 2006/2007 dan kelas konsentrasi sistem informasi, serta kelas Statistika 2008

6. Teman-teman Penulis dimanapun berada yang selalu memberikan dukungan
7. *the last but not least*, Yayah, Mama, Mas Ardi, Mba Eka, Tri yang selalu mengingatkan dan mendukung serta memberikan doanya yang tiada terputus

Penulis menyadari bahwa Karya Akhir ini masih jauh dari sempurna, namun kiranya dapat bermanfaat bagi pihak-pihak yang membutuhkan. Segala kritik dan saran Penulis harapkan untuk menyempurnakan penulisan di masa mendatang.

Wassalamualaikum Wr .Wb
Jakarta, November 2009

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama	:	Dwi Prihatini
NPM	:	0606148765
Program Studi	:	Magister Akuntansi
Departemen	:	Akuntansi
Fakultas	:	Ekonomi Universitas Indonesia
Jenis Karya	:	Karya Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

Audit Tata Kelola Teknologi Informasi dengan
Kerangka COBIT

Studi Kasus :
Penerapan Audit Tata Kelola TI pada PT Bank XYZ oleh Divisi Audit Intern

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di :
Pada tanggal :
Yang Menyatakan

(DWI PRIHATINI)

ABSTRAK

Nama : Dwi Prihatini
Program Studi : Magister Akuntansi, Konsentrasi : Sistem Informasi

Judul : Audit Tata Kelola Teknologi Informasi dengan Kerangka COBIT
Studi Kasus :
Penerapan Audit Tata kelola TI pada PT Bank XYZ oleh Divisi Audit Intern

Karya Akhir ini membahas penerapan audit tata kelola TI dengan kerangka COBIT pada PT Bank XYZ oleh Divisi Audit Internal ("DAI"). Penulis juga memposisikan diri sebagai audit eksternal yang melakukan audit dengan *scope* yang terbatas terhadap tata kelola TI Perusahaan untuk menganalisis hasil audit yang dilakukan DAI tersebut. Pemaparan mengenai proses audit tatakelola TI diharapkan dapat memberikan gambaran kepada pembaca bagaimana suatu organisasi terutama perbankan melakukan audit tatakelola TI. Metodologi penulisan melalui studi literatur, melakukan tanya jawab, pemahaman atas dokumentasi terkait, pengisian kuisioner. Hasil yang didapatkan berupa paparan melakukan audit tata kelola TI, *maturity model level* TI PT Bank XYZ, rekomendasi.

Kata kunci :
COBIT, audit, tatakelola TI, *IT governance*, *Information technology*, TI, perbankan, *maturity model*, internal audit, ITGI, *control objectives*, tujuan TI, tujuan Perusahaan, program audit

ABSTRACT

Name : Dwi Prihatini
Study Program : Master of Accountancy, Concentration : Information System
Title : The Information Technology Governance Audit using COBIT Framework
Case Study : The Implementation of IT Governance Audit in PT Bank XYZ by Internal Audit Division

The focus of this study concerning the implementation of IT governance audit using COBIT frameworks in PT Bank XYZ by Internal Audit Division ("DAI"). The writer is also positioned as external auditor, performed the IT governance audit, with limited scope, in order to analyzed the IT audit's result done by DAI. This study is expected to make some clear description to the reader regarding the process of IT audit governance in banking industries. The methodology of the writing is through literatures study, interview, understanding documents, fulfilling questioners. The result of this study is to know how to perform IT governance audit based on COBIT framework, maturity model level, and some recommendations.

Key words :
COBIT, audit, IT governance, information technology, banking, maturity model, internal audit, ITGI, control objectives, IT objectives, Company objectives, audit program

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR RUMUS

DAFTAR LAMPIRAN

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kesuksesan perusahaan dapat dicapai dengan melakukan penyelarasan *objectives* perusahaan dengan *objectives* teknologi informasi ("TI")[1]. Banyak Perusahaan telah berinvestasi dengan nilai yang sangat tinggi pada TI dengan tujuan agar TI tersebut dapat memberikan manfaat yang sepadan. Penelaahan seperti audit ataupun *review* tata kelola TI pada perusahaan dianggap sebagai perangkat yang efektif untuk mengetahui sejauh mana dan bagaimana TI telah memberikan manfaat yang optimum untuk mendukung operasional perusahaan dan mencapai *value* yang diinginkan oleh para *stakeholder*-nya serta meminimalkan risiko TI yang berdampak pada Perusahaan.

Dalam mendukung suatu proses bisnis, teknologi informasi dapat dimungkinkan menjadi *enabler* dan *critical success factor*, yaitu faktor penyebab kesuksesan, karena pihak manajemen perusahaan sudah sangat tergantung dan mengandalkan TI yang memberikan informasi yang dibutuhkan dalam pencapaian *organization objectivities*.

Dan terlebih pada zaman yang telah memasuki era globalisasi, di mana hubungan antarmanusia dan organisasi di berbagai belahan dunia semakin dekat, dituntut sebuah keefektifan *(effectivity)* dan keefisienan *(efficiency)* dari pemerolehan sebuah informasi agar dapat diandalkan *(reliability)*, mempunyai integritas *(integrity)* dan mampu menjaga kerahasiaan *(confidentiality)*, tersedia pada saat dibutuhkan *(availability)*, dan taat (*comply)* terhadap aturan-aturan yang ada. Hal-hal di atas merupakan kriteria informasi yang berkualitas yang

[1] Teknologi informasi suatu organisasi berkaitan erat dengan sisi teknologi dari sebuah sistem informasi. Sistem informasi digunakan perusahaan untuk mengumpulkan, memproses, menyimpan dan menganalisa serta menyebarkan informasi untuk tujuan tertentu. Karena sistem, maka terdiri dari input, process dan output, serta feedback yang mengendalikan operasi, di dalamnya juga termasuk personil, prosedur, fasilitas fisik dan beroperasi dalam suatu lingkungan (Turban, Efraim, et al. *Information Technology for Management : Transforming Organizations in the Digital Economy 6th Edition.* John Wiley and Sons: 2008)

dicari perusahaan dan *value* inilah yang harus di-*deliver* oleh suatu teknologi informasi. Di sisi lainnya, TI juga mengandung risiko yang dapat menyebabkan *organization objectives* tidak tercapai. Sebut saja, kasus fraud, *Societe Generale*, salah satu bank terbesar di Prancis. Pada awal tahun 2008, Bank tersebut telah mengumumkan bahwa telah terjadi kerugian sebesar €4,9 miliar atau setara dengan Rp66,4 Triliun. Nilai kerugian tersebut merupakan salah satu yang terbesar sepanjang sejarah perbankan yang diakibatkan *fraud*. *Fraud* ini dilakukan oleh karyawan Societe Generale yang menjadi *trader* di bank tersebut. Ia menggunakan keahlian TI-nya serta memanfaatkan berbagai kelemahan internal TI perusahaan untuk melakukan transaksi derivatif fiktif. *Internal control* Perusahaan tidak mampu memberikan peringatan atau melakukan pencegahan terhadap transaksi fiktif tersebut.

Lain halnya lagi, Bank Sumitomo cabang Inggris, merugi sebesar 220 juta poundsterling setelah dikenai serangan *hacker*[2]. *Hacker* tersebut membobol Bank Sumitomo dengan cara menginfiltrasi sistem komputer bank, kemudian mentransfer sejumlah uang ke akun pribadinya.

Kemudian, pada pertengahan tahun 2007, organisasi bank dunia, World Bank, yang menyediakan sumber keuangan vital dan penyediaan bantuan teknik kepada negara berkembang di seluruh dunia telah diserang. Hampir lebih dari 40 server World Bank telah diinfiltrasi oleh *hacker*. Menurut beberapa pihak, World Bank tidak melaksanakan uji penilaian terhadap keamanan sistemnya.

Dengan demikian, ketika perusahaan telah menetapkan bahwa informasi serta sistem teknologi yang mendukungnya merupakan aset yang sangat vital, maka perusahaan harus berbuat sesuatu untuk melindungi informasi dan sistem teknologi tersebut, salah satunya adalah dengan melakukan usaha-usaha peningkatan pengendalian internal melalui tata kelola TI.

---

[2] *Hacker* adalah seseorang yang melakukan penetrasi terhadap sistem komputer secara ilegal dan dan tidak etis (Turban, Efraim, et al. *Information Technology for Management : Transforming Organizations in the Digital Economy 6th Edition*. John Wiley and Sons: 2008)

Tata kelola TI akan terus ada selama pencapaian strategis dan objektif perusahaan terus berkembang. Dan untuk pencapaian tersebut adalah melalui kepemimpinan, struktur organisasi dan proses TI. Suatu kerangka, yang dianggap tepat mewakili pengorganisasian atau tata kelola TI tersebut adalah COBIT *framework*. Dalam *Executive Overview* yang dikeluarkan ITGI, COBIT *framework* ("COBIT"), mempunyai tujuan diantaranya yaitu COBIT mendukung tata kelola TI atau *IT Governance*, COBIT menyediakan kerangka untuk mendapatkan jaminan bahwa TI selaras dengan bisnis dan TI memberdayakan kegiatan fungsi bisnis serta memaksimalkan *benefit*, sumber daya TI digunakan secara bertanggung jawab dan terdapat manajemen risiko yang dilakukan secara tepat atas TI.

Kemudian dalam kerangka pengendalian yang diperkenalkan COBIT, terdapat domain-domain yang setara dengan fungsi TI yang diperkenalkan oleh ilmu manajemen. Sehingga lebih mudah dipahami Perusahaan, karena sudah diterapkan di dalam Divisi Teknologinya yaitu *plan and organize (PO), acquire and implement (AI), deliver and support (DS)* serta *monitor and evaluate (ME)*. Dalam domain tersebut dibagi ke *level control objectives* dan *level control activities*.

COBIT *framework* mewakili standar yang dapat diaplikasikan secara umum dan telah diterima secara internasional sebagai *good practice* untuk *IT controls*, COBIT independen terhadap platform teknikal, berorientasi pada manajemen dan proses bisnis pemilik perusahaan, serta telah menjadi standar internasional *de facto* bagi *IT governance*.

Melihat tujuan dan kerangka COBIT tersebut di atas, perusahaan dapat mengimplementasikan COBIT sebagai alternatif metodologi *IT governance* untuk perlindungan aset informasinya dan sistem teknologinya.

Berbagai perusahaan yang ada di Indonesia dapat menerapkan COBIT, karena melihat *value* dan *benefit* bagi perusahaan. Khususnya, bagi sektor perbankan yang sangat erat kaitannya dengan pemanfaatan TI untuk mengakselerasi proses bisnisnya dan mengorganisasikan TI-nya. Dimana persaingan bank sekarang ini semakin ketat, TI harus berfungsi 24 jam dengan

berkembangnya *internet banking*, *sms banking*, ATM, dan sebagainya.Namun demikian, selain risiko yang dimunculkan oleh TI terhadap perusahaan juga semakin tinggi, seperti beberapa kasus di atas tadi, jika dilihat secara khusus pada sektor perbankan, terdapat risiko yang berasal dari karakteristik industri tersebut, jika dibandingkan dengan industri lainnya, karena ia *high regulated company* terkait dengan regulasi Bank Indonesia, kalangan internasional, hukum dan sebagainya. Dikarenakan juga karena transaksi harian yang sangat banyak *massive*, melewati batas-batas teritorial negara, dan juga variasi dari produk perbankan yang makin beragam dan mempunyai risiko sendiri. Timbulnya risiko ini menyebabkan semakin diperlukannya suatu manajemen risiko yang memadai, dan tentunya COBIT dengan sangat optimis mampu mengakomodasi semua kebutuhan tersebut.

COBIT memberikan panduan bagi para eksekutif perusahaan melalui *maturity model level* bagi TI, untuk mengetahui sampai di mana TI perusahaan berada, dan bagaimana TI telah mendukung berjalannya bisnis dalam memberikan informasi yang berkualitas, dan manajemen risiko dari TI itu sendiri.

Sebagaimana pengalaman sukses atas penerapan COBIT yang terjadi pada Kuwait Turkish-Participation Bank Inc[3]. Perusahaan perbankan tersebut pada awalnya menggunakan COBIT untuk memenuhi persyaratan dari regulator bank. Namun kemudian pada perjalanannya menemukan bahwa COBIT memberikan manfaat yang lebih, terutama dalam menyelaraskan perencanaan jangka panjang perusahaan dan juga memberikan bantuan bagi TI untuk mendesain dukungan bagi proses bisnis dan tujuannya. Alat kendali internal seperti kebijakan dan standar telah dikembangkan untuk mereduksi risiko agar mencapai level yang dikehendaki selain itu fungsi kualitas TI juga telah dibangun untuk memonitor perkembangan dari proses dan selaras dengan control COBIT.

[3] ISACA. *Case Study: Kuwait Turk Participation Bank Uses COBIT for Compliance and Reaps Additional Benefits*. 2008
<http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=31694>

Di sisi lainnya, terdapat audit teknologi informasi menggunakan COBIT. Ini merupakan evaluasi terhadap tata kelola TI perusahaan yang menggunakan kerangka COBIT. Perusahaan dapat melakukan audit tata kelola TI dengan tim audit internalnya, maupun audit eksternal untuk mendapatkan keyakinan yang memadai bahwa *IT governance* pada perusahaannya telah berjalan sesuai dengan *objective*-nya. Namun demikian, audit eksternal mempunyai keterbatasan dalam me-*review* COBIT, mengingat adanya hambatan waktu, *scope* dan *audit objectives* yang dimilikinya.

Selain itu terdapat evaluasi yang akan memberikan saran ataupun rekomendasi bagi tata kelola TI untuk dapat diperbaiki atau dikembangkan dengan tujuan agar *objectivities* perusahaan dapat tercapai, tentunya dengan memperhatikan risiko-risiko yang menjadi ancaman bagi perusahaan, sehingga terdapat keselarasan antara tujuan bisnis dengan tujuan TI. Sebagaimana yang selama ini diinginkan perusahaan.

PT Bank XYZ yang menjadi objek studi kasus Karya Akhir ini, telah menerapkan kerangka COBIT sebagai kerangka tata kelola TI. Walaupun belum lama diterapkan, kerangka ini diakui Perusahaan telah memberi manfaat bagi Perusahaan dalam menerapkan tata kelola TI yang lebih komprehensif, dan telah menyatukan bahasa antara Divisi Teknologi dan Informasi, Manajemen (pucuk pimpinan) juga termasuk Divisi Audit Intern dan Audit eksternal Perusahaan serta pihak regulator. PT Bank XYZ pun telah menerapkan audit tata kelola TI untuk mendapatkan arahan dan posisi TI yang tepat bagi Perusahaan dan juga memberikan perbaikan dan pengembangan TI Perusahaan secara berkesinambungan.

Berdasarkan hasil survey IT Governance Global Status Report 2008[4] dari Pricewaterhouse Cooper dan ITGI, TI telah berkontribusi sangat penting kepada sektor perbankan sebesar 77%. Hal ini membuktikan bahwa TI bagi perbankan mempunyai kaitan erat atas sumber kesuksesan objektif Perusahaan. Dengan demikian tata kelola atas TI di PT Bank XYZ perlu ditingkatkan.

[4] IT Governance Global Status Report 2008, PWC and IT Governance Institute

1.2 Permasalahan

Dari latar belakang permasalahan terlihat bahwa, peranan teknologi informasi telah memberikan manfaat bagi banyak kalangan, terutama bagi perusahaan. Namun selain manfaat, terdapat risiko yang begitu besar dalam penerapan TI ini. Diantaranya yaitu, investasi perusahaan terhadap TI yang lebih besar biayanya dibandingkan dengan *benefit* yang diberikan, gagalnya TI pada saat implementasi akibat kesalahan pada tahap perencanaan, tidak sesuainya arsitektur TI dengan yang diperlukan oleh perusahaan, TI tidak dapat dikendalikan secara memadai sehingga mengancam aset informasi perusahaan, mulai karena *human error* ataupun karena sistem TI yang tidak mampu mendukung pengendalian tersebut, serangan dari pihak luar, risiko gagal bisnis karena TI tidak mampu mendukung proses bisnis, dan lain sebagainya.

Menurut George Westerman dan Richard Hunter, diterjemahkan dari buku *IT Risk : Turning Business Threats into Competitive Advantage (2007)*[5], Harvard Business School, dari riset yang telah dilakukannya telah memperlihatkan bahwa sebagian besar *IT risk* yang terjadi bukan diakibatkan isu yang berasal dari bidang teknikal ataupun karyawan level bawah, namun berasal dari kesalahan pengawasan perusahaan dan proses tata kelola TI. Beberapa kesalahan menghasilkan serial keputusan yang tidak sesuai dan struktur TI yang sangat buruk menyebabkan tata kelola TI tidak efektif, kompleksitas TI yang semakin tidak terkendali, dan minim perhatian terhadap risiko.

Dengan kata lain, banyak risiko TI dihasilkan bukan dari teknologi itu sendiri namun berasal dari proses pengambilan keputusan yang melupakan bahaya yang akan menyerang bisnis perusahaan dari sisi pemanfaatan teknologi.

Audit terhadap tata kelola TI merupakan salah satu perangkat fungsi pengawasan bagi TI. Baik itu audit internal yang dilakukan oleh pihak divisi audit internalnya atau oleh audit eksternal. Hasil dari audit TI akan diberikan kepada pihak manajemen puncak sebagai sarana pemerolehan informasi terhadap

[5] Westerman, G., Richard Hunter. *IT Risk : Turning Business Threats into Competitive Advantage.* Boston, Massachusetts : Harvard Business School Press, *2007*

status TI pada perusahaannya dan pengetahuan untuk pengambilan keputusan yang strategis untuk merancang strategi bisnis dan TI.

Dengan demikian, karya akhir ini akan membahas audit tata kelola TI dengan menggunakan kerangka COBIT, dengan contoh penerapan di PT Bank XYZ oleh pihak divisi audit internal dan juga audit eksternal oleh pihak luar sebagai pihak yang independen. Sehingga akan menjawab pertanyaan :

1. Bagaimana penerapan audit tata kelola TI dengan kerangka COBIT di dalam industri perbankan khususnya yang dilakukan oleh audit internal dan bagaimana jika dilakukan oleh audit eksternal ?
2. Bagaimana langkah-langkah audit *IT governance* dengan menggunakan kerangka COBIT tersebut?
3. Bagaimana hasil *maturity model level* dalam PT Bank XYZ yang menjadi perangkat monitor manajemen terhadap status TI dan pemanfaatan pada masa sekarang dan masa depan?
4. Kemudian temuan serta rekomendasi apa yang mampu diberikan oleh audit tata kelola TI untuk meningkatkan dan mengembangkan TI Perusahaan agar TI menjadi *enabler* bagi bisnis ?

1.3 Tujuan Penelitian

Berikut tujuan penelitian yang diharapkan dari penulisan karya akhir ini :

1.3.1 Bersifat umum :

Studi ini bertujuan memberikan gambaran penerapan audit tata kelola teknologi informasi dengan menggunakan kerangka COBIT dalam industri perbankan baik dari sisi audit internal dan audit eksternal.

1.3.2 Bersifat Khusus :

1. studi ini bertujuan menelaah audit tata kelola Teknologi Informasi (TI) menggunakan kerangka COBIT pada PT Bank XYZ
2. memberikan rekomendasi kepada pihak Bank untuk meningkatkan pengembangan tata kelola teknologi informasi di perusahaan tersebut.

1.4 Manfaat Penelitian

Penelitian tata kelola audit teknologi informasi dengan menggunakan COBIT akan memberikan perluasan khazanah keilmuan terutama dalam bidang audit TI dan memberikan manfaat bagi Perusahaan berupa paparan dan rekomendasi. Dan juga memberi manfaat kepada Penulis dan Pembaca karya akhir ini.

1.5 Metode Penulisan

Metode penulisan pada awalnya, dilakukan dengan studi literatur dengan berbagai bahan teori dari *textbook* dan media internet. Selanjutnya, Penulis melakukan riset di PT Bank XYZ dengan melakukan wawancara atau tanya jawab, pengisian kuisioner, pemahaman dokumen, serta catatan yang diberikan PT Bank XYZ yang dengan ini diwakili oleh pihak Divisi Audit Intern ("DAI") dan Divisi Teknologi dan Informasi ("DTI"). Penulis melakukan praktek audit namun dalam lingkup yang terbatas.

1.6 Ruang Lingkup Penulisan

Ruang lingkup penulisan mencakup teori-teori mengenai audit tata kelola TI dengan melihat kerangka COBIT yang dikeluarkan oleh ITGI. Kemudian, dengan melakukan penelaahan pada PT Bank XYZ, bagaimana Bank tersebut melakukan audit tata kelola TI yang dilakukan oleh DAI yang mencakup hal-hal yang *unrestricted* atau diizinkan oleh pihak Bank dengan menelaah dokumentasi hasil audit, serta wawancara dan pengisian kuisioner. Maka dengan alasan tersebut, kekurangan dari penulisan mungkin dapat terjadi, terutama karena pembatasan hal-hal yang dianggap *confidential* bagi Perusahaan, seperti bukti-bukti audit, pembatasan terhadap akses dokumentasi, dan sebagainya padahal dibutuhkan untuk penulisan ini.

1.7 Sistematika Penulisan

BAB 1 PENDAHULUAN

1.1 Latar Belakang
1.2 Permasalahan
1.3 Tujuan Penelitian
1.4 Manfaat Penelitian
1.5 Metode Penulisan
1.6 Ruang Lingkup Penulisan
1.7 Sistematika Penulisan

BAB 2 LANDASAN TEORI

2.1 Pendahuluan : Hubungan Tata Kelola Perusahaan, Tata Kelola TI, Audit COBIT
2.2 Tata Kelola Perusahaan (*Corporate Governance*)
2.3 Tata Kelola TI (*IT Governance*)
2.4 COBIT, ISACA dan IT Governance Institute
2.5 COBIT *Framework*
2.6 Audit : Audit Internal, Audit Eksternal, Audit Teknologi Informasi
2.7 Langkah-langkah Audit
2.8 Bukti Audit
2.9 Audit Berbasis Risiko
2.10 *Internal Control* – COSO *Frameworks*
2.11 Industri Perbankan

BAB 3 GAMBARAN UMUM

3.1 Profil PT Bank XYZ
3.2 Rencana Strategis Teknologi Informasi PT Bank XYZ
3.3 Divisi Teknologi dan Informasi
3.4 Lingkungan Teknologi Informasi PT Bank XYZ
3.5 Audit TSI pada PT Bank XYZ
3.6 Proses Audit

BAB 3 GAMBARAN UMUM (lanjutan)

BAB 4 ANALISIS DAN HASIL AUDIT

BAB 5 KESIMPULAN DAN SARAN

BAB 2
LANDASAN TEORI

2.1 Pendahuluan : Hubungan Tata Kelola Perusahaan, Tata Kelola TI, Audit COBIT

Isu mengenai tata kelola perusahaan *(enterprise governance)* pada tataran dunia bisnis merupakan isu yang sedang hangat. Komite Nasional Good Governance yang terdiri dari pihak pemerintah RI, akademisi, pelaku bisnis, telah mengeluarkan pedoman mengenai *good corporate governance*-GCG (*enterprise governance*). Perusahaan dapat mengikuti pedoman yang didukung oleh pemerintah tersebut, karena tujuan *enterprise governance* akan memberikan *benefit* kepada semua pihak, tidak hanya para pemilik perusahaan (*shareholder*), namun juga para *stakeholder* (pemangku kepentingan), yang menjadi faktor pendukung suksesnya perusahaan juga.

Tata kelola TI (*IT Governance*) mempunyai hubungan yang erat dengan *corporate governance* ini. *IT Governance* berfungsi sebagai *enabler* yang mendampingi *corporate governance*, TI akan memberikan value kepada perusahaan untuk mencapai target tujuan (*objective*) yang ingin dicapai perusahaan. Hal itu akan dapat diwujudkan jika TI dapat dikelola dengan baik, ia memberikan manfaat karena memberi nilai tambah bagi perusahaan terutama meningkatkan *competitiveness* dengan kompetitornya.

Di sisi lain, terdapat COBIT *framework*, ia merupakan kerangka *IT governance*, yang akan mempermudah para pelaku TI untuk menerapkan *good IT governance*. Praktek audit *IT governance* dengan menggunakan kerangka COBIT akan memberikan suatu *finding* dan *feedback* berupa *value* bagi perusahaan untuk mencapai tujuan TI dan tujuan perusahaan yang dicita-citakan. Pada paragraf berikutnya akan dijelaskan secara singkat konsep mengenai tata kelola perusahaan, tata kelola TI, serta Audit tata kelola TI dengan kerangka COBIT.

2.2 Tata Kelola Perusahaan (*Corporate Governance*)

2.2.1 Definisi

Lawrence dan Weber (2008) mendefinisikan *corporate governance* sebagai : "*the process by which company is controlled or governed. Just as nation have government that respond to the needs of citizens and that established policy, so do corporations have systems of internal governance that determine overall strategic direction and balance sometimes divergent interest*[1]."

Menurutnya, *corporate governance* adalah proses dimana suatu perusahaan mengendalikan atau memerintah. Kemudian, ditambahkan pada definisi tersebut, bahwa proses *corporate governance* pada perusahaan sama halnya dengan proses yang terjadi di dalam pemerintahan negara di mana pemerintah merespon kebutuhan dari penduduknya dan menetapkan kebijakan. Selain itu, perusahaan juga mempunyai tata kelola internal yang menentukan keseluruhan dari arahan strategis dan keseimbangan yang suatu ketika terdapat banyak kepentingan yang berbeda.

Sedangkan definisi dari Hunton (2008) yang menggunakan istilah *corporate governance* dengan *enterprise governance* menyatakan bahwa, *enterprise governance* merupakan proses dalam menetapkan dan menerapkan strategi perusahaan, memastikan bahwa organisasi mencapai objektifnya secara efisien dan mengelola risiko yang ada. *Enterprise governance is the process of setting and implementing corporate strategy, making sure the organization achieves its objective efficiently and manage risks*[2].

Definisi dari Lawrence-Weber ("LW") dan Hunton di atas bersifat saling melengkapi. Definisi dari LW yang lebih memberikan penjelasan *corporate governance* secara lebih umum, sedangkan dari Hunton melengkapi definisi LW

---

[1] Lawrence, Anne T., James Weber. *Business and Society : Stakeholders, Ethics, Public Policy 12th Edition*. New York : McGraw-Hill/Irwin, 2008, *p.324*

[2] Hunton, James E., et al. *Core Concepts of Information Technology Auditing*. USA : John Wiley & Sons : 2008 , p.2

dengan menjelaskan secara khusus, yaitu proses yang dilakukan perusahaan, proses apa dan untuk apa. Dari kedua definisi tersebut, kita dapat mengatakan bahwa, pertama, perusahaan mempunyai suatu proses dalam mengendalikan perusahaannya, dengan memulai dengan menetapkan objektif perusahaan yaitu visi dan misi perusahaan serta budaya perusahaan, kemudian penetapan strategi perusahaan berupa penetapan perencanaan jangka pendek dan jangka panjang dan terdapat proses pelaksanaan, pengendalian dan monitoring dari pelaksanaan strategi tersebut. Dan kedua, bahwa organisasi telah menjalankan kegiatannya sesuai dengan visi dan misinya itu secara efisien, dan efektif dengan tidak melupakan adanya risiko-risiko internal dan eksternal perusahaan dengan melakukan manajemen risiko.

Agar perusahaan dapat mengendalikan atau minimal memitigasi entitasnya dari segala risiko, maka perusahaan harus dapat mengidentifikasi dirinya dan mengukur atas apa yang telah dikerjakan atas perencanaan yang telah ditetapkan.

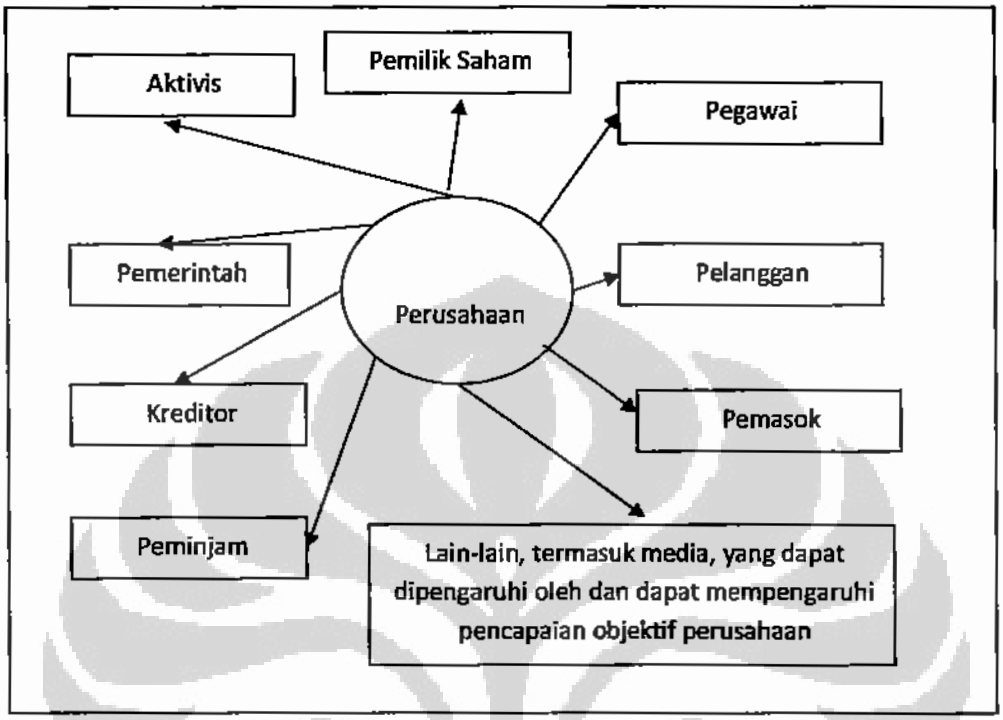
Dalam teori manajemen, terdapat konsep *balance scorecard* ("BSC"), yang mengacu pada 4 dimensi penting perusahaan, yaitu dimensi keuangan, pelanggan, proses bisnis internal dan dimensi pembelajaran dan pertumbuhan. Perusahaan dapat mengenali dirinya dengan menggunakan perangkat BSC dengan 4 dimensi tersebut. BSC tidak akan dibahas di dalam karya akhir ini.

2.2.2 *Corporate Governance* berdasarkan kepentingan *Stakeholder*

Proses *corporate governance* berjalan sesuai dengan dinamika berkembangnya bisnis. Terutama perhatian manajemen sebagai pihak yang menjalankan *corporate governance* dan mengemban amanah yang dibebankan pemilik modal (*shareholder*). Ia harus semakin sensitif terhadap perkembangan yang terjadi di lingkungan bisnis perusahaannya.

Perusahaan harus berupaya untuk mengelola kepentingan para *stakeholder* yaitu pemilik saham, pegawai, pelanggan, pemasok, kreditor, pemerintah, dsb (gambar 2.1) dengan cara mempertimbangkan semua kepentingan tersebut di dalam mengejewantahkan visi dan misi perusahaan dan perencanaan strategi jangka pendek dan jangka panjang. Tanpa pengelolaan yang tepat, atas semua

kepentingan tersebut, maka akan muncul berbagai risiko yang akan mengancam gol atau tujuan perusahaan.



Gambar 2.1 Peta Akuntabilitas Pemangku Kepentingan Perusahaan

Telah diolah kembali dari buku *Business & Professional Ethisc for Directors, Executives & Accountant*, Leonard J. Brooks (2006)

Untuk mencapai kesinambungan usaha perusahaan, seperti yang sudah diungkapkan pada paragraf sebelumnya, perusahaan harus memperhatikan kepentingan para pemangku kepentingan, dengan memperhatikan asas-asas sebagai berikut ini yaitu transparansi, akuntabilitas, responsibilitas, independensi serta kesetaraan dan kewajaran. Asas-asas tersebut selaras dengan fungsi *IT governance*, terutama ketika berkaitan dengan kriteria informasi yang akan dijelaskan pada bagian berikutnya. Maka dapat dikatakan, bahwa penerapan *IT governance* akan selalu mendukung *corporate governance*. Hal inilah yang menjadikan mengapa *IT governance* begitu penting untuk diterapkan.

2.3 Tata Kelola TI (*IT Governance*)

2.3.1 Definisi

Hunton, mendefinisikan *IT governance* sebagai proses mengendalikan sumber daya teknologi informasi suatu organisasi, dimana sumber daya ini termasuk diantaranya sistem informasi dan komunikasi dan juga teknologi,

"the process for controlling an organization's information technology resources, where these resources are defined to include information and communication system as well as technology".[3]

Sedangkan *IT governance*, menurut **ISACA** adalah

" IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consist of the leadership and organizational structures and processes that ensure that organization's IT sustains and extends the organization's strategies and the objectives". [4]

Dan ditambahkan, bahwa *IT governance* merupakan

"A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes ." [5]

IT governance dilihat oleh ISACA, sebagai suatu struktur hubungan dan proses-proses dalam mengarahkan dan mengendalikan perusahaan untuk mencapai tujuan perusahaan dengan cara menggunakan nilai tambah yang diberikan oleh TI sekaligus menyeimbangkan risiko yang berasal dari TI serta prosesnya tersebut.

Selain itu, ISACA juga melihat bahwa *IT governance* merupakan bagian yang menyatu dari *corporate governance*, sehingga pemimpin puncak, haruslah

[3] Ibid.

[4] ITGI. *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models.* USA : 2007

[5] Ibid.

bertanggung jawab atas berjalannya *IT governance*. Konsep *IT governance* menurut ISACA mencakup kepemimpinan dan struktur organisasi dan proses yang memastikan bahwa TI dari organisasi bertahan dan sekaligus TI akan mengembangkan tujuan dan kebijakan strategis perusahaan.

Sedangkan Weill dan Ross (2004) mendefinisikan *IT governance* yaitu *"specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT"* [6]

IT governance adalah membuat keputusan dan kerangka akuntabilitas yang benar untuk mendukung tingkah laku yang diinginkan pada penggunaan TI.

Ketiga definisi tersebut mempunyai redaksional yang berbeda dalam mendefinisikan *IT governance*, namun ketiganya mempunyai mempunyai pemahaman yang sama, bahwa *IT governance* merupakan pengendalian terhadap sumber daya teknologi informasi, yang dapat memberikan suatu nilai tambah bagi perusahaan untuk mencapai objektifnya, sekaligus menyeimbangkan *risk and return* yang didapatkan dari TI tersebut.

2.3.2 Urgensi dari Tata Kelola TI

IT governance diharapkan berjalan lebih efektif untuk memberikan nilai tambah bagi perusahaan. *Good IT governance* akan memberikan suatu harmonisasi keputusan antara manajemen, tingkah laku yang diinginkan dari penggunaan TI dan objektif dari bisnis.

Menurut Weill dan Ross, ada beberapa alasan mengapa pengambilan keputusan TI tidak boleh ditinggalkan dan untuk itu perlu adanya *IT governance* yang baik. Berikut 8 hal alasan tersebut [7]:

---

[6] Weill, Peter. , Jeanne W. Ross. IT Governance : *How Top Performers Manage IT Decision Rights for Superior Results*. Harvards Business School Press : 2000

[7] *Ibid.* p.14-18

1. *Good IT Governance pays off*

Menurut penelitian di Amerika Serikat, perusahaan yang menerapkan good *IT governance* dibandingkan perusahaan yang *IT governance*-nya berjalan tidak baik, mendapatkan profit yang tinggi padahal strategi yang diterapkan sama (misalnya strategi kedekatan dengan konsumen, atau operasional yang baik). Nilai *Return on Asset* (rasio penggunaan asset yang menghasilkan laba) 20 % lebih tinggi pada perusahaan yang tidak menerapkan *good IT governance*.

2. *IT is expensive*

Investasi pada TI sangat mahal, oleh karena itu *IT governance* yang baik diharapkan dapat memicu TI agar memberikan *value* lebih kepada perusahaan.

3. *IT is pervasive*

Terkadang anggaran dan sumber daya TI tidak hanya ditetapkan di bagian divisi TI perusahaan saja, namun tersebar di bagian lain perusahaan. Misalnya bagian pengembangan produk, membutuhkan komputer untuk divisinya. Dengan adanya desain *IT governance* yang baik, maka pengaturan mengenai pengambilan keputusan dengan hal yang berkaitan dengan TI tersebut dapat didistribusikan kepada pihak yang mempunyai kepentingan tersebut.

4. *New Information technologies bombard enterprises with new business opportunities*

Perusahaan mempunyai berbagai kesempatan untuk mengembangkan bisnis baru karena TI semakin maju terutama dalam mendukung bisnis proses yang diinginkan perusahaan

5. *IT governance is critical to organizational learning about IT value*

Nilai dari TI tidak dapat diukur dengan mudah. Namun ketika TI dapat merespon hal-hal dalam bisnis perusahaan dengan mengatasi permasalahan tersebut maka kita dapat mengatakan itu adalah *value* dari TI.

6. *IT Value depends on more than good technology*

Nilai TI bergantung pada 2 hal, yaitu teknologi itu sendiri dan juga orang yang tepat, *the right person on the right place*. Dengan kombinasi kedua hal tersebut suksesnya perusahaan akan tercapai

7. *Senior management has limited bandwith*

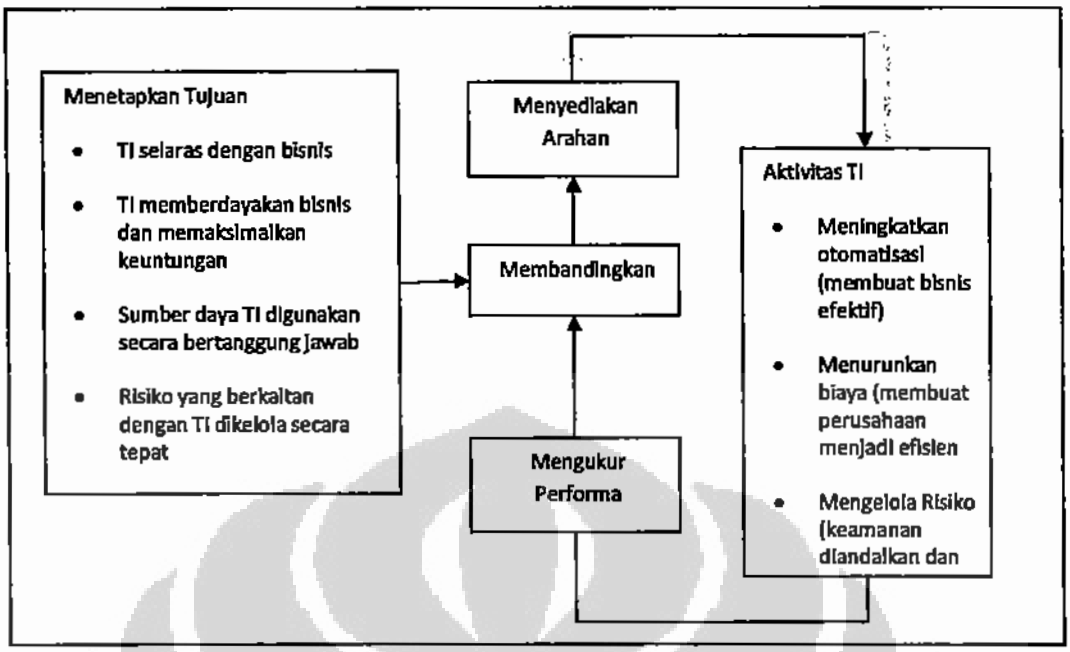
Manajemen puncak tidak mempunyai kapasitas yang cukup untuk menangani semua permasalahan. Jika pun dapat ditangani, maka akan terjadi *bottleneck*, penyumbatan karena permasalahan yang terlampau banyak namun ditangani sendiri oleh manajemen senior, sehingga waktu pengambilan keputusan akan semakin panjang. Perencanaan membentuk *IT governance* yang hati-hati akan menyediakan proses pengambilan keputusan yang jelas, transparan, yang membawa cara yang konsisten dengan visi manajemen senior, ketika setiap orang diberdayakan untuk pengambilan keputusan.

8. *Leading enterprises govern IT differently*

Menurut Ross dan Weill, Perusahaan yang unggul dibandingkan perusahaan lainnya, memiliki *IT governance* yang disesuaikan dengan keadaan perusahaannya, dia tidak mengambil secara utuh kerangka *IT governance* yang ada.

2.3.3 ITGI *Framework*

ITGI juga menjelaskan dalam kerangka ITGI-nya yang memberikan pandangan mengenai hubungan tujuan dan aktivitas TI. Dimana tujuan akan memberikan arahan kepada aktivitas TI mengenai apa yang harus dilakukannya, dan ketika diimplementasikan akan dimonitor sehingga memberikan *feedback* yang akan memberikan masukan kembali bagi aktivitas TI agar berjalan lebih baik dibandingkan dengan aktivitas yang telah dilakukan sebelumnya. Seperti di dalam gambar 2.2 berikut ini.



Gambar 2.2 Kerangka *IT Governance* –ISACA

Telah diolah kembali dari *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)*

2.4 COBIT , ISACA dan IT Governance Institute

Control Objective for Information and related Technology atau disingkat COBIT, dalam bahasa terjemahan bebasnya, berarti sasaran atau capaian pengendalian yang diperuntukkan bagi informasi dan teknologi yang mendukungnya. COBIT merupakan kerangka atau *framework*, suatu sistem konsep dasar yang saling berhubungan terutama dalam proses mengelola informasi dan teknologi. Informasi dan teknologi tersebut memberikan *value* (nilai) sekaligus *risk* (risiko), sehingga dengan adanya *control objectives*, *value* tersebut dapat dicapai, dan risiko tersebut dapat di-*control*. Dengan penjelasan tersebut, COBIT dapat disebut sebagai kerangka tata kelola TI atau *IT governance*, sesuai dengan definisi *IT governance* yang telah diungkapkan sebelumnya.

COBIT mulai dikembangkan pada tahun 1998 setelah ISACA (Information System Audit and Control Association) mendirikan IT Governance Institute (ITGI), suatu organisasi yang berdiri untuk mengklarifikasi dan menyediakan

petunjuk mengenai isu-isu terkini dan masa mendatang mengenai *IT governance*, *control* dan juga *assurance*.

ITGI pun sampai dengan saat ini telah mengeluarkan COBIT versi 4.1, yang terdiri dari :

- *Framework*—menjelaskan bagaimana COBIT mengorganisasikan manajemen *IT governance* dan *control objectives* serta *good practice* dengan domain TI dan prosesnya dan menghubungkannya dengan kebutuhan bisnis.
- *Process descriptions*—terdiri dari 34 proses TI yang meliputi area tanggung jawab dari awal sampai akhir
- *Control objectives*—menyediakan tujuan manajemen yang merupakan *best practice* yang umum untuk proses TI
- *Management guidelines*—Menyediakan perangkat untuk membantu menetapkan tanggung jawab, mengukur kinerja dan *benchmark* dan menyelesaikan ketidakmampuan dari adanya kesenjangan
- *Maturity models*—Menyediakan profil proses TI dalam menjelaskan keadaan saat kini dan masa mendatang.

Selain itu, terdapat *COBIT IT Assurance*, yang dapat digunakan oleh tim audit *IT governance*, baik audit internal perusahaan maupun audit eksternal dari konsultan.

Dalam menerapkan kerangka *IT governance*, COBIT dapat dirangkaikan dengan kerangka lainnya yang sudah menjadi standar *best practice* semisal COSO (kerangka pengendalian internal), ISO, ITIL, atau bagi industri tertentu misalnya bank, terdapat BASEL II (kerangka manajemen risiko untuk perbankan) dan Peraturan Bank Indonesia (PBI). Jadi implementasi COBIT pada organisasi dapat disesuaikan dengan kebutuhan organisasi tersebut.

Dalam *framework* COBIT 4.1 dinyatakan dalam misi nya :

"To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals.[8]*"*

COBIT memiliki keunggulan karena dia *uptodate*, dikembangkan melalui riset, disebarluaskan sehingga diterima pihak internasional dan menjadikannya standar *IT governance*, yang dapat diadopsi oleh perusahaan dan dipergunakan sehari-hari oleh manajer pada bisnis, profesional baik TI dan *assurance.*

Dengan demikian COBIT dapat memenuhi keperluan bisnis dan penerapannya menjadi daya tarik COBIT dilirik oleh banyak entitas organisasi.

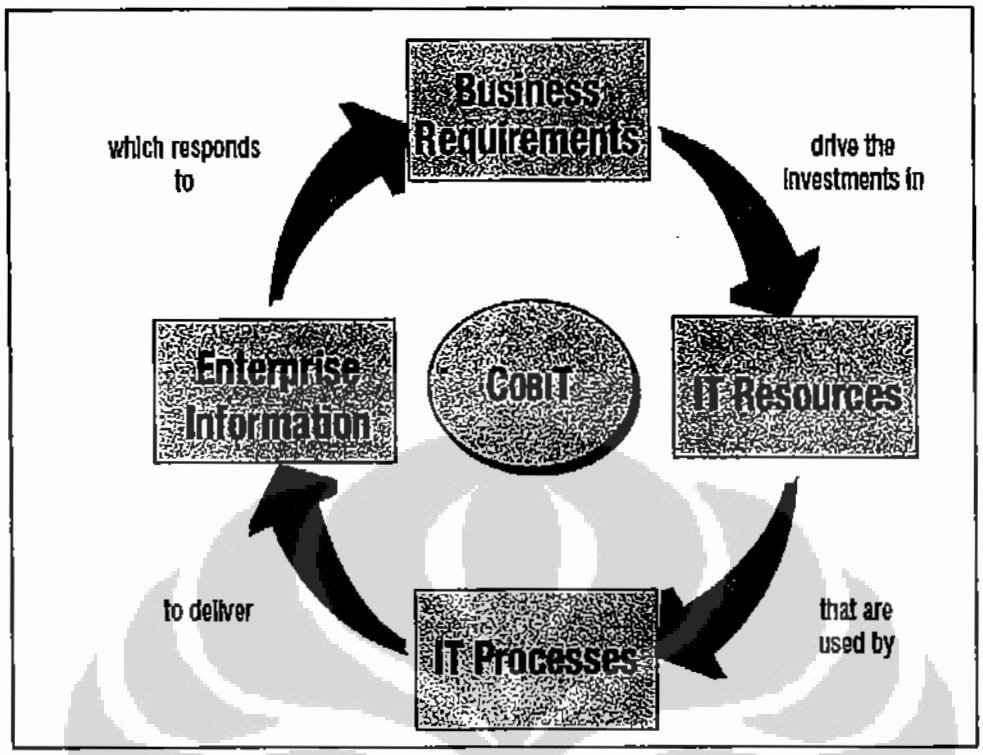
2.5 COBIT *Framework*

Karakteristik dari kerangka COBIT adalah berdasarkan 3 hal yaitu, *business focused, process oriented*, juga *control based*. Selain itu, di dalam COBIT frameworks terdapat *maturity model* yang merupakan hal penting dalam menentukan profil TI bagi suatu organisasi. Hal ini akan dijelaskan pada paragraf berikutnya.

2.5.1 *Business Focused*

Seperti dalam gambar 2.3. prinsip dasar COBIT, diawali ketika perusahaan membutuhkan informasi untuk tujuan mencapai objektifnya, maka perusahaan akan berinvestasi, mengelola, dan mengendalikan sumber daya TI-nya. Sumber daya tersebut akan digunakan pada proses TI, dari proses TI inilah infomasi yang berkualitas didapatkan perusahaan.

[8] ITGI. *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models.* USA : 2007



Gambar 2.3 Prinsip Dasar COBIT

Sumber : dari *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)*

Jantung dari COBIT adalah mengatur dan mengendalikan informasi sekaligus memastikan bahwa informasi selaras dengan kebutuhan bisnis. Alasan yang dikemukakan inilah berarti bahwa harus ada keselarasan antara *IT goals* dan *business goals*, terutama karena TI merupakan perangkat yang menyalurkan informasi. Dan dengan demikian diperlukan suatu kriteria tertentu agar informasi benar-benar mendukung keselarasan kedua hal tersebut. Berikut beberapa hal yang berkaitan dengan perangkat dalam menyalurkan informasi :

2.5.1.1 *Kriteria Informasi*

Organisasi membutuhkan infomasi yang dapat membantu pencapaian objektif perusahaan. Jumlah banyaknya informasi tidak menjamin bahwa perusahaan dapat terbantu dalam mencapai golnya tersebut. COBIT telah membantu memberikan penjelasan mengenai kriteria informasi apa saja yang sesuai dengan *business requirement*. Berikut 7 kriteria informasi :

1. *Effectiveness* – Efektif

Berkaitan dengan informasi yang relevan dan keterhubungan informasi dengan proses bisnis yang diberikan secara tepat waktu, benar, konsisten dan juga dapat digunakan.

2. *Efficiency* - Efisiensi

Berkaitan dengan pengumpulan informasi dilakukan dengan cara yang optimal. Penggunaan sumber daya untuk mendapatkan informasi adalah yang paling produktif dan ekonomis.

3. *Confidentiality* – Kerahasiaan

Berkaitan dengan proteksi terhadap informasi yang sensitif yang datang dari adanya pengungkapan oleh pihak yang tidak berwenang

4. *Integrity* - Integritas

Berhubungan dengan keakuratan dan kelengkapan informasi serta mengenai validitasnya, kesesuaiannya dengan nilai bisnis

5. *Availability* - Ketersediaan

Berhubungan dengan ketersediaan informasi, tersedia pada saat dibutuhkan oleh proses bisnis pada saat kini dan masa mendatang.

6. *Compliance* - Kesesuaian

Berhubungan dengan kesesuaian dengan hukum, regulasi dan perjanjian kontrak di mana bisnis proses menjadi subjek, misalnya kriteria bisnis yang secara eksternal mengandung pemaksaan dan juga kebijakan internal

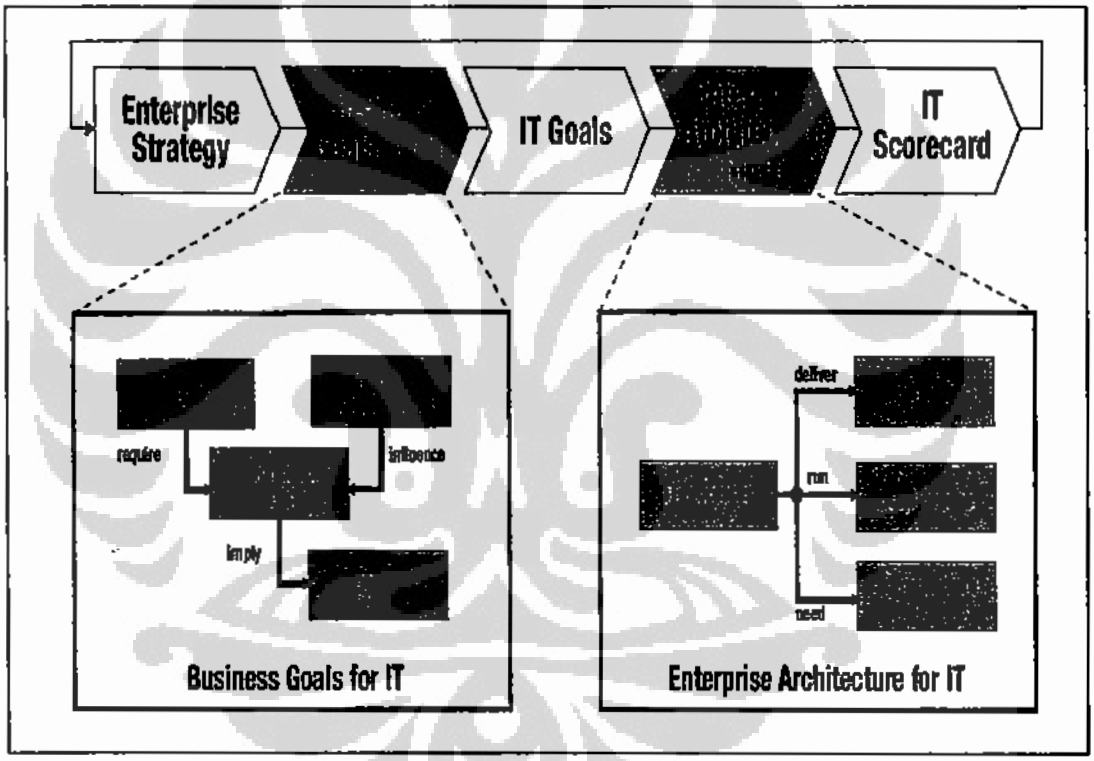
7. *Reliability* – Dapat diandalkan

Berhubungan dengan ketentuan dari informasi yang tepat bagi manajemen dalam operasional dan penjaminan serta tanggung jawab tata kelolanya.

Ketujuh kriteria informasi harus menjadi perhatian oleh TI, karena penyampaian informasi dengan kualitas kriteria tersebut yang melatarbelakangi bahwa tata kelola TI menjadi lebih memberi nilai.

2.5.1.2 *Keselarasan business goals dan IT goals*

Keselarasan tujuan bisnis dan TI (dapat dilihat pada gambar 2.4), dimulai ketika perusahaan menerapkan *enterprise strategy*, pada bagian ini pihak-pihak seperti *stakeholder*, *shareholder*, manajemen dan juga tidak ketinggalan pelanggan, pemasok dsb, menjadi bagian utama dalam penetapan strategi perusahaan, apa yang ingin dicapai perusahaan dalam masa mendatang.



Gambar 2.4 Menetapkan tujuan IT dan Arsitektur perusahaan untuk IT

Sumber : dari *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)*

Untuk tujuan tersebut, maka bisnis mempunyai tujuan bagi TI (*business goal for IT*) yaitu bagaimana TI dapat membantu perusahaan untuk mencapai tujuan Perusahaan. TI kemudian menetapkan tujuannya sendiri agar memahami,

mengetahui bagaimana, dan apa yang akan diberikan kepada perusahaan, untuk itu perlu adanya *IT goals*.

Untuk mencapai *IT goal* maka diperlukan adanya sumber daya TI (*IT resources*) dan arsitekturnya (*Enterprise Architecture for IT*), melalui proses TI (*IT process*).

Setelah ditetapkannya strategi, realisasi atas keseluruhan proses tersebut menjalani suatu sistem pengawasan (monitoring). Suatu metrik yang berasal dari *IT goal* akan menjadi panduannya. Dan *IT scorecard* akan digunakan untuk memastikan apakah ada perbedaaan antara aktual penerapan dari pelaksanaan proses TI dengan ekspektasinya.

2.5.1.3 *IT Resources* (Sumber Daya TI)

Seperti yang sudah dijelaskan agar *IT goal* tercapai maka diperlukan suatu sumber daya TI yang akan memproses informasi tersebut agar bermanfaat bagi manajemennya.

Di sini terdapat proses TI yang memproses penyampaian informasi (*information*) dengan melibatkan aplikasi (*application*) dan untuk itu diperlukan fasilitas infrastruktur (*infrastucture*) dan orang (*people*). Informasi, aplikasi, infrastruktur dan orang merupakan elemen *IT Resources*. Berikut merupakan definisi dari elemen tersebut, yang dikutip dari kerangka ISACA COBIT 4.1

- **Aplikasi** merupakan sistem pengguna yang terotomatisasi dan prosedur manual yang digunakan untuk memproses informasi
- **Informasi** merupakan data, dalam bentuk apapun, di- *input*, diproses dan *output* dengan sistem informasi yang dalam bentuk apapun yang dipergunakan oleh bisnis
- **Infrastruktur** merupakan teknologi dan fasilitas (misalnya, perangkat keras, sistem operasi, sistem manajemen database, jaringan, multimedia, dan lingkungan yang menjadi rumah dan mendukungnya) yang mampu memproses aplikasi

- **Orang** merupakan personel yang melakukan perencanaan *(plan)*, mengorganisasikan (*organise*), mendapatkan (*acquire*), mengimplementasikan (*implement*), menghantarkan (*deliver)*, mendukung (*support*), mengawasi (*monitor*) and *evaluasi* (evaluate) sistem informasi dan jasa. Mereka berasal dari intern perusahaan, tenaga dari luar (*outsource*) atau kontrak

2.5.2 *Process Oriented*

COBIT berorientasi pada proses. Proses yang dimaksudkan adalah bahwa COBIT memperhatikan tatanan organisasi yang terjadi di dalam suatu perusahaan. Dengan berorientasi pada proses berarti, hal ini mendukung adanya sebuah kepemilikan dari sebuah proses (*process ownership*), sehingga dapat diketahui dan menetapkan siapa yang bertanggung jawab (*responsibility*) dan bagaimana pertanggungjawabannya (*accountability*).

Proses COBIT sama dengan proses area tanggung jawab TI perusahaan tradisional, di mana terdapat perencanaan (*planning*), pembangunan (*build*), pelaksanaan (*run*), dan pengawasan (*monitor*). Di dalam COBIT, proses tersebut diistilahkan dan dikategorikan dalam suatu domain, hal ini dimaksudkan agar perusahaan dapat mudah memetakan proses tersebut, sehingga terdapat kesamaan bahasa yang bermanfaat bagi seluruh bagian dari bisnis. Dan mencapai tujuan akhir yaitu mencapai *good IT governance.*

Domain, dalam Kamus Besar Bahasa Indonesia bisa berarti wilayah, daerah, atau ranah[9]. Dalam referensi lainnya *domain* mengacu pada istilah komputer yang diartikan sebagai sekumpulan grup komputer dan peralatan pada sebuah jaringan yang diadministrasikan sebagai sebuah unit dengan aturan umum dan prosedur. Dengan demikian, melihat referensi tersebut, *domain* dalam COBIT dapat diartikan sebagai sebuah wilayah dari operasional TI yang dijalankan sebagai sebuah unit untuk menjalankan suatu prosedur atau fungsi tertentu dengan objektif tertentu.

[9] http://pusatbahasa.diknas.go.id/kbbi/index.php

Terdapat 4 *domain* dalam COBIT yaitu *Planning and Organizing (PO), Acquiring and Implementing (AI), Deliver and Support (DS) dan Monitoring and Evaluating (ME).* Dengan adanya 4 domain ini, diharapkan agar COBIT ini dapat mudah diterapkan karena disesuaikan dengan struktur operasional dari TI.

Masing-masing domain memiliki aktivitas, pada COBIT 4.1 terdapat 34 aktivitas, dan dari tiap-tiap aktivitas terdapat *control objective.*

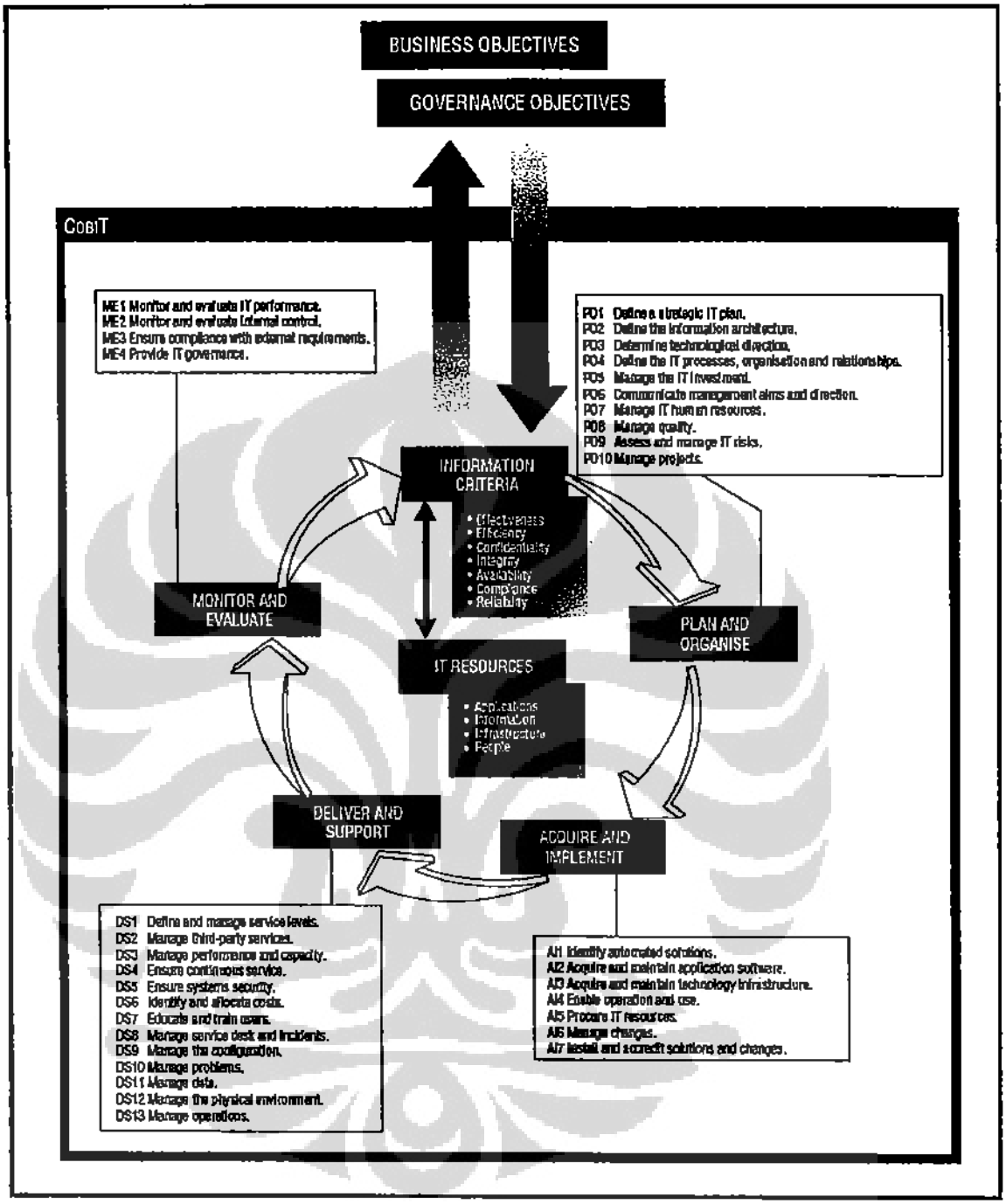
Berikut domain dan aktivitas berdasarkan kerangka COBIT yang ditetapkan oleh ISACA (gambar 2.5) :

1) Plan and Organise (PO)

Definisi yang diberikan oleh COBIT adalah bahwa domain ini meliputi pembentukan strategi, taktik dan bagaimana mempertimbangkan identifikasi atas cara TI untuk mampu memberikan kontribusi yang terbaik bagi pencapaian suatu objektif dari bisnis. PO menjelaskan apakah strategi bisnis dan TI sudah selaras, apakah risiko TI sudah dipahami dan diatur, lalu mengenai apakah semua orang dalam organisasi telah mengetahui tujuan TI dan sebagainya. PO menyediakan arahan solusi bagi AI dan DS. Terdapat 10 proses di dalam PO ini

2) Acquire and Implement (AI)

AI menyediakan solusi dan pelayanan. COBIT mendefinisikan bahwa untuk merealisasikan strategi TI, solusi TI harus diidentifikasikan, dikembangkan dan didapatkan, serta diimplementasikan dan integrasikan menjadi proses bisnis. Sebagai tambahan, perubahan dan perawatan dari sistem yang ada termasuk ke dalam domain ini untuk memastikan solusi berkelanjutan untuk mencapai tujuan bisnis. Dalam domain ini biasanya dipertanyakan mengenai : Apakah proyek baru dapat memberikan solusi sesuai dengan kebutuhan bisnis ? Apakah sistem baru bekerja sebaik-baiknya ketika diimplementasikan ? Apakah perubahan yang dibuat akan mempengaruhi operasi bisnis yang sedang berjalan? AI mempunyai 7 proses



Gambar 2.5 COBIT *Frameworks*

Sumber : dari *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)*

3) Deliver and Support (DS)

COBIT mendefinisikan DS sebagai domain yang berhubungan dengan penghantaran aktual dari jasa yang dibutuhkan, yang termasuk diantaranya penghantaran jasa, manajemen sekuriti dan kontinuitas, pendukung jasa bagi *users*, dan manajemen data dan fasilitas operasional. Pertanyaan mengenai DS yang diajukan diantaranya adalah apakah jasa TI yang dihantarkan sesuai dengan prioritas bisnis ? Apakah biaya TI sesuai dengan manfaatnya? DS memiliki 13 proses.

4) Monitor and Evaluate (ME)

Semua proses harus dinilai setiap waktu untuk mengetahui kualitas dan kepatutannya dengan persyaratan pengendalian. Domain ini melihat kinerja manajemen, mengawasi pengendalian internal, kepatuhan terhadap peraturan dan tata kelola. Dan biasanya pertanyaan berikut ini mencakupi ruang lingkup ME, yaitu apakah kinerja diukur untuk mendeteksi permasalahan sebelum terlambat? Apakah manajemen memastikan bahwa pengendalian internal telah efektif dan efisien? Dapatkan kinerja TI disambungkan dengan tujuan bisnis? ME akan mengawasi keseluruhan proses untuk memastilkan bahwa arahan yang disediakan telah diikuti. Terdapat 4 proses pada domain ME.

2.5.3 *Control Based*

COBIT terdiri dari 34 proses dan memiliki *control objectives* yang melekat pada masing-masing proses yang disebut *process control*

Setiap proses membutuhkan pengendalian agar berjalan sesuai dengan tujuannya. COBIT memberikan petunjuk mengenai *process control* ini, sehingga manajemen dapat mengorganisasikan dan mengelola aktivitas TI.

Definisi dari *control* atau pengendalian itu sendiri adalah kebijakan, prosedur, praktik dan struktur organisasi yang didesain untuk menyediakan keyakinan yang memadai bahwa objektif dari bisnis akan tercapai dan kejadian yang tidak diinginkan akan tercegah atau terdeteksi dan diperbaiki. Keefektifan dari pengendalian akan mengurangi risiko, meningkatkan kemungkinan penghantaran

nilai (*service delivery*) dan meningkatkan efisiensi karena akan terdapat sedikit *error* dan pendekatan manajemen yang lebih konsisten.

2.5.4 *Measurement Driven : Maturity Model*

Maturity model dalam konsep yang umum adalah suatu metodologi untuk mengevaluasi organisasi. Namun, *maturity model* yang pertama kali dikembangkan oleh Software Engineering Institute (SEI), adalah untuk mengetahui perkembangan kemampuan software. Konsep ini dapat diimplementasikan dalam berbagai bidang, termasuk di dalam menilai manajemen dan pengendalian TI yang digunakan oleh COBIT.

Di sisi yang lain, Perusahaan mempunyai kebutuhan untuk mengetahui status sistem TI-nya dan kemudian memutuskan sampai level mana manajemen harus mengembangkan dan mengendalikannya. Dan juga apakah biaya dikeluarkan sebanding dengan keuntungannya. *Maturity model*, dapat menyediakan perangkat untuk menilai hal tersebut.

COBIT menggunakan *maturity model* untuk menjawab kebutuhan perusahaan. Dengan cara mengembangkannya pada 34 proses yang terdapat di dalam COBIT. Kemudian perusahaan dapat mengidentifikasi, hal berikut ini :

- Kinerja aktual perusahaan — berada di mana perusahaan saat ini
- Status dari industri pada saat ini — perbandingannya
- Target perusahaan untuk pengembangan—dimana perusahaan ingin berada
- Kebutuhan akan jejak pertumbuhan antara status saat ini dan ingin menjadi apa

Komponen yang digunakan di dalam maturity model ini adalah *maturity level* dan *maturity model scale*. *Maturity level* didesain sebagai profil dari proses TI, perusahaan dapat melihat keadaan perusahaan pada saat ini dan mendatang dari mulai dari level 0 (Non Existent) sampai dengan 5 (Optimised).

0 *Non Existent* — Tidak ada proses. Perusahaan bahkan tidak mengetahui bahwa terdapat masalah yang harus diselesaikan

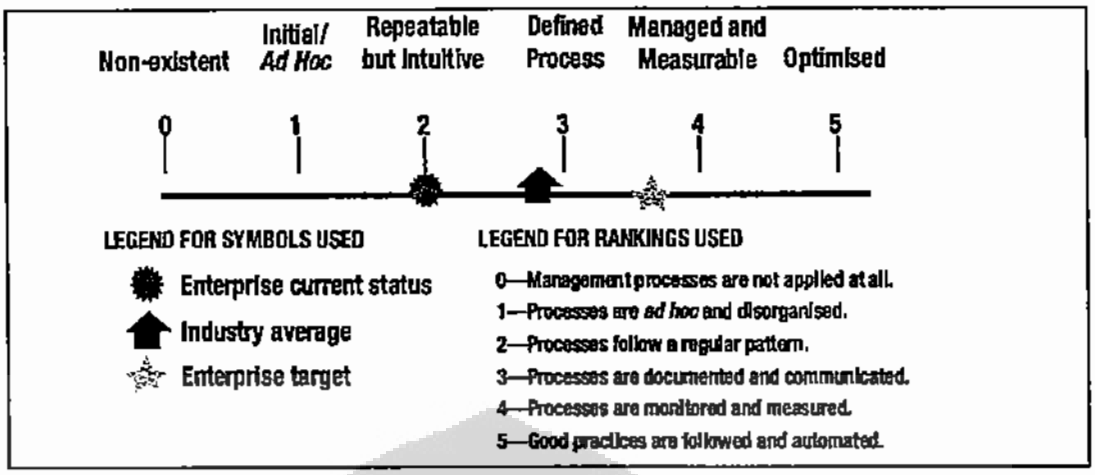
1 *Initial/Ad Hoc* — Terdapat bukti bahwa perusahaan telah mengakui bahwa terdapat masalah dan harus diselesaikan. Ada proses, namun belum terstandarisasi, bahkan terdapat pendekatan *ad hoc* yang berusaha untuk diaplikasikan pada kasus per kasus. Pendekatan manajemen semuanya tidak terorganisir

2 *Repeatable but Intuitive* — Proses telah dikembangkan pada tahapan dimana prosedur yang sama diikuti oleh orang yang berbeda yang melakukan tugas sama. Tidak ada training formal ataupun komunikasi atau prosedur standar, tanggung jawab dibebankan kepada individu. Terdapat derajat ketergantungan yang tinggi terhadap pengetahuan individu, untuk itu kesalahan dapat sekali sering terjadi

3 *Defined Process* — Prosedur telah terstandarisasi dan didokumentasikan, dan dikomunikasikan melalui training. Terdapat mandat bahwa proses ini harus diikuti, namun, tidak jarang deviasi dapat dideteksi. Prosedur itu sendiri tidak terlalu kompleks namun merupakan formalisasi dari praktek yang ada.

4 *Managed and Measurable* — Pihak manajemen mengawasi dan mengukur ketaatan terhadap prosedur dan mengambil tindakan ketika proses tidak berjalan secara efektif. Proses berada di bawah pengembangan yang konstan dan menyediakan praktek yang baik. Otomatisasi dan perangkat digunakan pada cara yang terbatas dan terfragmen.

5 *Optimised*—Proses telah dimurnikan menjadi level praktek yang baik, berdasarkan dengan hasil pengembangan yang berkelanjutan dan *maturity model* dengan perusahaan yang lain. TI digunakan dengan cara yang terintegrasi untuk mengotomatisasi alur kerja, menyediakan perangkat untuk meningkatkan kualitas dan efektifitas, membuat perusahaan menjadi cepat beradaptasi.



Gambar 2.6 Grafik Representasi *Maturity Model*

Sumber : dari *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)*

Perusahaan dapat menempatkan posisinya di dalam skala seperti yang terdapat di dalam gambar 2.6 di atas ini. Dengan menilai kriteria yang ada sesuai dengan kapabilitas, cakupan dan pengendalian perusahaan, yang disesuaikan dengan maturity level 0-5 dengan atribut yang telah diberikan kepada COBIT, diantaranya : kesadaran dan komunikasi; kebijakan, perencanaan dan prosedur; perangkat dan otomatisasi; keahlian dan kemampuan; responsibilitas dan akuntabilitas serta penetapan gol dan pengukuran.

COBIT juga memberikan arahan untuk pengukuran kinerja bagi TI–nya. Sistematika pengukuran kinerja didasari oleh prinsip balance scorecard (BSC).

2.6 Audit : Audit Internal, Audit Eksternal dan Audit Teknologi Informasi

Audit menurut Arens (2000) adalah akumulasi dan evaluasi dari bukti mengenai informasi untuk menentukan dan melaporkan derajat korespondensi antara informasi dan kriteria yang telah ditetapkan[10].

Audit dapat dilakukan oleh pihak auditor internal dan auditor eksternal yang kompeten, independen. Auditor memberikan *assurance* atau keyakinan untuk

[10] Arens, Alvin A., James K.Loebbecke. *Auditing : An Integrated Approach 8th Edition*. New Jersey : Prentice Hall.Inc : 2000

memberikan kenyamanan bagi para pengguna laporan audit untuk pengambilan keputusan.

2.6.1 Audit Internal

Audit internal menurut Konrath (2002), merupakan fungsi yang didirikan dalam suatu organisasi untuk memeriksa dan mengevaluasi aktivitasnya. Internal audit dapat berfokus pada laporan keuangan (*financial audit*), ketaatan terhadap kebijakan, prosedur, hukum atau regulasi (*compliance audit*), deteksi fraud (audit fraud) atau keefektifitasan dan keefisienan dari operasional (*operational audit*). Termasuk diantaranya audit terhadap teknologi sistem informasi[11].

Untuk bekerja secara efektif, menurut Arens dan Loebbeck (2000), internal auditor harus mempunyai independensi terhadap garis fungsi pada organisasi namun dia tidak dapat independen terhadap entitas tersebut selama hubungan antara perusahaan-pegawai tetap ada[12].

Internal auditor menyediakan informasi yang dibutuhkan manajemen untuk pengambilan keputusan atas kriteria yang telah ditetapkan sebelumnya. Kriteria tersebut tergantung dengan fokus audit yang diambilnya.

Pengguna hasil audit dari luar perusahaan, tidak dapat bersandar pada hasil audit internal karena faktor ketiadaan independensi. Berbeda dengan auditor eksternal.

2.6.2 Audit Eksternal

Audit eksternal atau independen audit dilaksanakan oleh auditor eksternal. Menurut Konrath (2002) audit independen dilaksanakan oleh auditor yang independen dari manajemen dan melayani pengguna pihak ketiga (misalnya

---

[11] Konrath, Larry F. Auditing : A Risk Analysis Approach 5th Edition. USA : South Western, 2002

[12] Arens, Alvin A., James K.Loebbecke. *Auditing : An Integrated Approach 8th Edition.* New Jersey : Prentice Hall.Inc : 2000

stockholder dan kreditor).[13] Auditor ini dalam penugasannya terbatas pada pelaporan keuangan pihak yang diaudit untuk itu seringkali disebut dengan auditor laporan keuangan. Namun demikian, atas dasar perikatan tertentu, audit eksternal juga menyediakan jasa audit internal yang bertanggung jawab kepada manajemen.

Menurut SPAP (Standar Profesional Akuntan Publik), SA Seksi 110[14], tugas auditor adalah bertanggung jawab untuk merencanakan dan melaksanakan audit untuk memperoleh keyakinan memadai tentang apakah laporan keuangan bebas dari salah saji material, baik yang disebabkan oleh kekeliruan atau kecurangan. Auditor eksternal juga mengkaji permasalahan pengendalian intern namun terbatas pada apa yang diperolehnya dalam audit.

Hasil dari audit eksternal adalah opini bagi laporan keuangan yang dapat digunakan oleh pemakai laporan keuangan tersebut setelah melakukan proses audit lapangan dengan mendapatkan bukti audit tersebut.

2.6.3 Perbedaan antara audit internal dan audit eksternal

Faktor pembeda yang terpenting antara audit internal dan audit eksternal adalah independensi. Dengan adanya independensi, laporan yang dihasilkan oleh auditor eksternal lebih *reliable* bagi para pengguna, baik manajemen maupun pihak ketiga. Independensi ini merupakan faktor adanya ketidakberpihakan auditor kepada siapan pun, termasuk orang yang memberikan *fee* kepadanya atas pekerjaan audit. Dengan demikian auditor eksternal lebih dipercayai dalam mengeluarkan opini audit laporan keuangan.

Agar lebih mendalami perbedaan antara audit internal dan audit eksternal, berikut ini merupakan bagan perbedaan audit internal dan audit eksternal :

---

[13] Konrath, Larry F. Auditing : A Risk Analysis Approach 5th Edition. USA : South Western, 2002

[14] IAI. *Standard Profesional Akuntan Publik*. Salemba Empat : 2001

Tabel 2.1 Perbedaan Audit Internal dan Audit Eksternal

Faktor	Audit Internal	Audit Eksternal
Yang melakukan audit	Karyawan Perusahaan	Pihak luar yang menjalin perikatan dengan perusahaan
Pertanggungjawaban	Kepada manajemen dan *Board of Directors*, Komite Audit	Kepada pihak ke-3 (pengguna laporan keuangan)
Subjek penelaahan	• Operasional (efektifitas, efisiensi) • Ketaatan (hukum, kebijakan, prosedur, regulasi) • Deteksi fraud (audit fraud) • *Financial audit*	• *Internal control* untuk menentukan cakupan audit • Laporan keuangan • Penugasan khusus (fungsi internal audit, review laporan keuangan)
Hasil Audit	Sesuai kriteria yang ditetapkan (apakah operasional yang dijalankan sudah efektif?)	Opini laporan keuangan (assurance terhadap laporan keuangan
Standar	SOP Perusahaan, peraturan internal audit	SPAP, GAAP

2.6.4 Audit Teknologi Informasi

Auditor TI akan memberikan *assurance* (keyakinan) mengenai teknologi informasi dan juga tata kelola TI. Auditor akan berperan dalam menilai risiko dan pengendalian TI. Beberapa audit spesifik yang dilakukan oleh auditor TI adalah mengevaluasi aplikasi seperti *e-business*, *Enterprise Resource Planning* (ERP) dan juga *software*; menyediakan *assurance* untuk prosedur tertentu, mendukung auditor laporan keuangan dan lain sebagainya.

Selain itu, COBIT, yaitu kerangka tata kelola TI dari ISACA, yang telah dibahas pada paragraf-paragraf sebelumnya dapat digunakan oleh auditor untuk menilai dan memberikan saran kepada manajemen mengenai pengendalian internal bagi perusahaan dengan berbasiskan kepada penyelarasan antara tujuan TI dan perusahaan.

2.7 Langkah-langkah Audit

2.7.1 IT Assurance Guide Using COBIT : *IT audit roadmap*

IT Assurance Guide Using COBIT yang dikeluarkan oleh ISACA memberikan langkah-langkah untuk melakukan audit TI yang menggunakan kerangka COBIT. Petunjuk yang dikeluarkan oleh COBIT tersebut merupakan petunjuk yang dapat dikustomisasi, sehingga dapat dikembangkan oleh para auditor internal dan eksternal. Petunjuk tersebut bukanlah suatu resep yang harus diikuti secara detil, namun dapat disesuaikan dengan penggunaannya di lapangan, dan dapat dipadukan dengan petunjuk lainnya yang sudah menjadi standar.

Langkah-langkah audit menurut *IT Assurance Guide Using* COBIT, sebagaimana yang dikenal dengan *IT audit roadmap* (gambar 2.7) dimulai dengan *Planning* (Perencanaan), *Scoping* (Cakupan), dan *Executing* (Pelaksanaan).

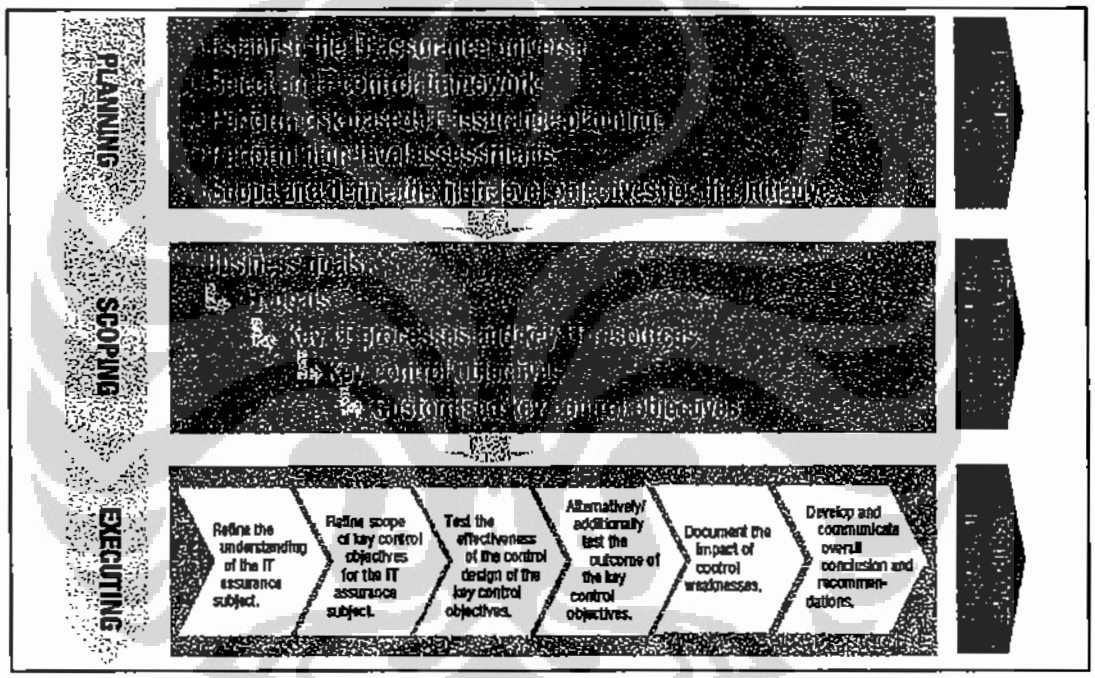
1) *Planning* (Perencanaan),

Tahap perencanaan dilakukan terlebih dahulu untuk menetapkan audit apa saja yang akan dilakukan oleh para auditor, misalnya dengan mengetahui *IT assurance universe* yaitu hal-hal yang berkaitan dengan lingkungan TI dimana audit akan

dilakukan. Setelah itu, memilih kerangka pengendalian TI-nya. Melakukan perencanaan audit TI dengan melihat risiko dan penilaian level tinggi, serta menentukan cakupan dan objektif untuk audit. Hasil dari tahapan perencanaan akan memberikan suatu perencanaan audit tahunan.

2) *Scoping* (Cakupan)

Tahapan cakupan akan memberikan hasil suatu cakupan dan objektif dari suatu audit. Adanya cakupan dan objektif dari suatu audit adalah mempermudah dan memfokuskan pekerjaan lapangan dari audit.



Gambar 2.7 *IT Assurance Road Map*

Sumber : dari COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models (2007)

3) *Executing* (Pelaksanaan)

Tahapan pelaksanaan merupakan inti proses bagi auditor dalam melaksanakan audit. Karena proses ini ditujukan untuk mendapatkan bukti yang cukup bagi auditor sehingga pada nantinya akan mempunyai informasi untuk membuat opininya. Detil tahapan pelaksanaan dapat dilihat sebagai berikut :

1. memahami subjek dari audit TI
2. memahami cakupan dari tujuan pengendalian kunci bagi subjek audit TI
3. menguji keefektifan dari desain
4. pengendalian dari objek pengendali kunci
5. secara alternatif/ menambahkan suatu pengujian hasil dari tujuan pengendalian kunci
6. mendokumentasikan dampak dari kelemahan pengendalian
7. mengembangkan dan mengkomunikasikan keseluruhan kesimpulan dan komunikasi.

2.7.2 Langkah audit berdasarkan Hunton

Berikut ini ditampilkan juga langkah-langkah audit berdasarkan Hunton, untuk membandingkan metodologi yang dikeluarkan oleh COBIT. Berikut tahapannya :

1. Perencanaan (*Planning*), yaitu dengan menentukan risiko bawaan apa yang berasal dari audit, kemudian menetapkan cakupan, pengendalian, materialitas. Pada tahapan ini masuk diantaranya penetapan mengenal lingkungan yang akan diaudit, menentukan staf yang akan melakukan audit.
2. Penilaian terhadap risiko *(Risk Assessment)*, yaitu menilai risiko yang mempengaruhi audit objektif kita. Penilaian risiko mencakup risiko yang dibawa oleh perusahaan, risiko audit dan risiko dari pengendalian. Di sini konsep *materiality* akan berguna untuk menentukan risiko. Materialitas dapat berkaitan dengan pengendalian, yang dapat didefinisikan adalah pengendalian atau sekelompok pengendalian yang tanpanya prosedur pengendalian tidak dapat menyediakan keyakinan yang memadai bahwa tujuan pengendalian dapat tercapai. Bagian mengenai audit risk dapat dilihat pada 2.5.5.
3. Pengembangan program audit. Aktivitas ini akan mencakup beberapa elemen seperti *audit scope, audit objective, audit procedure*, dan penjelasan mendetail mengenail administrasi perencanaan dan pelaporan
4. Mendapatkan bukti (*evidence)*. Bukti yang didapat dari pekerjaan lapangan harus merupakan bukti yang cukup *(sufficient)*, dapat diandalkan (*reliable*), relevan, dan berguna untuk mencapai tujuan dari audit secara efektif.

5. Menetapkan kesimpulan *(conclusion)*. Kesimpulan dibuat dari analisa atas bukti-bukti yang telah didapatkan.
6. Menyiapkan opini audit. Setelah kesimpulan didapatkan auditor dapat menyiapkan opini yang akan dikomunikasikan kepada pihak klien.
7. *Following up*. Setelah mengkomunikasikan opini, hasil dan beberapa rekomendasi atas kekurangan yang dimiliki klien. Auditor dapat memantau, rekomendasi yang telah diberikan kepada klien apakah diikuti atau tidak, misalnya dengan menetapkan jangka waktunya.

2.8 Bukti Audit

Tujuan dari pekerjaan lapangan adalah mendapat bukti audit yang cukup, dapat diandalkan, relevan, dam berguna dengan tujuan untuk mencapai *audit objectives* secara efektif. Temuan audit dan kesimpulan didukung oleh analisis dan interpretasi yang tepat dari adanya bukti audit. Berikut merupakan tipe dari bukti audit.

2.8.1 Tipe Bukti Audit

Terdapat 2 tipe bukti audit yang paling utama, yaitu [15]:

1) Direct evidence

Dapat disebut sebagai bukti langsung jika bukti tersebut dapat membuktikan keberadaan sebuah fakta tanpa penarikan kesimpulan (*inference*) atau dugaan (*presumption*). Contoh dari bukti langsung ini adalah pengakuan dari saksi mata tanpa ada ubahan apapun dan dokumen tertulis.

2) Indirect evidence

Bukti tidak langsung ini, mendapatkan bukti dengan menggunakan hipotesis tanpa *direct evidence* untuk membuat suatu klaim, jadi dibutuhkan suatu *inference* dan *presumption*. Bukti ini berdasarkan suatu rantai keadaan yang akan membentuk adanya klaim, dengan tujuan membuktikan suatu eksistensi ataupun non eksistensi

[15] Cannon, David L. *CISA Certified Information System Auditor, Study Guide 2nd Edition*. Indiana : Wiley Publishing Inc: 2008

dari suatu fakta. *Indirect evidence* dapat juga disebut dengan *circumstantional evidence.*

Tugas auditor adalah mendapatkan bukti yang paling dapat diandalkan selama proses audit. Ini berarti, semakin banyak *direct evidence* maka semakin diandalkan bukti audit, dan semakin bermutu hasil auditnya. Justifikasi atau pendapat dari auditor akan semakin dapat diandalkan jika direct evidence lebih banyak didapatkan dibandingkan jika menggunakan *indirect evidence*, yang jika digunakan kemungkinan besar akan *unacceptable*, karena adanya *unsure presumption* bukan fakta yang sebenarnya.

2.8.2 Pengambilan Bukti Audit

Bukti audit didapatkan melalui observasi, pengujian dokumen, *computer assisted audit tools* (CAAT), m*ereview minutes of meeting* dan sebagainya. Dari bukti-bukti yang ada terkadang mempunyai nilai yang tinggi dan sebaliknya. Kuantitas dan kualitas bukti juga diperhatikan dan dilakukan penilaian. Bukti yang banyak namun tidak berkualitas, akan menghasilkan kesimpulan yang tidak berkualitas juga.

2.8.3 Sampel Audit

Penentuan jumlah sampel untuk bukti audit dapat dilakukan dengan menerapkan perangkat-perangkat statistika. Seperti *statistical sampling*, contohnya *random sampling* ataupun *non statistical sampling* yaitu berdasarkan *judgment* auditor. Sampel yang dipilih merupakan sampel yang representatif dari populasi. Auditor harus mempertimbangkan teknik pemilihan yang akan menyediakan bukti yang paling relevan.

2.8.4 Bukti Audit untuk Audit Teknologi Informasi

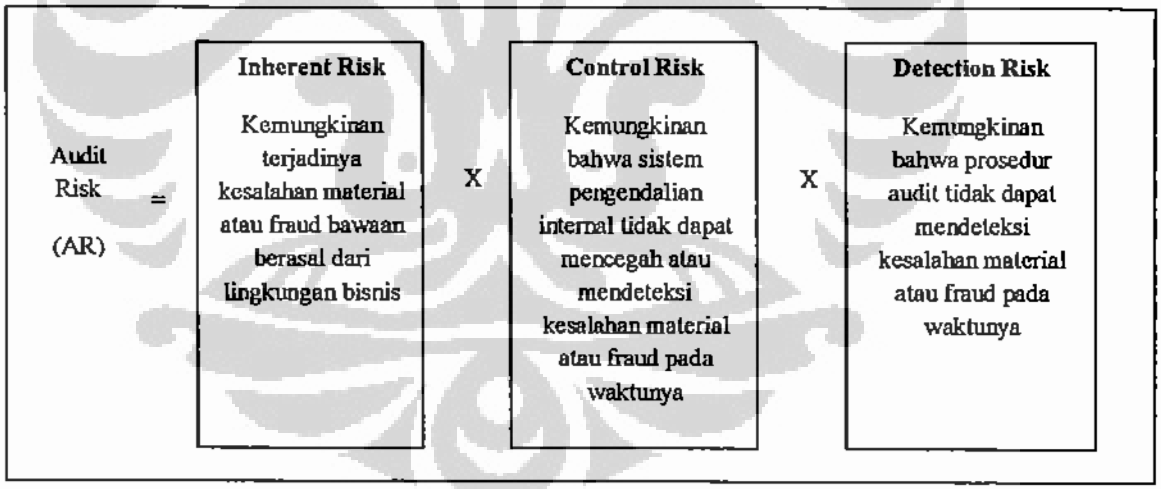
Berikut beberapa contoh dari bukti audit untuk audit TI :

- Bukti dokumen, misalnya catatan transaksi bisnis, bukti penerimaan, faktur dan *log*

- Ekstraksi data, misalnya detail dari *file* data yang menggunakan perangkat otomatis
- Klaim dari *auditee*, yang dipresentasikan baik dalam bentuk lisan maupun tertulis
- Analisa atas perencanaan, kebijakan, prosedur dan diagram alir
- Hasil dari audit kepatuhan (*compliance*) dan uji substantif
- Observasi dari auditor dari pekerjaan *auditee* atau pengulangan pekerjaan (reperforma) dari proses terpilih

2.9 Model Audit berbasis Risiko

Model audit berbasis risiko merupakan metodologi audit untuk mengidentifikasi dan menilai komponen dari risiko audit, dan mengalokasikan sumber daya audit kepada lingkup audit atau cakupan audit yang memiliki risiko tinggi. Nilai risiko bisa berupa kuantitatif (persentase) ataupun kualitatif (low, medium, high).



Gambar 2.9 Audit Risk Model

Sumber : *Core Concepts of Information Technology Auditing (James E. Hunton)*

- *Inherent risk* atau risiko bawaan ini, telah ada sebelum diterapkannya internal control. Bisnis dalam jenis apapun mempunyai risiko, jadi sudah melekat ketika bisnis itu dijalankan. Misalnya saja, perusahaan yang

bergerak di perdagangan internasional memiliki risiko lebih tinggi dibandingkan dengan perdagangan lokal, karena faktor fluktuasi valuta asing yang mempengaruhi nilai tukar. Untuk mengetahui jenis risiko tersebut Perusahaan dapat membuat analisa risiko bisnis sesuai dengan karakteristik perusahaannya. Untuk meminimalkan eksposur dari risiko ini adalah dengan menerapkan *internal control.*

- *Internal control risk* merepresentasikan penilaian apakah *internal control* perusahaan efektif mencegah adanya kesalahan serta seberapa besar auditor ingin membuat penilaian atas risiko tersebut tidak terlalu tinggi. Semakin efektif *internal control* maka risikonya tidak terlalu tinggi. Jika auditor beranggapan bahwa internal control efektif, maka ia harus menguji keefektifan dari internal control tersebut.
- *Detection Risk* merupakan ukuran dari risiko bukti audit gagal untuk mendeteksi kesalahan. Risiko deteksi ini tergantung dari 3 faktor risiko dalam model tersebut. Detection risk akan berubah jika auditor merubah faktor risiko lainnya. Selain itu, risiko deteksi akan menentukan jumlah bukti yang direncanakan auditor untuk dikumpulkan. Ketika risiko ini ingin diturunkan maka auditor harus memperbanyak bukti yang harus dikumpulkan.
- *Audit risk,* yaitu kemungkinan bahwa auditor eksternal organisasi membuat kesalahan dalam memberikan opini atau auditor TI gagal untuk menemukan kesalahan material atau fraud.

Dengan menggunakan model risiko audit, terdapat hubungan langsung antara risiko audit yang dapat diterima dan risiko deteksi, dan hubungan tidak langsung antara risiko audit dan perencanaan pengambilan bukti. Jadi ketika, auditor menginginkan bahwa audit risk yang tidak terlalu tinggi, maka ia harus mengelola agar risiko deteksi dikurangi, tidak tinggi , dengan memperbanyak bukti-bukti audit, jalannya adalah mengintensifkan fokus audit pada audit objek yang dinilai material dapat memberikan lebih risiko tinggi dibandingkan yang lainnya.

2.10 *Internal Control* – COSO Frameworks

Penerapan internal control di dalam perusahaan merupakan usaha-usaha untuk meminimalkannya risiko yang terjadi di Perusahaan. COSO (*Committee of Sponsoring Organization Treadway Commission*) mengeluarkan COSO Framework, yang merupakan kerangka internal audit yang komprehensif. Kerangka ini, membagi 5 kategori untuk pengendalian internal, diantaranya yaitu :

1. *control environment*, terdiri dari tindakan, kebijakan, prosedur yang merefleksikan keseluruhan tingkah laku dari manajemen , direksi dan pemilik perusahaan mengenai pengendalian internal dan pentingnya hal tersebut di dalam perusahaan, termasuk diantaranya adalah etika, nilai-nilai, komitmen, partisipasi direktur atau adanya komite audit, filosofi manajemen dan gaya operasi, struktur organisasi, adanya otorisasi dan tanggung jawab, kebijakan sumber daya manusia
2. *risk assessment*, merupakan penilaian risiko oleh manajemen, manajemen mengidentifikasi dan menganalisa risiko atas apa yang dapat terjadi pada Perusahaan
3. *control activities*, merupakan kebijakan dan prosedur, misalnya pemisahan tugas, pemrosesan informasi, kendali fisik, dan adanya *review*
4. *information and communication*, merupakan sistem informasi yang memberikan informasi kepada di Perusahaan dalam mengelola dan mengendalikan operasinya. Sistem informasi merupakan suatu proses penyajian laporan mengenai kegiatan operasional, keuangan dan ketaatan atas ketentuan yang berlaku
5. *monitoring*, merupakan aktivitas yang berhubungan dengan periode penilaian dari kualitas kinerja pengendalian internal oleh manajemen untuk menentukan bahwa pengendalian berjalan sesuai dengan yang diharapkan dan termasuk adanya modifikasi ketika terdapat perubahan kondisi.

2.11 Industri Perbankan

Setelah mengetahui hubungan antara tata kelola Perusahaan, tata kelola TI, dan Audit COBIT itu sendiri. Maka Penulis akan memaparkan secara singkat mengenai karakteristik industri perbankan. Dengan mengetahui dan memahami karakteristik industri yang akan diaudit maka, para praktisi yang akan mengaudit perbankan akan mengetahui apa saja yang akan dihadapinya dalam menjalankan tugas audit di lapangan.

2.11.1 Pengertian Perbankan

Berdasarkan UU No. 10 Tahun 1998 tentang Perbankan, Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak.

Jadi bank menerima dan meminjamkan dana kepada pihak lain, atau menginvetasikannya di tempat lain, dan dari usahanya tersebut bank mendapatkan keuntungan. Misalnya saja, bank menerima dana dari pihak lain dengan memberikan tingkat bunga 10% dan kemudian meminjamkan kepada pihak lain dengan tingkat pengembalian sebesar 14%, maka bank menerima penghasilan, sebesar dari selisih tingkat pengembalian sebesar 4 %.

2.11.2 Fungsi Bank

Menurut ketentuan Pasal 6 Undang-Undang No. 10 Tahun 1998 tentang Perbankan, usaha-usaha yang dilakukan oleh Bank selain menghimpun dana dari masyarakat dalam bentuk simpanan, berupa giro, deposito berjangka, sertifikat deposito, tabungan dan memberikan kredit, bank juga memberikan jasa pemindahan dana, jasa *letter of credit*, penyimpanan aset seperti penyewaan brangkas, transaksi valuta asing, perantara *hedging*, manajemen dana, mengeluarkan produk konsumsi, seperti kartu kredit, debit, dan lain sebagainya. Bank mendapatkan *fee* sebagai penghasilannya dari jasa yang diberikan kepada nasabahnya tersebut.

2.11.3 Produk-produk perbankan pada era kemajuan TI

Produk perbankan semakin bervariasi sejalan dengan semakin majunya perkembangan teknologi. Misalnya saja, sebelum TI belum maju sekarang ini, nasabah yang akan menabung atau menarik dana yang dimilikinya di bank harus datang ke bank terlebih dahulu. Dibandingkan dengan era sekarang ini, nasabah dapat melakukan transaksi melalui elektronik banking, ATM (Anjungan Tunai Mandiri), SMS banking, bahkan menyetor uang melalui mesin, dan sebagainya, kapan saja, tanpa perlu datang ke Bank langsung.

2.11.4 Industri bank dipengaruhi banyak regulasi

Perbankan merupakan industri yang sarat dipengaruhi regulasi. Diantaranya sebagai berikut :

- Peraturan BI

BI sebagai pihak otonom yang mengatur industri perbankan banyak mengeluarkan peraturan-peraturan yang harus diikuti bank. Seperti Peraturan Bank Indonesia (PBI), Surat Edaran Bank Indonesia.

Diantaranya yang berkaitan dengan teknologi informasi dan risikonya adalah dikeluarkannya Peraturan Bank Indonesia nomor: 9/15/PBI/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum. Penjelasan mengenai PBI ini akan dijelaskan pada bagian lain di bab ini.

- Basel II

Basel II merupakan rekomendasi hukum dan ketentuan perbankan. Basel II memberikan kerangka perhitungan modal yang bersifat lebih sensitif terhadap risiko *(risk sensitive)* serta memberikan insentif terhadap peningkatan kualitas penerapan manajemen risiko di bank. Hal ini dicapai dengan cara penyesuaian persyaratan modal dengan risiko dari kerugian kredit dan juga dengan memperkenalkan perubahan perhitungan modal dari eksposur yang disebabkan oleh risiko dari kerugian akibat kegagalan operasional.[16] Basel II dikembangkan

[16] Bank Indonesia. *Sekilas Implementasi Basel II di Indonesia*. Jakarta <http://www.bi.go.id/web/id/Perbankan/Implementasi+Basel+II/>

oleh sekelompok Negara dan kemudian diterapkan menjadikannya standar di seluruh industri perbankan di dunia termasuk di Indonesia. Basel II memastikan kecukupan modal di bank dan menerapkan *best-practice* dari manajemen risiko agar memperkuat kestabilan dari sistem perbankan.

2.11.5 Risiko yang dihadapi Perbankan

Karakteristik industri perbankan sering dikaitkan dengan industri yang sarat dengan risiko, Bank Indonesia (BI) pun sebagai otoritas perbankan telah mengeluarkan Peraturan BI Nomor : 5/8/PBI/2003 tentang penerapan manajemen risiko bagi bank umum dengan tujuan bahwa perbankan mampu melakukan manajemen terhadap risiko.

Risiko-risiko yang telah diidentifikasi dalam peraturan tersebut antara lain, adalah sebagai berikut : risiko kredit, risiko pasar, risiko likuiditas, risiko operasional, risiko hukum, risiko reputasi, risiko strategik, risiko kepatuhan.

Risiko-risiko yang telah teridentifikasi tersebut akan memberikan eksposur kepada perbankan jika tidak dikendalikan dengan melakukan suatu manajemen risiko. BI mengharapkan agar perbankan meningkatkan tata kelola perusahaan, dengan mengintegrasikannya ke dalam sistem bank terutama dalam pengelolaan risiko, sehingga hal ini akan meminimalkan terjadinya kerugian yang akan mengancam keberadaan bank itu sendiri.

2.11.6 Penerapan Manajemen Risiko atas Teknologi Informasi di Bank

BI juga turut mencermati meningkatnya peranan teknologi informasi dalam memajukan industri perbankan. Namun, meningkatnya ketergantungan terhadap TI, berarti meningkatkan risiko yang akan dihadapi oleh perbankan. Dengan mempertimbangkan hal tersebut, BI mengeluarkan peraturan BI No. 9/15/PBI/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum.

Dalam PBI tersebut, Bank diwajibkan menerapkan manajemen risiko secara efektif dalam penggunaan Teknologi Informasi. Bank wajib melaporkan

perencanaan manajemen risiko atas TI tersebut kepada BI setahun sekali, dan jika tidak dipatuhi akan dikenakan denda.

Dalam PBI tersebut Penerapan manajemen risiko diantaranya mencakup :

a. pengawasan aktif dewan Komisaris dan Direksi;
b. kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi;
c. kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan Teknologi Informasi; dan
d. sistem pengendalian intern atas penggunaan Teknologi Informasi

Penerapan di dalam perusahaan wajib disesuaikan dengan melihat tujuan,, kebijakan usaha, ukuran dan kompleksitas usaha Bank.

Dengan adanya kewajiban ini, pihak perbankan, berarti harus membentuk suatu tata kelola TI. BI juga mengharuskan adanya audit terhadap sistem TI atau tata kelola TI tersebut. Audit dapat dilakukan baik oleh pihak internal ataupun jika terkendala dengan sumber daya maka dapat dibantu oleh pihak audit eksternal. COBIT sebagai kerangka *IT governance* dapat digunakan untuk memenuhi kewajiban terhadap BI bagi perusahaan.

BAB 3

GAMBARAN UMUM

3.1 Profil PT Bank XYZ

3.1.1 Sejarah Pendirian PT Bank XYZ dan Visi Misi

PT Bank XYZ (Perusahaan) merupakan bank komersial pemerintah yang dikenal oleh masyarakat sebagai lembaga keuangan penyedia Kredit komersial. Pendirian Bank XYZ dan visi misinya mempunyai sejarah panjang bersamaan dengan sejarah berdirinya Negara Kesatuan Republik Indonesia (NKRI) ini. Cikal bakal Bank XYZ bermula pada era penjajahan pemerintah Belanda pada tahun 1897 dengan berdirinya bank di Batavia, dengan tujuan menghimpun dana dari masyarakat.

Kemudian berlanjut pada masa penjajahan Jepang pada tahun 1940an, Jepang mengalihkan bank tersebut dengan sebuah bentuk bank baru, yang mempunyai misi mengajak masyarakat untuk menabung.

Dan akhirnya sampai pada zaman kemerdekaan NKRI, Bank XYZ berdiri dengan mengganti beberapa kali nama identitas dan misi, sampai akhirnya menjadi nama PT Bank XYZ yang kepemilikannya dikuasai oleh pemerintah dan mempunyai visi dan misi sebagai berikut :

Visi : *"Menjadi bank yang terkemuka dalam pembiayaan komersial dan mengutamakan kepuasan nasabah"*

Untuk mencapai visi nya tersebut Bank XYZ juga menetapkan Misi yaitu :

- *memberikan pelayanan unggul dalam pembiayaan komersial dan industri yang terkait, serta menyediakan produk dan jasa perbankan lainnya.*
- *menyiapkan dan mengembangkan sumber daya manusia yang berkualitas dan professional serta memiliki integritas yang tinggi.*
- *meningkatkan keunggulan kompetitif melalui inovasi berkelanjutan sesuai dengan kebutuhan nasabah.*

- *melaksanakan manajemen perbankan yang sehat sesuai dengan prinsip kehati-hatian dan good corporate governance untuk meningkatkan Shareholder Value*
- *mempedulikan kepentingan masyarakat dan lingkungannya.*

3.1.2 Bisnis PT Bank XYZ

Sesuai dengan visi dan misi yang diembannya, maka inti bisnis Bank XYZ adalah memberikan pelayanan pembiayaan komersial dan industri yang terkait, namun Bank XYZ juga menyediakan produk dan jasa perbankan lainnya sebagai strategi untuk memenangkan nasabah. Jasa perbankan yang diberikan oleh Bank XYZ meliputi 3 hal yang masing-masing mempunyai jabaran produknya sendiri diantaranya adalah :

1) Produk Dana, terdiri dari : tabungan, deposito Rupiah dan Dollar, giro, tabungan haji;
2) Produk Jasa, terdiri dari : ATM, pengiriman uang, Bank Garansi, RTGS, Payroll, SPP, BPIH, Safe deposit, money changer;
3) Produk Kredit, terdiri dari : KPR Perseorangan, KPR Umum

PT Bank XYZ telah mengembangkan perusahaan dengan tetap meningkatkan pelayanan bagi masyarakat berpendapatan menengah ke bawah. Bank XYZ telah menggeluti pembiayaan komersial selama 32 tahun.

3.1.3 Kondisi Keuangan

Total Aset PT Bank XYZ pada akhir tahun 2007 adalah sebesar Rp36,7 triliun, sedangkan pada akhir tahun 2006 menjadi Rp32,6 triliun atau meningkat sebesar Rp4,1 triliun. Hal ini dipengaruhi oleh meningkatnya aktiva produktif sebesar Rp 3,6 triliun.

Laba bersih setelah pajak mengalami kenaikan sebesar 10,2%, atau Rp37,3 miliar, dari Rp364,7 miliar pada tahun 2006 menjadi Rp402 miliar pada tahun 2007.

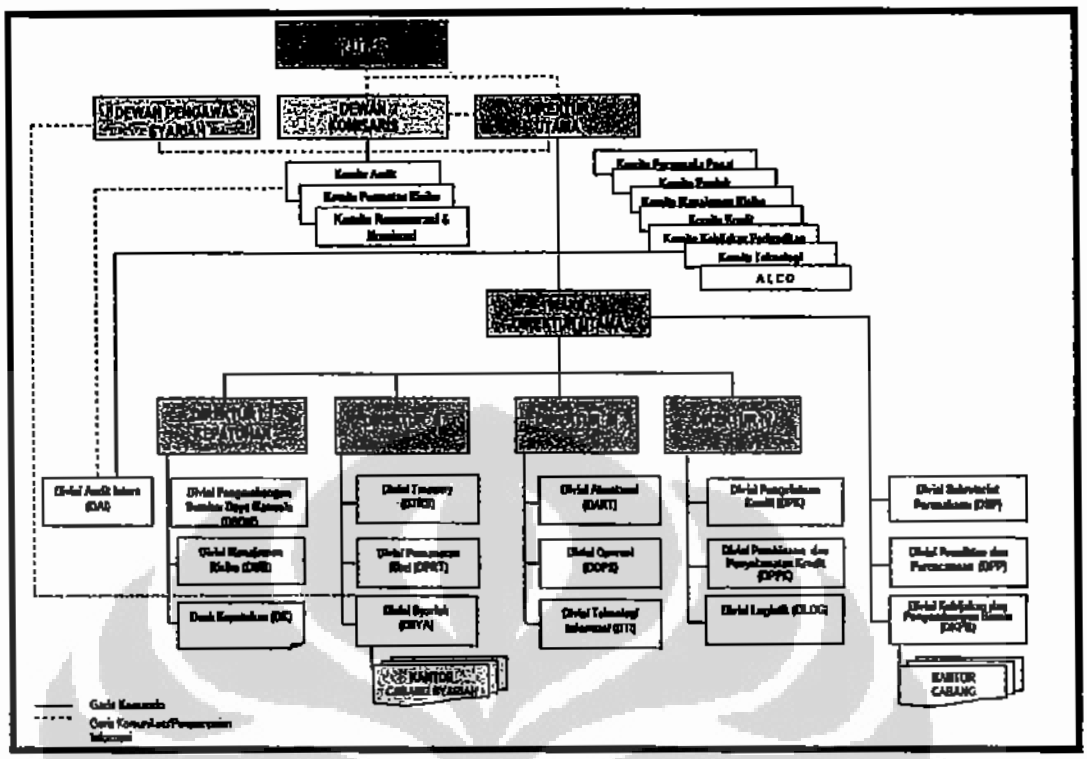
Rasio kecukupan modal PT Bank XYZ per akhir tahun 2007 adalah sebesar 21,9% dengan hanya memperhitungkan risiko kredit, dibandingkan

dengan 18,23% pada akhir tahun 2006. Sedangkan rasio CAR dengan memperhitungkan risiko pasar dan risiko kredit mencapai 21,12%, dibandingkan dengan 17,52% di akhir tahun 2006.

Dengan demikian, dari beberapa indikator keuangan singkat PT Bank XYZ tersebut di atas telah memperlihatkan bahwa perusahaan masih terus tumbuh. Dengan dukungan sistem informasi yang handal, *objectivities* perusahaan diharapkan dapat lebih meningkatkan kinerja perusahaan, terutama dalam menterjemahkan dan responsif terhadap kebutuhan bisnis.

3.1.4 Organisasi PT Bank XYZ dan *Good Corporate Governance*

Prinsip *good corporate governance* (GCG) telah diterapkan oleh Bank XYZ, seperti yang terlihat pada bagan organisasi berikut ini, unsur-unsur GCG telah diterapkan, karena terdapat pemisahan wewenang bagi pihak eksekutif dan pengawasan. Pihak Eksekutif yang diwakili oleh Direktur Utama dipilih dan menjalankan tugasnya berdasarkan amanat Rapat Umum Pemegang Saham (RUPS). Dewan Komisaris sebagai pihak pengawas membawahi Komite Audit, Komite Pemantauan Risiko serta Komite Remunerasi dan Nominasi. Selain itu terdapat Komite lainnya yang harus dimiliki oleh industri perbankan seperti Komite Personalia Pusat, Komite Produk, Komite Manajemen Risiko, Komite Kredit, Komite Kebijakan Perkreditan, Komite Teknologi serta ALCO (Komite Pengelolaan Aset dan Liabilities). Semua hal tersebut di atas adalah untuk menjamin bahwa manajemen perusahaan dapat menjalankan operasional perusahaan dan memenuhi amanat RUPS dengan didasari pertanggungjawaban kepada *shareholder yaitu pemerintah RI* dan *stakeholder* (karyawan, nasabah, *supplier*, masyarakat, BI) yang diawasi oleh Dewan komisaris. Bagan struktur organisasi dapat dilihat pada gambar 3.1.



Gambar 3.1 Bagan Organisasi PT Bank XYZ

Sumber www.bankxyz.co.id

3.1.5 Perkembangan Bank XYZ pada saat ini

Bank XYZ sudah mempunyai 56 cabang dan ribuan kantor kas yang tersebar di seluruh penjuru provinsi Indonesia. Namun pada tahun 2005 di Jakarta, Bank XYZ telah melakukan ekspansi perusahaan dengan mendirikan unit bisnis syariah. Pada saat ini telah berdiri 16 bisnis unit. Hal tersebut adalah sebagai pemenuhan respon dari nasabah yang menginginkan perasaan aman dan tentram dalam menginvestasikan dananya di Bank karena sesuai syariah.

3.2 Rencana Strategis Teknologi Informasi PT Bank XYZ

Pada *annual report* PT Bank XYZ, disebutkan bahwa fokus TI PT Bank XYZ adalah sebagai berikut

"*Upaya penyempurnaan infrastruktur TI, yang memberi penekanan pada aspek pelayanan nasabah serta keamanan (security) TI itu sendiri.*

Platform Teknologi Informasi (TI) yang terpadu merupakan suatu keharusan bagi setiap bank yang berkeinginan untuk melayani dan mengelola jutaan informasi nasabahnya dalam satu platform terpadu. Disamping itu, ketentuan undang-undang perbankan maupun praktik perbankan moderen menuntut setiap bank untuk menjalankan dan memelihara sistem TI terkini dalam rangka memantau risiko secara efektif, serta memastikan keabsahan transaksi keuangan sehubungan dengan program Know Your Customer dari Bank Indonesia.

Investasi TI Bank XYZ disiapkan tidak hanya untuk memenuhi peraturan namun juga untuk mendukung pencapaian sasaran dan laju pertumbuhan usaha. Sejak tahun 2000 Bank XYZ telah berinvestasi di sistem perbankan baru dari Silverlake yang akan mendukung kegiatan pendanaan dan pemberian pinjaman Bank XYZ di segmen perbankan komersial dan konsumer, serta pengelolaan risiko, dengan kapasitas di atas puluhan ribu transaksi per menit."

Rencana strategis bagi pencapaian TI PT Bank XYZ ditetapkan dengan berfokus pada hal tersebut di atas. Bagi manajemen, hal tersebut akan menjadi pedoman dalam mengatur tata kelola TI-nya termasuk diantaranya penetapan strategi jangka pendek perusahaan yang kemudian diimplementasikan pada kegiatan sehari-hari Perusahaan.

PT Bank XYZ telah memiliki dan mengembangkan strategi jangka pendek dan jangka panjang, bagi TI secara terperinci, namun Penulis tidak mendapatkan dokumentasi hal tersebut untuk dikutip pada karya akhir ini karena faktor *confidentiality* yang ditetapkan oleh Perusahaan. Namun tujuan TI secara umum, untuk implementasi pembuatan audit program telah diberikan perusahaan, hal itu dapat dilihat pada bagian Bab 3 ini.

3.3 Divisi Teknologi dan Informasi

Divisi Teknologi dan Informasi (DTI) pada PT Bank XYZ terdiri dari 3 bagian, yaitu Bagian Infrastruktur dan Operasional Komputer, Bagian Perencanaan dan Pengembangan Sistem serta *Quality Assurance* dan *Security Control*. Masing-masing bagian terdiri dari berbagai unit kerja. Berikut ini uraian akan menjelaskan hal tersebut. Bagan organisasi dari Divisi TI dapat dilihat pada gambar 3.2.

3.3.1 Bagian Infrastruktur dan Operasional Komputer

- Grup Dukungan Infrastruktur

  Unit ini bertanggung jawab sebagai pendukung operasional perusahaan yang memastikan bahwa perangkat keras dan komunikasi data telah menjalankan fungsinya.

- Grup Data Center

  Operasional dari *Data Center* (pusat data-DC) dan *Disaster Recovery Plan* (DRP) menjadi tanggung jawab grup *data center*, dengan memastikan keduanya berjalan efisien. Dengan tujuan meminimalkan gangguan dan kegagalan operasi dalam menunjang kegiatan operasional bank.

- Grup Help Desk

  Grup Help Desk akan membantu *user* (pengguna) sistem jika terjadi kesulitan. Dengan demikian *help desk* akan mengkoordinasikan pemberian dukungan dan bimbingan kepada user untuk memberikan solusi dari permasalahannya dengan tepat waktu.

3.3.2 Bagian Perencanaan dan Pengembangan Sistem

Bagian ini juga terdiri tiga grup yang dipimpin oleh seorang kepala bagian. Berikut uraiannya :

- Grup Perencanaan Teknologi Informasi

  Grup ini bertanggung jawab untuk menganalisa dan mempersiapkan rencana Teknologi Informasi. Serta mengoptimalkan anggaran dan sumber daya dengan melakukan koordinasi bersama dengan unit kerja terkait.

- Grup Pengembangan Aplikasi

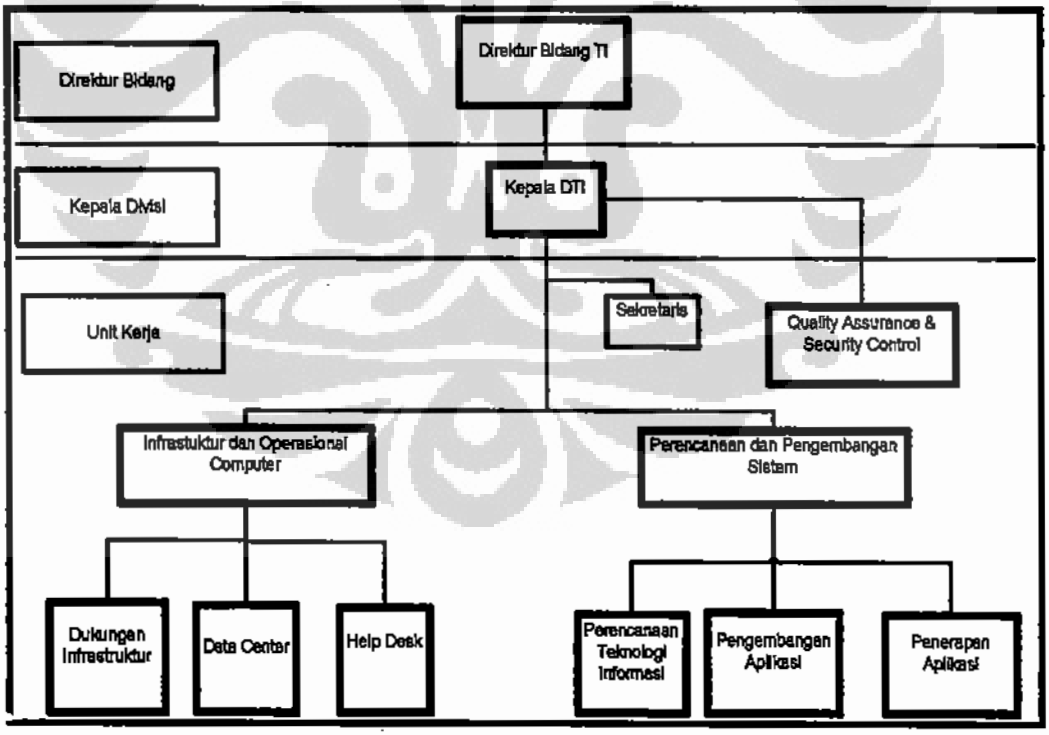
  Grup ini bertanggung jawab jawab untuk memastikan bahwa aplikasi yang dikembangkan dan disempurnakan sesuai dengan kebutuhan bisnis perusahaan dan standar kualitas yang telah ditentukan.

- Grup Penerapan Aplikasi

  Grup penerapan aplikasi akan bertanggung jawab untuk memastikan bahwa implementasi dari sistem aplikasi adalah handal dan sesuai dengan kebutuhan bisnis perusahaan.

3.3.3 *Quality Assurance* dan *Security Control*

Bagian *quality assurance* dan *security control* bertanggung jawab langsung kepada kepala divisi. Bagian ini berfungsi untuk memastikan bahwa kualitas dan kendali atas keamanan dari penerapan sistem informasi, yaitu perangkat lunak, perangkat keras dan jaringan komunikasi data sesuai dengan standar dan kualitas yang telah ditetapkan.



Gambar 3.2 Struktur Organisasi DTI

Sumber dari Audit Internal PT Bank XYZ

3.4 Lingkungan Teknologi Informasi PT Bank XYZ

Perusahaan berusaha mencapai objektifnya dengan didukung oleh teknologi informasi yang efisien dan efektif. Demikian dengan PT Bank XYZ, lingkungan teknologi yang direncanakan, didapatkan dan diimplementasikan, diupayakan sesuai standar. Berikut ini merupakan uraian dari lingkungan dari teknologi informasi perusahaan

3.4.1 Silverlake Intergrated Banking System (SIBS)

Sumber daya teknologi informasi dikendalikan secara terpusat di Kantor Pusat PT Bank XYZ dengan didukung oleh sistem *core banking* SIBS (Silverlake Intergrated Banking System). SIBS merupakan aplikasi pemrosesan transaksi perbankan nasabah yang mencakup kredit, tabungan, dan giro

Sebagai informasi tambahan, SIBS merupakan sistem perbankan yang didesain oleh Silverlake, sebuah perusahaan asing yang bergerak di bidang pemberian solusi TI. SIBS sudah diterapkan oleh banyak bank baik yang berada di Asia Pasifik, maupun Indonesia khususnya. Karena kemampuan SIBS akan mendukung operasional perbankan yang dapat beroperasi selama 24 jam, 7 hari penuh, dan menawarkan solusi yang terintegrasi bagi bank dan memahami kebutuhan bisnis perbankan. Disamping itu fitur-fitur SIBS dianggap dapat membantu mengatur sistem akses dan memastikan bahwa tercapainya kerahasiaan informasi, integritas data dan pencegahan terhadap *fraud*.

3.4.2 Karakteristik Sistem SIBS pada PT Bank XYZ

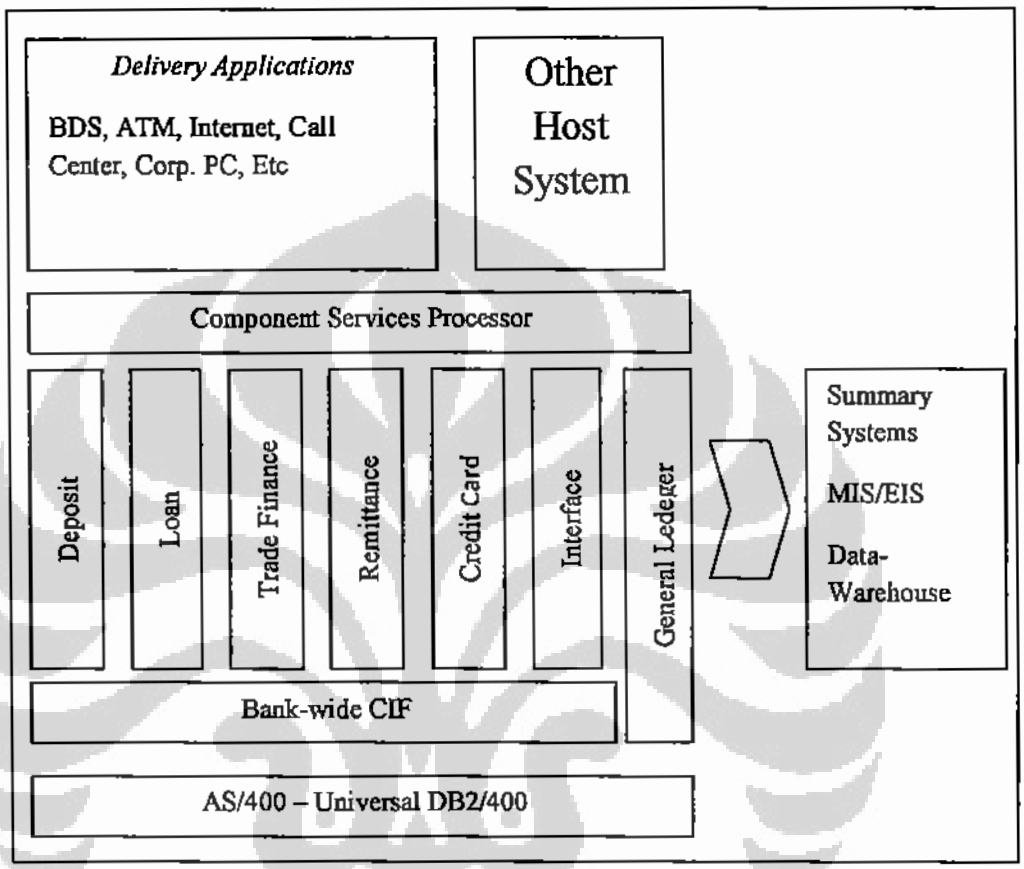
Sistem SIBS yang diimplementasikan pada PT Bank XYZ memiliki karakteristik sebagai berikut :

Tabel 3.1 Karakteristik Sistem SIBS pada PT Bank XYZ

No	Keterangan	Karakteristik Sistem
1	Koneksi	• *Online Realtime* seluruh Cabang • Sentralisasi di Data Center (termasuk Kancapem dan Kankas)
2	Aplikasi	Integrasi semua aplikasi
3	*Database*	RDBMS menggunakan IBM AS/400-DB/2 400 + MS SQL Server
4	Sistem Operasi	• O/S 400 • Windows 98 • Windows NT/2000
5	*Server*	IBM AS/400 (Host) Windows NT (BDS)
6	Bahasa Pemrograman	RPG AS/400, Visual Basic, Visual C++
7	*Front-end*	GUI (Graphical User Interface) dari Microsoft Windows
8	EOD	Dilakukan di Data Center, cabang hanya melakukan *close branch*
9	Pelaporan	Laporan keuangan (Neraca & Rugi Laba) dapat dikeluarkan oleh Kantor Cabang, Kancapem dan Kankas
10	*Setting* parameter produk (bunga, kurs, dll)	Dilakukan di Kantor Pusat
11	*Maintenance* Aplikasi	Hanya dilakukan perubahan setting parameter, tidak dilakukan pemrograman ulang
12	*Feature* : SVS (Signature Verification System)	• Ada (langsung di layar) • Konfirmasi saldo, penarikan, pembayaran KPR, Bill payment, Telkom, Interaccount transfer, Pencetakan 5 transaksi terakhir, integrasi dengan ATM

Sumber : Divisi Audit Intern PT Bank XYZ

Konektivitas SIBS secara logis menghubungkan antara mesin, database, sistem dan aplikasi dalam SIBS dan di luar sistem. Bagan konektivitas dapat dilihat berikut ini :



Gambar 3.3 Konektivitas SIBS

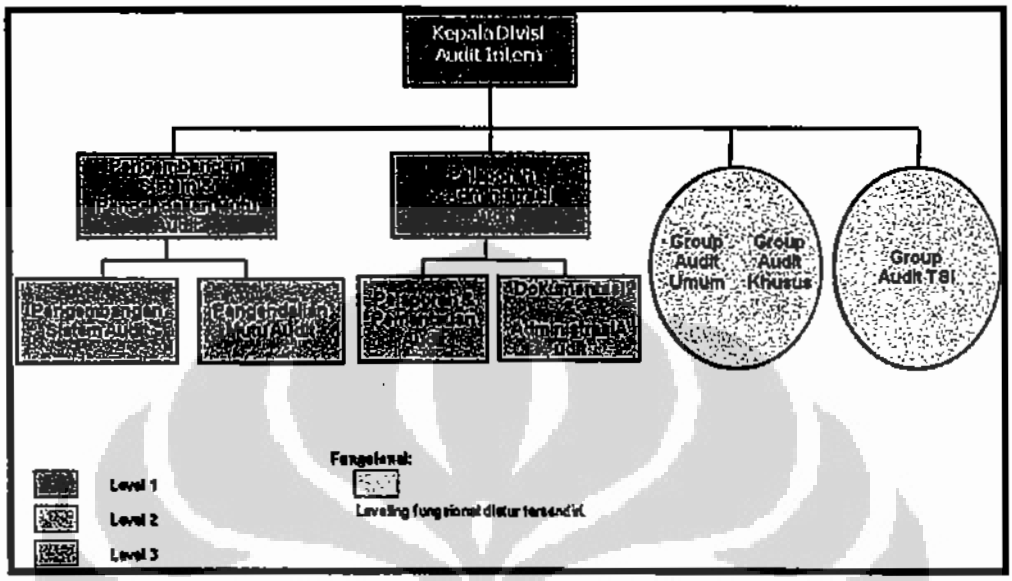
Sumber : Divisi Audit Intern PT Bank XYZ

3.5 Audit TSI pada PT Bank XYZ

3.5.1 Divisi Audit Intern (DAI) – Grup Teknologi Sistem Informasi

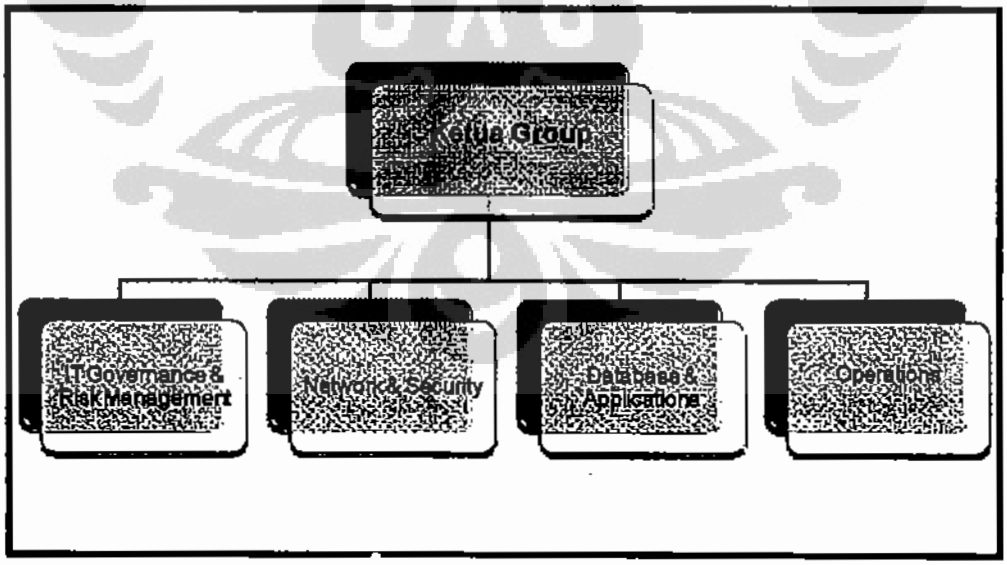
Fungsi audit internal dari PT Bank XYZ dilaksanakan oleh Divisi Audit Intern (DAI). Dalam struktur organisasi dari Perusahaan, DAI bertanggung jawab kepada Komite Audit yang berada di bawah Dewan Komisaris. DAI membawahi beberapa bagian, diantaranya bagian Pengembangan Sistem dan Pengendalian Mutu Audit, bagian Pelaporan & Administrasi Audit, bagian Group Audit Umum

dan Group Audit Khusus serta yang terakhir dan yang menjadi fokus adalah Group Audit TSI (dapat dilihat pada gambar 3.4)



Gambar 3.4 Struktur Organisasi Audit Intern PT Bank XYZ

Sumber dari Audit Internal PT Bank XYZ



Gambar 3.5 Struktur Organisasi DAI - Group Audit TSI

Sumber dari Audit Internal PT Bank XYZ

Grup Audit Teknologi Sistem Informasi (TSI) melaksanakan audit dalam lingkup audit teknologi sistem informasi perusahaan. Grup TSI dipimpin oleh seorang Ketua Grup yang membawahi beberapa bagian, diantaranya adalah *IT Governance & Risk Management, Network & Security, Database & Applications serta Operations* (Gambar 3.5)

3.5.2 Ruang Lingkup Audit (TSI)

Pelaksanaan audit TSI (TI) yang dilakukan bersifat khusus terhadap Teknologi Sistem Informasi meliputi :

1. informasi yang diolah dengan sistem komputer harus mempunyai karakteristik : *integrity, confidentiality dan availability*
2. pengawasan terhadap akses logik,
3. pengawasan sistem aplikasi dan informasi, lisensi dan penggunaan *software*,
4. perlindungan terhadap virus,
5. infrastruktur/jaringan komunikasi data
6. pengamanan fisik terhadap pengelolaan TSI pada PT Bank XYZ pada Divisi Teknologi dan Informasi.

3.5.3 Tujuan dan Sasaran audit

Menurut yang tercantum dari Laporan Persiapan Audit PT Bank XYZ, tujuan dan sasaran audit dari PT Bank XYZ adalah sebagai berikut :

1) Memastikan bahwa hasil audit TSI tahun lalu telah ditindaklanjuti sebagaimana mestinya.
2) Memastikan bahwa sistem pengendalian intern fungsi TSI yang ada telah berjalan dengan baik dan benar.
3) Meyakinkan bahwa sumber daya sistem informasi sudah diamankan dengan memadai dan digunakan secara bertanggung jawab.
4) Meyakinkan bahwa akses ke data komputer sudah dikendalikan secara memadai dan hanya dilakukan oleh yang berwenang.
5) Meyakinkan bahwa ketentuan-ketentuan dan pedoman-pedoman yang berlaku telah ditaati dan dilaksanakan dengan sepenuhnya.

6) Memastikan bahwa dalam pelaksanaan operasional obyek audit tidak terdapat hal-hal yang membahayakan kelangsungan usaha.
7) Memastikan bahwa Pengelolaan TSI telah dilakukan dengan efektif dan efisien dan risiko yang ada sudah diminimalisasi sampai pada tingkat yang dapat diterima bisnis.

3.5.4 Ketentuan untuk melakukan proses audit TSI

Auditor intern TSI PT Bank XYZ melakukan proses audit TSI dengan berpatokan pada ketentuan-ketentuan berikut ini :

1. Standar Pelaksanaan Fungsi Audit Intern Bank Umum (SPFAIB) dan BI.
2. SK Dir BI No. 27/164/KEP/DIR tanggal 31 Maret 1995 tentang Panduan Pengamanan Penggunaan TSI oleh Bank.
3. Peraturan Direksi No. 06/PD/DSDM/0699 tanggal 16 Juni 1999 tentang Pengenaan Sanksi terhadap Penyalahgunaan Kewenangan Teknologi Informasi (TSI).
4. Peraturan Direksi No. 03/PD/DTI/0304 tanggal 8 Maret perihal Pedoman Pengamanan Teknologi Informasi.
5. Surat Edaran No.11/DIR/DOPS/2004 tanggal 23 Maret 2004 tentang Manajemen Teknologi Sistem Informasi SIBS dan BDS serta AS/400.
6. Peraturan Direksi No. 13/PD/DOPS/1103 tanggal 3 November 2003 tentang Manajemen Teknologi Sistem Informasi (MTSI) PT. XYZ
7. Surat Edaran No.15/DIR/DOPS/2001 tanggal 1 Desember 2001 tentang SOP berdasarkan sistem aplikasi baru perbankan SIBS (termasuk perubahan/penyempurnaan dan penambahannya).
8. COBIT dan BS17799.

3.6 Proses Audit

Audit TI yang dilakukan di PT Bank XYZ dilakukan mengikuti dengan 4 proses tahapan yaitu :

1. Persiapan Audit
2. Pelaksanaan Audit
3. Pelaporan Audit
4. dan Monitoring audit

penjelasan secara detail mengenai proses audit TI dapat dilihat pada lembar Lampiran 1.

3.7 Metodelogi Audit

Penulis telah memilih 2 metode mengaudit TI, sebagaimana di dalam Bab II Landasan Teori, masing-masing berturut-turut metodelogi COBIT dan Hunton. Metode dari COBIT yang diperkenalkan dengan nama *IT Assurance Road Map* secara garis besar menjelaskan pelaksanaan audit COBIT dengan membagi dalam 3 tahapan yaitu *planning* (perencanaan), *scoping* (cakupan audit) dan terakhir *execution* (pelaksanaan) yang didalamnya terdapat penarikan kesimpulan dan rekomendasi.

Sedangkan berdasarkan Hunton, proses audit TI dimulai pertama kali dengan melakukan perencanaan (*planning*) kemudian melakukan penilaian terhadap risiko *(risk assessment),* melakukan pengembangan program audit, mendapatkan bukti *(evidence),* menetapkan kesimpulan *(conclusion) serta* menyiapkan opini audit, dan terakhir *following up.*

Kedua metodologi tersebut mempunyai langkah-langkah yang sama, dengan demikian, sebenarnya teori-teori mengenai metodologi yang ada secara umum bertujuan, menawarkan dan memberikan arahan bagaimana melakukan audit dengan agar objektif audit tercapai dan auditor mendapatkan bukti-bukti audit yang berkualitas, dengan cara yang efisien dan hasil yang efektif sesuai dengan kriteria yang telah ditetapkan

Pada paragraf berikut adalah pembahasan dari tahapan audit atas proses audit PT Bank XYZ, sebagaimana pada Lampiran 1.

3.8 Planning (Perencanaan) - Tahap Persiapan Audit

Tahap pertama dari setiap audit adalah melakukan persiapan audit. Dengan kata lain melakukan perencanaan agar pada tahap pelaksanaan dan penyelesaian audit tidak timbul suatu permasalahan yang menghambat jalannya audit. Dengan melakukan perencanaan audit, auditor memiliki panduan untuk menyelesaikan auditnya sesuai dengan tujuan audit yang telah direncanakannya.

PT Bank XYZ melakukan perencanaan audit dengan tujuan agar audit berjalan sesuai dengan waktu, tujuan serta biaya yang telah ditetapkan. Perusahaan membuat jadwal audit dan estimasi waktu, KPI (*Key Performance Indicator*) serta LPA (Laporan Persiapan Audit) dan Administrasi dan biaya audit. Perusahaan juga memilih sampel cabang Perusahaan yang akan diaudit dengan metode tertentu. Sebagai tambahan informasi, kantor pusat PT Bank XYZ yang diwakili oleh DTI akan selalu diaudit, karena diwajibkan oleh pihak regulator yaitu BI. Jadi PT Bank XYZ mengaudit beberapa sampel dari kantor Cabang dan Kantor Pusat dalam kurun waktu setahun. Penetapan personil untuk menjalankan audit juga ditentukan pada fase ini.

3.8.1 Pemilihan sampel cabang sebagai objek audit.

PT Bank XYZ mempunyai 56 cabang dan ribuan kantor kas yang tersebar di seluruh provinsi di Indonesia. Perusahaan tidak melakukan audit atas keseluruhan 56 cabang, namun melakukan pemilihan atas cabang-cabang tertentu dengan melihat risiko audit dari masing-masing cabang. Cabang yang mempunyai risiko tinggi adalah objek audit yang terpilih serta faktor lainnya.

Untuk menentukan cabang mana yang akan terpilih, Perusahaan melakukan analisa risiko yang berdasarkan atas kecenderungan dan dampak risiko. Semakin tinggi tingkat kecenderungan dan dampak risiko, maka kemungkinan mempunyai risiko tinggi dan terpilih menjadi objek audit akan mungkin terjadi. Rumusnya adalah sebagai berikut :

Risiko = Dampak x Kecenderungan **(3.1)**

Tingkat kecenderungan risiko biasanya dipengaruhi banyaknya transaksi, jumlah SDM, banyaknya komputer, jumlah user ID, dan sebagainya sedangkan dampak risiko biasanya dipengaruhi oleh banyaknya permasalahan yang dilaporkan ke *helpdesk*, jumlah PC dengan modem aktif, komputer tanpa ada antivirus, *hardware* komputer yang tidak mempunyai spesifikasi yang sesuai, dan sebagainya.

DAI membuat suatu analisa tertentu dengan bantuan *software* komputer, kemudian hasil akhirnya adalah diperlihatkan tingkat risiko dari keseluruhan cabang. Cabang yang mempunyai risiko tinggi akan dijadikan objek audit. Pada audit yang dilakukan oleh PT XYZ ini, dipilih 13 cabang yang akan jadi objek audit ditambah 1 Kantor Pusat yaitu pada Divisi Teknologi Informasi.

3.8.2 Pengembangan Audit Program

Audit program merupakan hal yang kritikal bagi auditor. Audit program menentukan arah bagi auditor. Di dalam audit program terdapat tujuan audit, hal-hal apa yang harus dicapai oleh auditor untuk mendapatkan bukti audit yang berkualitas. Tanpa audit program, auditor yang berpengalaman tetap dapat menjalankan tugasnya, namun hal-hal yang penting untuk dicapai mungkin saja dapat terlupakan, sehingga pengambilan kesimpulan menjadi tercederai karena aspek penting telah terabaikan oleh auditor.

PT Bank XYZ telah mengembangkan program audit *IT Governance*. Pengembangan audit program berasal dari pemetaan antara objektif Perusahaan dan objektif TI agar mencapai keselarasan. Objektif perusahaan berkaitan dengan *Balance Scorecard* (BSC) sedangkan objektif TI dengan *COBIT framework*. Berikut adalah pemetaan BSC dan COBIT *framework*, sehingga nantinya didapatkan suatu area pemeriksaan yang menjadi fokus audit TSI pada Divisi Teknologi Informasi.

3.8.3 Objektif Perusahaan – BSC

Tabel 3.2 adalah objektif PT Bank XYZ, yang dijabarkan dalam *balance scorecard*. Daftar susunan BSC ini didapatkan Penulis dari DAI. Kolom Tujuan

Bisnis adalah orientasi objektif perusahaan yang didasarkan pada BSC yang terdiri dari 4 perspektif, yaitu : perspektif finansial, pelanggan, internal dan pembelajaran pengembangan bisnis. Kolom relevansi adalah tingkat relevansi antara objektif perusahaan dengan TI (TSI) dari mulai tingkatan sangat relevan sampai dengan tidak relevan. (Tabel ini sudah dihubungkan dengan tabel tujuan TI)

Tabel 3.2 Relevansi Objektif PT Bank XYZ

NO	TUJUAN BISNIS	RELEVANSI			
		Sangat Relevan	Sedikit Relevan	Tidak Yakin	Tidak Relevan
	Sudut Pandang *Financial*				
1.	Memberikan *return of investment* yang bagus pada investasi TSI				
2.	Pengelolaan risiko bisnis yang terkait dengan TSI				
3.	Meningkatkan *corporate governance* dan transparansi	√			

NO	TUJUAN BISNIS	RELEVANSI			
		Sangat Relevan	Sangat Relevan	Tidak Yakin	Tidak Relevan
	Sudut Pandang *Customer*				
4.	Meningkatkan layanan dan orientasi customer	√			
	Menawarkan produk dan layanan yang kompetitif	√			
5.	Menetapkan kelangsungan layanan dan ketersediaan	√			
6.	Pencapaian optimalisasi penyampaian layanan				
7.	Pencapaian optimalisasi penyampaian layanan Mendapatkan informasi yang dapat dipercaya dan berguna untuk pembuatan keputusan strategis				
8.	Mendapatkan informasi yang dapat dipercaya dan berguna untuk pembuatan keputusan strategis				

Dapat disarikan dari bagan tersebut, bahwa relevansi antara objektf perusahaan dan objektif TI dari sudut pandang finansial mengenai peningkatan *corporate governance* dan transparansi mempunyai hubungan sangat relevan, (No.3). Dari sudut pandang pelanggan, hubungan sangat relevan terdapat pada peningkatan layanan dan orientasi customer, penawaran produk dan layanan yang kompetitif, dan penetapan kelangsungan layanan dan ketersediaan (No.4, 5, 6). Dari sudut pandang internal, tujuan untuk patuh pada hukum, regulasi dan kontrak eksternal mempunyai relevansi dengan tujuan TI (No.12).

Sedangkan pada bagan berikut memperlihatkan hubungan relevansi tujuan bisnis dengan TI dari sudut pandang internal.

Tabel 3.2 Relevansi Objektif PT Bank XYZ – (lanjutan)

NO.	TUJUAN BISNIS				
	Sudut Pandang Produktifitas				
9.	Meningkatkan dan memelihara fungsionalitas proses bisnis				
10.	Menurunkan biaya proses				
11.	Kepatuhan pada hukum, regulasi dan kontrak eksternal	√			
12.	Kepatuhan dengan kebijakan internal				
13.	Pengelolaan perubahan bisnis				
14.	Peningkatan dan pemeliharaan produktifitas staff dan operasional				
	Sudut Pandang : Pembelajaran dan Perkembangan Bisnis				
15.	Pengelolaan produk dan inovasi bisnis				
16.	Pengadaan dan pemeliharaan sumber daya manusia yang memiliki pengetahuan, kemampuan dan motivasi				

Sumber : Dokumentasi Divisi Audit Intern PT Bank XYZ

3.8.4 Objektif TI

Berikut adalah objektif TI yang telah ditetapkan oleh PT Bank XYZ. Objektif perusahaan dan TI akan dipetakan untuk menentukan fokus audit dan audit program yang berbasis pada COBIT. Penulis mendapatkan dari DAI PT Bank XYZ.

Tabel 3.3 Objektif TSI

No.	[illegible]
1.	Merespon kebutuhan bisnis dalam rangka mencapai keselarasan dengan strategi bisnis
2.	Merespon kebutuhan pemerintah berdasarkan arahan direksi
3.	Memastikan kepuasan *user* dengan layanan yang ditawarkan dan tingkat layanan yang diberikan
4.	Mengoptimalkan penggunaan informasi
5.	Menciptakan kesigapan dalam TSI
6.	Menetapkan bagaimana fungsi bisnis dan kebutuhan kontrol ditranslasikan ke dalam solusi otomatis secara efektif dan efisien
7.	Menyediakan dan memelihara sistem aplikasi yang terintegrasi dan terstandarisasi
8.	Menyediakan dan memelihara infrastruktur TSI yang terintegrasi dan terstandarisasi
9.	Menyediakan dan memelihara kemampuan TSI yang mampu merespon strategi TSI
10.	Memastikan kepuasan timbal balik dalam hubungan dengan pihak ketiga
11.	Memastikan integrasi aplikasi ke dalam proses bisnis
12.	Memastikan transparansi dan pemahaman terhadap biaya, keuntungan, strategi, kebijakan dan tingkat layanan TSI
13.	Memastikan penggunaan dan kinerja yang benar terhadap aplikasi dan solusi teknologi
14.	Memelihara dan melindungi semua aset TSI
15.	Mengoptimalkan infrastruktur, sumber daya dan kemampuan TSI

No	TUJUAN TSI
16.	Mengurangi *defect* dan *rework* pada solusi dan penyampaian layanan
17.	Melindungi pencapaian tujuan TSI
18.	Menciptakan kejelasan terhadap analisa dampak bisnis pada tujuan dan sumber daya TSI
19.	Memastikan kalau informasi kritis dan rahasia dilindungi dari pihak yang tidak berhak mengakses
20.	Memastikan bahwa transaksi bisnis otomatis dan pertukaran informasi dapat dipercaya
21.	Memastikan bahwa layanan dan infrastruktur TSI dapat bertahan dan pulih dari kegagalan akibat *error*, serangan atau bencana
22.	Memastikan dampak bisnis akibat gangguan pada layanan TSI minimal
23.	Memastikan kalau layanan TSI tersedia ketika dibutuhkan
24.	Meningkatkan efisiensi biaya TSI dan kontribusinya pada keuntungan bisnis
25.	Menghasilkan proyek secara tepat waktu dan tepat biaya serta memenuhi standar kualitas
26.	Memelihara integritas informasi dan infrastruktur
27.	Memastikan kepatuhan dengan hukum dan regulasi
28.	Memastikan bahwa TSI memberikan kualitas layanan yang efektif dari segi biaya, meningkat secara berkelanjutan dan kesiapan terhadap perubahan di masa depan

Sumber : Dokumentasi Divisi Audit Intern PT Bank XYZ

3.8.5 Pemetaan Objektif Perusahaan dan Objektif TSI

Setelah mengetahui objektif masing-masing, maka langkah selanjutnya adalah memetakan antara objektif Perusahaan dengan objektif TSI. Inilah yang dapat mewujudkan keselarasan antara kedua objektif tersebut. Pada bagan berikut diperlihatkan pemetaan dengan menyatukan kolom tujuan bisnis dan tujuan TSI. Kolom tujuan TSI yang disi dengan angka, merupakan angka nomor untuk tujuan TSI yang tertera di atas.

Tabel 3.4 Pemetaan antara Objektif Perusahaan dengan Objektif TSI

RELEVANSI	TUJUAN BISNIS	TUJUAN TSI							
	Sudut Pandang *Financial*								
	Memberikan return of investment yang bagus pada investasi TSI	24							
	Pengelolaan risiko bisnis yang terkait dengan TSI	2	14	17	18	19	20	21	22
√	Meningkatkan *corporate governance* dan transparansi	2	18						
	Sudut Pandang *Customer*								
√	Meningkatkan layanan dan orientasi customer	3	23						
√	Menawarkan produk dan layanan yang kompetitif	5	24						
√	Menetapkan kelangsungan layanan dan ketersediaan	10	16	22	23				
	Menciptakan ketangkasan dalam merespon perubahan kebutuhan bisnis	1	5	25					
	Pencapaian optimalisasi penyampaian layanan	7	3	10	24				
	Mendapatkan informasi yang dapat dipercaya dan berguna untuk pembuatan keputusan strategis	2	4	12	20	26			

Tabel 3.4 Pemetaan antara Objektif Perusahaan dengan Objektif TSI (lanjutan)

REQ'V ANSI	TUJUAN BISNIS	TUJUAN TSI							
	Sudut Pandang Internal								
	Meningkatkan dan memelihara fungsionalitas proses bisnis	6	7	11					
	Menurunkan biaya proses	7	8	13	15	24			
√	Kepatuhan pada hukum, regulasi dan kontrak eksternal	2	19	20	21	22	26	27	
	Kepatuhan dengan kebijakan internal	2	13						
	Pengelolaan perubahan bisnis	1	5	6	11	28			
	Peningkatan dan pemeliharaan produktifitas staf dan operasional	7	8	11	13				
	Sudut Pandang Pembelajaran dan Perkembangan Bisnis								
	Pengelolaan produk dan inovasi bisnis	5	25	28					
	Pengadaan dan pemeliharaan sumber daya manusia yang memiliki pengetahuan, kemampuan dan motivasi	9							

Sumber : Dokumentasi Divisi Audit Intern PT Bank XYZ

3.8.6 Fokus Audit pada PT Bank XYZ

Hasil pemetaan di atas menjadi landasan area atau domain yang akan dijadikan objek atau cakupan audit. PT Bank XYZ ingin mengetahui seberapa besar tingkat ketersediaan (*availability*) informasi ketika dibutuhkan oleh proses bisnis baik saat ini maupun saat mendatang, dan juga mengenai pengamanan dari sumber daya yang dimiliki oleh perusahaan. Maka untuk memenuhi keingintahuan PT Bank XYZ terhadap 2 hal tersebut, maka objektif TSI yang menjadi fokus yang berkaitan dengan hal tersebut adalah objektif TSI No.21, 22, 23 dan 26 (tabel 3.5). Dan rekap proses COBIT yang dijadikan objek audit adalah seperti yang terlihat dalam tabel 3.5 berikut ini. Audit program akan dikembangkan dari proses COBIT tersebut.

Tabel 3.5 Fokus Audit pada PT Bank XYZ

NO	URAIAN TSI	PROSES TSI (COBIT)						
21	Memastikan bahwa layanan dan infrastruktur TSI dapat bertahan dan pulih dari kegagalan akibat error, serangan atau bencana	PO6	AI7	DS4	DS5	DS12	DS13	ME2
22	Memastikan dampak bisnis akibat gangguan pada layanan TSI minimal	PO6	AI6	DS4	DS12			
23	Memastikan kalau layanan TSI tersedia ketika dibutuhkan	DS3	DS4	DS8	DS13			
26	Memelihara integritas informasi dan infrastruktur	PO7	AI6	DS5				

Sumber : Dokumentasi Divisi Audit Intern PT Bank XYZ

Tabel 3.6 Proses COBIT yang akan diaudit

NO	PROSES TI (COBIT)	
1	PO6	Komunikasi Sasaran dan Petunjuk Manajemen
2	PO7	Pengelolaan Sumber Daya Manusia
3	AI6	Manajemen Perubahan
4	AI7	Instalasi Dan Akreditasi Solusi Dan Perubahan
5	DS3	Pengelolaan Kinerja Dan Kapasitas
6	DS4	Kepastian Kelangsungan Layanan
7	DS5	Kepastian Keamanan Sistem
8	DS8	Manajemen *Service Desk* Dan Gangguan
9	DS12	Pengelolaan Lingkungan Fisik
10	DS13	Pengelolaan Operasi
11	ME2	Monitor dan Evaluassi Pengendalian Internal

3.8.7 Audit Program

Pihak DAI mengembangkan audit program berdasarkan penyelarasan antara objektif Perusahaan dengan objektif TI. Dan akhirnya, terdapat 11 proses TI (tabel 3.6) dari 34 proses yang akan menjadi fokus audit. Alasan DAI hanya mengambil 11 proses karena adanya hambatan masalah, SDM, waktu dan juga dengan melihat risiko yang dihadapi oleh Perusahaan.

Penulis tidak melampirkan audit program untuk 11 proses TI tersebut, karena masalah restriksi dokumentasi.

3.9 Tahapan Pekerjaan Lapangan

DAI melakukan *audit field work* untuk mendapatkan bukti-bukti yang diperlukan. Berdasarkan *audit program*, DAI harus mendapatkan bukti-bukti yang mencukupi untuk nantinya memformulasikan kesimpulan, berdasarkan teknik audit tertentu, semisalnya melalui pengujian, observasi, wawancara, dan lain

sebagainya Objek yang dijadikan audit yaitu 13 cabang dan kantor pusat, mereka harus menyediakan informasi yang dibutuhkan oleh DAI. Namun sebelum tahapan pekerjaan lapangan dimulai, DAI telah membuat dan mengirimkan suatu daftar kebutuhan data kepada *auditee* tersebut pada tahap persiapan awal. Penentuan alokasi waktu untuk pekerjaan lapangan adalah antara 7 sampai dengan 14 hari, tergantung besar kecil objek audit juga kompleksitas TI dari cabang tersebut.

3.10 Tahap Pelaporan Audit

Setelah melaksanakan audit dan mengetahui hasilnya, maka tim audit akan menyiapkan LHA (Laporan Hasil Audit). LHA ini sebagai dokumentasi dari audit dari tahap perencanaan sampai dengan akhir pekerjaan lapangan. Di dalam LHA terdapat juga hasil *maturity model level* dari masing-masing level yang telah diaudit, temuan atas hasil audit lapangan.

3.10.1 Maturity Model

Maturity model level disusun setelah DAI mendapatkan informasi pada saat melaksanakan pekerjaan lapangan. Kemudian DAI membuat suatu kertas kerja untuk menentukan penilaian tersebut. Hasil penilaian atas maturity model level yang ditetapkan untuk suatu proses, terdiri dari penilaian atas level proses COBIT dan skor yang dimiliki oleh level yang ditetapkan untuk proses COBIT tersebut.

Penilaian atas level proses COBIT adalah untuk mengakomodasi kriteria-kriteria yang ada di atas level yang diberikan, yaitu kategori terpenuhi, atau sebagian terpenuhi, namun karena ada kriteria yang berada pada level bawah tersebut tidak terpenuhi, maka nilai level yang lebih di atas tersebut menjadi tidak dapat diberikan.

DAI menetapkan penentuan *maturity model level* DAI berdasarkan pemenuhan kriteria untuk tiap proses untuk dikategorikan pada level tertentu. Jika pada level tersebut ada karakterisik yang tidak dipenuhi maka DAI tidak dapat mengkategorikan ke level berikutnya, walaupun ada kriteria lain yang

memenuhi pada level berikutnya tersebut. Dengan kata lain, keseluruhan kriteria harus terpenuhi terlebih dahulu jika ingin naik level.

Metode penetapan *maturity model* yang dibuat oleh DAI adalah sebagai berikut : (sebagai catatan, contoh perhitungan dapat dilihat pada **Lampiran 2**, namun perhitungan secara mendetail (keseluruhan 11 proses) dari *maturity model* TI PT Bank XYZ tidak dapat diungkapkan pada Karya Akhir ini)

1. menentukan detail dari kriteria per level.

   Level 0- *Non existence* sampai dengan level 5-Optimised mempunyai kriteria yang harus dipenuhi
2. kemudian menghitung skor : Total skor = importance x score

   Tiap kriteria dari tiap level akan diberikan timbangan (*importance)* tersebut. Importance terdiri dari 4 kategori yaitu : None (0) , Low (L=0,5), Medium (M=1) dan H(High=2)

   Dan setelah menentukan timbangan tersebut, tiap kriteria juga akan diberi skor. *Score* yang terdiri dari :

   Nilai 0 (jika kriteria tidak dipenuhi) ; 0,5 (kriteria tidak sepenuhnya dipenuhi) ; 1 (kriteria memenuhi, atau melebihi)

   Kemudian per kriteria tersebut dihitung untuk mendapatkan total skor dengan rumus di atas.
3. membuat *score summary* :

   Total Skor yang diberikan atas setiap level dari proses COBIT dibuat rekapannya. Mulai dari level 0 sampai dengan 5.
4. penentuan level

   Penentuan level dari 0 (Non Existence) sampai dengan 5 (Optimised) ditentukan berdasarkan kriteria dari tiap level jika setiap kriteria tersebut mempunyai skor : terpenuhi atau sebagian terpenuhi (skor 1 atau 0,5).
5. penentuan Skor

   Total penilaian skor dijumlah (yang tergantung dengan timbangan skor) dari tiap kriteria, dan ditentukan (100/6) % per level. Jadi setiap kriteria dengan semua level untuk yang terpenuhi, terdapat nilai 0% - 100% skor penuh akan diberikan kepada setiap level tersebut.

Dengan demikian, penentuan skor ini akan membuat semua level akan dapat dihitung sesuai dengan kriteria nilai terpenuhi, jika terdapat kriteria satu atau dua level yang berada di bawahnya tidak terpenuhi/hilang. Dengan hal yang seperti ini, level mungkin rendah, namun total skor lebih tinggi dibandingkan dengan level yang diindikasikan.

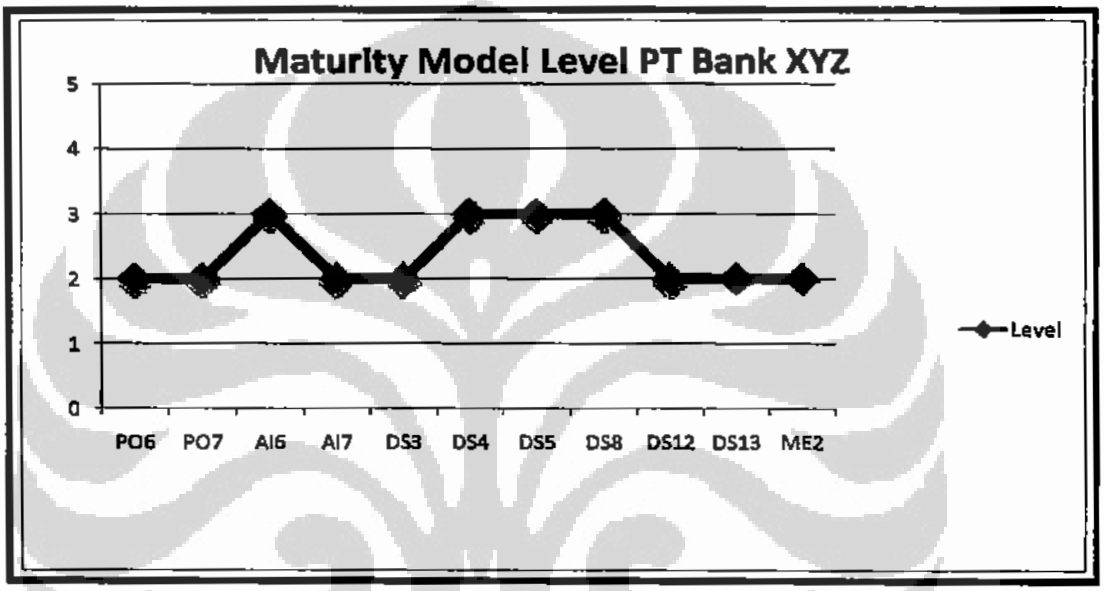
3.10.2 Hasil Maturity Model Level

Hasil maturity model level per proses didapatkan Penulis dari Laporan Hasil Audit TI PT Bank XYZ. Detail perhitungan sebagaimana pada 3.10.1 tidak dapat diungkapkan pada Karya Akhir ini. DAI mendapatkan hasil maturity model level setelah menerapkan formula pada (3.10.1).untuk masing-masing 11 proses. Berdasarkan 11 proses TI yang telah diaudit oleh DAI tersebut, hasil rekapan *maturity model level* PT Bank XYZ dapat dilihat pada tabel 3.7 (disusun oleh Penulis) dan gambar 3.6. Nilai rata-rata sebesar 2,36 merupakan status level TI PT Bank XYZ sehingga berada pada rentang level 2 *repeatable but intuitive* dan level 3 *defined process*

Tabel 3.7 *Maturity Model Level*

No	Proses COBIT		Maturity					Skor
			0	1	2	3	4	
1	PO6	*Communicate Management Aims and Direction*			√			2
2	PO7	*Manage IT Human Resources*			√			2
3	AI6	*Manage Changes*				√		3
4	AI7	*Initial and Accredit Solutions and Changes*			√			2
5	DS3	*Manage Performance and Capacity*			√			2
6	DS4	*Ensure Continous Service*				√		3
7	DS5	*Ensure Systems Security*				√		3
8	DS8	*Manage Service Desk and Incidents*				√		3
9	DS12	*Manage the Physical Environment*			√			2

No	Proses COBIT		Maturity						Skor
10	DS13	*Manage Operation*			√				2
11	ME2	*Monitor and Enable Internal Control*			√				2
		Jumlah							**26**
		Rata-rata							**2.36**



Gambar 3.6 Maturity Model Level PT Bank XYZ berdasarkan Audit DAI

3.11 Tahap Monitoring Audit

Tim audit memantau temuan hasil audit yang perlu ditindaklanjuti. Tim audit akan memberikan surat pemberitahuan kepada *auditee* dan mengawasi tindaklanjut dari surat pemberitahuan tersebut. Jika surat pemberitahuan tidak ditindaklanjuti pada kurun waktu tertentu, maka akan dikirimkan surat peringatan.

Dengan demikian audit internal yang dilakukan DAI merupakan suatu siklus, yang tidak berhenti, secara terus menerus, untuk memperbaiki TI PT Bank XYZ.

BAB 4
ANALISIS DAN HASIL AUDIT

4.1 Urgensi Tata Kelola TI bagi PT Bank XYZ dan Audit Tata Kelola TI

Audit tata kelola TI pada perusahaan bertujuan untuk memberikan *assurance* atau kepastian bagi manajemen atas tata kelola TI yang sedang berjalan di Perusahaan. DAI menjalankan proses audit *IT governance* dari perencanaan sampai dengan monitoring pada DTI dan bank cabang, yang hasil akhirnya akan dilaporkan kepada pimpinan puncak yaitu Direktur Utama. Bagi Dirut dan jajarannya, laporan audit yang berupa *executive summary* nantinya akan digunakan sebagai bahan pengambilan keputusan yang akan mendukung pencapaian objektif perusahaan dan objektif TI.

PT Bank XYZ meyakini bahwa tata kelola TI terutama dengan melakukan auditnya akan memberikan perbaikan TI dan arahan untuk mencapai tingkat TI yang diinginkan perusahaan.

Urgensi tata kelola TI yang diungkapkan oleh Weill dan Ross (2002)[1], juga menyebutkan bahwa nilai investasi untuk TI sangat mahal maka untuk itu dibutuhkan suatu tata kelola TI yang akan memberikan hasil sepadan. Dengan adanya audit tata kelola TI, PT Bank XYZ dapat mengetahui sebenarnya nilai apa yang telah diberikan oleh TI untuk organisasi. Apakah TI telah mencapai tujuan yang telah diharapkan oleh PT Bank XYZ yang berfokus pada penyempurnaan infrastruktur yang memberikan penekanan pada sistem pelayanan nasabah dan keamanannya, sebagaimana yang menjadi tujuan manajemen yang diungkapkan pada *annual report*-nya atau sebaliknya.

Proses audit dan metodelogi tata kelola TI oleh Divisi Audit Internal PT Bank XYZ telah dijelaskan pada Bab III Gambaran Umum. Pada Bab IV Analisis dan Hasil Audit berikut ini, akan dipaparkan audit tata kelola yang dilakukan oleh Penulis, yang langkah-langkahnya adalah sebagai berikut :

---

[1] Peter, Weill dan Jeanne W.Ross, *IT Governance, How Top Performers Manage IT Decisions Rights for Superior Results.*

1) Penulis melakukan perencanaan

2) Melakukan penilaian terhadap risiko (*risk assessment*)

   Menentukan risiko dengan model audit berbasis risiko seperti dalam persamaan (4.1). Berupa pemaparan *inherent risk, internal control risk* dan kelemahannya, termasuk mitigasi internal control terhadap *inherent risk.* Paparan mengenai *Internal control* yang diterapkan oleh PT Bank XYZ didapatkan melalui kuisioner dan wawancara dengan personil DTI yang kompeten.

3) Pengembangan audit program

   Berdasarkan audit objektif yang sesuai *IT assurance guide* yang dikeluarkan ISACA. Penulis telah menetapkan audit program untuk 34 proses berdasarkan kerangka COBIT yang dapat dilihat pada bagian Lampiran 3. Di dalamnya terdapat pemaparan *audit scope, audit objective, audit procedures.*

4) Pengambilan Bukti

   Didapatkan melalui proses audit lapangan dengan cara mendapatkan dokumen, observasi, wawancara dan pengisian kuisioner. Kuisioner dapat dilihat pada Lampiran 4. Kuisioner diberikan kepada 1 orang dari DTI. Penyusunan kuisioner berdasarkan audit program yang dilihat pada Lampiran 3. Kuisioner yang terdapat pada Karya Akhir ini, bersumber dari Karya Akhir yang berjudul "Audit TI Menggunakan COBIT 4.1 di Direktorat Jenderal Anggaran Departemen Keuangan" oleh Risnawati Kumala Dewi, . Hasil dari kuisioner tercantum juga pada paparan dari 34 proses COBIT pada PT Bank XYZ (bagian 4.4)

5) Kesimpulan

   Kesimpulan diambil dari paparan 34 proses COBIT untuk menetapkan status TI PT Bank XYZ berdasarkan *maturity model level* yang dibuat Penulis beserta perbandingan dengan maturity model yang dibuat oleh DAI (bagian 4.5)

6) Menyiapkan opini audit.

Menyiapkan opini yang akan dikomunikasikan kepada PT Bank XYZ yang terdapat pada bagian 4.5

7) Rekomendasi

Memberikan rekomendasi kepada PT Bank XYZ (pada bagian 4.6 dan Bab 5 Kesimpulan dan Saran)

4.2 Model Audit Berbasis Risiko – PT Bank XYZ

Seperti yang telah dipaparkan dalam BAB II Landasan Teori, 2.9 Model Audit Berbasis Risiko. Formula dari risiko audit adalah :

Audit risk =

Inherent Risk (IR) x Internal Control Risk (CR) x Detection Risk (DR) (4.1)

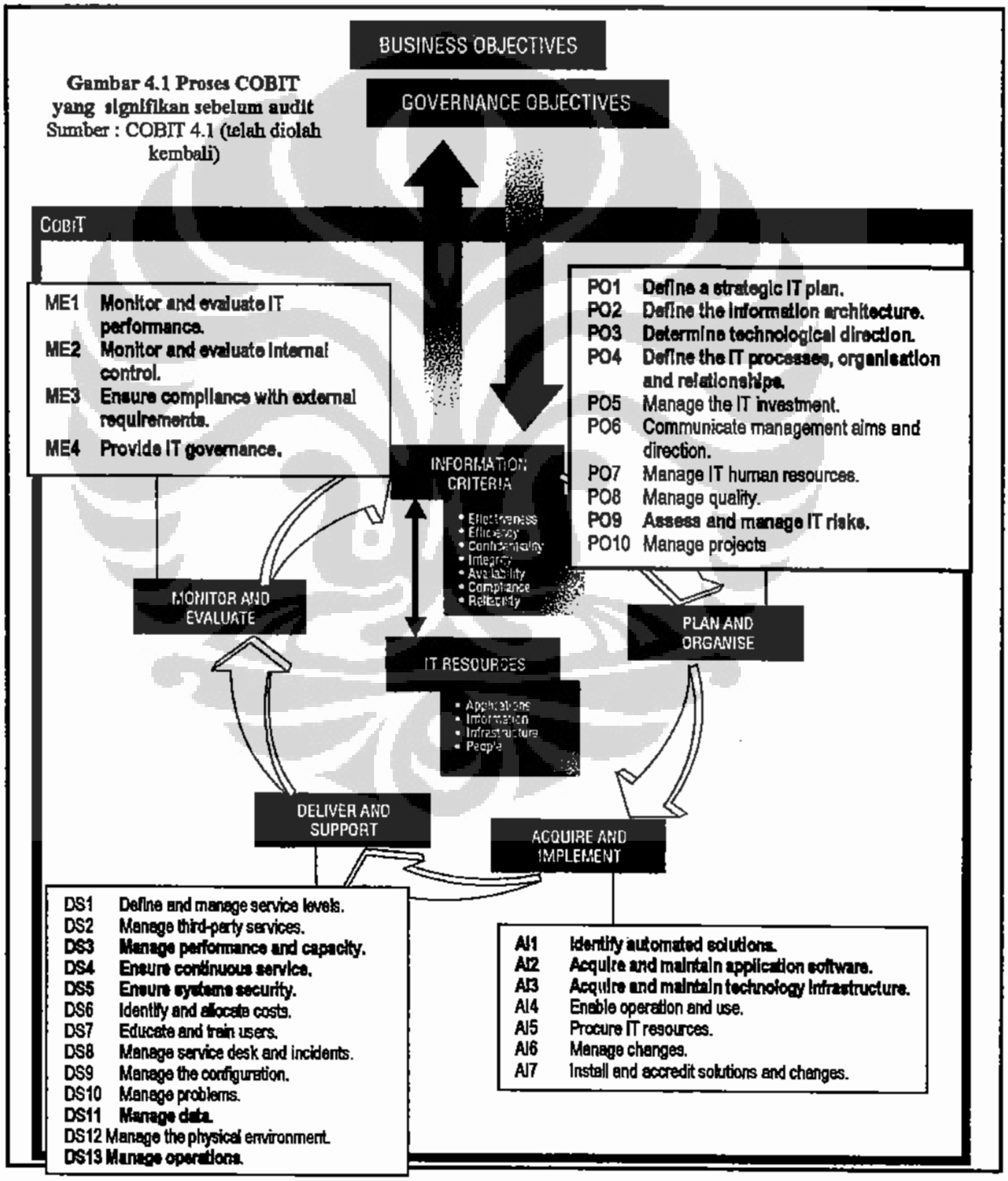
Risiko audit merupakan kombinasi antara *inherent risk*, *internal control risk* dan *detection risk*. Auditor biasanya menggunakan judgement untuk menentukan risiko tersebut, agar mencapai level risiko yang dapat diterima oleh auditor. Dengan demikian, jika auditor menginginkan *audit risk* tidak tinggi, maka ia harus mengumpulkan lebih banyak bukti, dan memfokuskan pada area cakupan audit dalam hal ini cakupan proses COBIT yang kemungkinan *IT control objective*-nya lebih mempengaruhi Perusahaan, lebih signifikan dibandingkan yang proses yang lainnya.

Penulis telah menetapkan tingkat level dari *audit risk* adalah **medium**. Dasar atas penetapan tersebut adalah atas penelahaan risiko bawaan Perusahaan dan *judment* Penulis, berikut uraiannya :

- *inherent risk* perusahaan : tinggi (bagian **4.3 *Inherent risk***)
- *internal control risk* : tinggi (sebelum dilakukan audit lapangan)
- *detection risk* : rendah

Sehingga, Audit risk = tinggi (IR) X tinggi (CR) x rendah (DR) = medium

➢ Dengan demikian, Penulis sebagai auditor, akan mengumpulkan lebih banyak bukti dan memfokuskan pada area proses COBIT tertentu. Penulis telah membuat asumsi awal dan **dapat dimodifikasi** setelah proses audit mengenai proses COBIT yang akan dipilih berdasarkan *judgment* penulis yang didasari bahwa proses tersebut dapat memitigasi risiko di atas. Proses COBIT yang difokuskan adalah 17 item proses COBIT yang ditulis tebal pada gambar *COBIT frameworks* berikut ini :



Gambar 4.1 Proses COBIT yang signifikan sebelum audit
Sumber : COBIT 4.1 (telah diolah kembali)

4.2.1 Inherent Risk (Risiko Bawaan)

Sebagaimana di dalam Bab 2 Landasan Teori, seorang auditor harus memahami entitas yang akan diaudit (telah dijelaskan pada Bab 3. Gambaran Umum), dan seberapa risiko yang melekat pada sebuah entitas. Risiko bawaan bagi PT Bank XYZ adalah termasuk risiko tinggi, hal tersebut dikarenakan :

1) PT Bank XYZ merupakan bagian dari industri perbankan, industri perbankan dipengaruhi oleh banyak risiko, diantaranya risiko kredit, risiko pasar, risiko likuiditas, risiko operasional, risiko hukum, risiko reputasi, risiko strategik, risiko kepatuhan. Risiko-risiko ini, sesuai dengan Peraturan BI, PBI No.5/8/PBI/2003 tentang penerapan manajemen risiko bagi bank umum
2) Banyaknya regulasi dan ketentuan berbagai pihak
   PT Bank XYZ sebagai salah satu bank di Indonesia harus mengikuti regulasi Bank Indonesia. Dan sebagai salah satu bank BUMN, ketentuan pemerintah yang berkait dengan jalannya Perusahaan. Ketidaktaatan terhadap regulasi dan ketentuan pemerintah akan menimbulkan risiko bagi PT Bank XYZ. Juga pihak asing jika terdapat transaksi internasional
3) Transaksi harian tinggi
   Dibandingkan dengan industri lainnya, transaksi harian yang terjadi di bank jauh lebih banyak dibandingkan industri lainnya, misalnya jika dibandingkan dengan perusahaan manufaktur atau perdagangan. Kesalahan pencatatan transaksi lebih mungkin terjadi pada perusahaan perbankan
4) PT Bank XYZ mempunyai banyak kantor Cabang
   Dengan banyaknya cabang, dan setiap kantor cabang mempunyai risiko bawaan sendiri, PT Bank XYZ juga ikut menanggung risiko bawaan tersebut.
5) Penerapan Teknologi Informasi
   Tidak bekerjanya infrastruktur TI menyebabkan berbagai risiko. Termasuk adanya efek ke nasabah, misalnya dengan bervariasinya produk perbankan yang ditawarkan oleh PT Bank XYZ yang didukung oleh sarana TI, seperti transaksi *bank online*, ATM, SMS Banking, menimbulkan risiko dimana para nasabah akan kesulitan melakukan transaksi perbankan dari TI ketika TI mengalami permasalahan. Atau contoh lainnya, adanya keterlibatan pihak

ketiga sebagai penyedia layanan bagi TI perusahaan, menimbulkan risiko terhadap kerahasiaan Perusahaan. Beberapa uraian di atas hanya sebagian kecil dari risiko-risiko dari TI.

4.2.2 Paparan dan Analisis Pengendalian Internal, Kelemahan serta Risikonya

1) Pengendalian internal pada Perusahaan

PT Bank XYZ telah menerapkan pengendalian internal untuk pengamanan aset perusahaan yang digunakan dalam bisnisnya. Bila dikaitkan dengan *internal control* pada TI Perusahaan, PT Bank XYZ telah menerapkan pengendalian internal baik untuk TI dan non TI.

Berkaitan pengendalian internal dengan TI, sistem COBIT telah diterapkan di PT Bank XYZ sejak tahun 2005. COBIT diterapkan oleh PT Bank XYZ karena dianggap implementasinya akan memberi benefit terutama bagi pengendalian internal untuk TI secara komprehensif.

Pengendalian internal TI lainnya adalah PT Bank XYZ telah membuat perencanaan TI yang mendukung bisnis. PT Bank XYZ juga telah membuat struktur organisasi yang mendukung fungsi TI termasuk diantaranya terdapat CIO dan jajarannya, juga Komisi Pengarah Teknologi Informasi sebagai *IT Steering dan strategy Committee*. Berbagai *Standard Operational Procedures* (SOP) TI juga telah dibuat, disahkan dan diimplementasikan. Penulis hendak memasukkan perincian SOP yang dimiliki oleh PT Bank XYZ namun karena adanya kendala restriksi, tidak dapat dipaparkan dalam Karya Akhir ini. Beberapa bagian yang telah disebutkan di atas hanya sebagian kecil dari internal control TI yang diterapkan oleh PT Bank XYZ.

2) Kelemahan, Risiko dan rekomendasi kelemahan Pengendalian internal

Walaupun perusahaan telah menerapkan pengendalian internal, namun di dalam pengendalian tersebut masih terdapat kelemahan. Berikut ini merupakan analisis dari kelemahan pengendalian internal perusahaan dan rekomendasinya.

Hasil ini dicapai setelah sebelumnya membuat audit program (dapat dilihat dalam bagian Lampiran 3) dan melakukan fase audit lapangan. Dan berikut ini merupakan daftar kelemahan, risiko dan rekomendasi kelemahan pengendalian internal yang didapatkan dari kuisioner (Lampiran 4) dan wawancara kepada salah satu orang staf DTI.

Tabel 4.1 Kelemahan, Risiko dan Rekomendasi Kelemahan Pengendalian Internal

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
1	Pemutakhiran kebijakan TI sesuai dengan kebutuhan tidak berbasis perencanaan jangka pendek dan jangka panjang	Pemutakhiran kebijakan TI yang berbasis pada kebutuhan saja, akan melenceng dari jalur perencanaan strategi TI.	Kebijakan dibuat sesuai waktu yang telah ditetapkan Perusahaan, dengan memperhatikan keselarasan antara tujuan TI dan bisnis, dengan perencanaan jangka pendek dan panjang	PO1 - Berdasarkan proses wawancara dengan personil TI. (KM)
2	Adanya beberapa SOP yang belum dapat diimplementasikan karena belum disetujui oleh manajemen.	Kebijakan yang belum disetujui padahal dibutuhkan segera, akan menghambat kinerja	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO1 - Berdasarkan proses wawancara dengan personil TI (KM)
3	Proses yang digunakan untuk memperbarui model arsitektur informasi atas kebutuhan bisnis, bukan berdasarkan perencanaan jangka pendek atau jangka panjang seperti yang direkomendasikan COBIT.	Perubahan pada model arsitektur sesuai dengan kebutuhan bisnis merupakan hal yang positif karena itu berarti selarasnya tujuan TI dan bisnis, namun perubahan yang terjadi secara tiba-tiba tanpa perencanaan terlebih dahulu, akan mungkin terjadi ketidakonsistenan pada model arsitektur TI yang sudah ada sebelumnya.	Memperbarui model arsitektur sesuai dengan waktu yang telah ditetapkan Perusahaan, dengan memperhatikan keselarasan perencanaan jangka pendek dan panjang serta kebutuhan bisnis	PO2 KK-PO2 (2)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
4	Belum ada SOP yang menerangkan/menjelaskan peran dan tanggung jawab seluruh personel dalam organisasi, yang berhubungan dengan sistem informasi, pengendalian internal dan keamanan (masih dalam proses pengerjaan, namun terdapat peraturan direksi mengenai susunan organisasi)	Belum adanya SOP tersebut, akan menyebabkan pembagian kerja, pengendalian internal dan keamanan menjadi menjadi tidak efektif.	Membuat target waktu dan memonitor penyelesaian SOP yang menjelaskan peranan dan tanggung jawab personil dengan sistem pengendalian internal dan keamanan	PO4-KK-PO4 (10)
5	Belum ada SOP yang mencakup kepemilikan data dan sistem bagi seluruh sumber data utama dan sistem (sedang dalam proses pengerjaan)	Praktek yang terjadi di lapangan, tidak sesuai dengan standar, atau tidak sesuai dengan yang diharapkan Perusahaan. Akan timbul risiko lainnya	- Membuat target waktu dan memonitor penyelesaian SOP kepemilikan data dan sistem - Memitigasinya dengan peraturan yang sesuai	PO4,KK-PO4(27)
6	Belum ada SOP untuk melakukan evaluasi kembali dari deskripsi posisi (pekerjaan) TI , namun, DTI masih dalam proses pembuatan kebijakan tersebut.	Ketiadaan SOP tersebut, menyebabkan tidak adanya *review* atas pekerjaan yang sudah dilakukan oleh personil DTI, jadi tidak diketahui apakah sudah benar atau tidak yang dikerjakannya, apalagi jika terdapat perkembangan TI yang pesat di PT Bank XYZ	- Membuat target waktu dan memonitor penyelesaian SOP yang berisi kriteria untuk evaluasi pekerjaan - Memitigasinya dengan peraturan yang sesuai	PO4, KK-PO4(27)
7	Belum ada SOP dalam menangani proses TI, yang meliputi perumusan tindakan-tindakan untuk menghadapi kejadian di luar dugaan, pendokumentasian pengetahuan yang penting, pelatihan bagi personel TI, transfer tanggung jawab, dsb, sehingga jika personel yang	Ketiadaan dari SOP tersebut, akan menyebabkan praktek yang dilakukan menjadi tidak sesuai dengan standar yang diharapkan Perusahaan.	- Membuat target waktu dan memonitor penyelesaian SOP proses TI yang komprehensif - Memitigasinya dengan peraturan yang sesuai	PO4, KK-PO4(29)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
	bertanggung jawab terhadap suatu proses/personel utama berhalangan hadir, maka personel lain dapat menggantikannya. (Masih dalam proses pembuatan)			
8	Belum adanya KPI (*Key Performance Indicator*) dan KSF (*Key Success Factor*) yang tepat dan efektif dalam mengukur hasil-hasil dari fungsi TI dalam mencapai tujuan Perusahaan (PT Bank XYZ sedang menyusun KPI dan KSF)	Ketidaan KPI dan KSF, menyebabkan sulitnya untuk mengukur kinerja dari fungsi TI. Tidak diketahui apakah telah efektif dan efisien fungsi TI dalam mencapai tujuan Perusahaan. Termasuk bagi personil TI	Membuat KPI dan KSF bersama pihak ketiga (konsultan, vendor) yang disesuaikan dengan kondisi perusahaan	PO4,KK-PO4(31)
9	Belum ada SOP TI untuk mengendalikan berbagai aktifitas konsultan dan personel kontrak untuk memastikan perlindungan dari aset. (Masih dalam proses Penyusunan)	Ketiadaan dari SOP tersebut menyebabkan kemungkinan terjadinya ancaman terhadap aset Perusahaan oleh pihak ketiga.	- Membuat target waktu dan memonitor penyelesaian SOP aktivitas konsultan. - Memitigasinya dengan peraturan yang sesuai	PO4, KK-PO4(32)
10	Belum ada SOP yang dapat diterapkan pada jasa TI kontrakan untuk kecukupan dan konsistensi dengan kebijakan akuisisi yang dimiliki oleh Perusahaan. (Masih dalam proses penyusunan)	Ketiadaan dari SOP tersebut menyebabkan praktek yang tidak sesuai standar dalam menghadapi jasa TI kontrak, lebih lanjut Perusahaan akan bisa dirugikan oleh pihak pemberi jasa tersebut, terutama karena akhirnya akuisisi layanan, sebenarnya tidak menunjang dengan apa yang dibutuhkan oleh bisnis Perusahaan	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO4,KK-PO4(33)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
11	Belum ada SOP untuk memastikan persiapan dan persetujuan dari sebuah anggaran operasi TI tahunan Perusahaan serta rencana jangka panjang dan jangka pendek. (Masih dalam proses penyusunan)	Ketiadaaan dari SOP tersebut, menyebabkan praktek dalam persiapan dan persetujuan anggaran terjadi tidak konsisten, ada hal-hal yang terlewat untuk menetapkan suatu anggaran.	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO5, KK-PO5(2) (KM)
12	Belum ada SOP untuk menjamin bahwa jasa yang diberikan oleh fungsi TI dijelaskan/dibuktikan dalam hal biaya, dan memiliki kesesuaian dengan biaya rata-rata pada umumnya. (Masih dalam proses Penyusunan)	Ketiadaaan dari SOP tersebut, menyebabkan adanya praktek penyelewengan anggaran, terjadinya mark up biaya.	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO5,KK-PO5(7)
13	Belum ada SOP yang memenuhi kebutuhan dilakukannya review secara periodik dan persetujuan kembali terhadap standar-standar, aturan, kebijakan, dan prosedur utama/pokok yang berhubungan dengan TI. (masih dalam proses Penyusunan).	Ketiadaan dari SOP tersebut, akan menyebabkan standar-standar yang telah ada tidak *up to date*, tidak mampu mengatasi permasalahan yang timbul, karena cara penanganannya telah berbeda, akibat dinamisasi perkembangan TI.	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO6,KK-PO6(9)
14	Belum ada dokumen kerangka keamanan dan pengendalian internal yang menspesifikasikan kebijakan keamanan dan pengendalian internal, maksud dan tujuan, struktur organisasi, ruang lingkup dalam organisasi, pemberian tanggung jawab, dan definisi dari pinalti serta tindakan disiplin lainnya yang berhubungan dengan kegagalan untuk mematuhi kebijakan keamanan (Masih dalam	Ketiadaan dokumen tersebut, menyebabkan ketika terjadi pelanggaran, tidak ada hukum yang membuat efek jera pelaku pelanggaran, sehingga kesalahan yang sama memungkinkan terjadi di masa mendatang	- Membuat target waktu dan memonitor penyelesaian pembuatan dokumen kerangka keamanan - Memitigasinya dengan peraturan yang sesuai	PO6,KK-PO6(11)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
	tahap penyusunan)			
15	Belum terdapat SOP yang sejalan dengan strategi TI dan lingkungan pengendalian.	Perusahaan menetapkan strategi perusahaan tanpa melihat lingkungan pengendalian. Sehingga kesuksesan pencapaian strategi Perusahaan akan terhambat.	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	PO6,KK-PO6(17)
16	Belum diterapkan sanksi-sanksi administratif yang sesuai terhadap pelanggaran kebijakan TI Perusahaan.	Kemungkinan pelanggaran kebijakan akan terulang kembali.	Melakukan sosialisasi mengenai peraturan dan sanksi jika melakukan pelanggaran,dan memfungsikan perangkat pengawasan	PO6
17	Belum ada kebijakan terhadap semua pegawai, kontraktor dan vendor di Perusahaan yang memadai.	Ketiadaaan menimbulkan risiko bagi keamanan aset Perusahaan.	Menyusun kebijakan tersebut sesuai target yang ditetapkan	PO7, KK-PO7(13), (KM)
18	Belum terdapat suatu *Quality Management System* (QMS) atau semacamnya yang mengidentifikasi kebutuhan kualitas dan kriteria TI di Perusahaan; proses TI yang penting; kebijakan, kriteria dan metode untuk mendefinisikan, mendeteksi, mengkoreksi dan mencegah terjadinya pelanggaran. (dalam proses penyusunan)	Aktivitas TI tidak didorong untuk mencapai tingkat efektif dan efisien.	Membuat target waktu dan memonitor untuk penyelesaian QMS tersebut dengan konten yang menyeluruh	PO8,KK-PO8(1)
19	Belum adanya SOP untuk mengimplementasikan suatu pendekatan *procurement* pusat, yang menggambarkan serangkaian prosedur dan standar yang harus diikuti dalam mendapatkan perangkat keras TI, perangkat lunak, dan jasa lainnya. (Masih dalam proses pengembangan)	Tanpa adanya procurement secara terpusat, pengadaannya dapat terjadi secara serampangan, masing-masing pihak ingin terpenuhi kebutuhannya.	- Membuat target waktu dan memonitor penyelesaian SOP - Menggunakan peraturan Perusahaan untuk pengadaan logistik	AI1, KK-AI1(5), (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
20	PT Bank XYZ tidak memanfaatkan *artificial intelligence system* dalam interaksi atau pengendalian dengan operator manusia, untuk memastikan pengambilan keputusan yang penting telah disetujui.	Pemecahan masalah akan lebih memakan waktu	Menggunakan AI sebagai alternatif pengambilan keputusan	AI2, KK-AI2(7) , (KM)
21	Tidak terdapat SOP yang memastikan dibuatnya suatu rencana evaluasi formal untuk menilai pengaruh/dampak perangkat keras dan perangkat lunak baru terhadap performa keseluruhan sistem	Tidak diketahui apakah pelaksanaan untuk mengetahui infrastruktur TI tersebut sudah memberikan kinerja yang efektif atau efisien dilaksanakan sesuai standar atau tidak	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
22	Tidak terdapat SOP yang membahas dibatasinya kemampuan untuk melakukan akses sistem perangkat lunak	Tanpa pembatasan akses perangkat lunak akan terjadi penyalahgunaan perangkat lunak	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
23	Tidak terdapat SOP mengenai proses *set-up*, instalasi dan pemeliharaan perangkat lunak sistem tidak membahayakan keamanan data dan program yang sedang disimpan dalam sistem	Tanpa SOP tersebut, proses set up, instalasi, pemeliharaan, berlangsung tidak aman.	- Membuat target waktu dan memonitor penyelesaian SOP mengenai perangkat lunak - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
24	Tidak terdapat SOP yang mengatur perangkat lunak sistem di-*install* dan dipelihara sesuai dengan kerangka akuisisi dan pemeliharaan infrastruktur teknologi	Perangkat lunak yang di-*install* tidak sesuai dengan yang ditetapkan oleh kerangka akuisisi dan pemeliharaan infrastruktur teknologi. Terdapat inkonsistensi.	- Membuat target waktu dan memonitor penyelesaian SOP pengaturan perangkat lunak - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
25	Tidak terdapat SOP yang mengatur pemasok (*vendor*) perangkat lunak	Perangkat lunak dari pemasok tidak dapat dijamin integritasnya	- Membuat target waktu dan memonitor	AI3, KK-AI3(1), (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
	dimana sistem tersebut memberikan kepastian integritas akan perangkat lunak mereka dan modifikasi pada perangkat lunak mereka	bahkan tidak mempunyai integritas.	penyelesaian SOP mengenai pemasok - Memitigasinya dengan peraturan akuisisi logistik Perusahaan	
26	Tidak terdapat SOP yang memastikan dilaksanakannya pengujian yang menyeluruh dari perangkat lunak sistem sebelum digunakan dalam lingkungan yang sebenarnya, yang meliputi pengujian terhadap *functionality, security, availability,* dan *integrity condition*	Tidak diketahui kepastian kinerja dari perangkat lunak.	- Membuat target waktu dan memonitor penyelesaian SOP mengenai perangkat lunak - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
27	Tidak terdapat SOP yang memastikan diubahnya kata sandi (*password*) instalasi perangkat lunak yang diberikan oleh pemasok pada saat dilakukannya instalasi	Keamanan dari sistem perangkat lunak tidak terjamin	- Membuat target waktu dan memonitor penyelesaian SOP mengenai perangkat lunak - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(1), (KM)
28	Tidak terdapat SOP yang memastikan pemeliharaan preventif dari perangkat keras (yang dioperasikan oleh fungsi TI dan fungsi pengguna) untuk mengurangi frekuensi dan dampak kegagalan performa sistem.	Perangkat keras menjadi cepat usang dan berdampak terjadinya pengurangan frekuensi dan kegagalan kinerja sistem	- Membuat target waktu dan memonitor penyelesaian SOP mengenai perangkat keras - Memitigasinya dengan peraturan yang sesuai	AI3, KK-AI3(2), (KM)
29	Tidak terdapat SOP yang memastikan bahwa perubahan formal agar seluruh permintaan yang mencakup perubahan aplikasi, proses, sistem dan layanan dan *platform*, ditangani sesuai standar yang berlaku.	Proses perubahan aplikasi, proses, sistem dan layanan tidak ditangani sesuai standar, sehingga dapat terjadi kesalahan	- Membuat target waktu dan memonitor penyelesaian SOP perubahan - Memitigasinya dengan peraturan yang sesuai	AI6, KK-AI6(1), (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
30	Pendokumentasian mengenai status perubahan infrastruktur dan aplikasi pada PT Bank XYZ masih kurang lengkap	Proses pelacakan status perubahan akan sulit dilakukan.	- Membuat SOP yang berisi mengenai perubahan infrastruktur, termasuk di dalam SOP tersebut pihak mana yang bertugas membuat status perubahan	AI6, Sumber : dari personil PT Bank XYZ, (KM)
31	Materi pelatihan untuk setiap perubahan masih kurang.	Kurang pemahaman mengenai manajemen perubahan yang berpengaruh kepada kinerja personil TI	Tim pembuat materi membuat materi sesuai dengan kebutuhan organisasi	AI6, Sumber : dari personil PT Bank XYZ, (KM)
32	Tidak optimalnya proses perubahan yang disebabkan lambatnya respon dari pihak yang terkait dengan proses perubahan.	Proses perubahan yang lama berpengaruh kepada kinerja TI dan operasional perusahaan	Adanya penugasan disertai dengan target penyelesaian	AI7, Sumber : dari personil PT Bank XYZ (KM)
33	Tidak ada SOP yang memastikan terdapatnya proses persetujuan tingkat jasa/layanan (*service level agreement*) diidentifikasi dengan kebijakan.	Pembuatan SLA tidak menjadi suatu standar proses persetujuan tingkat layanan. Tingkat layanan menjadi tidak jelas	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	DS1,KK-DS(1)
34	Belum terdapat SOP mengenai hubungan TI dengan pihak ketiga (*third party relationship*)	Hubungan antara DTI dan pihak ketiga menjadi tidak jelas, terutama mengenai pengaturan hak dan kewajibannya	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	DS2,KK-DS2(2), (KM)
35	Belum ada aktifitas untuk memprediksi beban kerja dan sumber daya TI yang diperlukan.	Dapat terjadi over limit berpengaruh kepada kinerja	Membuat suatu analisis beban kerja, sumber daya TI yang diperlukan	DS3, Sumber : dari personil PT Bank XYZ, (KM)
36	Belum ada proyeksi mengenai beban kerja yang dibutuhkan pada saat puncak.	Dapat terjadi over limit pada saat puncak, berpengaruh kepada kinerja sistem	Membuat suatu analisis beban kerja secara regular dan dimasukan di dalam SOP	DS3, Sumber : dari personil PT Bank XYZ (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
37	Masih terdapat permasalahan di dalam mesin produksi, adanya duplikasi data	integritas data operasional bank terancam	Melakukan pemantauan secara regular. Menerapkan software khusus untuk menghilangkan duplikasi data	DS3, Sumber : dari personil PT Bank XYZ, (KM)
38	Belum ditetapkannya SOP mengenai kepatuhan terhadap kebijakan dalam hal keamanan	Kualitas keamanan menjadi dipertanyakan	- Membuat target waktu dan memonitor penyelesaian SOP mengenai kepatuhan Keamanan - Memitigasinya dengan peraturan yang sesuai	DS3,KK-DS5(3) , (KM)
39	Belum ditetapkannya SOP mengenai komunikasi eksternal dalam hal kebijakan keamanan	Bila terjadi *contigency*, Perusahaan akan kesulitan dalam mengkontak pihak keamanan	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(3), (KM)
40	Belum ditetapkannya SOP mengenai kebijakan dalam hal keamanan e-mail	Email komersial akan membebani sistem, selain itu keamanannya tidak terjamin, adanya virus, trojan,dll	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(3), (KM)
41	Belum ditetapkannya SOP mengenai kesepakatan untuk mematuhi kebijakan sistem informasi yang ada	Kecenderungan untuk melanggar kebijakan sistem informasi yang ada lebih mudah	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(3), (KM)
42	Belum ditetapkannya SOP mengenai kebijakan pengamanan dalam hal laptop/desktop	Kecenderungan untuk meng-*install software* yang tidak sesuai dengan bisnis, dan software bacakan lebih sering	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya	DS5,KK-DS5(3), (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
		terjadi	dengan peraturan yang sesuai	
43	Belum ditetapkannya SOP mengenai kebijakan dalam hal penggunaan internet	Penggunaan internet dilakukan karyawan pada jam kerja, mengganggu kinerja karyawan dan sistem informasi	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(3), (KM)
44	Belum ditetapkannya SOP mengenai *IT security plan* mempertimbangkan *IT tactical plans*, klasifikasi data, standar teknologi, keamanan dan kebijakan pengendalian, manajemen risiko dan syarat kepatuhan dari pihak eksternal	Sekuriti sistem menjadi lebih rentan, lebih lanjut keamanan TI Perusahaan terancam	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(4), (KM)
45	Belum ditetapkannya SOP mengenai terdapatnya suatu proses yang secara periodik yang akan meng-*update IT security plan*, dan proses *update* tersebut di-*review* dan disetujui oleh manajemen	Sekuriti sistem menjadi sedikit lebih rentan terhadap ancaman dari luar	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(5) (KM)
46	Belum ditetapkannya SOP *IT Security plan* menyangkut kebijakan keamanan yang lengkap dan standar yang sejalan dengan kerangka kebijakan keamanan informasi yang dikembangkan	Sekuriti sistem menjadi sedikit lebih rentan terhadap ancaman dari luar	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)
47	Belum ditetapkannya SOP *IT Security plan* menyangkut implementasi kebijakan dan standar	Tidak adanya pemutakhiran terhadap pemecahan masalah dari sekuriti	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
48	Belum ditetapkannya *SOP IT Security plan* menyangkut Peran dan tanggung jawab staf	Peran dan tanggung jawab diantara personil menjadi tumpang tindih, bahkan satu sama yang lain saling mengandalkan	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)
49	Belum ditetapkannya SOP *IT Security plan* menyangkut Kebutuhan staf	Alokasi staf tidak tepat	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai -	DS5,KK-DS5(6) (KM)
50	Belum ditetapkannya *SOP IT Security plan* menyangkut kepedulian terhadap keamanan dan pelatihan	Tidak ada yang merasa bertanggung jawab terhadap keamanan	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)
51	Belum ditetapkannya *SOP IT Security plan* menyangkut praktek pelaksanaan keamanan	Tidak ada yang merasa bertanggung jawab terhadap keamanan TI	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)
52	Belum ditetapkannya *SOP IT Security plan* menyangkut investasi pada sumber daya keamanan yang dibutuhkan (*required security resources*)	Sumber daya keamanan cepat usang, menjadi tidak dapat diandalkan, karena faktor ancaman teknologinya lebih maju	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(6) (KM)
53	Belum ditetapkannya *SOP IT Security plan* menyangkut suatu	Sistem keamanan TI menjadi terkotak-kotak.	- Membuat target waktu dan memonitor	DS5,KK-DS5(7) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
	proses yang mengintegrasikan kebutuhan keamanan informasi dalam *IT security plan* yang mencakup pengembangan *Service Level Agreement* dan *Operational Level Agreement*, *automated solution requirements*, *application software*, dan komponen infrastruktur TI		penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	
54	Belum ditetapkannya *SOP IT Security plan* menyangkut keamanan yang tersentralisir berada pada tempatnya, untuk memastikan akses yang tepat/sesuai terhadap sumber daya sistem	Koordinasi mengenai keamanan menjadi tersebar, konsentrasi keamanan terpecah, permasalahan tidak dapat diberi solusi tepat waktu, dan tepat tindakan	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(8) (KM)
55	Belum ditetapkannya *SOP IT Security* plan menyangkut skema klasifikasi data berada pada tempatnya dan sedang digunakan, untuk memastikan bahwa semua sumber daya sistem memiliki seorang pemilik yang bertanggung jawab atas keamanan dan isinya	Kerahasiaan data menjadi ancaman.	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(9) (KM) (KM)
56	Belum ditetapkannya SOP *information security system* yang cukup responsif terhadap perubahan yang terjadi akibat kebutuhan organisasi	Keamanan sistem menjadi rentan, tidak dipercaya oleh pihak ketiga, terutama nasabah	- Membuat target waktu dan memonitor penyelesaian SOP *IT security plan* - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(10) (KM)
57	Belum ditetapkannya SOP menyangkut profil keamanan pengguna berada pada tempatnya, yang mewakili "*least access as required*" dan secara reguler di-*review*	Terdapat *unathorized user*	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan pengguna - Memitigasinya	DS5,KK-DS5(11) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
	oleh pihak manajemen untuk akreditasi kembali		dengan peraturan yang sesuai	
58	Belum terdapat prosedur yang berhubungan dengan pemeliharaan kunci dan modul *cryptographi.*	Integritas dari sistem informasi dipertanyakan	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(14) (KM)
59	Belum ada SOP mengenai keamanan jaringan meliputi layanan yang diberikan, lalu lintas data, tipe koneksi yang diperbolehkan	Keamanan jaringan menjadi rentan dan tidak dapat diandalkan	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(32) (KM)
60	Belum terdapat SOP untuk mengatur semua komponen jaringan yang penting misalnya *router, DMZ, VPN switches* yang diperbaharui secara reguler dan perubahan tersebut didokumentasikan dengan baik	Keamanan jaringan menjadi rentan dan tidak dapat diandalkan	- Membuat target waktu dan memonitor penyelesaian SOP Keamanan - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(33) (KM)
61	Belum ditetapkannya *Computer Emergency Response Team* (CERT) yang mampu mengendalikan keadaan darurat dari kejadian yang berkaitan dengan keamanan.	Ketika terjadi keadaan darurat, sulit diambil tindakan karena belum ada team-nya	- Menetapkan team CERT karena pentingnya fungsi CERT	DS5,KK-DS5(40) (KM)
62	Belum ditetapkannya CERT terkait dengan penanganan insiden - Terdapat prosedur umum dan khusus untuk menangani insiden secara efektif dan melaporkan bila terjadi serangan/ancaman dari luar	Penanganan insiden berdasarkan intuisi, sehingga solusi yang diberikan belum tentu efektif	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
63	Belum ditetapkannya CERT terkait *Vendor relation* - Tugas dan tanggung jawab vendor dalam mencegah dan menindaklanjuti insiden yang terjadi, melakukan koreksi terhadap kesalahan perangkat lunak dan area TI lainnya	Vendor tidak mengetahui kewajibannya ketika terjadi insiden.	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
64	Belum ditetapkannya CERT terkait komunikasi - Kebutuhan, implementasi dan penanganan keadaan darurat dikomunikasikan ke manajemen	Komunikasi ketika terjadi insiden menjadi terhambat	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
65	Belum ditetapkannya CERT terkait investigasi terhadap isu hukum dan kriminal - Isu dipicu oleh pertimbangan hukum dan kebutuhan atau batasan yang dihasilkan akibat investigasi kriminal selama terjadinya insiden	Ketika terjadi insiden, akan ada kesulitan dalam melakukan investigasi	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
66	Belum ditetapkannya CERT terkait *Constituency relation - respon centre* akan memberikan dukungan terhadap pemberian layanan dan metode pelatihan, kepedulian, manajemen konfigurasi dan autentifikasi	Tidak ada personel yang terlatih dalam menghadapi insiden	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
67	Belum ditetapkannya CERT terkait agenda riset dan interaksi - identifikasi terhadap kegiatan riset yang ada dan riset yang perlu dilakukan dalam hubungannya dengan kegiatan *response centre*	Isu-isu mengenai insiden dan penangannya menjadi lebih sempit	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
68	Belum ditetapkannya CERT terkait *Model of the threat* - Pembangunan suatu pemodelan yang mengkarakteristikkan ancaman dan risiko yang mungkin timbul untuk membantu mengurangi kegiatan yang berisiko	Tanpa adanya *model of the threat*, penanganan ketika terjadi insiden, akan terjadi semacam kebingungan. Sehingga penanganan insiden, menjadi tidak efektif	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
69	Belum ditetapkannya CERT terkait isu eksternal - Faktor-faktor yang berada di luar pengendalian dan pengawasan organisasi (contoh hukum, kebijakan, syarat prosedural)	Tidak diketahui penangan insiden akibat faktor dari luar	- Membuat target waktu dan memonitor penyelesaian SOP CERT - Memitigasinya dengan peraturan yang sesuai	DS5,KK-DS5(40) (KM)
70	Revisi anggaran terhadap RKAP	Jika terjadi revisi terus menerus, kemungkian tujuan TI yang telah ditetapkan pada awal periode penyusunan menjadi tidak tercapai	- Revisi anggaran dibuat jika keadaan benar-benar memaksa	DS6, Sumber : dari personil PT Bank XYZ
71	SOP kebijakan yang mendorong dilakukannya modifikasi tepat waktu terhadap alokasi biaya untuk mencerminkan kebutuhan organisasi yang berubah-ubah masih dalam proses pengerjaan	Implementasi perubahan akan terhambat	- Membuat target waktu dan memonitor penyelesaian SOP anggaran TI - Memitigasinya dengan peraturan yang sesuai	DS6,KK-DS6(10)
72	Belum adanya SOP persiapan data yang memastikan kelengkapan, ketepatan, dan validitas data. (Dalam proses penyusunan SOP)	Integritas data dan informasi menjadi dipertanyakan	- Membuat target waktu dan memonitor penyelesaian SOP Data - Memitigasinya dengan peraturan yang sesuai	DS11,KK-DS11(1) (KM)
73	Belum adanya prosedur otorisasi untuk semua dokumen sumber.	Integritas data dan informasi menjadi dipertanyakan	- Membuat target waktu dan memonitor penyelesaian SOP Data	DS11,KK-DS11(2) (KM)

No	Kelemahan Pengendalian Internal	Risiko	Rekomendasi	Ref
			- Memitigasinya dengan peraturan yang sesuai	
74	Belum adanya prosedur yang memastikan kelengkapan dan ketepatan dokumen sumber dan konversi dokumen sumber yang tepat waktu. (Dalam proses penyusunan SOP)	Data dan informasi menjadi tidak lengkap, tidak dapat diandalkan	- Membuat target waktu dan memonitor penyelesaian SOP Data - Memitigasinya dengan peraturan yang sesuai	DS11,KK-DS11(8) (KM)
75	Belum ada SOP untuk menangani hal-hal di luar kebiasaan. (Dalam proses penyusunan SOP)	Implementasi ketika ada hal-hal di luar kebiasaan, menjadi di luar prosedur standar. Sehingga menjadi tidak tepat solusi	- Membuat target waktu dan memonitor penyelesaian SOP - Memitigasinya dengan peraturan yang sesuai	DS13,KK-DS13(11) (KM)
76	Belum terdapat penggunaan data untuk memantau/mengawasi sumber daya TI (*IT resources*) meliputi manusia, fasilitas, aplikasi, teknologi dan data telah sesuai/tepat	Tanpa ada data yang sesuai untuk memantau, akan sulit dilakukan monitoring yang memadai	- Membuat kebijakan (SOP) penggunaan data	ME1,KK-ME1(1) (KM)
77	Belum terdapat penggunaan *Key Performance Indicator* (KPI) dan/atau *Balanced Score Card* untuk mengukur kinerja TI.	Tanpa ada KPI dan BSC sulit untuk melakukan pengukuran kinerja yang tepat	- Membuat KPI dan BSC pengukuran kinerja TI dengan target tertentu.	ME1,KK-ME1(2) (KM)

Keterangan: KK = Kertas Kerja Kuesioner , KM = Kelemahan Material , Ref. = Referensi

4.2.3 Mitigasi *Internal Control* untuk *Inherent Risk*

Inherent risk dari PT Bank XYZ merupakan faktor risiko bawaan yang akan memberikan risiko bagi kelangsungan hidup perusahaan jika tidak dimitigasi dengan pengendalian internal Perusahaan. Berdasarkan hasil tanya jawab, pemahaman dokumen, serta observasi, Perusahaan telah menerapkan pengendalian internal untuk meminimalkan risiko. Tabel berikut ini terdapat perincian *inherent risk* dengan pengendalian internalnya dengan menggunakan kerangka COSO untuk risiko non TI, dan COBIT untuk risiko TI. Kerangka COSO telah dijelaskan pada Bab 2 Landasan Teori 2.10 *Internal Control-COSO frameworks*. Tabel 4.2 berikut menjelaskan Inherent risk dengan internal control-nya.

Tabel 4.2 *Inherent risk* dengan *internal control*-nya

No	Inherent Risk	Internal Control	Keterangan
1	Banyaknya risiko yang dihadapi industri perbankan	➢ *Control Environment :* 1) Penerapan *good corporate governance* 2) Adanya komitmen Perusahaan untuk menciptakan lingkungan yang terkendali dengan menetapkan nilai-nilai Perusahaan, seperti adanya "segitiga iman", "Etika Perorangan", "Pedoman Pegawai". 3) Perencanaan strategi perusahaan, termasuk penetapan visi misi Perusahaan, tujuan TI perusahaan yang diselaraskan antara keduanya 4) Adanya komite-komite untuk pengawasan, seperti komite audit, komite pengarah teknologi informasi 5) Terdapat berbagai SOP berkaitan dengan operasional dan TI perusahaan. 6) Jika tidak terdapat SOP, maka sebagai gantinya terdapat surat ketetapan direktur. 7) terdapat struktur organisasi yang berisi tugas dan tanggung jawab 8) adanya kebijakan mengenai sumber daya manusia ➢ *Risk Assessment :* Dibentuknya divisi manajemen risiko yang mengkhususkan pada penilaian risiko perusahaan, komite pemantau risiko, komite manajemen risiko . ➢ *Control Activities* 1. Terdapat berbagai SOP berkaitan dengan operasional dan TI perusahaan. Jika terdapat beberapa SOP yang belum ada, maka sebagai gantinya terdapat surat ketetapan direktur. 2. Terdapat kendali fisik atas aset 3. Adanya pemisahan tugas 4. terdapat aturan HRD ➢ *Information and Communication* Adanya sistem informasi untuk operasional, keuangan dan ketaatan terhadap ketentuan yang berlaku	Kategori berbagai risiko : Peraturan BI Nomor : 5/8/PBI/2003

No	Inherent Risk	Internal Control	Keterangan
1	Sambungan : Banyaknya risiko yang dihadapi industri perbankan	➢ *Monitoring* Adanya audit eksternal, dan internal Perusahaan, (audit operasional, audit TI) ➢ *COBIT* Terkait dengan risiko TI	
2	Banyaknya regulasi dan ketentuan pemerintah.	➢ *Information and Communication* Adanya sistem informasi untuk operasional, keuangan dan ketaatan terhadap ketentuan yang berlaku ➢ *Risk Assessment :* Dibentuknya divisi manajemen risiko yang mengkhususkan pada penilaian risiko perusahaan, termasuk memantau ketaatan regulasi dan ketentuan	Regulasi dari BI, aturan internasional (Basel II)
3	Transaksi harian tinggi	➢ *Control Environment :* - Adanya pemisahan tugas ➢ *Information and Communication* Adanya sistem informasi untuk operasional, keuangan dan ketaatan terhadap ketentuan yang berlaku ➢ *Monitoring* Adanya audit eksternal, dan internal Perusahaan, (audit operasional, audit TI) ➢ *COBIT* Terkait dengan risiko TI yang digunakan dalam memroses transaksi	Transaksi simpan pinjam, transfer, aset manajemen, dll, bisa ratusan transaksi sehari.

No	Inherent Risk	Internal Control	Keterangan
4	PT Bank XYZ mempunyai banyak kantor Cabang	➢ *Control Environment :* - Adanya komitmen Perusahaan untuk menciptakan lingkungan yang terkendali dengan menetapkan nilai-nilai Perusahaan, seperti adanya "segitiga iman", "Etika Perorangan", "Pedoman Pegawai" - terdapat struktur organisasi yang berisi tugas dan tanggung jawab - adanya kebijakan mengenai sumber daya manusia - Terdapat berbagai SOP berkaitan dengan operasional dan TI perusahaan. ➢ *Information and Communication* Adanya sistem informasi untuk operasional, keuangan dan ketaatan terhadap ketentuan yang berlaku ➢ *Monitoring* Adanya audit eksternal, dan internal Perusahaan, (audit operasional, audit TI) ➢ *COBIT* Terkait dengan risiko TI yang digunakan pada cabang PT Bank XYZ	Kantor cabang mempunyai risikosendiri-sendiri
5	Penerapan Teknologi Informasi	➢ *COBIT* Terkait dengan risiko TI yang diterapkan PT Bank XYZ	Penerapan TI pada layanan perbankan, seperti ATM, SMS banking

4.3 Hasil Penelahaan Risiko Audit

Rangkaian penelaahan dari *inherent risk*, *internal control risk* serta mitigasi dari *inherent risk* oleh *internal control* akan memberikan rekomendasi area *process control* mana yang akan dijadikan area fokus audit. Modifikasi terhadap *audit risk* setelah menelaah risiko tersebut telah dilakukan, dan hasilnya adalah sebagai berikut .

Audit risiko :

- *inherent risk* : **tinggi** (auditor memilih konservatif agar tidak mengurangi penilaian (*under assess*) *inherent risk* , walaupun ada mitigasi atas *inherent risk* dengan *internal control,* sehinga *inherent risk* masih ditetapkan tinggi
- *internal control risk* : **tinggi**

  (karena masih adanya kelemahan pada internal control perusahaan)
- detection risk : **rendah**
- sehingga audit risk : **medium.**

Walaupun audit risk tidak mengalami perubahan tingkat risiko yaitu medium, area fokus proses COBIT mengalami perubahan karena adanya beberapa kelemahan dari internal *control* yang telah dipaparkan sebelumnya. Area fokus proses COBIT dapat dilihat pada paragraf berikut ini.

Fokus area audit COBIT bagi DAI

Pada bagian awal bab ini, Penulis telah membuat prediksi awal untuk fokus area audit kepada 17 proses COBIT berkaitan dengan *audit risk* yang dapat diterima. Namun setelah melakukan audit lapangan maka terjadi perubahan fokus area untuk proses COBIT tersebut menjadi 22 proses, yang merupakan *judgment* Penulis atas dasar :

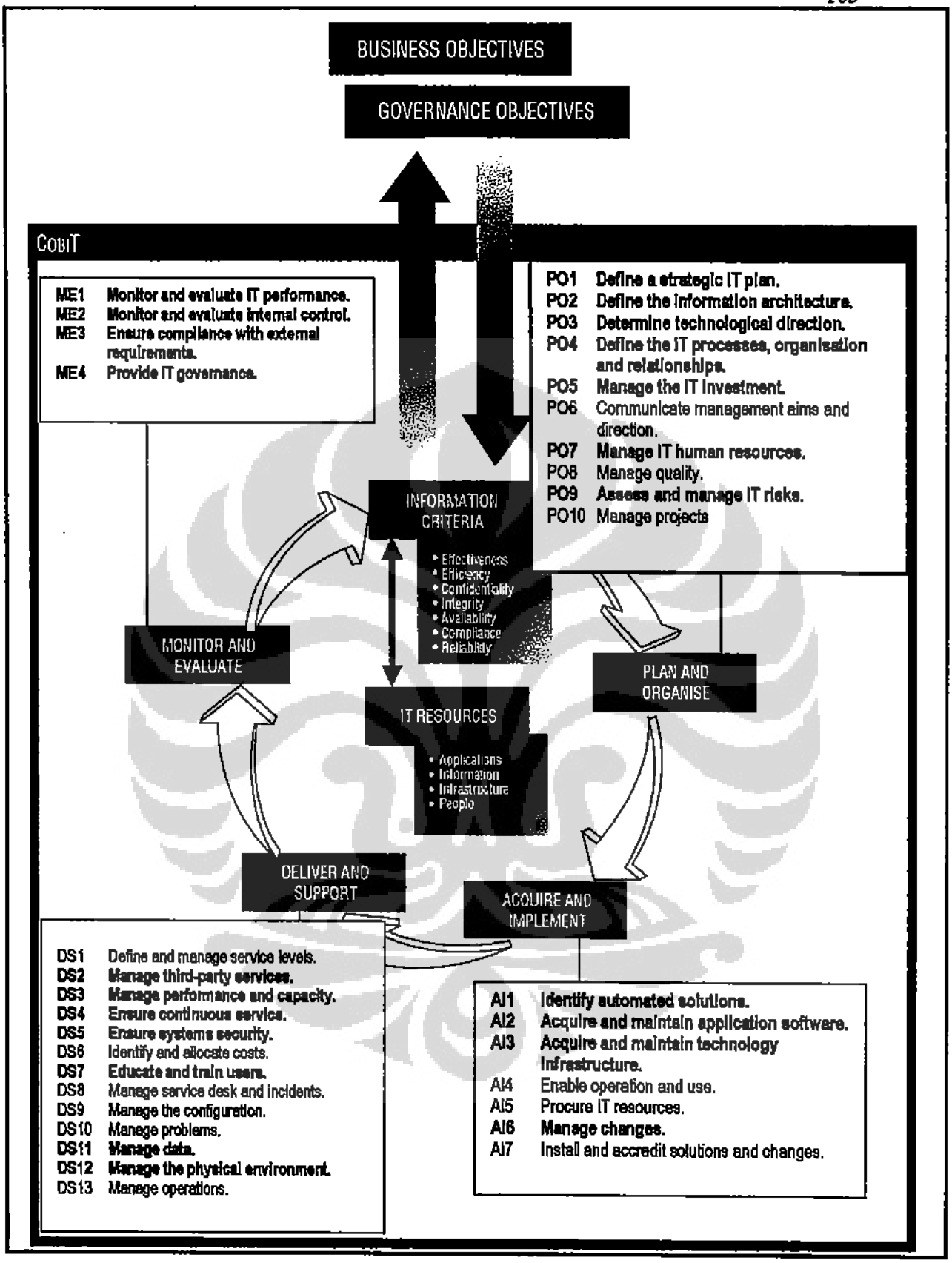
1. terkait dengan *inherent risk*, proses yang dipilih tersebut dianggap dapat memitigasi inherent risk
2. dan terkait dengan *internal control*, terdapat temuan kelemahan material pada internal control yang diterapkan.

Dengan adanya dua persyaratan tersebut, konsekuensinya adalah terdapat proses COBIT yang tidak dipilih di awal namun ditambahkan setelah penelahaan karena 2 kriteria *judgment* di atas tersebut.

Daftar proses COBIT yang dijadikan area fokus dapat dilihat di dalam tabel 4.3 atau dapat juga dilihat dalam COBIT *frameworks* yang diberi *highlight* (Gambar 4.2) berikut ini.

Tabel 4.3 Proses COBIT yang dijadikan Fokus

No	Proses COBIT	Keterangan
1	PO1	*Define a Strategic Information Technology Plan*
2	PO2	*Define the information architecture*
3	PO3	*Determine technological direction.*
4	PO4	*Define the IT processes, organisation and relationships.*
5	PO5	*Manage the Information Technology Investment*
6	PO7	*Manage IT Human Resources*
7	PO9	*Assess and Managed IT Risks*
8	AI1	*Identify Automated Solution*
9	AI2	*Acquire and Maintain Application Software*
10	AI3	*Acquire and Maintain Technology Infrastructure*
11	AI6	*Manage Changes*
12	DS2	*Manage Third Party Services*
13	DS3	*Manage Performance and Capacity*
14	DS4	*Ensure continuous service*
15	DS5	*Ensure Systems Security*
16	DS7	*Educate and trains users*
17	DS11	*Manage Data*
18	DS12	*Manage the Physical Environment*
19	ME1	*Monitor and Evaluate IT Performance*
20	ME2	*Monitor and evaluate internal control.*
21	ME3	*Ensure compliance with external requirements.*
22	ME4	*Provide IT governance.*



Gambar 4.2 Proses COBIT yang signifikan sesudah audit
Sumber : COBIT 4.1 (telah diolah kembali)

4.4 Pemaparan Maturity Model Level

Maturity model level juga merupakan hasil rangkaian dari audit tata kelola TI dengan COBIT. Berikut ini, merupakan hasil dari analisis kuisioner dan wawancara yang telah diberikan kepada personil yang berkompeten dari DTI PT Bank XYZ ketika audit lapangan. Sebagaimana yang kita ketahui *maturity model level* akan memberikan informasi dimana letak keberadaan TI bagi manajemen, apa yang telah diberikannya kepada Perusahaan, dan akan kemana TI ini diarahkan. Keseluruhan dari proses COBIT yang berjumlah 34 telah dianalisis. Pemberian level adalah berdasarkan *judgment Penulis* yang didasari oleh deskripsi atribut *maturity model level* yang telah dipaparkan oleh COBIT. Berikut hasil *maturity model level* dari 34 proses dari 4 domain COBIT.

4.4.1 Domain 1 – *Plan and Organized (PO)*

- PO1 *Define a Strategic Information Technology Plan (Level 3 – Defined)*

  PT Bank XYZ telah mempunyai perencanaan strategis Teknologi Informasi. Perencanaan tersebut telah dibuat secara seksama dalam kurun waktu yang telah ditetapkan. Rencana Strategis Teknologi Informasi (RSTI) terbaru dari PT Bank XYZ ketika karya akhir ini dibuat, diperuntukan untuk 4 tahun, periode 2008-2012. RSTI mencakup arsitektur PT Bank XYZ, standar-standar operasional, *IT Roadmap* yang berisi langkah-langkah implementasi rencana TI dan struktur organisasi.

  DTI telah membuat suatu kebijakan dan prosedur menurut suatu pendekatan yang terstruktur. Dimana terdapat suatu metodologi untuk memformulasikan dan memodifikasikan rencana-rencana yang mengandung misi dan tujuan Perusahaan, usaha-usaha TI untuk mendukung misi dan tujuan Perusahaan dan sebagainya. Kebijakan tersebut mencakup rencana jangka panjang dan jangka pendek TI yang mencerminkan keselarasan antara tujuan bisnis dengan tujuan TI.

  Dalam menjalankan proyek-proyek yang telah disusun dalam perencanaan, Perusahaan mempunyai perangkat pengawasan, yaitu *Project*

Management Officer, yang bertugas untuk mengawasi apakah proyek yang telah direncanakan , dijalankan oleh TI tepat waktu atau tidak.

PT Bank XYZ juga mempunyai Komite Pengarah Teknologi Informasi (KPTI). KPTI ini bisa dianggap sebagai *IT Steering committee*. Setiap bulan KPTI mengadakan pertemuan, untuk mengetahui permasalahan TI yang ada di Perusahaan. KPTI terdiri dari Direktur TI sebagai Ketua, Kepala Divisi TI sebagai sekretaris, dan beranggotakan Divisi operasional dan bisnis, serta Direktur bidang risiko.

Sosialisasi kebijakan TI pun telah dilakukan dengan metode *training for trainer* bagi personil TI.

Pemutakhiran kebijakan dilakukan sesuai dengan kebutuhan. Beberapa kebijakan, *Service Level Agreement* (SLA) DTI dengan Divisi Lain, beberapa *Standard Operating Procedures* (SOP) DTI, sudah dibuat oleh DTI, namun belum dapat diimplementasikan karena belum disetujui oleh Manajemen PT Bank XYZ.

Pada periode perencanaan 2008-2012, PT Bank XYZ telah berkomitmen untuk menyusun berbagai standar operasional untuk meningkatkan tata kelola TI pada Perusahaan.

- PO2 - *Define the Information Architecture (Level 3 – Defined)*

Fungsi dari sistem informasi adalah menciptakan dan memutakhirkan model informasi bisnis dan menetapkan sistem yang tepat untuk mengoptimalkan penggunaan dari informasi ini. Dengan demikian harus ada pemutakhiran atas kamus data, aturan syntax data, yang sudah terklasifikasi dalam skema dan memperhatikan level keamanan.

PT Bank XYZ mempunyai sistem Taksonomi sebagai model arsitektur TI yang sekarang sedang dikembangkan oleh Divisi TI Perusahaan.

Proses yang digunakan untuk memperbaharui model arsitektur informasi pada PT Bank XYZ adalah berdasarkan kebutuhan bisnis, bukan berdasarkan perencanaan jangka pendek dan jangka panjang. Jadi, meskipun Perusahaan telah menetapkan perencanaan atas TI pada awal periode, rencana-rencana tersebut masih dapat diubah, karena kondisi bisnis di luar, menjadikan

TI harus merespon dengan kondisi yang telah terjadi dan kemudian menetapkan perubahan yang baru.

PT Bank XYZ akan mengembangkan *warehouse data* dengan tujuan memberikan manfaat kepada manajemen, membuat laporan dengan analisis data lengkap dengan satu sumber data.

Kebijakan dan prosedur TI PT Bank XYZ pun mencakup pengembangan dan pemeliharaan kamus data. Untuk mengakses kamus data tersebut telah diterapkan proses otorisasi, tingkat keamanan dan akses didefinisikan secara jelas untuk tiap-tiap klasifikasi data.

- PO3 *Determine Technological Direction (Level 3 – Defined)*

  Dampak dari tidak adanya perencanaan arah teknologi, akan mengakibatkan akuisisi teknologi tidak konsisten dengan rencana stratejik TI, selain itu akan tidak sesuai dengan kebutuhan organisasi yang mengakibatkan meningkatnya biaya TI.

  PT Bank XYZ memiliki proses penciptaan dan pembaharuan secara teratur dari rencana infrastruktur teknologi yang sesuai dengan rencana stratejik yang telah ditetapkan. Proses tersebut dilakukan dengan mengkonfirmasi bahwa setiap perubahan diusulkan, diuji terlebih dahulu untuk menilai biaya dan risikonya, serta terdapat persetujuan dari pimpinan, sesuai dengan Rencana Kerja Anggaran Perusahaan (RKAP).

  Strategi TI dan perencanaan infrastruktur teknologi sejalan dengan pengembangan TI yang dilakukan. Proses akuisisi diintegrasikan mengikuti kebijakan PT Bank XYZ yang dilakukan oleh divisi logistik dengan keterlibatan divisi TI.

  Training formal dan komunikasi mengenai peranan dan tanggung jawab telah ada. Bagian Perencanaan TI adalah yang bertanggung jawab terhadap arsitektur TI Perusahaan.

- PO4 *Define the Information Technology Organisation and Relationship (Level 2- Repeatable but intuitive)*

  PT Bank XYZ telah mempunyai KPTI sebagai *IT Steering committee* yang memastikan bahwa tata kelola TI merupakan bagian dari tata kelola organisasi

yang harus diterapkan dan memberikan arahan bagi TI dan juga berfungsi menentukan bahwa program investasi TI diprioritaskan supaya sesuai dengan yang dibutuhkan oleh strategi bisnis. Pada Bab 3 Gambaran Umum, gambar 3.2 juga telah dijelaskan struktur organisasi dari organisasi TI PT Bank XYZ.

PT Bank XYZ telah mempunyai kerangka proses TI untuk melaksanakan rencana strategi TI yang memuat struktur dan hubungan antar struktur TI, namun SOP yang menerangkan atau menjelaskan peran dan tanggung jawab seluruh personel dalam organisasi, yang berhubungan dengan sistem informasi, pengendalian internal dan keamanan, masih dalam proses pengerjaan. Selain itu, beberapa SOP lainnya juga masih dalam proses pengembangan diantaranya adalah kebijakan dan prosedur untuk melakukan evaluasi kembali yang meliputi perumusan tindakan-tindakan untuk menghadapi kejadian di luar dugaan, pendokumentasian pengetahuan yang penting, pelatihan bagi personel TI, transfer tanggung jawab.

PT Bank XYZ saat ini belum mempunyai SOP KPI *(Key Performance Indicator* dan KSF *(Key Success Factor)* dalam mengukur hasil-hasil dari fungsi TI dalam pencapaian tujuan. Proses penilaian personil TI pun merupakan pemformalan dari praktek yang telah terjadi, dimana pada awal tahun tiap-tiap personil TI menetapkan rencana pencapaian dalam setahun yang didiskusikan kepada pimpinan, dan evaluasi atas pencapaian rencana tersebut dilakukan pada tengah tahun dan akhir tahun. Namun, pada saat ini telah dimulai proses penyusunan KPI dan KSF tersebut.

PT Bank XYZ juga masih melakukan upaya pengembangan kebijakan dan prosedur yang mencakup kepemilikan data dan sistem bagi seluruh sumber data utama dan sistem.

Perusahaan pun sedang membuat SOP kebijakan dan prosedur TI untuk mengendalikan berbagai aktifitas konsultan kontrak untuk memastikan perlindungan dari aset DTI juga termasuk pembuatan prosedur yang dapat diterapkan pada jasa TI kontrakan untuk kecukupan dan konsistensi dengan kebijakan akuisisi yang dimiliki DTI.

- PO5 *Manage the Information Technology Investment (Level 2- Repeatable but intuitive)*

  PT Bank XYZ mempunyai RKAP sebagai kerangka finansial yang memadai untuk mengendalikan investasi dan biaya yang ditimbukan oleh aset TI dan layanannya. RKAP memberikan arahan bagi TI untuk melakukan akuisisi sesuai dengan aktivitas yang akan dilakukan sesuai dengan perencanaan yang telah ditetapkan.

  Namun, SOP untuk memastikan persiapan dan persetujuan dari sebuah anggaran operasi TI tahunan Perusahaan serta rencana jangka panjang dan jangka pendek masih dalam proses penyusunan. Selain itu kebijakan untuk menjamin bahwa jasa yang diberikan oleh fungsi TI dijelaskan/dibuktikan dalam hal biaya, dan memiliki kesesuaian dengan biaya rata-rata pada umumnya masih belum terealisasi.

- PO6 *Communicate Management Aims and Direction (Level 2- Repeatable but intuitive)*

  Manajemen proses komunikasi sasaran dan petunjuk manajemen merupakan tujuan TI terhadap bisnis dengan cara memberikan informasi yang akurat dan tepat waktu pada layanan TI masa sekarang dan mendatang dan diasosiasikan dengan risiko dan tanggung jawabnya.

  PT Bank XYZ telah mengupayakan suatu lingkungan pengendalian positif dan memenuhi aspek-aspek integritas, nilai-nilai etika, standar-standar profesional dalam bertindak, dan sebagainya. Hal tersebut telah tercantum dalam misi dan visi Perusahaan, "Etika Perorangan", "Pedoman Pegawai" serta "Segitiga Iman" yang wajib diketahui dan diterapkan oleh semua pegawai. Nilai-nilai yang dianut oleh Perusahaan tersebut merupakan salah satu kerangka kendali internal.

  Perusahaan belum mempunyai SOP untuk memenuhi kebutuhan dilakukannya review secara periodik dan persetujuan kembali terhadap standar-standar, aturan, kebijakan, dan prosedur utama/pokok yang berhubungan dengan TI belum terwujud. SOP atas sekumpulan kebijakan,

standar dan prosedur yang sejalan dengan strategi TI dan lingkungan pengendalian tersebut masih dalam proses pengerjaan.

Belum ada dokumen kerangka keamanan dan pengendalian internal yang menspesifikasikan kebijakan keamanan dan pengendalian internal, maksud dan tujuan, struktur organisasi, ruang lingkup dalam organisasi, pemberian tanggung jawab, dan definisi dari pinalti serta tindakan disiplin lainnya yang berhubungan dengan kegagalan untuk mematuhi kebijakan keamanan. Perusahaan sedang memproses penyusunan SOP tersebut.

Belum terdapat SOP yang sejalan dengan strategi TI dan lingkungan pengendalian.

Belum diterapkan sanksi-sanksi administratif yang sesuai terhadap pelanggaran kebijakan TI Perusahaan.

- *PO7Manage IT Human Resources (Level 3- Defined))*

  PT Bank XYZ telah melakukan proses pelatihan bagi pegawai Divisi TI termasuk training untuk lintas bagian (*cross training).* Sudah ada penetapan kebijakan dan prosedur sumber daya manusia termasuk perubahan dan pemberhentian karyawan.

  DTI dengan persetujuan Divisi Sumber Daya Manusia sudah melakukan perencanaan manajemen sumber daya manusia DTI, termasuk kebijakan berkaitan dengan periode kerja karyawan TI.

  Namun, belum ada kebijakan rotasi bagi karyawan yang memegang peranan kunci dengan rentang waktu yang relatif lama.

  Proses *security clearance* terhadap semua pegawai, kontraktor dan vendor di perusahaan masih belum terealisasi.

- PO8 *Manage Quality (Level 2- Repeatable but intuitive)*

  PT Bank XYZ telah mempunyai bagian di dalam Divisi TI-nya yaitu *Quality Assurance* dan *Security Control* yang berfungsi untuk memastikan bahwa kualitas dan kendali atas keamanan dari penerapan sistem informasi, yaitu perangkat lunak, perangkat keras dan jaringan komunikasi data sesuai dengan standar dan kualitas yang telah ditetapkan.

Namun demikian, secara keseluruhan Perusahaan masih mengembangkan Quality Management System (QMS) yang mengidentifikasi kebutuhan kualitas dan kriteria TI di Perusahaan.

- PO9 *Asses and Manage IT Risks (level 3 – Defined)*

  PT Bank XYZ telah menerapkan prosedur untuk penilaian risiko. Jadi telah ada prosedur khusus. Prosedur tersebut mengisyaratkan untuk melakukan perbaikan terus menerus.

  Telah ada dokumentasi penilaian risiko yang mencakup diantaranya deskripsi dari metodologi penilaian risiko, identifikasi dari *exposure* signifikan dan apa risikonya serta risiko dan exposure yang ditangani.

  Sebagaimana yang telah dibahas dalam Bab sebelumnya, PT Bank XYZ harus mentaati peraturan regulasi. Diantaranya peraturan BI : 9/15/PBI/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum. Perusahaan telah memenuhi peraturan tersebut, salah satunya adalah dengan melakukan audit sistem informasi sebagaimana yang dilakukan oleh DAI.

- PO10 *Manage Projects (level 2 – Repeatable but intuitive)*

  PT Bank XYZ telah memiliki kerangka manajemen proyek lengkap. Termasuk diantaranya melakukan studi kelayakan proyek yang mencakup kelayakan lingkungan dari proyek yaitu perangkat keras, perangkat lunak, mengenai hambatan, serta manfaat dan biayanya.

  Milestone dan biaya proyek aktual dan yang dianggarkan, dipantau, dan dilaporkan kepada pimpinan pada setiap fase utama dari proyek.

4.4.2 Domain 2 - *Acquire and Implement* (AI)

- AI1 *Identify Automated Solution (level 3 – Defined)*

  Proses ini memastikan bahwa organisasi telah melakukan proses identifikasi terhadap kebutuhan organisasi dengan mempertimbangkan sumber daya yang dibutuhkan, penelaahan terhadap kelayakan teknologi dan ekonomi,

melakukan analisis risiko dan analisis antara biaya dan keuntungannya, sebelum melakukan akuisisi atau pembuatan aplikasi baru.

PT Bank XYZ telah mempunyai kebijakan dan prosedur untuk mencapai tujuan tersebut di atas. Perusahaan juga telah melakukan analisis dan pendokumentasian pada waktu melakukan tahapan pengembangan, implementasi dan modifikasi sistem dengan memperhatikan risiko serta mengeliminasi risiko yang teridentifikasi. Otorisasi juga telah diterapkan jika ada perubahan

- AI2 *Acquire and Maintain Application Software (Level 4 - Managed and Measureable)*

  PT Bank XYZ telah mempunyai kebijakan dan prosedur mengenai akuisisi dan pemeliharaan dari perangkat lunak aplikasi. Prosedur yang ada tersebut memastikan bahwa :

  - pada saat perancangan telah melibatkan *user* dan spesifikasi rancangan telah disetujui oleh para pimpinan di Perusahaan dan pengguna yang berkepentingan
  - telah ada mekanisme yang memadai untuk, mendefinisikan, mendokumentasikan kebutuhan dari input, output, pengembangan modifikasi sistem, dan pengembangan sistem terbaru.
  - sudah terdapat fungsi *online help*
  - perangkat lunak aplikasi diuji dengan proses pengujian
  - dan telah dibuat referensi pemakai dan *manual support* yang memadai
  - Selain itu terdapat penilaian kembali terhadap rancangan sistem pada saat terjadinya penyimpangan teknologi atau logika yang signifika selama pengembangan dan pemeliharaan sistem.

  Apabila dalam pengembangan sistem dilakukan oleh pihak ketiga, Perusahaan juga membuat perjanjian atau kesepakatan selama proses perancangan, pengembangan dan implementasi sistem.

- AI3 *Acquire and Maintain Technology Infrastructure (Level 2 – Repeatable and Intuitives)*

  Proses ini berkaitan dengan adanya rencana akuisisi, pemeliharaan dan perlindungan terhadap infrastruktur teknologi agar dapat mendukung berbagai aplikasi.

  PT Bank XYZ belum merealisasikan kebijakan dan prosedur yang berkaitan dengan dengan pemeliharaan infrastruktur teknologi tersebut. Pada saat ini Perusahaan masih memproses penyusunan prosedur tersebut.

  Menurut Personil DTI, tidak terdapat SOP yang memastikan bahwa :

  1. dibuatnya suatu rencana evaluasi formal untuk menilai pengaruh/dampak perangkat keras dan perangkat lunak baru terhadap performa keseluruhan sistem
  2. dibatasinya kemampuan untuk melakukan akses perangkat lunak sistem
  3. proses *set-up*, instalasi dan pemeliharaan perangkat lunak sistem tidak membahayakan keamanan data dan program yang sedang disimpan dalam sistem
  4. perangkat lunak sistem diinstal dan dipelihara sesuai dengan kerangka akuisisi dan pemeliharaan infrastruktur teknologi
  5. pemasok (*vendor*) perangkat lunak sistem memberikan kepastian integritas akan perangkat lunak mereka dan modifikasi pada perangkat lunak mereka
  6. dilaksanakannya pengujian yang menyeluruh dari perangkat lunak sistem sebelum digunakan dalam lingkungan yang sebenarnya, yang meliputi pengujian terhadap *functionality, security, availability,* dan *integrity condition*
  7. diubahnya kata sandi (*password*) instalasi perangkat lunak yang diberikan oleh pemasok pada saat dilakukannya instalasi

  Namun menurut personil TI, SOP mengenai kebijakan tersebut masih dalam proses pembuatan.

- AI4 *Enable Operation and Use (Level 3 –Defined)*

  Agar penggunaan dari solusi TI bagi bisnis dapat mempermudah pengguna, maka dibuat suatu dokumentasi dan manual bagi user dan juga Divisi TI , yang berisi hal teknis dan operasional serta penggunaan suatu sistem. PT Bank XYZ telah membuat manual dan pelatihan bagi user secara berkala. Semua pemutakhiran atas teknologi yang bermanfaat bagi user mempunyai manual pelatihan.

  Manual pelatihan bagi pengguna tersebut memberikan gambaran umum dari sistem dan lingkungan sistem, penjelasan dari seluruh input sistem, program, output, dan integrasi dengan sistem yang lain. Selain itu, manual tersebut juga memberikan penjelasan dari seluruh layar entri data dan layar tampilan data, penjelasan dari seluruh pesan-pesan kesalahan dari respon yang tepat untuk menangani kesalahan tersebut. Manual pelatihan juga dimutakhirkan oleh DTI.

- AI5 *Procure IT Resources (Level 4 – Managed and Measurable)*

  Proses ini memastikan adanya proses pengadaan yang meliputi: sumber daya manusia, perangkat keras, perangkat lunak dan layanan TI lainnya, dengan mengikuti prosedur pengadaan dari mulai pemilihan vendor, pembuatan kontrak dan proses akuisisi itu sendiri. Proses procurement yang terjadi di PT Bank XYZ adalah dengan melibatkan divisi lain. Misalnya saja untuk perekrutan sumber daya manusia, Divisi Sumber Daya Manusia yang mengambil peranan penting untuk perekrutan, DTI melaporkan dibutuhkannya personil tambahan untuk mendukung divisinya, itu pun melalui mekanisme peran pihak ketiga, yang mengevaluasi kebutuhan dari DTI apakah diperlukan adanya tenaga tambahan atau tidak. Prosedur mengenai hal ini telah diatur di dalam kebijakan mengenai perekrutan PT Bank XYZ.

  Mengenai pengadaan perangkat lunak, perangkat keras dan layanan TI lainnya, telah ada prosedur khusus mengenai Pengadaan, yang diatur oleh Manajemen Perusahaan. DTI bekerja sama dengan Divisi Logistik yang akan mengatur proses akuisisi tersebut. Divisi Logistik akan menyeleksi supplier

untuk akuisisi tersebut. Jadi sistem akuisisi adalah terintegrasi di dalam Perusahaan, dan mencakup semua divisi, tidak berdiri-sendiri.

Kesemuanya diatur melalui mekanisme yang telah ditentukan, dan melalui proses persetujuan dari masing-masing divisi yang terkait. Dan telah ada penilaian terhadap kualitas dan *acceptance process* untuk seluruh akuisisi sumber daya TI.

- AI6 *Manage Changes (Level 2 – Repeatable but intuitive)*

Proses ini idealnya mencakup bahwa semua perubahan infrastruktur dan aplikasi telah diatur dan dikendalikan secara formal. Segala perubahan baik itu dalam hal prosedur, proses, sistem dan layanan telah dicatat (dalam *log file*), telah dinilai dan diotorisasi sebelum dilakukan implementasi dan *review* terhadap rencana implementasi. Hal ini mampu menghilangkan risiko negatif yang berpengaruh pada stabilitas dan integritas sistem.

PT Bank XYZ saat ini telah melakukan proses pengembangan prosedur perubahan yang formal agar seluruh permintaan yang mencakup perubahan aplikasi, proses, sistem dan layanan dan platform ditangani sesuai dengan standar yang berlaku. Menurut personil TI, hal tersebut akan terealisasi pada tahun 2010. Praktek yang dilakukan pada saat ini sudah mencakup bahwa setiap permintaan perubahan telah disetujui secara formal oleh pimpinan dan pihak yang berkepentingan. Sudah ada log atas permintaan perubahan pada sistem dan aplikasi di dalam prosedur pengelolaan perubahan, sudah dilakukan pengujian atas seluruh perubahan pada saat sebelum implementasi.

Namun pendokumentasian pada PT Bank XYZ masih kurang lengkap yang menyebabkan pelacakan status perubahan sangat sulit dilakukan karena kurangnya dokumentasi progres pengembangan. Selain itu materi pelatihan untuk setiap perubahan masih kurang.

- AI7 *Install and Accredit Solutions and Changes (Level 3 – Defined)*

  Setiap sistem baru yang sudah selesai dikembangkan akan dioperasikan oleh Perusahaan. Untuk itu diperlukan pengujian sebelum dilepas dan digunakan oleh *user*. Sehingga diharapkan sistem operasional dan hasilnya sesuai dengan yang diharapkan semua pihak.

  PT Bank XYZ telah menerapkan metodologi SDLC (*System Development Life Cycle*) dalam setiap pengembangan dan perubahan sistem. Namun, penerapannya belum optimal dimana hasil observasi yang dilakukan ditemukan tidak optimalnya proses perubahan yang disebabkan lambatnya respon dari pihak yang terkait dengan proses perubahan. Hal ini mengakibatkan proses pengembangan aplikasi menjadi memakan waktu yang relatif lama.

  Namun demikian, telah ada dokumentasi, review, persetujuan atas perubahan. Telah ada pemisahan peran dan tanggung jawab terkait dengan program coding, pengujian dan persetujuan program, serta pemindahan (transfer) dari lingkungan pengembangan ke dalam lingkungan produksi. Telah ada proses pelatihan untuk setiap perubahan.

4.4.3 Domain 3 - *Deliver and Support* (DS)

- DS1 *Define and Manage Service Levels (Level 3 – Defined)*

  Tujuan dari proses ini adalah bahwa layanan yang diberikan telah memenuhi tingkat layanan yang dibutuhkan oleh seluruh *stakeholder* yang disesuaikan dengan kriteria kinerja/performa yang diharapkan oleh organisasi selain itu dilakukan juga pengawasan dan monitoring terhadap tingkat layanan.

  PT Bank XYZ telah mempunyai *Service Level Agreement* (SLA) antara DTI dan *user*. SLA tersebut memuat partisipasi dari pengguna dalam membuat dan memodifikasi agreement. Kewajiban dari pengguna dan provider didefinisikan dengan jelas. DTI juga memantau dan melaporkan pencapaian dari kriteria performa jasa tertentu.

  PT Bank XYZ masih melakukan pengembangan dari SOP tersebut. Kebijakan dilakukan berdasarkan ketentuan direksi.

- DS2 *Manage Third Party Services (Level 3 – Defined)*

  Dengan adanya proses yang mengatur jasa layanan dari pihak ketiga (*vendor, supplier,* dan *partner),* misalnya tentang tanggung jawab, tugas, peran, dan layanan, maka akan meminimalkan risiko yang berdampak atas performa TI bagi PT Bank XYZ. Pengaturan tersebut dituangkan dalam sebuah perjanjian yang terdiri dari berbagai hal yang telah distandarisasikan, misalnya tentang jasa-jasa yang diberikan, persetujuan tingkat jasa (*service level agreement*) baik kualitatif maupun kuantitatif, proses penghentian, biaya jasa/layanan, jangka waktu kontrak, jaminan kerajasiaan dam sebagainya.

  Jasa-jasa layanan yang telah diterima oleh PT Bank XYZ misalnya dalam pengembangan *IT governance* bekerja sama dengan pihak lembaga universitas non profit, SIBS dengan Silverlake, lokasi *server* yang menyewa di beberapa tempat,

  Namun demikian, SOP TI mengenai hubungan dengan pihak ketiga *(third party relationship)* belum terealisasi, dan masih dalam proses pengerjaan. Kebijakannya diatur dalam peraturan direksi.

- DS3 *Manage Performance and Capacity (Level 2 – Repeatable but intuitive)*

  Tujuan dari audit ini adalah memastikan apakah terdapat perencanaan yang mencakup prediksi kebutuhan di masa mendatang berdasarkan beban kerja yang ada, kebutuhan akan *storage* dan tindakan untuk menangani hal yang di luar dugaan dan penilaian terhadap kinerja dan kemampuan sumber daya TI, sehingga memberikan kepastian bahwa sumber daya informasi yang ada mendukung kebutuhan organisasi.

  PT Bank XYZ telah mempunyai perangkat penilaian atas kinerja dan kemampuan sumber daya TI. Dalam masalah infrastruktur perangkat keras, Perusahaan mempunyai *Performance Navigator* yang memonitor *resources* mesin AS 400, ini untuk melihat kinerja dan kapasitas penyimpanannya. Kemudian *Net Monitoring System –NMS* untuk memonitor mesin server/client bagi kinerja jaringan. PT Bank XYZ juga telah melakukan proses analisis dengan melakukan prediksi dampak perubahan komponen dalam sistem.

Informasi mengenai *capacity plan*, yang nantinya berguna dalam melakukan perubahan terhadap aplikasi, server, dan sumber daya TI lainnya hanya diberikan kepada staf DTI tertentu saja yang mempunyai kewenangan.

Namun demikian, belum ada aktifitas untuk memprediksi beban kerja dan sumber daya TI yang diperlukan. Belum ada proyeksi mengenai beban kerja yang dibutuhkan pada saat puncak. Selain itu masih terdapat permasalahan di dalam mesin produksi yang berdampak pada integritas data operasional bank, misalnya saja beberapa objek masih terduplikasi di dalam *library* mesin.

- DS4 *Ensure Continous Service (Level 3 – Defined)*

Kepastian kelangsungan layanan telah dilakukan oleh DTI PT Bank XYZ. Usaha-usaha pengendalian tersebut diantaranya adalah dengan adanya *Disaster Recovery Center* (DRC) yang bertempat di salah satu kota di Pulau Jawa. PT Bank XYZ memulai untuk mengembangkan lokasi DRC, di daerah yang berjauhan, sesuai dengan analisis kelayakan terhadap pemilihan lokasi DRC baik dari segi geografis maupun historis bencana.

Penentuan sumber daya TSI yang diperlukan untuk menjalankan rencana kelangsungan TSI. Pelatihan staf terkait atas peranan dan tanggung jawabnya dalam rencana pemulihan (*recovery plan*).

Penyimpanan *offsite*, mencakup lokasi penyimpanan, *access control*, frekuensi update material *offsite*, dan frekuensi pengujian terhadap pemulihan materi *offset*.

Mengenai prosedur dan standar di PT Bank XYZ, pengembangan dokumen *Disaster Recovery Plan* (DRP), sudah selesai disusun, dan statusnya dalam tahap persetujuan dari pihak pimpinan PT Bank XYZ.

Perusahaan telah melakukan pengujian terhadap kelangsungan TI (*IT Continuity Plan)*. Dalam pelaksanaan tersebut, terdapat pencatatan dan pembahasan hasil-hasil pengujian.

- DS5 *Ensure Systems Security (Level 3 – Defined)*

  Proses manajemen atas keamanan diperlukan untuk menjamin integritas dari informasi dan melindungi aset TI. PT Bank XYZ telah menaruh perhatian terhadap hal ini, walaupun demikian kebijakan, standar, atau prosedur yang mendetail dalam keamanan, masih dalam proses pengerjaan.

  Selain itu, usaha-usaha yang telah dilakukan adalah terdapat kebijakan atas password, terdapat sanksi resmi terhadap karyawan yang melakukan pelanggaran yang diatur di dalam Peraturan Direksi tentang pengenaan sanksi terhadap penyalahgunaan kewenangan Teknologi Sistem Informasi (TSI).

  Telah ada pengamanan atas seluruh hardware yang terkait dengan keamanan informasi melalui penggunaan *physical access control* pada ruang penyimpanannya.

  Telah ada proteksi terhadap virus, dan file definis virus (virus definitions) dengan menggunakan Symantec Antivirus.

  Telah ada pengamanan terhadap firewall terhadap kemungkinan penetrasi. Namun SOP terhadap hal tersebut masih dikembangkan.

  Pengamanan akses ke jaringan belum optimal dimana adanya privileges khusus ke firewall tanpa disertai adanya dokumen persetujuan dari manajemen terkait.

  Belum ditetapkannya Computer Emergency Response Team (CERT) yang mampu mengendalikan keadaan darurat dari kejadian yang berkaitan dengan keamanan.

- DS6 *Identify and Allocate Costs (Level 3 – Defined)*

  Pengendalian ini memastikan adanya suatu sistem pengalokasian biaya TI yang mampu mencatat, menghitung, mengalokasikan dan melaporkan biaya TI secara tepat dan sesuai dengan kebutuhan organisasi.

  PT Bank XYZ mempunyai Rencana Kerja Anggaran Perusahaan (RKAP), di dalamnya terdapat rencana kerja dan anggaran semua divisi. Tidak terkecuali DTI. RKAP berlaku setiap tahun, namun tidak menutup kemungkinan terjadi revisi anggaran, misalnya jika terjadi kebutuhan bisnis yang mendesak sehingga DTI harus menyediakan jasa atau layanan yang tidak

ada pada RKAP tersebut, misalnya dengan menyediakan software atau hardware tertentu yang belum direncanakan sebelumnya. RKAP tersebut dipertanggungjawabkan setiap tahun.

Namun SOP ataupun kebijakan yang mendorong dilakukannya modifikasi tepat waktu terhadap alokasi biaya untuk mencerminkan kebutuhan organisasi yang berubah-ubah masih dalam proses pengerjaan.

- DS7 *Educate and Train Users (Level 3 – Defined)*

  PT Bank XYZ sedang mengembangkan prosedur atau ketentuan sistem pelatihan bagi seluruh personil karyawan. Termasuk diantaranya bagi user DTI maupun non DTI. Kebijakan diatur di dalam ketentuan direksi.

  Program Pelatihan dan Pendidikan yang telah berjalan merupakan program yang *mandatory*, harus diikuti oleh semua personil. Program tersebut biasanya dilakukan secara berkala setahun sekali dengan materi pelatihan difokuskan pada kebutuhan organisasi terhadap TI, misalnya seperti kesadaran akan keamanan dan pengendalian yang berkelanjutan.

  Program pelatihan biasanya dilakukan di PT Bank XYZ ataupun di tempat penyelenggara pelatihan dari pihak ketiga PT Bank XYZ.

- DS8 *Manage Service Desk and Incidents (Level 4 Managed and Measureable)*

  Pengendalian ini memastikan apakah permintaan user terhadap TI dan permasalahannya direspon dengan cepat, efektif dan tepat waktu, serta disertai dengan pelaporan yang efektif.

  PT Bank XYZ telah mempunyai SOP Pengelolaan *Help Desk*. Penggunaan software sehubungan *service desk* juga telah diterapkan. Dimana software tersebut mengelola penerimaan, pencatatan, pengklasifikasian, eskalasi dan penyelesaian masalah. Termasuk penyediaan status dari semua permintaan yang belum terselesaikan serta analisis trend permintaan untuk mengidentifikasi pola kesalahan yang sering terjadi.

- DS9 *Manage the Configuration (Level 4 Managed and Measurable)*

  Proses ini memastikan adanya pengendalian yang dapat menjaga integritas konfigurasi perangkat lunak dan perangkat keras. Dengan demikian, diperlukan pengkokohan dan pemeliharaan penyimpanan konfigurasi yang akurat dan komplit.

  PT Bank XYZ telah memiliki prosedur pengendalian konfigurasi yang meliputi pemeliharaan configuration baseline, prosedur pengendalian perubahan untuk perangkat lunak atas pemeliharaan program aplikasi yang dilisensi. Perusahaan juga menggunakan *library management software.*

  Telah ada proses penyimpanan perangkat lunak yang mencakup pendeteksian, pendokumentasian, dan pelaporan bila terdapat penyimpangan. Pemutakhiran dokumentasi termasuk jika ada aset baru harus dicatat. Semua perubahan juga diotorisasi oleh pihak yang berwenang.

  Pengendalian konfigurasi mencakup individu-individu yang memiliki pengetahuan, keahlian dan kemampuan yang sesuai.

- DS10 *Manage Problems (Level 3 – Defined)*

  Divisi TI PT Bank XYZ melakukan manajemen masalah yang efektif. Setiap kejadian yang berbeda atau permasalahan dari standar yang ditetapkan dicatat, diidentifikasi dianalisis dan dicari penyelesaiannya tepat waktu. Termasuk terdapat prosedur otorisasi akses yang bersifat sementara dan darurat.

  Permasalahan yang diidentifikasi sebagai risiko Perusahaan dilaporkan kepada Divisi Manajemen Risiko PT Bank XYZ untuk kemudian ditindaklanjuti pemecahannya secara bersama. Perangkat Komisi Pengarah Teknologi Informasi, juga dapat dijadikan sarana untuk pembahasan permasalahan yang ada. KPTI melakukan pertemuan sebulan sekali untuk melakukan pembahasan berkaitan dengan TI

- DS11 *Manage Data (Level 2 – Repeatable but intuitive)*

  Manajemen data yang efektif dimulai dari pengidentifikasiaan keperluan data. Proses dari manajemen data meliputi penetapan prosedur yang efektif atas *media library, backup* dan *recovery data* serta media pemusnahan data yang tepat.

  Telah ada pengimplementasian dari manajemen data untuk media penyimpanan, *back up* dan *recovery data* serta media pemusnahan data yang tepat.

  Pada saat ini, PT Bank XYZ sedang mempersiapkan SOP yang terkait dengan prosedur manajemen data. Diantaranya :

  - SOP persiapan data yang memastikan kelengkapan, ketepatan, dan validitas data (Dalam proses penyusunan SOP)
  - SOP otorisasi untuk semua dokumen sumber
  - SOP yang memastikan kelengkapan dan ketepatan dokumen sumber dan konversi dokumen sumber yang tepat waktu

- DS12 *Manage the Physical Environment (Level 3 Defined)*

  Untuk mengamankan lingkungan fisik, PT Bank XYZ telah menerapkan beberapa pengendalian. Misalnya pengamanan fisik perangkat TI di data center dengan menggunakan *magnetic card*. Selain itu telah ada pembatasan akses ke dalam fasilitas data center dan hanya untuk pihak yang berwenang saja

  Telah ada penerapan fasilitas data center terhadap faktor-faktor lingkungan dengan menggunakan perangkat sebagai berikut : *raised floor, fire suppresion system, alarm system,* UPS, *power generator*, pendingin ruangan, *stabilizer*, antipetir, dan grounding.

  Telah ada pengujian berkala terhadap operasional peralatan yang dilakukan oleh vendor yang terkait dengan peralatan masing-masing.

  SOP berkaitam dengan hal ini belum ditandatangani oleh manajemen.

- DS13 *Manage Operation (Level 3 – Defined)*

  Perusahaan telah mempunyai SOP DTI yang digunakan sebagai panduan dalam proses operasi. Walaupun demikian proses pengembangan dari SOP terus dilakukan, untuk meng-*cover* beberapa SOP yang belum ada, karena teknologi, regulasi atas TI terus berkembang.

  Ada beberapa SOP yang telah berhasil dibuat untuk dijadikan panduan bagi operasional DTI, namun belum dapat diimplementasikan karena belum adanya persetujuan pihak manajemen terhadap SOP yang telah ada. Misalnya,belum ada SOP untuk menangani hal-hal operasional di luar kebiasaan.

4.4.4 Domain 4 - Monitor and Evaluate (ME)

- ME1 *Monitor and Evaluate IT Performance (Level 3 – Defined)*

  Proses ini memonitoring efektifitas kinerja TI dengan pendefinisian indikator kinerja yang relevan, sistematis dan tepat waktu dan melakukan tindakan untuk mengatasi tindakan penyimpangan yang terjadi, agar didapat suatu kepastian bahwa kinerja TI telah sejalan dengan tujuan dan kebijakan organisasi.

  PT Bank XYZ sedang memproses suatu sistem untuk memantau ataupun mengawasi sumber daya TI yang meliputi manusia, fasilitas, aplikasi, teknologi dan data dengan menggunakan sumber data. Termasuk diantaranya membuat Key Performance Indicator (KPI) dan Balance Score Card untuk mengukur kinerja TI, yang saat ini belum tersedia untuk melakukan pengukuran kinerja SDM dan TI.

  Namun demikian praktek pelaporan internal yang memadai dari pemanfaatan sumber daya TI telah ada. Termasuk pelaporan kinerja yang memadai kepada pihak bukan pengguna (*non user*) seperti auditor eksternal dan komite audit.

- ME2 *Monitor and Enable Internal Control (Level 3 – Defined)*

  PT Bank XYZ telah menggunakan data untuk memantau pengendalian internal TI, termasuk pelaporan dan *review* untuk pengendalian internal TI.

  Pelaksananan monitoring atas pengendalian internal melalui audit yang berkelanjutan oleh DAI. Kepatuhan atas kebijakan dan prosedur yang ada mengenai monitor atas pengendalian internal melalui supervisor review pihak ketiga. Telah ada review laporan kinerja dan pengendalian terhadap SLA (Service Level Agreement) melalui supervisi *review* pihak ketiga. Terdapat keterlibatan DTI dalam proses pemilihan pihak ketiga sehubungan dengan layanan yang dibutuhkan dan konsultan bagi DTI

- ME3 *Ensure Compliance with External Requirements (Level 3 – Defined)*

  PT Bank XYZ telah mempunyai kebijakan ataupun prosedur untuk memastikan adanya review kepatuhan terhadap hukum, aturan dan kontrak yang berlaku. Sebagai salah satu contohnya adalah penerapan audit internal dan eksternal untuk mengevaluasi pengendalian atas teknologi informasinya,

  PT Bank XYZ telah mempunyai *strategic IT plan* dimana hal ini terkait dengan peraturan Bank Indonesia, PBI No. 9/15/PBI/2007 yang berlaku efektif 31 Maret 2008.

  Penerapan prosedur keamanan sesuai dengan kebutuhan hukum dan secara memadai sedang dipenuhi atau ditangani yang mencakup proteksi password dan perangkat lunak yang membatasi akses, prosedur-prosedur otorisasi, adanya beberapa alat pengukuran, pengendalian firewall, proteksi virus, tindakan lanjut yang tepat waktu dari laporan pelanggaran.

  Selain itu telah ada program pelatihan dan pendidikan bagi personil TI mengenai masalah kepatuhan terhadap hukum, aturan, tata kelola TI.

- ME4 *Provide IT Governance (Level 3 – Defined)*

  PT Bank XYZ telah menyadari pentingnya tata kelola TI yang efektif. Hal tersebut dibuktikan dengan adanya prosedur atau kebijakan yang mengatur tata kelola TI. Dan pada saat ini, Perusahaan akan terus

mengembangkan SOP untuk memberikan standarisasi terhadap operasional TI. PT Bank XYZ juga telah mempunyai KPTI yang memberikan perhatian kepada TI yang diimplementasikan di Perusahaan. *IT strategic plan* telah dimiliki oleh Perusahaan, yang disesuaikan dengan perencanaan strategis Perusahaan.

Telah ada pelatihan yang mendukung tata kelola TI Perusahaan. Rencana Anggaran TI juga mencerminkan kebutuhan TI yang diselaraskan dengan kebutuhan bisnis Perusahaan.

Terdapat alat pengukuran untuk mengukur kinerja dari sumber daya TI, walaupun masih harus banyak pengembangan dan penyempurnaan.

Telah ada review terhadap tata kelola TI yang dilaksanakan oleh audit internal (DAI) dan juga audit dari pihak eksternal.

4.5 Hasil Audit Tata Kelola TI dengan COBIT

Setelah dilakukan audit lapangan maka disusun sebuah laporan mengenai hasil audit tata kelola dengan menggunakan kerangka COBIT tersebut. Hasil ini dapat dijadikan rekomendasi bagi Divisi Audit Intern dan Manajemen PT Bank XYZ. Dari penelahaan tersebut didapatkan hasil sebagai berikut :

1) *finding* kelemahan pengendalian internal TI perusahaan berdasarkan kerangka COBIT yang sudah dibahas sebelumnya (Tabel 4.1)
2) Area fokus dari proses COBIT (Tabel 4.3)
3) Status TI Perusahaan berdasarkan *Maturity Model Level*

Dari hasil proses audit lapangan dan pemaparan setiap proses pada paragraf sebelumnya (bagian 4.4), berikut adalah rangkuman penilaian dari proses COBIT, rentang nilai 0 *(Non existence)* sampai dengan 5 *(Optimised)*. *Maturity model level* tersebut dibandingkan antara yang telah disusun oleh Penulis dan DAI PT Bank XYZ. Berikut adalah bagan maturity model level tersebut :

Tabel 4.4 Maturity Model Level Penulis-DAI

		Penulis							IT Bank XYZ
	IT Process (A)	Maturity (B)						Skor (C)	Skor (D)
(B)		0	1	2	3	4	5		
PO	**Plan and Organized**								
PO1	*Define a Strategic Information Technology Plan*				√			3	-
PO2	*Define the Information Architecture*				√			3	-
PO3	*Determine Technological Direction*				√			3	-
PO4	*Define the Information Technology Organisation and Relationship*			√				2	-
PO5	*Manage the Information Technology Investment*			√				2	-
PO6	*Communicate Management Aims and Direction*			√				2	2
PO7	*Manage IT Human Resources*				√			3	2
PO8	*Manage Quality*			√				2	-
PO9	*Asses and Manage IT Risks*				√			3	-
PO10	*Manage Projects*			√				2	-
PO	Jumlah								
	Rata-Rata								
AI	**Acquire and Implement**								-
AI1	*Identify Automated Solution*				√			3	-
AI2	*Acquire and Maintain Application Software*					√		4	-
AI3	*Acquire and Maintain Technology Infrastructure*			√				2	-
AI4	*Enable Operation and Use*				√			3	-
AI5	*Procure IT Resources*					√		4	-

AI6	*Manage Changes*			√				2	3
AI7	*Initial and Accredit Solutions and Changes*				√			3	2
DS	**Deliver and Support**								
DS1	*Define and Manage Service Levels*				√			3	-
DS2	*Manage Third Party Services*				√			3	-
DS3	*Manage Performance and Capacity*			√				2	2
DS4	*Ensure Continous Service*				√			3	3
DS5	*Ensure Systems Security*				√			3	3
DS6	*Identify and Allocate Costs*				√			3	-
DS7	*Educate and Train Users*				√			3	-
DS8	*Manage Service Desk and Incidents*					√		4	3
DS9	*Manage the Configuration*					√		4	-
DS10	*Manage Problems*				√			3	-
DS11	*Manage Data*			√				2	-
DS12	*Manage the Physical Environment*				√			3	2
DS13	*Manage Operation*				√			3	2
ME	**Monitor and Evaluate**								
ME1	*Monitor and Evaluate IT Performance*				√			3	-
ME2	*Monitor and Enable Internal Control*				√			3	2
ME3	*Ensure Compliance with External Requirements*				√			3	-

ME4	*Provide IT Governance*				√			3	-

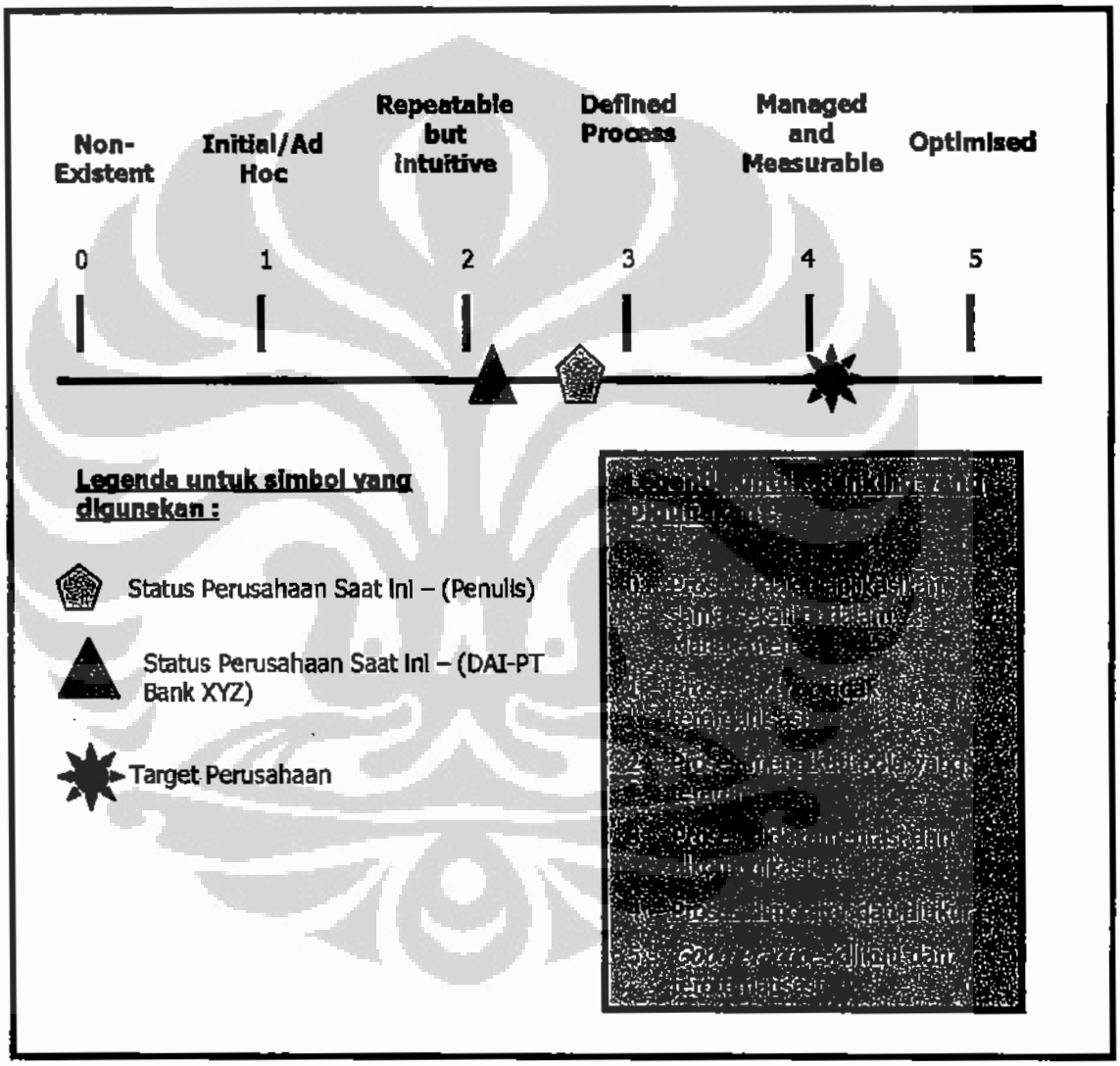
Dari tabel maturity model tersebut, dapat disimpulkan kondisi tata kelola TI pada PT Bank XYZ adalah sebagai berikut :

1. Maturity model level berdasarkan Penulis adalah di dalam rentang nilai level 2 dan 3 yaitu 2,85. Secara keseluruhan *maturity model level* dari tata kelola TI PT Bank XYZ untuk 34 proses lebih mendekati Level 3 *defined. (Lihat Gambar 4.4 Maturity model Level* – PT Bank XYZ-Penulis*)*.

2. Maturity model level berdasarkan uraian dari DAI PT Bank XYZ berada pada rentang level 2 dan 3 yaitu 2,36 , walaupun hanya melakukan audit pada 11 proses. Secara keseluruhan *maturity model level* PT Bank XYZ lebih mendekati Level 2 – *Repeatable but intuitive. (Bagan 4.2 Maturity model Level*-PT Bank XYZ-Penulis*)*.

3. Penulis telah mengkonfirmasikan atas perbedaan nilai maturity model level dengan pihak PT Bank XYZ (DAI) per domain (seperti dalam tabel di atas), menurut pihak Perusahaan, bahwa nilai maturity model tersebut tidak diberi skor tinggi (lebih banyak diberi nilai *2- repeatable and intuitive)* dengan tujuan terbentuknya suatu motivasi bagi Perusahaan untuk terus melakukan perbaikan di dalam tata kelola TI.

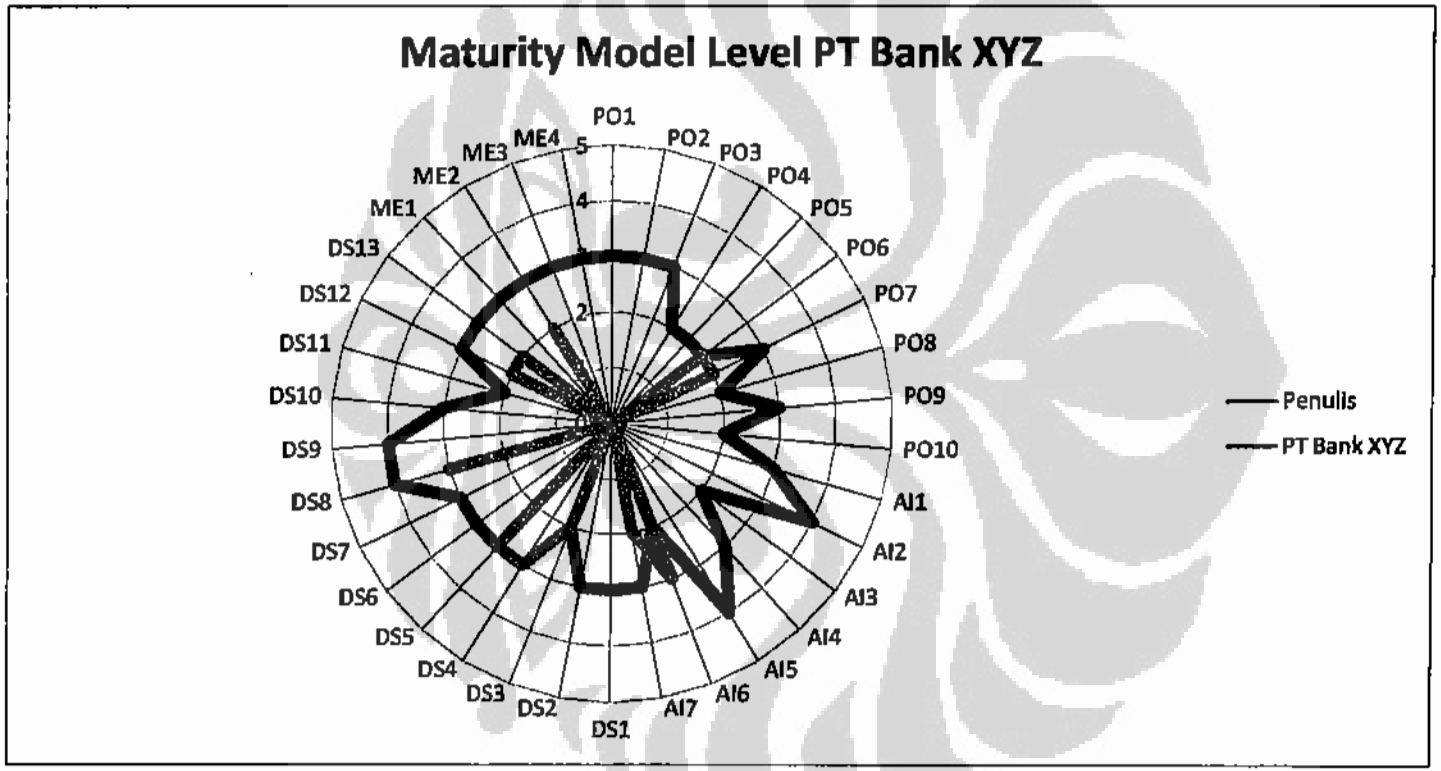
4. Perbedaan cakupan yang dipakai antara Penulis dan Perusahaan, menyebabkan adanya perbedaan jumlah area proses yang dapat dijadikan objek audit. Audit COBIT yang dilakukan Perusahaan adalah 11 proses, Penulis melakukan 34 proses. Untuk gambar grafik perbandingan dapat dilihat pada Bagan 4.3 Maturity Model Level-Perbandingan Penulis – PT Bank XYZ.



Gambar 4.3 Status Maturity Model Level (Penulis-DAI PT Bank XYZ)

Sumber : COBIT 4.1 (Telah diolah kembali)

Berikut bagan dari Maturity Model Level – per tiap proses COBIT yang dibandingkan antara disusun oleh Penulis dan PT Bank XYZ :



Gambar 4.4

Maturity Model Level-Perbandingan Penulis – PT Bank XYZ

4.6 Rekomendasi atas Hasil Audit Tata Kelola TI PT Bank XYZ

Sebagai salah satu nilai tambah dari audit adalah memberikan semacam rekomendasi atas hasil audit lapangan. Rekomendasi tersebut merupakan respon atas penelahaan yang telah dilakukan oleh auditor dalam melihat kelemahan, atau kekurangan sebagai referensi untuk melakukan perbaikan.

Penulis telah membuat beberapa rekomendasi atas diantaranya :

a. Rekomendasi atas kelemahan pengendalian internal yang dapat dilihat pada tabel 4.1 Kelemahan, risiko dan rekomendasi bagi kelemahan pengendalian internal
b. Pengembangan untuk *maturity model level* tata kelola TI PT Bank XYZ. Dapat dilihat pada tabel 4.6 Atribut untuk pengembangan maturity model level.

Penulis mencantumkan rekomendasi bagi pengembangan *maturity model level* yang berasal dari *Maturity Attributable – Framework, Control Objective, Management Guideline, Maturity Model* COBIT 4.1[2], sehingga Perusahaan dapat mengembangkannya sendiri sesuai dengan keadaan Perusahaan. Table 4.5 mencantumkan rekap maturity model level yang dibuat Penulis, sedangkan tabel. 4.6 merupakan atribut maturity model level sebagai panduan untuk meningkatkan maturity model level bagi PT Bank XYZ.

Tabel 4.5 Tabel Rekapan *Maturity Model level* atas Proses COBIT

No	Maturity Model Level	Jumlah
0	*Non Existent*	0
1	*Initial/Ad Hoc*	0
2	*Repeatable but Intuitive*	9
3	*Defined Process*	21
4	*Managed and Measurable*	4
5	*Optimised*	0

[2] ITGI - *Framework, Control Objective, Management Guideline, Maturity Model COBIT 4.1*

Tabel 4.6 Atribut untuk pengembangan *maturity model level*

Level	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Level 2 ke Level 3	▪ Terdapat pengertian dari manajemen bahwa harus adanya suatu tindakan. ▪ Manajemen lebih formal dan terstruktur dalam mengkomunikasikan	Penerapan *good practice* sangat mendesak Proses, kebijakan dan prosedur telah didefinisikan dan didokumentasikan di dalam setiap aktivitas.	▪ Perencanaan telah didefinisikan bagi penggunaan dan standarisasi perangkat untuk mengotomatisasi proses. ▪ Perangkat telah digunakan untuk tujuan dasar, namun belum semuanya sesuai dengan perencanaan dan beberapa belum terintegrasi dengan peralatan lainnya.	▪ Persyaratan keterampilan telah ditentukan dan didokumentasikan di seluruh area ▪ Training formal telah dikembangkan, namun training formal berdasarkan inisiatif individual	Tanggung jawab dan akuntabilitas dari proses telah diterima dan didefinisikan dan pemilik proses pun biasanya mempunyai otorisasi penuh untuk mengembangkan tanggung jawabnya tersebut	▪ Beberapa efektif gol dan pengukuran telah ditetapkan, namun belum dikomunikasikan, dan terdapat hubungan yang jelas dengan tujuan bisnis. ▪ Proses pengukuran penting, namun belum secara konsisten diterapkan. Ide BSC TI telah diadaptasi, juga penggunaan *root cause analysis* secara intuitif.

Level	Komunikasi dan Pemahaman	Kebijakan, Perencanaan dan Prosedur	Perangkat dan Otomatisasi	Keterampilan dan Kecakapan	Tanggung Jawab dan Akuntabilitas	Goal Setting dan Pengukuran
Level 3 ke Level 4	▪ Terdapatnya suatu pengertian untuk memenuhi semua persyaratan. ▪ Teknik komunikasi telah matang dan diaplikasikan serta perangkat komunikasi standar telah digunakan	▪ Proses telah disuarakan dan komplit, *best practices* internal Perusahaan diaplikasikan ▪ Semua proses telah didokumentasikan dan berulang. Kebijakan telah disahkan dan ditandatangani oleh manajemen. Standar untuk mengembangkan dan memelihara proses dan prosedur telah diadopsi dan diikuti.	▪ Perangkat diimplementasikan menurut perencanaan yang telah terstandarisasi dan beberapa telah terintegrasikan dengan perangkat lainnya. ▪ Perangkat digunakan di area utama untuk mengotomatisasi manajemen proses dan memonitor aktivitas kritikal serta pengendaliannya	Persyaratan keterampilan secara rutin di-*update* di semua area. Kecakapan dipastikan di seluruh area kritikal, dan peraihan sertifikasi diandalkan	Tanggung jawab dan akuntabilitas dari proses diterima dan bekerja dengan cara pemilik proses dapat melepas tanggung jawabnya. Terdapat budaya pemberian penghargaan untuk memotivasi pegawai	Tingkat efisiensi dan efektifitas telah diukur dan dikomunikasikan dan menghubungkan tujuan bisnis dan dengan perencanaan strategi TI. BSC TI telah diimplementasikan pada beberapa area dengan pengecualian yang diperhatikan manajemen dan *root cause analysis* telah distandarisasikan. Pengembangan yang berkelanjutan merupakan hal penting.

Level	Kesadaran dan Komunikasi	Kebijakan, Standar dan Prosedur	Perangkat dan Otomatisasi	Keahlian	Tanggung Jawab dan Akuntabilitas	Goal Setting dan Pengukuran
Level 4 ke Level 5	▪ Terdapat pengertian yang jauh ke depan terhadap pemahaman dari pemenuhan persyaratan ▪ Komunikasi pro-aktif terhadap isu-isu berdasarkan tren yang ada, Teknik komunikasi telah matang dan diaplikasikan serta perangkat komunikasi standar telah digunakan, dan perangkat komunikasi yang terintegrasi telah digunakan.	▪ *Best practice* eksternal telah diaplikasikan ▪ Proses dokumentasi telah berevolusi dimana alur kerja menjadi terotomatisasi. Proses, kebijakan dan prosedur telah terstandarisasi dan diintegrasikan untuk memudahkan manajemen dan pengembangannya	▪ Perangkat standarisasi digunakan di setiap bagian Perusahaan. ▪ Perangkat diintegrasikan dengan peralatan lainnya yang secara simultan mendukung proses ▪ Perangkat digunakan mendukung perkembangan prose dan secara otomatis mendeteksi adanya *control exceptions.*	▪ Organisasi secara formal memberikan dukungan untuk mengembangkan keahlian, berdasarkan tujuan personal dan organisasi. ▪ Training dan pendidikan mendukung *best practice* eksternal dan menggunakan konsep dan teknis yang paling maju. Pembagian ilmu pengetahuan , merupakan budaya perusahaan, *knowledge-based system* tengah diperdayakan. Ahli dari luar dan pemimpin industi digunakan sebagai pemberi petunjuk	▪ Pemilik proses diberi kekuasaan untuk membuat keputusan dan mengambil tindakan. ▪ Penerimaan tanggung jawab telah diturunkan melalui organisasi dengan cara yang konsisten	▪ Terdapat pengukuran kinerja yang terintegrasi yang menghubungkan antara kinerja TI dan tujuan bisnis dengan aplikasi menyeluruh dari BSC TI. ▪ Pengecualian secara keseluruhan dan konsisten merupakan catatan bagi manajemen dan *root cause analysis* telah diterapkan. Pengembangan yang secara terus menerus merupakan *way of life*

Sumber : *Framework, Control Objective, Management Guideline, Maturity Model* COBIT 4.1 (telah diolah kembali)

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

5.1.1 Maturity Model Level - Status TI PT Bank XYZ

Sejak tahun 2005 PT Bank XYZ telah mempercayakan kerangka tata kelola TI, COBIT *framework* sebagai perangkat penting dalam mengukur status dan pencapaian teknologi informasi dalam mendukung visi misi nya. *COBIT framework* mempunyai proses TI dan *maturity model level* yang dapat digunakan sebagai alat ukur hal tersebut.

Audit tata kelola TI dengan menggunakan COBIT sangat bermanfaat bila dilakukan oleh audit internal dibandingkan dengan audit eksternal. Ini dikarenakan, audit internal akan memberikan masukan kepada Manajemen mengenai status TI pada saat ini, dan rekomendasi perbaikan bagi divisi TI agar tata kelola TI dapat dikembangkan berkesinambungan yang tercermin di dalam domain-domain serta proses-prosesnya tersebut.

Divisi Audit Intern ("DAI") PT Bank XYZ telah melakukan upaya audit terhadap berjalannya tata kelola TI di PT Bank XYZ berdasarkan kerangka COBIT . DAI telah melakukan audit dengan hasil akhir memberikan status TI dengan *maturity model level*-nya dan rekomendasi kepada DTI PT Bank XYZ. Dari 34 proses COBIT, DAI telah melakukan audit terhadap 11 proses COBIT, dan memberikan skor terhadap *maturity model level* yang berada pada rentang level 2 – *repetitive but intuitive* dan level 3 – *defined process* dengan total skor 2,36.

Di lain sisi, Penulis juga menjalankan audit eksternal dengan kerangka COBIT PT Bank XYZ terhadap proses TI. Walaupun audit tersebut mempunyai keterbatasan waktu, *scope* dan *audit objective* yang berbeda dengan audit internal, namun telah memberikan hasil berupa 22 fokus area atas proses COBIT yang dapat dijadikan rekomendasi oleh DAI. Juga skor *maturity model level* atas 34 proses, serta beberapa saran dan rekomendasi perbaikan.

Maturity model level yang dihitung oleh Penulis atas TI PT Bank XYZ tersebut dengan skor sebesar 2,85 pada rentang yang sama dengan pengukuran DAI yaitu antara rentang level 2 – *repetitive but intuitive* dan level 3 – *defined process*.

Berdasarkan audit tata kelola TI PT Bank XYZ yang berbasis kerangka COBIT yang dilakukan penulis menyatakan bahwa posisi TI PT Bank XYZ berada pada level yang lebih mendekati level 3 – *defined process* yaitu 2,85, dan memang proses COBIT yang mencapai level tersebut ada 23 proses, atau sebesar 61,8 % sehingga level tersebut lebih dominan dalam pencapaian *maturity model level*. Dengan demikian interpretasi menurut kerangka COBIT berdasarkan level tersebut adalah, bahwa posisi TI PT Bank XYZ sudah mencapai tahapan dimana Manajemen PT Bank XYZ telah memahami dan melakukan tindakan terhadap permasalahan TI yang ada, dengan demikian Manajemen menjadi lebih formal dan terstruktur dalam hal komunikasi. Terlihat sudah ada sudah ada struktur organisasi TI yang komplit. Proses, kebijakan dan prosedur TI PT Bank XYZ telah ada dan didokumentasikan. Prosedur yang ada tersebut harus dipatuhi oleh segenap karyawan, namun demikian karena pengawasan pada tahapan ini masih kurang, penyimpangan terhadap kebijakan TI sulit dideteksi.

Interpretasi atas Maturity Model Level per Tingkat Pencapaian Level

Tabel 5.1 Tabel Rekapan *Maturity Model level* atas Proses COBIT
(disajikan kembali dari tabel 4.5)

Level	Keterangan	Jumlah Proses
0	*Non Existent*	-
1	*Initial/Ad Hoc*	-
2	*Repeatable but Intuitive*	9
3	*Defined Process*	21
4	*Managed and Measurable*	4
5	*Optimised*	-

Dari tabel 5.1 di atas, disarikan bahwa 9 atau 26,4% proses COBIT termasuk dalam skor *maturity model level* 2 – *repeatable but intuitive*, interpretasi dari level ini adalah bahwa proses TI yang berjalan pada PT Bank XYZ tersebut, telah dikembangkan pada tahapan dimana suatu prosedur yang sama diikuti oleh orang yang berbeda yang melakukan tugas sama, tidak adanya *training* formal ataupun komunikasi atau prosedur standar, tanggung jawab dibebankan kepada individu. Terdapat derajat ketergantungan yang tinggi terhadap pengetahuan individu, untuk itu kesalahan dapat sekali sering terjadi.

Posisi level 3-defined proses telah dijelaskan di atas dimana, level proses tersebut mewarnai status TI PT Bank XYZ.

Kemudian Level level 4-*managed and measurable*, terdapat 4 atau 11,8 % proses COBIT, dengan demikian menyatakan bahwa kondisi TI PT Bank XYZ pada 4 proses ini sudah mencapai tahapan dimana Manajemen telah memahami seluruh persyaratan yang harus dipenuhi atas TI. Semua aspek dan proses telah didokumentasikan dan dilakukan berulang, kebijakan dan standar telah diakui dan ditandatangani oleh manajemen. Proses dan prosedur telah diadopsi dan diikuti. Tingkat efektifitas dan efisiensi dari proses telah dikomunikasikan dan diukur.

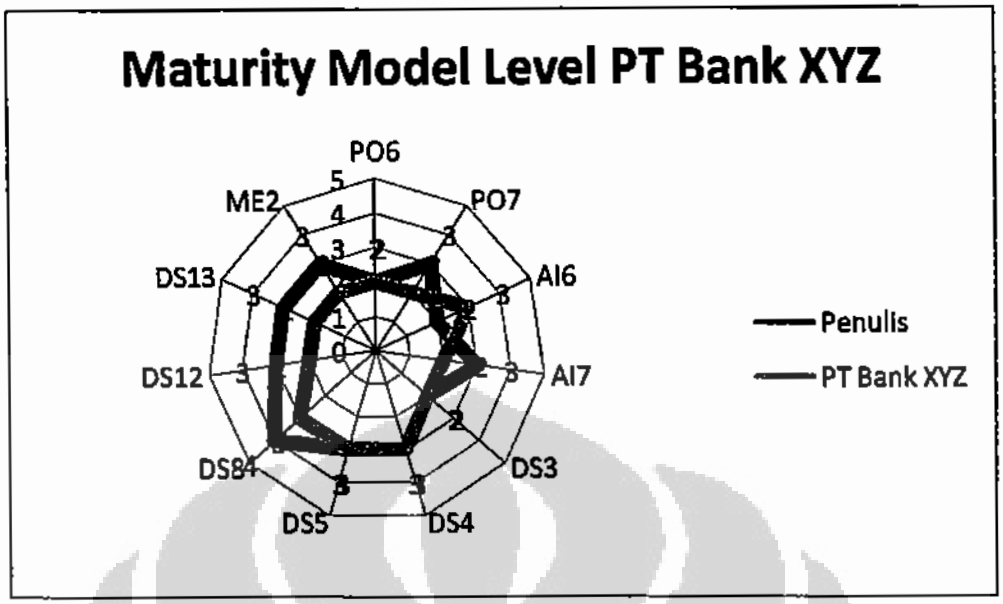
Dengan mengetahui posisi TI tersebut dan pencapaian atas proses TI, maka, PT Bank XYZ dapat memulai perencanaan kembali dengan target pencapaian yang lebih maju lagi, yang selaras dengan strategi Perusahaan untuk pencapaian visi misinya.

5.1.2 Melakukan Audit Tata Kelola TI dengan Tidak Menelaah Keseluruhan Proses.

DAI telah memberikan penilaian terhadap 11 proses TI berdasarkan COBIT dengan nilai 2,36 sedangkan Penulis memilih 11 proses yang sama dari 34 proses COBIT dengan nilai 2,82 (lihat tabel 5.2 dan Gambar 5.1) Dengan melakukan perbandingan ini, dihasilkan maturity model level yang sama, yaitu berada pada rentang level 2 – *repetitive but intuitive* dan level 3 – *defined process*.

Table 5.2 Rekap 11 Proses COBIT

Proses TI Berdasarkan COBIT	Penulis	DAI Dan Ex V
PO6 Communicate Management Aims and Direction	2	2
PO7 Manage IT Human Resources	3	2
AI6 Manage Changes	2	3
AI7 Initial and Accredit Solutions and Changes	3	2
DS3 Manage Performance and Capacity	2	2
DS4 Ensure Continous Service	3	3
DS5 Ensure Systems Security	3	3
DS8 Manage Service Desk and Incidents	4	3
DS12 Manage the Physical Environment	3	2
DS13 Manage Operation	3	2
ME2 Monitor and Enable Internal Control	3	2
Jumlah	31	26
Nilai Rata-Rata	2,82	2,36



Gambar 5.1 Maturity Model Level PT Bank XYZ dengan 11 Proses

Nilai tersebut pun memberikan gambaran yang sama, jika dikaitkan dengan pencapaian nilai maturity model level dengan 34 proses yang dilakukan oleh Penulis, seperti yang telah disebutkan sebelumnya yaitu dengan skor nilai 2,85. Ketiga-tiganya berada pada rentang level 2 dan level 3 maturity model level dari COBIT. Dan penilaian 11 proses COBIT dan 34 proses COBIT yang dilakukan oleh Penulis memberikan nilai yang hampir sama, 11 proses sebesar 2,82 sedangkan 34 proses sebesar 2,85.

Jadi ada penggambaran secara khusus dari 11 proses tersebut yang memberikan penjelasan atau gambaran umum atas posisi TI PT Bank XYZ dengan 34 proses.

Dengan adanya penjabaran tersebut di atas, dimungkinkan untuk melakukan audit tata kelola TI dengan kerangka COBIT—yang sebenarnya pun merupakan audit internal terhadap kepatuhan dari kriteria yang telah ditetapkan oleh COBIT —dengan mengambil beberapa proses dari COBIT tersebut, dan tidak secara keseluruhan dilakukan dengan 34 proses TI. Penetapan pemilihan proses tersebut bisa dengan melakukan *risk analysis*, seperti yang telah dilakukan

oleh penulis untuk memberikan rekomendasi 22 proses COBIT sebagai area fokus kepada DAI.

Namun demikian, pernyataan tersebut masih perlu dibuktikan lewat penelitian lebih lanjut.

5.1.3 Penerapan Audit Tata kelola TI oleh Audit Internal dan Eksternal

Penerapan audit tata kelola TI dengan kerangka COBIT di dalam industri perbankan khususnya yang dilakukan oleh audit internal PT Bank XYZ mengikuti metodologi yang berlaku umum, seperti yang diuraikan oleh Hunton dalam Bab II Landasan Teori. Dalam hal urutan langkah-langkah metodologi audit pada PT Bank XYZ secara garis besar adalah, diantaranya persiapan audit, pelaksanaan audit, pelaporan audit dan monitoring audit. Langkah-langkah metodologi tersebut juga dilakukan oleh audit eksternal. Pembuatan audit program yang dibuat oleh DAI pun diselaraskan dengan *IT process,* IT *Objective* dan *Corporate Objectives,* sebagaimana dilihat dalam Bab 3 Gambaran Umum.

Perbedaan diantara keduanya adalah pada waktu, cakupan audit (*audit scope*) dan *audit objective.*

Audit internal memiliki waktu yang cukup banyak untuk melakukan audit tersebut karena ia berkedudukan di tempat yang sama dengan objek audit, *day to day operation* dari objek audit dapat dilihat secara langsung.

Cakupan audit dari auditor internal bisa dapat dikembangkan lebih luas. Cakupan audit DAI PT Bank XYZ adalah Divisi Teknologi Informasi (DTI) yang berada di kantor pusat juga ditambah beberapa kantor cabang di berbagai provinsi di Indonesia yang dijadikan sampel, sehingga lebih komprehensif, walaupun hanya dengan 11 proses COBIT, namun dapat masuk ke dalam areal yang tidak bisa dijangkau oleh Penulis sebagai auditor eksternal. Cakupan audit dari auditor eksternal terbatas pada DTI yang berada di kantor pusat dengan waktu yang terbatas, termasuk pembatasan *audit evidence* karena faktor *confidential.*

Sedangkan faktor *audit objective,* dari DAI adalah memperoleh keyakinan yang memadai mengenai bagaimana tata kelola TI telah dijalankan oleh PT Bank XYZ, bagaimana kondisi TI perusahaan saat ini apakah telah

memberikan *value*, dan rekomendasi atas temuan-temuan audit termasuk penentuan *maturity model level* tersebut. Bagi auditor eksternal, *audit objective* berkaitan dengan pengendalian internal dari Perusahaan yang nantinya (jika ia adalah auditor eksternal pembuat laporan keuangan) adalah, melihat *internal control* yang berasal dari TI itu dengan menggunakan kerangka COBIT. Maka, hasil akhir dari auditor eksternal, seperti yang telah dibahas pada Bab IV Analisis dan Hasil Audit, adalah rekomendasi cakupan area proses COBIT bagi audit intern, rekomendasi atas kelemahan *internal control* termasuk juga penentuan *maturity model level*. Rekomendasi dan saran tersebut diharapkan dapat meningkatkan dan mengembangkan TI Perusahaan agar nantinya TI menjadi *enabler* bagi bisnis secara berkesinambungan

5.1.4 Nilai Tambah Pemanfaatan Tata Kelola TI dengan COBIT

Dengan menerapkan audit tata kelola TI dengan COBIT, maka PT Bank XYZ telah mendapatkan beberapa keuntungan sekaligus, yaitu meningkatkan *good corporate governance(GCG)* yang dianjurkan pemerintah, memenuhi *compliance* dengan regulator yaitu BI dan menerapkan *internal control* bagi sistem TI yang telah dilakukan di Perusahaannya, karena COBIT adalah tujuan bagi *internal control* itu sendiri.

Dilihat dari sisi GCG terhadap COBIT. GCG mempunyai prinsip-prinsip yang harus dipenuhi oleh Perusahaan, seperti transparansi, akuntabilitas, responsibilitas, independensi serta kesetaraan dan kewajaran. Prinsip-prinsip tersebut berkaitan erat dengan tata kelola TI. Misalnya saja prinsip transparansi dimana Perusahaan harus menyediakan informasi tepat waktu yang relevan serta material yang dengan mudah diakses bagi *stakeholder*. Kualitas informasi itu pun merupakan *value* yang harus di-delivery oleh TI. Kemudian prinsip responsibilitas atau tanggung jawab, dimana Perusahaan harus memenuhi atau taat terhadap aturan, regulasi, hukum yang berlaku. Pemenuhan prinsip tersebut dapat difasilitasi oleh COBIT, karena kerangka COBIT terkait dengan pemenuhan regulasi, ini terkait dengan ME3 *Ensure Compliance with external requirement*.

ITGI pun menegaskan dalam COBIT 4.1, *bahwa IT governance* merupakan bagian yang tidak terpisah dari *enterprise governance*, dengan demikian penerapan tata kelola TI, sudah seharusnya menjadi perhatian manajemen Perusahaan.

PT Bank XYZ pun telah menerapkan Peraturan Bank Indonesia yaitu PBI No. 9/15/PBI/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum. Penulis menelaah peraturan BI tersebut dan pihak DAI pun telah memberikan konfirmasi, bahwa implementasi peraturan tersebut telah tercermin di dalam tata kelola TI yang diterapkan PT Bank XYZ saat ini. Dan sebagai informasi tambahan, peraturan BI tersebut juga mengadaptasi *COBIT framework,* sehingga secara tidak langsung, jika PT Bank XYZ telah menerapkan COBIT maka Peraturan BI pun juga sudah dipatuhi dan diterapkan.

5.2 Saran

1. Audit dengan kerangka COBIT secara khusus mampu memberikan petunjuk bagi Divisi Audit Intern untuk mempermudah pekerjaannya dalam mengevaluasi tata kelola TI. Dan bagi PT Bank XYZ kerangka COBIT mampu memberikan petunjuk bagi selarasnya objektif TI dan objektif Perusahaan. Namun, saat ini PT Bank XYZ belum dapat memanfaatkan kerangka COBIT sebagai kerangka tata kelola TI yang komprehensif, dan optimal, karena terdapat kendala waktu, sumber daya manusia yang kompeten. Untuk itu, PT Bank XYZ diharapkan mampu mengatasi permasalahan tersebut, dengan :

   - Membuat perencanaan yang berfokus pada audit tata kelola TI dengan peningkatan alokasi waktu yang optimal bagi DTI untuk mendukung audit tata kelola TI secara komprehesif karena *IT governance* merupakan hal penting bagi Perusahaan terutama berkaitan dengan banyak risiko yang mengancam eksistensi Perusahaan dan *value* yang diberikan lebih tinggi dibandingkan *cost*-nya

- Meningkatkan anggaran bagi DAI agar dapat melakukan banyak aktivitas yang mendukung audit tata kelola TI
- Meningkatkan jumlah sumber daya manusia di DAI, dengan melakukan rekruitmen pegawai dalam kurun waktu yang telah ditetapkan, agar ketika DAI melakukan audit, personil yang dibutuhkan telah siap melakukan tugasnya
- Memberikan pelatihan dan pendidikan khusus mengenai tata kelola TI dan bidang lain yang berhubungan, baik dengan mengundang pihak yang berkompeten dari luar, atau memberikan beasiswa tugas belajar ke perguruan tinggi bagi personil DAI

2. PT Bank XYZ mampu secara konsisten memanfaatkan hasil audit internal yang memberikan temuan serta rekomendasinya untuk meningkatkan status level TI dan perbaikan TI, sebagaimana Laporan Hasil Audit dari DAI dan juga masukan penulis di dalam Bab IV Analisis dan Hasil Audit.

3. Dari penelahaan pengendalian internal dari PT Bank XYZ, didapati faktor dominan kelemahan adalah SOP-SOP operasional belum ditandatangani atau masih dalam proses penyusunan. Tanpa adanya SOP tersebut, pelaksanaan operasional TI berjalan tanpa standar, sehingga penyelewengan ataupun kesalahan yang tidak diinginkan oleh Perusahaan dapat terjadi. Perusahaan sebaiknya segera mempercepat penyelesaian SOP tersebut.

4. Manajemen puncak sebagai penanggung jawab atas berjalannya *IT governance*, lebih menyadari peranannya, bahwa tanpa adanya keteladanan dari manajemen puncak, manfaat yang mampu diberikan oleh *IT governance* pada suatu Perusahaan tidak akan tercapai. Dengan demikian, Dewan Direksi beserta jajaran PT Bank XYZ harus meningkatkan perhatiannya terhadap aktivitas tata kelola TI pada organisasi, misalnya dengan membangun budaya yang perhatian terhadap keamanan TI, memberikan perhatian kebutuhan TI pada PT Bank XYZ dengan segera seperti menyegerakan persetujuan terhadap SOP yang sudah disusun, dan lain sebagainya.

DAFTAR REFERENSI

Arens, Alvin A., James K.Loebbecke. *Auditing : An Integrated Approach 8th Edition.* New Jersey : Prentice Hall.Inc : 2000

Bank Indonesia. *Sekilas Implementasi Basel II di Indonesia.* Jakarta <http://www.bi.go.id/web/id/ Perbankan/Implementasi+Basel+II/>

Brooks, Leonard J. *Business & Professional Ethisc for Directors, Executives & Accountant.* South-Western Publication : Juli 2006

Cannon, David L. *CISA Certified Information System Auditor, Study Guide 2nd Edition.* Indiana : Wiley Publishing Inc: 2008

Dewi , Risnawati Kumala. *Audit TI Menggunakan COBIT 4.1 di Direktorat Jenderal Anggaran Departemen Keuangan.* Jakarta : Program Magister Akuntansi FEUI, Mei 2009

http://pusatbahasa.diknas.go.id/kbbi/index.php

Hunton, James E., et al. *Core Concepts of Information Technology Auditing.* USA : John Wiley & Sons : 2008

IAI. *Standard Profesional Akuntan Publik.* Salemba Empat : 2001

ISACA. *Case Study: Kuwait Turk Participation Bank Uses COBIT for Compliance and Reaps AdditionalBenefits* .2008 <http://www.isaca.org/Template.cfm?Section=Home&Template=/Content Management/Cont ntDisplay.cfm&ContentID=31694>

ITGI. *COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models.* ITGI : 2007

ITGI. *IT Assurance Guide : Using COBIT.* ITGI : 2007

Konrath, Larry F. *Auditing : A Risk Analysis Approach 5th Edition.* USA : South Western, 2002

Lawrence, Anne T., James Weber. *Business and Society : Stakeholders, Ethics, Public Policy 12th Edition.* New York : McGraw-Hill/Irwin, 2008

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum

Peraturan BI Nomor 5/8/PBI/2003 tentang penerapan manajemen risiko bagi bank umum

PWC and IT Governance Institute . *IT Governance Global Status Report 2008* : 2008

Turban, Efraim, et al. *Information Technology for Management : Transforming Organizations in the Digital Economy 6th Edition.* John Wiley and Sons: 2008)

Undang – Undang Republik Indonesia No. 10 Tahun 1998 tentang Perbankan

Weill, Peter. , Jeanne W. Ross. IT Governance : *How Top Performers Manage IT Decision Rights for Superior Results.* Harvards Business School Press : 2000

Westerman, G., Richard Hunter. *IT Risk : Turning Business Threats into Competitive Advantage.* Boston, Massachusetts : Harvard Business School Press, *2007*

Lampiran 1

PROSES AUDIT PADA PT BANK XYZ

1. Tahap Persiapan Audit

Untuk mengawali proses audit TI diperlukan persiapan-persiapan khusus, agar audit berjalan sesuai dengan tujuannya. Berikut penjelasan masing-masing tahapan pertama persiapan audit.

1) Persiapan penyusunan Skedul Audit & Estimasi Waktu;

   Skedul audit dan estimasi waktu yang digunakan sebagai panduan audit dibuat oleh Divisi audit internal TSI, ditandatangani oleh unit pengendalian mutu dan disetujui oleh direktur utama. Kemudian DAI TSI akan menjalankan audit sesuai jadwal yang telah ditetapkan ini.

2) Persiapan Pengumpulan Data;

   Divisi audit akan membuat suatu Kuisioner Pengendalian Internal (KPI), yang bertujuan untuk mendapatkan pemerolehan data untuk persiapan Laporan Persiapan Audit (LPA). Kuisioner ini kemudian akan dikirimkan kepada pihak yang akan diaudit *(auditee)*.

3) Penyusunan Laporan Persiapan Audit;

   Laporan LPA diajukan oleh tim audit yang kemudian diserahkan kepada bagian Pengendalian Mutu Audit ("PMA"). Jika PMA sudah menyetujui LPA ini, tim audit akan mendokumentasikan LPA ini.

4) Administrasi dan Biaya Audit;

   Tim audit menyiapkan administrasi dan biaya audit yang sesuai dengan anggaran, yang tercantum di dalam LPA. PMA juga me-*review* administrasi dan biaya audit ini.

2. Tahap Pelaksanaan Audit :

Tahap pelaksanaan audit terdiri dari pelaksanaan audit TI dan konfirmasi hasil audit, berikut tahapannya :

1) Pelaksanaan Audit

a. Pelaksanaan audit dilakukan berdasarkan *audit program* yang telah ditetapkan. Masing-masing anggota tim audit bertanggung jawab terhadap *audit program* yang telah diamanatkan kepadanya.

b. Tim audit mengkomunikasikan segala kebutuhan auditnya kepada *auditee*, misalnya tujuan audit, kebutuhan akan data dan informasi yang relevan dan kompeten yang diperlukan dalam menjalani audit.

c. Dalam melakukan pekerjaannya, tim audit harus memastikan, memeriksa, mengevaluasi baik kebenaran atau penyimpangan terhadap obyek audit.

d. Permasalahan atau *finding* yang telah ditemukan oleh tim audit dikompilasi dan dilengkapi bukti-buktinya.

e. KKA (Kertas Kerja Audit).

Seluruh pekerjaan proses audit dan bukti-bukti yang relevan dalam mendukung audit tersebut, harus didokumentasikan di dalam KKA. KKA ini akan ditandatangani oleh anggota tim yang mengerjakan bagian audit tersebut dan di-*review* oleh Ketua Tim Audit.

Ketua tim audit harus memastikan bahwa KKA harus memenuhi adanya unsur-unsur berikut ini :

- Fakta/kondisi, merupakan bukti atau kondisi yang terjadi yang ditemukan oleh auditor
- Kriteria, keadaan yang seharusnya, standar atau ukuran yang digunakan dalam melakukan evaluasi atau verifikasi
- Dampak, merupakan risiko atau eksposur yang akan dihadapi oleh Bank karena fakta/kondisi yang terjadi tidak sesuai dengan kondisi yang seharusnya
- Penyebab merupakan penjelasan atas perbedaan antara kondisi yang diharapkan dengan kondisi sebenarnya.
- Langkah-langkah perbaikan yang dilakukan oleh *auditee*.

- Rekomendasi/saran perbaikan untuk mengoreksi kondisi yang ada dan menyempurnakan aktivitas operasional.
- Review dan Petunjuk Ketua Tim, dilakukan oleh ketua tim audit setelah mempelajari uraian temuan dari anggota tim.

2) Temuan atau finding yang ada didiskusikan bersama-sama.
3) Konfirmasi dan Klarifikasi Hasil Audit;

   Hasil dari audit termasuk temuan, rekomendasi atau saran perbaikan dikomunikasikan kepada *auditee*. Untuk selanjutnya ditindaklanjuti oleh *auditee* tersebut.

3. Tahap Pelaporan Audit

Setelah melaksanakan audit dan mengetahui hasilnya, maka tim audit akan menyiapkan LHA (Laporan Hasil Audit). LHA ini sebagai dokumentasi dari audit dari tahap perencanaan sampai dengan akhir pekerjaan lapangan. LHA akan disahkan oleh kepala divisi audit. Tahapan pelaporan audit dilakukan dengan aktivitas berikut ini :

1) Penyusunan dan pengesahan hasil audit

   Seluruh tim bertanggung jawab terhadap penyusunan dan pengesahan hasil audit. Setelah disahkan dan dicetak kemudian diberikan kepada *auditee*, atau pihak lainnya yang membutuhkan LHA.

2) Penyusunan dan pengesahan *executive summary*

   Executive summary disusun dan difinalisasikan oleh ketua tim audit, dengan pengesahan oleh audit super intendant dan kepala divisi.

3) Laporan Pertanggungjawaban Kegiatan dan Hasil Audit;

   Tim audit menyiapkan Laporan Pertanggungjawaban Kegiatan (LPK) dan hasil audit dan memberikannya kepada pihak Pengendalian Mutu Audit (PMA)

4) Serah Terima Monitoring Tindak Lanjut Audit;

   Berita acara serah terima monitoring sebagai tindak lanjut audit, diberikan kepada auditee.

5) Pengelolaan Ikhtisar Lintas Divisi;

Ikhtisar lintas divisi mengupayakan penyelesaian dari suatu temuan hasil audit dari suatu divisi pada kantor cabang, yang penyelesaiannya dilakukan di divisi yang berada di kantor pusat.

4. Tahap Monitoring Audit

1) Penyusunan Laporan Monitoring Hasil Audit;

Untuk penyusunan laporan monitoring hasil audit, tim audit memantau temuan hasil audit yang perlu ditindaklanjuti. Tim audit akan memberikan surat pemberitahuan kepada *auditee* mengenai tindaklanjut temuan tersebut, dengan melalui 3 tahapan. Temuan yang belum terselesaikan oleh *auditee* dalam kurun waktu 3 tahapan tersebut, maka akan dibuat laporannya pada Laporan Monitoring hasil audit dalam kolom pelampauan waktu.

2) Pelaksanaan Analisis Tindak Lanjut Hasil Audit;

Tim audit melakukan analisa terhadap tindak lanjut hasil audit.

3) Konfirmasi Monitoring Hasil Audit;

Tim audit akan membuat surat konfirmasi yang akan ditujukan kepada auditee, jika waktu jatuh tempo yang telah disepakati untuk menindaklanjuti temuan telah lewat. Surat konfirmasi mengenai tindak lanjut hasil audit dikirim sebanyak 2 kali, untuk jangka waktu yang berbeda.

Surat Konfirmasi I, dikirim oleh tim kepala divisi audit, dengan sepengetahuan Direktur Kepatuhan dan supervisor dari cabang yang bersangkutan. Jangka waktu bertanggungjawaban adalah 10 hari

Surat Konfirmasi II akan dikirim jangka waktu surat konfirmasi I telah lewat belum ada tanggapan. Surat ini dikirimkan kepada *auditee* dengan tembusan kepada Direktur Kepatuhan.

4) Pembuatan Surat Teguran kepada *Auditee*.

Tim audit akan membuat Surat Teguran kepada *auditee* jika Surat Konfirmasi II sampai dengan batas 7 hari, diabaikan, ataupun belum ada perbaikan atas tindak lanjut audit.

Surat Teguran akan ditandatangani oleh divisi audit dan disetujui oleh Direktur Kepatuhan serta Direktur SDM. Serta ditembuskan kepada Direktur Utama, satuan kerja yang mensupervisi cabang dan satuan kerja yang menangani SDM.

Aplikasi *Maturity Model Level* PT Bank XYZ - Contoh

Lampiran 2

			Importance				
	PO6 - COMMUNICATE MANAGEMENT AIMS AND DIRECTIONS		Weight	Value	Score	Total	Remarks (Evidence and Documentation)
Level 5 Optimised (Best Practice)	The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved		M	1	0	0	Total Star (A)
	Monitoring, self-assessment and compliance checking are pervasive within the organisation		M	1	0	0	
	Technology is used to maintain policy and awareness knowledge bases and to optimise communication, using office automation and computer-based training tools	Criteria	M	1	0	0	
	Internal and external experts are assigned to ensure that industry good practices are being adopted with respect to control guidance and communication techniques		M	1	0	0	
Level 4 Managed and Measurable (Understand full requirement)	Management accepts responsibility for communicating internal control policies and delegates responsibility and allocates sufficient resources to maintain the environment in line with significant changes		M	1	0,5	0,5	
	A positive, proactive information control environment, including a commitment to quality and IT security awareness, is established		M	1	0	0	
	A complete set of policies, plans and procedures is developed, maintained and communicated and is a composite of internal good practices		M	1	0,5	0,5	
	A framework for rollout and subsequent compliance checks is established		M	1	0	0	
Level 3 Defined Process (Understanding of need to act)	A complete information control and quality management environment is developed, documented and communicated by management and includes a framework for policies, plans and procedures		M	1	0,5	0,5	
	The policy development process is structured, maintained and known to staff, and the existing policies, plans and procedures are reasonably sound and cover key issues		M	1	0,5	0,5	
	[illegible]		M	1	1	1	
	[illegible]		M	1	1	1	
	While there is an overall development framework for control policies and procedures, there is inconsistent monitoring of compliance with these policies and enforcement		M	1	0,5	0,5	
	There is an overall development framework Techniques for promoting security awareness have been standardised and formalised		M	1	0	0	
Level 2 Repeatable but Intuitive (Awareness)	[illegible]		M	1	1	1	
	[illegible]		M	1	1	1	
	[illegible]		M	1	1	1	
	[illegible]		M	1	1	1	
Level 1 Initial/Ad Hoc (Recognition)	Management is reactive to addressing the requirements of the information control environment		M	1	1	1	
	Policies, procedures and standards are developed and communicated on an ad hoc basis, driven by issues		M	1	1	1	
	The development, communication and compliance processes are informal and not tested		M	1	1	1	

		PO5 - COMMUNICATE MANAGEMENT AIMS AND DIRECTIONS		Importance Weight	Value	Score	Total	Remarks (Evidence and Documentation)
Level 0	Non-existent (No issue)	[illegible]	●	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		[illegible]	●	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

	Score Summary	Count	Total	Possible	%	6/100	Level Met? = 1 = Yes
Level 5		4	0	4	0%	0	0
Level 4		4	1	4	25%	4	0
Level 3		6	3.5	6	58%	9	0
Level 2		4	4	4	100%	16	1
Level 1		3	3	3	100%	16	1
Level 0		2	2	2	100%	16	1
SCORE						61%	Level 2

Keterangan :

Count — Banyaknya kriteria pada tiap level
Total — Total skor (misalnya pada [A])
Possible — Kemungkinan terjadinya kriteria (jumlahnya sama dengan jumlah count)
% — cell total/cell possible
6/100 — % * (100/6)
Level — Jika kriteria pada level, semuanya memenuhi kriteria 1. Pada proses ini, kriteria terpenuhi tanpa terputus dari level 0-level 2, level 3 masih terdapat kriteria yang tidak dipenuhi, oleh karena itu level perusaan sampai pada level 2

LAMPIRAN 3

Sumber Program Audit ini berasal dari Karya Akhir berjudul Audit TI Menggunakan COBIT 4.1 di Direktorat Jenderal Anggaran Departemen Keuangan – oleh Risnawati Kumala Dewi, Program Magister Akuntansi FEUI, Mei 2009, yang berdasarkan IT Assurance Guide, ITGI.

PT Bank XYZ		Disiapkan oleh	:	**Program Audit**
Proses :	**PO 1 - Plan and Organized**	Tanggal	:	
Program Audit :	**Define a Strategic Information Technology Plan (PO1)**	Diperiksa oleh	:	**PO1**
		Tanggal	:	

Tujuan:

Memastikan adanya perencanaan strategis TI untuk mengatur dan mengarahkan agar semua sumber daya TI sejalan dengan strategi dan prioritas bisnis, memberikan pemahaman kepada *stakeholder* mengenai peluang dan keterbatasan TI, menilai performa TI saat ini dan menghitung berapa jumlah investasi yang dibutuhkan

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
IT Value Management			
Memastikan bahwa terdapat portfolio TI dengan mempertimbangkan risiko dan manfaat yang diinginkan, serta kebutuhan investasi yang jelas agar dapat menampung seluruh proses TI sehingga berjalan efektif dan efisien	Tidak adanya portfolio TI yang baik akan menyebabkan TI tidak sejalan dengan proses bisnis organisasi dan dapat menyebabkan kesalahan dalam mengambil keputusan sehingga investasi TI yang dilakukan menjadi merugi serta tidak jelas dan dipahaminya biaya, manfaat dan risiko TI	Memeriksa apakah terdapat kebijakan yang mendorong dibuatnya portfolio TI dan apakah bermanfaat atau tidak	
Business-IT Alignment			
Memastikan adanya proses dengan konsep pendidikan dua arah dan saling timbal balik dalam perencanaan strategis agar tujuan bisnis sejalan dan terintegrasi dengan TI	Tidak sejalannya TI dengan tujuan organisasi akan mengakibatkan tidak adanya dukungan TI terhadap seluruh misi organisasi	Memeriksa apakah terdapat proses yang demikian dan apakah berjalan efektif atau tidak	

Assessment of Current Capability and Performance			
Memastikan bahwa manajemen TI melakukan penilaian sistem yang mencakup kemampuan, kinerja, fungsionalitas, stabilitas, kompleksitas, biaya, kelebihan dan kekurangan, untuk menentukan sejauh mana sistem yang ada saat ini mampu mendukung proses bisnis organisasi	Tidak adanya penilaian terhadap kemampuan dan kinerja TI sehingga tidak dapat diketahui apakah sistem yang ada saat ini mampu mendukung proses bisnis organisasi atau tidak dan tidak diketahui apa kebutuhan sistem di masa mendatang	Memperhatikan apakah terdapat proses penilaian terhadap sistem yang ada saat ini	
Strategic Plan			
Memastikan bahwa manajemen TI membuat suatu rencana strategis yang mendefinisikan bagaimana TI mendukung tujuan strategis organisasi dengan memperhitungkan biaya dan risikonya	Tidak adanya rencana strategis TI dapat mengakibatkan TI tidak mampu mendukung proses bisnis yang penting serta dilakukannya investasi TI yang tidak bermanfaat	Memperhatikan apakah terdapat rencana strategis TI atau tidak	
Tactical Plans			
Memastikan bahwa manajemen TI membuat rencana taktis TI yang diturunkan dari rencana strategis TI, yang menjelaskan gagasan-gagasan TI, kebutuhan sumber daya, dan bagaimana menggunakan sumber daya agar memperoleh manfaat sesuai harapan	Tidak adanya rencana taktis TI mengakibatkan tujuan dan rencana jangka panjang TI tidak mampu dicapai dan dilaksanakan; sumber daya TI yang ada tidak mendatangkan manfaat bagi organisasi; tidak teridentifikasinya penyimpangan rencana TI	Memperhatikan apakah terdapat rencana taktis TI atau tidak	
Portfolio Management			
Memastikan bahwa terdapat penanganan portfolio TI dengan mengidentifikasi, mendefinisikan, mengevaluasi, memprioritaskan, memilih, menginisiasi, mengatur dan mengawasi berbagai program TI yang ada agar TI dapat mendukung dalam mencapai tujuan organisasi	Portfolio TI yang tidak tepat akan mengakibatkan hilangnya berbagai peluang akibat dari portfolio TI yang terlalu konservatif, tidak teridentifikasinya sumber daya TI dan penyimpangan dalam rencana TI tidak dapat diidentifikasi	Memperhatikan apakah terdapat portfolio TI atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**PO 1 - Plan and Organized**	Tanggal	:	
Program Audit :	**Define The Information Architecture (PO2)**	Diperiksa oleh	:	**PO2**
		Tanggal	:	

Tujuan:

Memastikan pengelolaan sistem informasi dilakukan secara maksimal, melalui pembuatan model informasi yang dibutuhkan, meliputi pembuatan kamus data yang terhubung dengan aturan sintaks data yang dimiliki oleh organisasi, skema klasifikasi data dan level keamanan data, sehingga akan memperbaiki kualitas pengambilan keputusan dengan memastikan bahwa terdapat informasi yang handal dan aman yang mampu memenuhi kebutuhan organisasi, dan akan meningkatkan integritas dan keamanan data agar pertukaran informasi di antara aplikasi atau entitas yang ada berjalan secara efektif

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Enterprise Information Architecture Model			
Memastikan adanya model arsitektur informasi organisasi yang memiliki integritas, fleksibel, fungsionalitas, efektif dari segi biaya, disampaikan secara tepat waktu dan aman untuk mendukung pengembangan aplikasi dan pengambilan keputusan yang konsisten dengan rencana TI yang telah dijelaskan di PO1	Tidak adanya model arsitektur informasi mengakibatkan tidak memadainya ketersediaan informasi; data yang ada tidak konsisten dengan pengembangan aplikasi; akumulasi data yang tidak relevan, konsisten atau dapat digunakan secara ekonomis	Memperhatikan apakah model arsitektur informasi yang ada telah memadai dan konsisten atau tidak dengan rencana TI jangka panjang	
Enterprise Data Dictionary and Data Syntax Rules			
Manajemen TI harus membuat dan memperbarui kamus data yang memuat elemen data dalam aplikasi, dan aturan sintaks data yang dimiliki organisasi	Tidak adanya kamus data dan aturan sintaks data serta tidak diperbaruinya kamus data akan menyulitkan berbagai pihak yang terlibat dalam menjalankan tugasnya	Memeriksa apakah terdapat kamus data dan aturan sintaks data dan apakah memadai atau tidak	
Data Classification Scheme			
Membangun suatu skema pengelompokkan data berdasarkan prioritas kepentingan dan sensitifitas	Tidak adanya perlindungan terhadap data dari pihak-pihak yang tidak seharusnya	Memeriksa apakah terdapat skema pengelompokkan data dan menilai	

data (apakah data bersifat publik, rahasia atau sangat rahasia) dan menjelaskan secara rinci mengenai kepemilikan data, definisi tingkat keamanan data, perlindungan data dan penjelasan mengenai penyimpanan data dan pemusnahan data, seberapa penting dan sensitifnya suatu data	mengetahui, sehingga kerahasiaan, integritas dan ketersediaan data tidak terjamin	apakah memadai atau tidak	
Integrity Management			
Menentukan dan mengimplementasikan prosedur untuk menjamin integritas dan konsistensi semua data yang disimpan dalam bentuk elektronis seperti database, *data warehouses* dan *data archives*	Data tidak terjamin integritas dan kehandalannya	Memeriksa apakah terdapat prosedur dan tingkat keamanan yang menjamin integritas dan konsistensi data dan menilai apakah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**PO 1 - Plan and Organized**	Tanggal	:	
	Determine Technological Direction (PO3)	Diperiksa oleh	:	**PO3**
		Tanggal	:	

Tujuan:

Memastikan adanya rencana infrastruktur teknologi dan bagian khusus yang menangani arsitektur TI agar teknologi dapat memberikan produk, layanan dan mekanisme *delivery* sesuai kebutuhan organisasi. Rencana infrastruktur teknologi ini meliputi arsitektur sistem, arah teknologi, rencana akuisisi, standar, strategi migrasi, tindakan apa yang perlu dilakukan dalam menghadapi perubahan lingkungan, perubahan skala ekonomi, platform dan aplikasi dan rencana jika terjadi hal-hal di luar dugaan, rencana ini harus diperbarui secara reguler.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Technological Direction Planning			
Manajemen TI harus melakukan analisis teknologi yang telah ada dan sedang dikembangkan, untuk kemudian merencanakan arah teknologi mana yang tepat untuk mewujudkan strategi TI dan arsitektur sistem yang mampu mendukung seluruh proses bisnis organisasi	Tidak adanya perencanaan arah teknologi, akan mengakibatkan akuisisi teknologi tidak konsisten dengan rencana stratejik TI dan tidak sesuai dengan kebutuhan organisasi yang mengakibatkan meningkatnya biaya TI	Memeriksa apakah terdapat rencana untuk menentukan arah teknologi agar mampu mendukung kebutuhan organisasi, dan apakah efektif atau tidak	
Technology Infrastructure Plan			
Manajemen TI membuat dan menjaga rencana infrastruktur teknologi agar tetap sesuai dengan strategi TI dan rencana taktis TI, dan arah perkembangan teknologi dimana didalamnya sudah terdapat cara penanganan jika terjadi hal-hal diluar dugaan, terdapat cara akuisisi sumber daya teknologi, dan mempertimbangkan: terjadinya perubahan akibat dari lingkungan yang bersifat kompetitif, skala ekonomi dari sistem informasi, investasi, perbaikan platform dan aplikasi	Tidak adanya perencanaan terhadap infrastruktur teknologi mengakibatkan implementasi sistem tidak konsisten dan mengakibatkan terjadinya banyak penyimpangan, meningkatnya biaya akibat tidak terstrukturnya rencana akuisisi, dan teknologi yang ada tidak digunakan semaksimal mungkin	Memeriksa apakah manajemen TI membuat rencana infrastruktur teknologi	

Monitor Future Trends and Regulations			
Manajemen TI membangun suatu proses untuk memonitor trend teknologi yang sedang berkembang, infrastruktur, lingkungan hukum dan peraturan, agar infrastruktur teknologi TI yang ada telah memperhitungkan semua hal tersebut	Tidak adanya monitoring terhadap peraturan yang berlaku, akan mengakibatkan ketidakpatuhan dengan peraturan yang ada dan tidak adanya monitor terhadap trend teknologi yang sedang berkembang akan menimbulkan isu teknis atau pemeliharaan terkait dengan infrastruktur TI	Memeriksa dan memastikan apakah manajemen TI melakukan monitor terhadap perkembangan teknologi yang ada beserta peraturannya	
Technology Standards			
Memastikan bahwa manajemen TI membuat suatu standar teknologi yang dituangkan dalam *technology guidelines*, serta mengukur kepatuhan terhadap *guidelines* dan standar tersebut agar dapat memberikan solusi teknologi yang konsisten, efektif dan aman	Tidak adanya standar teknologi dapat mengakibatkan ketidaksesuaian antara *platform* teknologi dan aplikasi, pelanggaran lisensi, serta meningkatnya biaya pemeliharaan teknologi	Memeriksa apakah terdapat suatu standar teknologi, dan menilai apakah efektif atau tidak	
Architecture Board			
Terdapat suatu bagian yang menangani arsitektur TI, agar dapat menyusun suatu *architecture guidelines* dan memberikan arahan terhadap suatu aplikasi dan juga seluruh arsitektur TI agar tetap mematuhi peraturan yang berlaku	Tidak adanya bagian yang khusus menangani arsitektur TI akan mengakibatkan tidak terkendali dan terawasinya proses akuisisi, dan penjagaan terhadap aset sistem informasi	Memeriksa apakah terdapat bagian yang menangani arsitektur TI dan nilai apakah berjalan efektif atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**PO - Plan and Organized**	Tanggal	:	
	Define The IT Processes, Organisation and Relationships (PO4)	Diperiksa oleh	:	**PO4**
		Tanggal	:	

Tujuan:

Suatu organisasi TI harus memiliki staf dengan kualifikasi dan kemampuan memadai, selain itu memiliki fungsi, tanggung jawab, otoritas, tugas dan melakukan pengawasan terhadap TI. Seluruh pihak dalam organisasi tersebut harus terlibat dalam melakukan pengawasan TI, agar proses TI berlangsung transparan dan berada dalam kendali. Untuk menjamin bahwa terdapat dukungan terhadap kepentingan organisasi, TI harus dilibatkan dalam semua proses pengambilan keputusan yang relevan

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Process Framework			
Memastikan adanya suatu kerangka proses TI untuk melaksanakan rencana strategi TI, yang memuat struktur dan hubungan antar proses TI, kepemilikan, *maturity*, ukuran kinerja, perbaikan, kepatuhan, target kualitas dan rencana untuk meraih itu semua	Tidak adanya kerangka proses TI yang jelas dapat mengakibatkan konflik di antara masing-masing proses TI, dan mengakibatkan terjadinya duplikasi proses	Memeriksa apakah terdapat suatu kerangka proses TI dan apakah berjalan efektif atau tidak	
IT Strategy Committee			
Memastikan adanya suatu komite strategi TI. Komite ini harus memastikan bahwa tata kelola TI merupakan bagian dari tata kelola organisasi yang harus diterapkan, dan memberikan arahan bagi TI di dalam organisasi	Jika tidak ada komite strategi TI maka semua risiko atau nilai lebih TI tidak dapat diketahui oleh para pimpinan	Memeriksa apakah terdapat komite strategi TI yang memadai	
IT Steering Committee			
Memastikan adanya komite pengawas TI atau semacamnya untuk menentukan area mana yang perlu mendapat prioritas investasi serta yang akan memonitor dan memperbaiki layanan TI	Tidak adanya komite pengawas TI mengakibatkan strategi TI tidak mampu sejalan dengan strategi organisasi, dan seluruh investasi TI tidak mendukung tujuan organisasi	Memeriksa apakah terdapat komite pengawas TI atau semacamnya dan apakah telah memadai atau tidak	
Organisational Placement of the IT Function			
Memastikan bahwa dalam struktur organisasi, TI	Tidak ditempatkannya TI dalam suatu struktur	Memeriksa apakah TI menjadi bagian dari	

memegang peran dan fungsi yang sangat penting bagi operasional organisasi untuk mendukung strategi organisasi	organisasi menyebabkan tidak adanya komitmen dari manajemen terhadap TI, sehingga TI tidak akan mendukung seluruh proses organisasi secara efektif	struktur organisasi	
IT Organisational Structure			
Memastikan adanya suatu struktur organisasi TI eksternal dan internal yang menggambarkan kebutuhan organisasi, dan memastikan adanya review terhadap struktur organisasi TI secara periodik untuk menyesuaikan kebutuhan staf TI dan sumber daya TI agar sesuai dengan tujuan organisasi	Tidak adanya struktur organisasi TI yang menggambarkan kebutuhan organisasi mengakibatkan tidak teridentifikasinya kebutuhan staf dan tidak tepatnya strategi perekrutam personil TI	Memeriksa apakah terdapat suatu struktur organisasi TI yang memadai	
Establishment of Roles and Responsibilities			
Manajemen TI membangun dan mengkomunikasikan definisi peran dan tanggung jawab personel TI dan *end user* yang menggambarkan personil TI, otoritas *end user*, tanggung jawab dan akuntabilitas agar dapat memenuhi kebutuhan organisasi	Tidak adanya pendefinisian peran dan tanggung jawab personil TI yang jelas memungkinkan personil TI untuk menyalahgunakan sistem	Memeriksa apakah manajemen TI telah mendefinisikan peran dan tanggungjawab personil TI	
Responsibility for IT Quality Assurance			
Memastikan bahwa manajemen TI melakukan *assurance* untuk menilai kinerja TI (*IT Quality Assurance*)	Tidak adanya *IT Quality Assurance* mengakibatkan tidak dapat diketahuinya risiko yang berdampak bagi proses bisnis organisasi yang berakibat memburuknya reputasi dan kinerja organisasi	Memeriksa apakah dilakukan *IT Quality Assurance*, dan menilai apakah memadai atau tidak	
Responsibility for Risk, Security and Compliance			
Manajemen TI harus menentukan siapa yang bertanggung jawab untuk mengendalikan risiko TI yang meliputi keamanan informasi, keamanan fisik dan kepatuhan, dan membangun suatu pengelolaan keamanan	Tidak ditentukannya pihak yang bertanggung jawab terhadap risiko, keamanan dan kepatuhan mengakibatkan tidak terlindungnya aset	Memeriksa apakah terdapat proses penentuan siapa yang bertanggung jawab terhadap risiko, keamanan dan kepatuhan dan apakah efektif atau	

yang bertanggung jawab terhadap isu-isu yang terjadi di dalam organisasi	informasi yang mengakibatkan kehilangan informasi yang sifatnya rahasia	tidak	
Data and System Ownership			
Memastikan bahwa terdapat prosedur dan *tools* yang mendeskripsikan tanggung jawab terhadap data dan sistem informasi.	Tidak adanya prosedur dan *tools* yang mendeskripsikan tanggung jawab terhadap data dan sistem informasi mengakibatkan tidak dilindunginya aset informasi agar tetap sejalan dengan kebutuhan organisasi	Memeriksa apakah terdapat prosedur dan *tools* yang demikian dan apakah memadai atau tidak	
Supervision			
Memastikan dilakukannya pengawasan memadai terhadap fungsi TI dengan tujuan: memastikan bahwa peran dan tanggung jawab yang dibebankan padanya dilaksanakan dengan baik, memastikan apakah seluruh personil TI memiliki otoritas dan sumber daya untuk menjalankan tugasnya, dan mereview kinerja organisasi	Tidak dilakukannya pengawasan mengakibatkan tidak teridentifikasi dan tidak dapat diatasinya isu kinerja TI dan TI tidak dapat berfungsi dengan baik	Mengamati apakah telah dilakukan pengawasan terhadap fungsi dan kinerja TI, dan apakah memadai atau tidak	
Segregation of Duties			
Memastikan adanya pembagian dan pemisahan tugas dan tanggung jawab untuk menghindari satu orang memiliki beberapa tugas penting. Pastikan bahwa seesorang hanya memiliki otoritas menjalankan kewajiban sesuai dengan tugas dan posisinya	Tidak adanya pemisahan tugas mengakibatkan satu individu dapat menjalankan beberapa tugas yang penting yang dapat menimbulkan kerugian dan kecurangan	Mengamati apakah terdapat pembagian dan pemisahan tugas dan tanggung jawab	
IT Staffing			
Manajemen TI mengevaluasi kebutuhan staf berdasarkan proses bisnis yang dimiliki organisasi, operasional organisasi atau lingkungan TI untuk memastikan bahwa TI berfungsi sebagaimana mestinya dan telah memiliki sumber daya yang memadai yang mampu mendukung organisasi dalam mencapai	Tidak adanya evaluasi terhadap kebutuhan staf mengakibatkan sumber daya yang ada tidak sesuai bagi departemen TI dan sumber daya yang ada tidak memiliki keahlian sesuai kebutuhan organisasi	Memeriksa apakah manajemen TI melakukan evaluasi kebutuhan staf	

tujuannya			
Key IT Personnel			
Manajemen TI menetapkan personil TI yang utama dan menetapkan personil pengganti atau cadangan sehingga dalam menjalankan tugas yang sangat penting tidak tergantung pada satu orang	Ketergantungan yang tinggi pada satu individu dan tidak memadainya proses *sharing* pengetahuan	Memeriksa apakah manajemen TI telah menetapkan personil TI utaman dan cadangan	
Contracted Staff Policies and Procedures			
Manajemen TI harus memastikan bahwa konsultan dan personil TI yang dikontrak mengetahui dan mematuhi kebijakan organisasi agar ikut melindungi aset informasi organisasi seperti yang telah disepakati pada perjanjian	Meningkatnya ketergantungan pada personil kontrak; tidak adanya transfer ilmu pengetahuan dari personil kontrak; personil kontrak tidak mematuhi kebijakan organisasi sehingga mereka tidak ikut melindungi aset informasi yang dimiliki organisasi	Memeriksa apakah organisasi menciptakan suatu prosedur dan kebijakan bagi personil kontrak	
Relationship			
Memastikan adanya suatu komunikasi, pendefinisian struktur hubungan antara fungsi TI dan beragam kepentingan di dalam maupun di luar fungsi TI seperti hubungan dengan pimpinan, unit yang terkait dengan proses bisnis organisasi, pengguna, *supplier*, *security officer*, *risk manager*, dan *outsourcers*	Tidak adanya komunikasi dan struktur hubungan yang jelas antara fungsi TI dan beragam kepentingan akan mengakibatkan tidak adanya kesesuaian antara tujuan organisasi, kebijakan, petunjuk dan metodologi TI	Memeriksa apaah terdapat komunikasi dan struktur hubungan yang demikian dan apakah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	PO 1 - Plan and Organized	Tanggal	:	
	Management the IT Investment (PO5)	Diperiksa oleh	:	PO5
		Tanggal	:	

Tujuan:

Memastikan adanya suatu kerangka proses untuk mengendalikan investasi TI yang dilakukan, dengan memperhatikan biaya, manfaat yang diperoleh, prioritas alokasi anggaran, proses penganggaran yang formal agar penggumaan sumber daya TI berjalan efektif dan efisien, serta memberikan suatu transparansi dan akuntabilitas dalam mengemukakan total biaya, manfaat dan *return* yang diperoleh dari investasi yang dilakukan

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref
Financial Management Framework			
Memastikan adanya suatu kerangka pengelolaan keuangan yang memadai berupa portfolio investasi TI dan anggaran TI, untuk mengendalikan investasi dan biaya yang ditimbulkan oleh aset	Tidak adanya kerangka pengelolaan keuangan menyebabkan lemahnya pengawasan terhadap anggaran TI, tidak didefinisikan dengan jelas proyek TI mana yang diprioritaskan untuk dibiayai, tidak efisiennya proses pengelolaan keuangan, serta anggaran TI yang ada tidak mencerminkan kebutuhan organisasi yang sesungguhnya	Memeriksa apakah terdapat kerangka pengelolaan keuangan yang memadai	
Prioritisation Within IT Budget			
Manajemen TI dalam mengambil keputusan untuk melakukan investasi TI terlebih dahulu menentukan prioritas area TI mana yang perlu dilakukan pengembangan dan pemeliharaan agar dapat meningkatkan/mengoptimalkan kontribusi TI untuk mendukung proses bisnis organisasi	Jika tidak dilakukan prioritas, maka alokasi TI menjadi tidak efisien	Memperhatikan apakah dibuat prioritas terlebih dahulu dalam menentukan anggaran TI	
IT Budgeting			
Manajemen TI telah	Tidak tepatnya	Memperhatikan	

implementasikan suatu praktek penganggaran yang menggambarkan prioritas investasi TI yang harus dilakukan dan mencakup biaya operasional dan pemeliharaan infrastruktur saat ini	pengalokasian anggaran operasional TI	apakah terdapat pengalokasian anggaran TI yang memadai	
Cost Management			
Manajemen TI mengimplementasikan suatu proses pengelolaan biaya yang akan membandingkan biaya sebenarnya dengan anggaran yang dialokasikan, dan semua biaya yang dikeluarkan harus dimonitor dan dilaporkan, mengidentifikasi semua penyimpangan yang terjadi, menilai dampak penyimpangan tersebut, dan menindaklanjuti penyimpangan itu	Tidak adanya proses pengelolaan biaya mengakibatkan tidak tepatnya biaya yang dikeluarkan untuk investasi TI, karena tidak sebanding dengan manfaat yang diperoleh	Memperhatikan apakah terdapat proses pengelolaan biaya yang memadai	
Benefit Management			
Manajemen TI mengimplementasikan suatu proses untuk memonitor manfaat yang ditimbulkan oleh TI (*benefit management*). Kontribusi TI terhadap organisasi harus diidentifikasi, didokumentasikan, dimonitor, dan dilaporkan. Semua laporan direview, dan ketika terdapat peluang untuk memperbaiki TI, harus segera diambil tindakan yang tepat.	Tidak adanya *benefit management* dari TI mengakibatkan tidak transparannya penyampaian nilai TI dan timbulnya persepsi yang salah mengenai TI	Memperhatikan apakah terdapat *benefit management* dari TI dan apakah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	PO 1 - Plan and Organized	Tanggal	:	PO6
	Communicate Management Aims and Direction (PO6)	Diperiksa oleh	:	
		Tanggal	:	

Tujuan:

Manajemen TI membangun suatu kerangka dan kebijakan pengendalian TI yang melibatkan seluruh manajemen organisasi, agar mereka peduli dan memahami seluruh risiko TI, tujuan dan arah perkembangan TI

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
IT Policy and Control Environment			
Tentukan elemen pengendalian TI yang harus sejalan dengan filosofi dan operasional organisasi, dan mempertimbangkan nilai yang ingin dicapai dari investasi TI, dugaan risiko, *integrity*, nilai etika, kompetensi staf, akuntabilitas dan tanggung jawab	Tidak transparannya pengendalian TI sehingga menimbulkan isu-isu keamanan	Memeriksa apakah terdapat kebijakan dan lingkungan pengendalian TI yang memadai	
Enterprise IT Risk and Control Framework			
Manajemen TI membangun suatu kerangka yang mendefinisikan risiko TI yang mungkin dihadapi oleh organisasi dan pengendalian yang sejalan dengan kebijakan TI	Tidak adanya kerangka pengendalian risiko TI dapat mengakibatkan terungkapnya informasi penting/sensitif ke pihak luar organisasi	Memperhatikan apakah ada kerangka pengendalian risiko TI dan menilai apakah memadai atau tidak	
IT Policies Management			
Bagian TI membuat berbagai kebijakan yang mencakup maksud dan tujuan; tugas dan tanggung jawab; *exception process*; *compliance approach*; prosedur, standar dan *guideline* untuk mendukung strategi TI, dan disetujui oleh para pimpinan di DJA	Tidak adanya kebijakan TI dapat mengakibatkan kesalahpahaman mengenai maksud dan arah TI di organisasi tersebut	Memperhatikan bahwa terdapat kebijakan TI dan menilai apakah telah memadai atau tidak	
Policy, Standard and Procedures Rollout			
Memastikan bahwa bagian TI membuat suatu kebijakan, standar dan prosedur TI yang	Kebijakan, standar dan prosedur TI tidak diketahui, tidak	Memeriksa apakah terdapat kebijakan, standar dan prosedur	

sama bagi seluruh staf yang relevan, dan menjadi bagian dari operasional DJA	dipahami dan tidak dapat diterima oleh seluruh personil di DJA	TI dan menilai apakah telah memadai atau tidak	
Communication of IT Objectives and Direction			
Mengkomunikasikan kepedulian dan pemahaman tujuan dan arah perkembangan TI bagi seluruh *stakeholder* dan pengguna	Tidak adanya komunikasi mengenai tujuan dan arah perkembangan TI mengakibatkan tidak dapat dicapainya tujuan TI	Memperhatikan apakah terdapat komunikasi mengenai tujuan dan arah perkembangan TI	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	PO 1 - Plan and Organized	Tanggal	:	
	Manage IT Human Resources (PO7)	Diperiksa oleh	:	PO7
		Tanggal	:	

Tujuan:

Tenaga kerja yang kompeten sangatlah dibutuhkan demi menjaga agar layanan TI dapat diberikan tepat waktu. Tenaga kerja yang kompeten dapat diperoleh melalui proses perekrutan yang tepat, pelatihan, evaluasi kinerja pegawai, dan promosi pegawai. Proses ini penting karena manusia merupakan aset yang penting dan tata kelola organisasi serta lingkungan pengendalian internal sangat tergantung dari motivasi dan kompetensi pegawainya

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Personnel Recruitment and Retention			
Memastikan bahwa proses rekruitmen personil/pegawai TI sejalan dengan kebijakan dan prosedur perekrutan pegawai di PT Bank XYZ, dan terdapat suatu proses untuk memastikan bahwa PT Bank XYZ memiliki tenaga kerja TI dengan kemampuan yang memadai	Tidak adanya proses rekruitmen yang benar mengakibatkan pegawai yang direkrut tidak memiliki keahlian yang dibutuhkan	Menilai apakah proses rekruitmen pegawai TI telah memadai atau tidak	
Personnel Competencies			
Pegawai TI diverifikasi secara reguler untuk memastikan apakah pegawai tersebut memiliki kompetensi dalam melakukan tugas dan tanggung jawabnya dengan melihat pendidikan yang dimiliki, pelatihan yang pernah diikuti dan atau pengalaman yang dimiliki	Tidak direviewnya pegawai TI secara reguler mengakibatkan keahlian yang dimiliki pegawai TI tidak sesuai dengan kebutuhan PT Bank XYZ dan dapat menimbulkan ketidakpuasan pegawai TI terhadap kemajuan karirnya	Memperhatikan apakah terdapat penilaian terhadap kompetensi pegawai TI, secara reguler	
Staffing of Roles			
Mendefinisikan, memonitor dan mengawasi peran, kerangka tanggung jawab dan kompensasi bagi pegawai, dengan berpedoman pada kebijakan dan prosedur, *code of ethics* dan *professional practices*	Tidak adanya pengawasan terhadap peran, tanggung jawab dan kerangka kompensasi bagi pegawai akan mengakibatkan terjadinya kesalahan	Menilai apakah terdapat monitoring dan pengawasan terhadap peran, tanggung jawab dan kompensasi pegawai, dan apakah memadai	

	dan insiden serta ketidakpuasan dari pegawai	atau tidak	
Personnel Training			
Bagian TI mengadakan program pelatihan bagi pegawainya agar pengetahuan, keahlian, dan kemampuannya terjaga, serta peduli terhadap pengendalian internal dan keamanan data	Tidak adanya pelatihan akan mengakibatkan tidak memadainya keahlian, kemampuan dan kepedulian pegawai TI terhadap keamanan data, yang akan menyebabkan terjadinya kesalahan atau insiden	Memperhatikan apakah terdapat pelatihan bagi pegawai TI dan menilai apakah telah memadai atau tidak	
Dependence Upon Individuals			
Meminimalkan ketergantungan terhadap satu individu/pegawai dengan cara mendokumentasikan pengetahuan yang dimiliki, berbagi pengetahuan (*knowledge sharing*) dan perencanaan penggantian pegawai (*successions planning*) dan menyiapkan pegawai cadangan (*staff backup*)	Meningkatnya jumlah kesalahan akibat pegawai tidak memiliki keahlian yang memadai, ketidakpuasan pegawai akibat tidak adanya program penggantian pegawai dan peluang kerja yang baik	Memperhatikan apakah terdapat pendokumentasian pengetahuan yang dimiliki, perencanaan penggantian pegawai dan pegawai cadangan, dan nilailah apakah memadai atau tidak	
Personnel Clearance Procedures			
Memastikan adanya *personnel clearance procedures* yang meliputi *background check* pada proses rekruitmen pegawai TI, dan berlaku juga pada proses pemilihan kontraktor dan *vendor*	Tidak adanya *personnel clearance procedures* mengakibatkan meningkatnya risiko dan ancaman	Memperhatikan apakah terdapat *personnel clearance procedures* dan menilai apakah memadai atau tidak	
Employee Job Performance Evaluation			
Memastikan adanya proses evaluasi secara tepat waktu terhadap kinerja pegawai apakah mereka telah bekerja sesuai standar dan tanggung jawab yang dibebankan padanya	Tidak dilakukannya proses evaluasi terhadap kinerja pegawai mengakibatkan tidak diketahuinya penyebab ketidakefisienan operasi TI yang disebabkan oleh faktor SDM	Memperhatikan apakah terdapat proses evaluasi terhadap kinerja pegawai	
Job Change and Termination			
Bagian TI melakukan beberapa tindakan yang bijaksana terkait dengan perubahan kerja khususnya	Tidak adanya pengaturan terhadap hak akses, mengakibatkan	Memperhatikan apakah terdapat prosedur atau kebijakan yang	

penghentian kerja, misalnya transfer pengetahuan, penugasan ulang tanggung jawab dan mengatur hak akses agar dapat meminimalkan risiko dan menjaga kelangsungan fungsi TI	pegawai yang sudah berhenti tetap dapat mengakses sistem dan dapat mengganggu kelangsungan fungsi TI yang penting	mendorong bagian TI untuk melakukan hal tersebut, dan apakah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**PO 1 - Plan and Organized**	Tanggal	:	
	Manage Quality (PO8)	Diperiksa oleh	:	**PO4**
		Tanggal	:	

Tujuan:

Terdapat suatu Quality Management System (QMS) yang merupakan suatu prosedur dan kebijakan mengenai syarat kualitas suatu sistem berdasarkan beberapa indikator. Penanganan kualitas ini sangat penting untuk menjamin bahwa TI memberikan nilai lebih bagi bisnis, dan memberikan perbaikan yang kontinyu dan transparan bagi *stakeholder*

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Quality Management System (QMS)			
Memastikan adanya suatu QMS yang mengidentifikasi syarat kualitas sistem berdasarkan kriteria tertentu; proses TI yang penting; kebijakan, kriteria dan metode untuk mendefinisikan, mendeteksi, mengkoreksi dan mencegah terjadinya pelanggaran, serta mendefinisikan struktur organisasi untuk menilai kualitas manajemen, yang mencakup tugas, peran dan tanggung jawab	Tidak adanya QMS mengakibatkan kualitas layanan dan solusi yang diberikan tidak memadai yang menimbulkan terjadinya kesalahan, pengerjaan ulang sehingga akan meningkatkan biaya	Memperhatikan apakah terdapat QMS, dan menilai apakah telah memadai atau tidak	
IT Standards and Quality Practices			
Bagian TI membuat standar, prosedur dan praktek proses TI yang utama berdasarkan kualitas tertentu sebagai tuntunan bagi organisasi dalam mencapai tujuannya	Proses TI tidak memiliki kualitas dengan standar dan prosedur yang telah ditentukan	Memperhatikan apakah terdapat standar kualitas TI yang memadai	
Development and Acquisition Standards			
Bagian TI membuat standar pembangunan/pengembangan dan akuisisi sistem/perangkat lunak/ perangkat keras, dengan mempertimbangkan standar pengkodean dalam pembangunan perangkat lunak; penamaan; format file; standar perancangan skema	Tidak adanya standar pengembangan dan akuisisi menimbulkan kesalahan dalam pengembangan dan implementasi yang mengakibatkan penundaan/delay, pengerjaan ulang dan	Memperhatikan apakah terdapat standar pengembangan dan akuisisi sistem, dan apakah memadai atau tidak	

dan kamus data; standar antar muka bagi pengguna; *interoperability* (kemampuan dua sistem atau lebih untuk bekerja sama secara harmonis), efisiensi kinerja sistem, *scalability* (kemampuan suatu sistem untuk dikembangkan/diperluas), standar pengembangan dan pengujian sistem, validasi apakah telah sesuai kebutuhan, rencana pengujian, pengujian apakah terjadi penyimpangan (*regression and integration testing*)	meningkatkan biaya; permasalahan dalam hal *interoperability* dan *integration system*; dan, permasalahan dalam hal dukungan dan pemeliharaan sistem;		
Customer Focus			
Bagian TI memperhatikan kebutuhan pengguna dengan memberikan layanan yang terbaik yang sesuai dengan standar dan praktek TI yang diterapkan di PT Bank XYZ	Bagian TI tidak memahami kebutuhan pengguna sehingga tidak mampu memberikan respon dan umpan balik yang memadai	Menilai apakah bagian TI memperhatikan kebutuhan pengguna atau tidak	
Continuous Improvement			
Bagian TI melakukan perbaikan sistem secara kontinyu	Tidak dilakukannya perbaikan secara kontinyu mengakibatkan *service delivery* tidak terkendali dan tidak efektif, kesalahan dalam pengembangan sistem dan kegagalan layanan TI	Menilai apakah dilakukan perbaikan sistem secara kontinyu, dan apakah memadai atau tidak	
Quality Measurement, Monitoring and Review			
Mengimplementasikan suatu pengukuran, monitoring dan review kualitas sistem untuk menilai kepatuhan pada QMS dan mengambil tindakan korektif serta pencegahan	Tidak dilakukannya pengukuran, monitoring dan review terhadap kualitas sistem mengakibatkan laporan kualitas sistem menjadi tidak memadai	Memperhatikan apakah terdapat pengukuran, monitoring dan review kualitas yang memadai	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	PO 1 - Plan and Organized	Tanggal	:	
	Assess and Manage IT Risks (PO9)	Diperiksa oleh	:	PO9
		Tanggal	:	

Tujuan:

Setiap dampak yang berpengaruh bagi tujuan organisasi disebabkan oleh kejadian tidak terencana yang berhasil diidentifikasi, dianalisis dan dinilai, untuk itu perlu dibuat suatu kerangka manajemen risiko yang mendokumentasikan level risiko TI, strategi pengurangan risiko dan *residual risk*. Strategi pengurangan risiko diadopsi untuk meminimalkan *residual risk*.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
IT Risk Management Framework			
Bagian TI membangun suatu kerangka manajemen risiko TI yang sejalan dengan kerangka manajemen risiko organisasi	Tidak adanya kerangka manajemen risiko TI mengakibatkan berbagai dampak risiko TI tidak dapat dideteksi	Memperhatikan apakah terdapat kerangka manajemen risiko TI yang memadai	
Establishment of Risk Context			
Memastikan adanya suatu keadaan (*context*) yang menerapkan kerangka penilaian risiko yang mencakup risiko internal maupun eksternal, tujuan penilaian dan kriteria penilaian risiko	Tidak adanya penilaian risiko yang tepat	Menilai apakah terdapat penilaian risiko internal maupun eksternal, dan menilai apakah memadai atau tidak	
Event Identification			
Melakukan identifikasi kejadian dengan dampak negatif yang potensial terjadi yang mempengaruhi tujuan atau operasional PT Bank XYZ	Kejadian penting yang menimbulkan risiko tidak dapat diidentifikasi	Memperhatikan apakah terdapat identifikasi kejadian yang berdampak negatif, dan apakah efektif atau tidak	
Risk Assessment			
Memastikan adanya penilaian dampak risiko dengan menggunakan metode kualitatif dan kuantitatif	Tidak adanya penilaian risiko menyebabkan tidak teridentifikasinya risiko yang cukup signifikan mempengaruhi proses TI	Memperhatikan apakah terdapat penilaian terhadap risiko, dan apakah memadai atau tidak	
Risk Response			
Memastikan adanya suatu prosedur/proses untuk memberikan respon terhadap	Tidak efektifnya penggunaan sumber daya dalam merespon	Memperhatikan apakah terdapat prosedur/proses	

risiko dengan cara menghindari, mengurangi, atau menerima dengan batas toleransi pada tingkat tertentu	risiko yang ada	untuk merespon risiko yang ada, dan apakah memadai atau tidak	
Maintenance and Monitoring of a Risk Action Plan			
Memastikan adanya perencanaan untuk memelihara dan memonitor seluruh aktifitas pengendalian/penanganan risiko dan melaporkan semua penyimpangan yang terjadi ke pimpinan	Pengendalian risiko tidak berjalan sebagaimana mestinya	Memperhatikan apakah terdapat rencana untuk memelihara dan memonitor aktifitas pengendalian risiko dan menilai apakah telah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	PO 1 - Plan and Organized	Tanggal	:	
	Manage Projects (PO10)	Diperiksa oleh	:	PO10
		Tanggal	:	

Tujuan:

Membangun suatu kerangka manajemen proyek untuk mengelola seluruh proyek TI, yang meliputi *master plan*, alokasi sumber daya, *Quality Assurance* (QA), rencana pengujian formal dan pengujian serta *post-implementation review* setelah installasi proyek selesai

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref
Programme Management Framework			
Memastikan adanya kerangka pengelolaan/manajemen program dari suatu proyek TI, yang meliputi identifikasi, pendefinisian, evaluasi, prioritasi, pemilihan, inisiasi, penanganan dan pengendalian/pengawasan proyek, agar mampu mencapai sasaran yang diharapkan dan memecahkan konflik yang ada	Tidak adanya kerangka manajemen program suatu proyek, mengakibatkan tidak tepatnya penentuan prioritas proyek dan tidak teratur dan efektifnya pendekatan program proyek	Memperhatikan apakah terdapat kerangka manajemen program, dan apakah memadai atau tidak	
Project Management Framework			
Memastikan adanya kerangka manajemen proyek yang mendefinisikan lingkup dan cakupan proyek yang terintegrasi dengan proses manajemen program	Tidak adanya penanganan proyek yang memadai	Memperhatikan apakah terdapat kerangka manajemen proyek dan apakah memadai atau tidak	
Project Management Approach			
Adanya suatu pendekatan manajemen proyek dengan ukuran, kompleksitas dan kebutuhan peraturan untuk masing-masing proyek. Struktur tata kelola proyek mencakup peran dan tanggung jawab dari *programme sponsor, project sponsors, steering committee, project office* dan *project manager* dan mekanisme agar tanggung jawab dapat	Tidak adanya pendekatan manajemen proyek mengakibatkan gagalnya merespon isu proyek secara optimal	Memperhatikan adanya pendekatan manajemen proyek yang memadai	

terlaksana dengan baik			
Stakeholder Commitment			
Memastikan adanya suatu komitmen dan partisipasi dari *stakeholder* dalam melakukan pendefinisian dan pelaksanaan proyek	Tidak adanya komitmen dan partisipasi dari *stakeholder*, mengakibatkan proyek yang dijalankan tidak menggambarkan kebutuhan yang sesungguhnya	Memperhatikan apakah terdapat komitmen dan partisipasi dari *stakeholder*	
Project Scope Statement			
Memastikan bahwa terdapat pendefinisian dan pendokumentasian lingkup proyek agar dapat dipahami oleh *stakeholder* dan dapat dilihat bagaimana kaitannya dengan proyek lain di dalam keseluruhan program investasi TI	Pemahaman yang salah tentang tujuan proyek sehingga tidak dapat memenuhi kebutuhan organisasi (PT Bank XYZ)	Memperhatikan apakah terdapat pendefinisian dan pendokumentasian lingkup proyek	
Project Phase Initiation			
Terdapat proses untuk menyetujui setiap tahapan proyek. Proses bisa bergerak ke tahap selanjutnya jika tahapan sebelumnya telah direview dan diterima	Tidak terdeteksinya penyimpangan yang terjadi	Menilai apakah terdapat prosedur yang demikian untuk setiap tahapan proyek	
Integrated Project Plan			
Memastikan adanya suatu rencana proyek yang terintegrasi dan telah disetujui sebagai tuntunan dalam menjalankan proyek dan mengawasi siklus tahapan proyek tersebut. Segala aktivitas dalam proyek harus didokumentasikan	Kesalahan yang tidak terdeteksi pada waktu proses perencanaan dan penganggaran proyek Proyek yang ada tidak sejalan dengan tujuan organisasi Tidak terdeteksinya penyimpangan dari rencana proyek	Memperhatikan apakah terdapat rencana proyek yang terintegrasi	
Project Resources			
Memastikan adanya pendefinisian tanggung jawab, hubungan, wewenang dan kriteria kinerja dari anggota tim proyek dan penugasan bagi staf dan kontraktor; terdapat perencanaan untuk pengadaan produk dan layanan bagi setiap proyek agar tujuan	Ketiadaan kemampuan dan sumber daya yang membahayakan proyek-proyek penting; penggunaan sumber daya yang tidak efisien	Memperhatikan apakah terdapat prosedur dan kebijakan yang mendorong dilakukannya pendefinisian tanggung jawab, hubungan, wewenang dan	

proyek dapat tercapai		kriteria kinerja dari anggota tim proyek dan penugasan bagi staf dan kontraktor	
Project Risk Management			
Memastikan adanya manajemen risiko proyek yang akan menghilangkan atau minimalkan risiko melalui proses perencanaan, identifikasi, analisis yang sistematis yang terkait dengan monitoring dan pengendalian area atau event yang berpotensial menyebabkan terjadinya perubahan yang tidak diinginkan	Tidak terdeteksinya risiko proyek, kurangnya tindakan penanganan risiko	Menilai apakah terdapat manajemen risiko proyek, dan apakah memadai atau tidak	
Project Quality Plan			
Memastikan adanya rencana penilaian kualitas proyek (*project quality plan*) yang telah direview dan disetujui oleh semua pihak yang relevan	Tidak adanya *project quality plan* dapat mengakibatkan suatu proyek tidak dapat diselesaikan tepat waktu dan output proyek tidak sesuai dengan kebutuhan organisasi (PT Bank XYZ)	Memperhatikan apakah terdapat *project quality plan* yang memadai	
Project Change Control			
Memastikan adanya suatu sistem pengendalian untuk masing-masing proyek, sehingga seluruh perubahan yang dilakukan meliputi perubahan biaya, jadwal, lingkup dan kualitas, akan direview	Tidak adanya sistem pengendalian untuk masing-masing proyek menyebabkan kurangnya pengawasan/pengendalian terhadap lingkup, biaya dan jadwal proyek	Memperhatikan apakah terdapat prosedur atau kebijakan yang mendorong dibuatnya sistem pengendalian proyek dan menilai apakah telah memadai atau tidak	
Project Planning of Assurance Methods			
Memastikan adanya metode penilaian perencanaan proyek, dengan tujuan untuk memberikan akreditasi terhadap sistem yang baru atau yang telah dimodifikasi, apakah telah memadai dan telah memperhitungkan pengendalian internal dan keamanan sistem	Tidak adanya metode penilaian proyek mengakibatkan tidak adanya akreditasi yang memadai untuk menilai sistem	Memperhatikan apakah terdapat prosedur atau kebijakan yang mendorong dilakukannya penilaian terhadap proyek, dan apakah memadai atau tidak	
Project Performance Measurement, Reporting and Monitoring			
Memastikan adanya prosedur	Tidak adanya prosedur	Memperhatikan	

untuk mengukur kinerja proyek, mengidentifikasi penyimpangan proyek, untuk kemudian dilaporkan dan dimonitoring jalannya proyek tersebut. Pengukuran kinerja proyek dilakukan dengan memperhatikan lingkup kinerja proyek, jadwal, kualitas, biaya dan kriteria risiko.	untuk melaporkan kinerja proyek mengakibatkan tidak efektifnya laporan kemajuan proyek dan tidak teridentifikasinya isu-isu yang terjadi Tidak adanya pengukuran terhadap kinerja proyek mengakibatkan kurangnya pengawasan terhadap kemajuan proyek	apakah terdapat prosedur atau kebijakan yang mendorong dilakukan pengukuran terhadap kinerja proyek untuk kemudian dilaporkan dan selanjutnya terus dimonitoring	
Project Closure			
Di akhir proyek, seluruh stakeholder dari proyek tersebut harus mengungkapkan apakah proyek tersebut memberikan hasil dan manfaat sesuai yang telah direncanakan, dan lakukan identifikasi seluruh kegiatan yang dibutuhkan untuk meraih hasil proyek sesuai rencana dan identifikasi serta dokumentasikan pembelajaran yang berhasil diperoleh untuk proyek dan program di masa mendatang	Kelemahan penanganan proyek tidak berhasil dideteksi, hilangnya peluang pembelajaran untuk proyek di masa mendatang	Memperhatikan apakah terdapat kebijakan atau prosedur yang mendorong dilakukannya pengungkapan proyek (*project closure*) setelah proyek tersebut selesai	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**AI - Acquire And Implement**	Tanggal	:	
	Identify Automated Solutions (AI1)	Diperiksa oleh	:	**AI-1**
		Tanggal	:	

Tujuan:

Memastikan adanya suatu proses identifikasi kebutuhan organisasi, mempertimbangkan sumber daya yang dibutuhkan, review terhadap kelayakan teknologi dan ekonomi, melakukan analisis risiko dan *cost-benefit*, sebelum melakukan akuisisi atau membuat aplikasi baru

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Definition and Maintenance of Business Functional and Technical Requirements			
Memastikan adanya proses identifikasi dan pemeliharaan agar seluruh kebutuhan teknis dan proses bisnis organisasi mampu dipenuhi oleh TI	Melaksanakan solusi yang salah akibat kurangnya pemahaman terhadap kebutuhan teknis organisasi	Melakukan penilaian bahwa terdapat proses yang demikian	
Risk Analysis Report			
Memastikan adanya dokumentasi dan laporan analisis risiko agar mampu merancang solusi yang sesuai dengan kebutuhan organisasi	Tidak teridentifikasinya risiko akuisisi, akibat ketidakpedulian manajemen terhadap risiko dan kegagalan untuk menerapkan pengendalian yang tepat	Melakukan penilaian bahwa terdapat dokumentasi dan laporan analisis risiko, dan apakah efektif atau tidak	
Feasibility Study and Formulation of Alternative Courses of Action			
Memastikan dilakukannya studi kelayakan yang menguji kemungkinan untuk mengimplementasikan suatu tindakan atau solusi	Solusi yang diambil tidak mampu memecahkan permasalahan yang dihadapi organisasi	Melakukan penilaian bahwa telah dilakukan suatu studi kelayakan	
Requirements and Feasibility Decision and Approval			
Memastikan bahwa kebutuhan teknis dan laporan studi kelayakan terhadap solusi yang ingin diambil, telah disetujui oleh pimpinan	Solusi tidak dapat memenuhi kebutuhan organisasi, akibat tidak teridentifikasinya alternatif solusi secara tepat	Melakukan penilaian apakah kebutuhan teknis dan studi kelayakan telah disetujui oleh pimpinan	

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI2
Tanggal		Tanggal :		
Proses :	ACQUIRE AND MAINTAIN APPLICATION SOFTWARE (AI2)			

Tujuan:

Membangun aplikasi sesuai dengan kebutuhan organisasi yang meliputi perancangan aplikasi, pengendalian aplikasi (*application control*) dan syarat keamanan sistem (*security requirements*) serta pengembangan dan konfigurasi sistem yang sejalan dengan standar, sehingga proses bisnis organisasi didukung oleh aplikasi yang terotomasi

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
High-level Design			
1. Memastikan bahwa kebutuhan organisasi dituangkan ke dalam suatu spesifikasi rancangan tingkat tinggi (*high level design*) akuisisi perangkat lunak dengan memperhatikan arah perkembangan teknologi dan arsitektur informasi 2. Memastikan bahwa dilakukan penilaian kembali terhadap rancangan tersebut selama proses pengembangan dan pemeliharaan agar tidak terjadi ketidaksesuaian antara teknis dan *logic*	Tidak terciptanya sistem aplikasi yang sesuai dengan spesifikasi rancangan dan tidak adanya kepastian bahwa sistem yang dibangun sesuai dengan kebutuhan organisasi dan pengguna	Memeriksa apakah terdapat prosedur dan kebijakan untuk membuat suatu spesifikasi rancangan (*high level design*) dan penilaian terhadap spesifikasi rancangan tersebut, dan apakah memadai atau tidak	
Detailed Design			
Memastikan adanya rancangan teknis secara mendetil dari aplikasi perangkat lunak yang akan dibuat dan sesuai dengan *high level design*	Tidak terciptanya sistem aplikasi yang sesuai dengan rancangan teknis sehingga data tidak dapat diproses dengan benar dan akan mengakibatkan meningkatnya biaya akibat harus melakukan perancangan ulang	Memeriksa apakah terdapat prosedur dan kebijakan untuk membuat rancangan teknis dan apakah memadai atau tidak	
Application Control and Auditability			
Memastikan adanya suatu pengendalian aplikasi	Integritas data tidak terjamin dan sulit untuk	Memeriksa apakah terdapat pengendalian	

sehingga proses akan akurat, lengkap, tepat waktu, terotorisasi dan dapat diaudit	diaudit	aplikasi yang memadai	
Application Security and Availability			
Memastikan bahwa terdapat keamanan aplikasi (*application security*) dan sejalan dengan klasifikasi data organisasi, arsitektur informasi, arsitektur keamanan informasi untuk menangani risiko yang ada	Mengurangi ketersediaan sistem dan integritas informasi yang diberikan	Memeriksa apakah terdapat prosedur yang demikian, dan apakah memadai atau tidak	
Major Upgrades to Existing Systems			
Memastikan adanya prosedur dan kebijakan yang harus diikuti pada waktu melakukan pengembangan sistem yang baru atau perubahan sistem	Mengurangi ketersediaan sistem, kerahasiaan, integritas dan ketersediaan data	Memeriksa apakah terdapat prosedur dan kebijakan yang demikian dan apakah berjalan efektif atau tidak	
Development of Application Software			
Memastikan bahwa telah dikembangkan suatu prosedur pengembangan aplikasi perangkat lunak dengan memperhatikan spesifikasi rancangan, standar dan dokumentasi pengembangan sistem, *QA requirements* dan standar persetujuan (*approval standards*)	Tidak dapat memelihara aplikasi secara efektif	Memeriksa apakah terdapat prosedur yang demikian dan apakah memadai atau tidak	
Software Quality Assurance			
Memastikan adanya kebijakan dan prosedur yang mengharuskan dilakukannya *assurance* untuk menilai kualitas perangkat lunak apakah telah sesuai dengan kebutuhan organisasi	Kualitas perangkat lunak menjadi buruk, harus melakukan pengujian ulang terhadap perangkat lunak yang tengah dikembangkan, terjadi pelanggaran terhadap syarat kepatuhan yang sudah ditentukan	Memeriksa kebijakan dan prosedur tersebut dan apakah memadai atau tidak	
Applications Requirements Management			
Manajemen TI harus memastikan apakah semua syarat yang harus dipenuhi oleh suatu aplikasi telah dilakukan atau tidak dari mulai perancangan, pengembangan sampai implementasi sistem	Aplikasi yang dibangun tidak sesuai dengan harapan	Memeriksa apakah manajemen melakukan hal tersebut	

Application Software Maintenance			
Memastikan adanya strategi dan rencana pemeliharaan aplikasi perangkat lunak	Terjadi perubahan yang tidak diotorisasi dan *system availability* berkurang	Memeriksa apakah terdapat kebijakan yang mendorong untuk dibuatnya strategi itu dan apakah benar-benar dilaksanakan	

PT Bank XYZ		Disiapkan oleh	:	Program Audit
Proses :	**AI - Acquire And Implement**	Tanggal	:	**AI-3**
	Acquire and Maintain Technology Infrastructure (AI3)	Diperiksa oleh	:	
		Tanggal	:	

Tujuan:

Memastikan adanya rencana akuisisi, pemeliharaan dan perlindungan terhadap infrastruktur teknologi agar dapat mendukung berbagai aplikasi

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Technological Infrastructure Acquisition Plan			
Memastikan adanya suatu rencana akuisisi, implementasi dan pemeliharaan infrastruktur teknologi agar sesuai kebutuhan teknis, fungsional, dan arah teknologi di organisasi tersebut	Apabila rencana dimaksud tidak ada, maka infrastruktur teknologi menjadi tidak konsisten sehingga tidak mampu mendukung proses bisnis organisasi	Melakukan pengamatan apakah terdapat rencana yang demikian, dan apakah efektif atau tidak	
Infrastructure Resource Protection and Availability			
Memastikan adanya pengendalian internal dan keamanan selama proses konfigurasi, integrasi dan pemeliharaan perangkat keras dan infrastruktur perangkat lunak untuk melindungi ketersediaan dan integritas sumber daya (*resources*) TI	Apabila tidak ada perlindungan terhadap sumber daya yang ada akan mengakibatkan terganggunya proses sistem, sehingga tidak mampu mendukung proses bisnis organisasi dan dapat mengakibatkan terjadinya akses yang tidak diotorisasi terhadap perangkat lunak yang sensitif dan kebutuhan	Memeriksa apakah terdapat perlindungan terhadap sumber daya TI dan menilai apakah personil TI mengerti tanggung jawabnya dan apakah terdapat monitoring dan evaluasi untuk menilai keefektifannya	
Infrastructure Maintenance			
Memastikan adanya kebijakan dan prosedur untuk memelihara infrastruktur, dan memastikan bahwa perubahan yang terjadi tetap dijaga agar tidak menyimpang dari prosedur perubahan yang dimiliki oleh organisasi	Terjadinya akses yang tidak diotorisasi terhadap perangkat lunak yang penting/sensitif dan teknologi tidak mampu mendukung kebutuhan organisasi	Melakukan penilaian apakah terdapat kebijakan dan prosedur yang demikian dan apakah memadai atau tidak	

Feasibility Test Environment			
Memastikan adanya kebijakan untuk melakukan pengujian terhadap kelayakan infrastruktur TI	Tidak memadainya infrastruktur yang ada	Melakukan pengamatan apakah terdapat kebijakan yang mendorong dilakukan studi kelayakan terhadap infrastruktur TI	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**AI - Acquire And Implement**			**AI-4**
	Enable Operation and Use (AI4)	Diperiksa oleh Tanggal		

Tujuan:

Memastikan adanya dokumentasi dan user manual bagi pengguna dan personil TI serta adanya pelatihan aplikasi dan infrastruktur TI yang ada

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Planning for Operational Solutions			
Memastikan adanya kebijakan dan prosedur untuk mengidentifikasi dan mendokumentasikan seluruh hal teknis dan operasional serta cara penggunaan sistem	Tidak sesuainya harapan akan TI dan kemampuan TI yang sesungguhnya	Melakukan penilaian bahwa terdapat kebijakan dan prosedur yang mendorong hal tersebut	
Knowledge Transfer to Business Management			
Memastikan adanya transfer pengetahuan ke manajemen bisnis/para pimpinan agar semua individu dapat mengambil alih sistem dan data dan menguji kualitas layanan yang diberikan, pengendalian internal yang ada dan administrasi aplikasi	Meningkatkan permasalahan yang tidak dapat diselesaikan	Memeriksa apakah terdapat transfer pengetahuan	
Knowledge Transfer to End Users			
Memastikan adanya transfer pengetahuan dan kemampuan ke pengguna (*end user*) agar pengguna dapat menggunakan sistem secara efisien dan efektif dalam mendukung proses bisnis	Penggunaan sistem yang tidak konsisten, tidak terdapat dokumentasi sistem, meningkatkan ketergantungan pada staf tertentu, meningkatkan permasalahan yang tidak dapat diselesaikan	Memeriksa apakah dilakukan transfer pengetahuan dan kemampuan ke pengguna (*end user*)	
Knowledge Transfer to Operations and Support Staff			
Memastikan adanya transfer pengetahuan dan kemampuan agar staf operasional dan teknis mampu memberikan layanan secara efektif dan	Tidak adanya dokumentasi sistem yang memadai, meningkatkan ketergantungan pada	Memeriksa apakah terdapat proses transfer pengetahuan dan kemampuan ke staf	

efisien, mendukung dan memelihara sistem serta infrastruktur yang ada	staf tertentu, meningkatnya permasalahan operasional, pelatihan yang dilakukan tidak mampu memenuhi kebutuhan organisasi	operasional dan teknis dan apakah memadai atau tidak	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**AI - Acquire And Implement**			**AI-5**
	PROCURE IT RESOURCES (AI5)	Diperiksa oleh Tanggal		

Tujuan:

Memastikan adanya proses pengadaan yang meliputi: sumber daya manusia, perangkat keras, perangkat lunak dan layanan TI lainnya, dengan mengikuti prosedur pengadaan dari mulai pemilihan vendor, pembuatan kontrak dan proses akuisisi itu sendiri.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Procurement Control			
Memastikan adanya prosedur dan standar proses pengadaan dan akuisisi infrastruktur, fasilitas, perangkat keras, perangkat lunak dan layanan TI yang sesuai dengan tujuan organisasi. Prosedur dan standar ini harus diikuti	Tidak memadainya kualitas perangkat lunak hasil dari proses pengadaan, kurangnya pengendalian terhadap biaya pengadaan, menyebarnya kontrak pengadaan akibat tidak adanya ketentuan yang mengatur kerahasiaanya	Memeriksa apakah terdapat prosedur dan standar proses pengadaan dan telah diikuti oleh organisasi	
Supplier Contract Management			
Memastikan adanya prosedur untuk penanganan kontrak yang meliputi pembuatan, modifikasi dan mengakhiri kontrak dengan semua supplier. Prosedur tersebut harus mencakup masalah hukum, keuangan, kinerja, keamanan, hak intelektual dan penghentian tanggung jawab dan hutang (mencakup klausa hukuman/pinalti	Ketiadaan manajemen biaya, harapan pihak organisasi tidak sesuai dengan kemampuan supplierm layanan yang diberikan supplier tidak sesuai dengan kebutuhan 0.organisasi	Memeriksa apakah terdapat prosedur tersebut dan apakah memadai atau tidak	
Supplier Selection			
Memastikan bahwa terdapat prosedur dan kebijakan yang mengharuskan dilakukannya pemilihan	Supplier dipilih dengan cara yang tidak benar dan tidak sesuai kebutuhan	Memeriksa apakah terdapat prosedur dan kebijakan yang demikian	

supplier secara benar, fair dan formal serta sesuai dengan kebutuhan			
IT Resources Acquisition			
Memastikan adanya perlindungan terhadap kepentingan organisasi dalam bentuk perjanjian kontrak jika akan melakukan akuisisi yang meliputi hak dan kewajiban semua pihak dalam masa kontrak untuk akuisisi perangkat lunak, pengembangan sumber daya, infrastruktur dan layanan TI	Perangkat lunak tidak dapat mendukung proses bisnis, perubahan aplikasi tidak sesuai dengan keinginan, sistem menimbulkan masalah dan insiden yang mengganggu proses bisnis	Memeriksa apakah terdapat perlindungan yang demikian	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	AI - Acquire And Implement			
	MANAGE CHANGES (AI6)	Diperiksa oleh Tanggal		AI-6

Tujuan:

Memastikan bahwa semua perubahan infrastruktur dan aplikasi telah diatur dan dikendalikan secara formal. Segala perubahan baik itu dalam hal prosedur, proses, sistem dan layanan telah dicatat (dalam *log file*), telah dinilai dan diotorisasi sebelum dilakukan implementasi dan review terhadap rencana implementasi. Hal ini mampu menghilangkan risiko negatif yang berpengaruh pada stabilitas dan integritas sistem

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Change Standards and Procedures			
Memastikan adanya prosedur manajemen perubahan yang formal agar seluruh permintaan yang mencakup perubahan aplikasi, proses, prosedur, sistem, layanan, *platform* ditangani sesuai standar yang berlaku	Tidak ada pelacakan terhadap perubahan yang terjadi, tidak memadainya pengendalian terhadap perubahan darurat, terjadinya perubahan yang tidak diotorisasi sehingga akan mengurangi ketersediaan sistem	Memeriksa apakah terdapat kebijakan dan prosedur yang mengendalikan perubahan, dan apakah efektif atau tidak	
Impact Assessment, Prioritisation and Authorisation			
Terdapat prosedur yang akan memastikan dilakukannya penilaian terhadap semua permintaan perubahan melalui suatu cara yang terstruktur untuk menentukan dampak atas operasional sistem dan fungsinya; terdapat prioritas, pengelompokkan dan pengotorisasian terhadap permintaan perubahan	Tidak dapat diantisipasinya berbagai dampak negatif yang akan mengganggu kinerja dan kegiatan operasional perusahaan	Memeriksa apakah terdapat kebijakan dan prosedur yang melakukan penilaian, prioritas dan otorisasi secara terstruktur dan apakah efektif atau tidak	
Emergency Changes			
Memastikan bahwa dilakukan suatu proses untuk mendefinisikan, menguji, mendokumentasikan, menilai dan mengotorisasi perubahan darurat yang tidak mengikuti proses perubahan yang telah ditentukan, dan berbagai	Ketidakmampuan melakukan respon secara efektif terhadap perubahan darurat yang dibutuhkan dan tidak adanya otorisasi terhadap perubahan darurat	Memeriksa apakah terdapat proses yang demikian dan apakah memadai atau tidak	

prosedur yang akan mengendalikan perubahan itu			
Change Status Tracking and Reporting			
Memastikan adanya suatu sistem yang melacak dan melaporkan jika terjadi penolakan terhadap perubahan yang diinginkan, dan juga akan mencatat perubahan yang telah disetujui untuk dilakukan, sedang dalam proses dan telah selesai dilakukan.	Perubahan yang terjadi tidak dicatat sehingga tidak dapat dilacak sehingga perubahan yang tidak terotorisasi pun tidak terdeteksi	Memperhatikan apakah terdapat kebijakan dan prosedur yang mendorong hal tersebut dan apakah efektif atau tidak	
Change Closure and Documentation			
Memastikan adanya prosedur yang mengharuskan dilakukan *update system*, dokumen dan prosedur, ketika mengimplementasikan suatu perubahan	Kurangnya dokumentasi sistem sehingga dokumentasi konfigurasi sistem yang ada tidak mampu menggambarkan konfigurasi sistem yang ada saat ini	Memperhatikan apakah terdapat prosedur yang demikian, dan apakah berjalan efektif atau tidak	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	AI - Acquire And Implement			AI-7
	INSTALL AND ACCREDIT SOLUTIONS AND CHANGES (AI7)	Diperiksa oleh Tanggal		

Tujuan:

Memastikan bahwa sistem yang baru dapat beroperasi dengan baik sesuai dengan tujuan dimaksud, dengan melalui pengujian yang tepat, prosedur migrasi yang tepat dan *post-implementation review*

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Training			
Memastikan adanya suatu pelatihan bagi staf yang terpengaruhi dan grup operasi dari fungsi TI, sesuai dengan rencana pelatihan yang telah ditentukan dan sesuai dengan material yang berhubungan	Kegagalan untuk mendeteksi permasalahan pada sistem yang digunakan dan ketiadaan pengetahuan untuk menjalankan kewajiban dan kegiatanya	Memeriksa apakah terdapat kebijakan dan prosedur yang mendorong pelaksanaan pelatihan dan apakah efektif atau tidak	
Test Plan			
Memastikan adanya suatu rencana pengujian berdasarkan standar yang telah ditentukan	Tidak adanya pengujian yang memadai mengakibatkan permasalahan yang berkaitan dengan kinerja sistem tidak dapat dideteksi	Memeriksa apakah terdapat kebijakan yang mendorong dibuatnya rencana pengujian, dan apakah berjalan efektif atau tidak	
Implementation Plan			
Terdapat suatu rencana implementasi dan *fallback/backout* dan mendapat persetujuan dari pihak yang relevan	Tanpa adanya rencana implementasi yang memadai dapat mengakibatkan pengalokasian sumber daya yang tidak tepat dan terjadinya pelanggaran keamanan	Memeriksa apakah terdapat kebijakan dan prosedur yang mendorong dibuatnya rencana implementasi, dan apakah berjalan efektif atau tidak	
Test Environment			
Terdapat prosedur yang mengharuskan dibangunnya suatu lingkungan TI yang aman (*secure*), dengan memperhatikan keamanan, pengendalian internal, praktek operasional, kualitas dan kerahasiaan data dan	Pengujian yang tidak memadai sehingga mengakibatkan tidak terdeteksinya permasalahan kinerja dan masalah keamanan sistem	Memperhatikan apakah terdapat prosedur yang demikian dan apakah efektif atau tidak	

beban kerja			
System and Data Conversion			
Terdapat rencana konversi data dan migrasi infrastruktur yang merupakan bagian dari metode pengembangan organisasi yang mencakup jejak audit (*audit trails*), *rollbacks* dan *fallbacks*	Jika rencana migrasi infrastruktur bukan merupakan bagian dari metode pengembangan organisasi maka sistem yang lama kemungkinan akan terhapus dan tidak tersedia ketika dibutuhkan; ketiadaan rencana konversi data akan mengakibatkan sistem dan hasil konversi tidak handal, tidak terjaminnya integritas data	Memeriksa apakah terdapat prosedur dan kebijakan yang mendorong dibuatnya rencana konversi data dan migrasi infrastruktur, dan apakah berjalan efektif atau tidak	
Testing of Changes			
Memastikan apakah terdapat prosedur untuk melakukan pengujian terhadap perubahan yang terjadi secara independen sesuai dengan rencana pengujian yang telah didefinisikan sebelumnya dan telah mempertimbangkan aspek keamanan dan kinerja sistem	Perubahan yang dilakukan berdampak pada kinerja dan ketersediaan sistem	Memeriksa apakah terdapat prosedur pengujian yang memadai	
Final Acceptance Test			
Memastikan bahwa seluruh manajemen TI dan pihak-pihak yang berkepentingan melakukan evaluasi terhadap hasil dari proses pengujian (*final acceptance test*) apakah sesuai dengan yang ditentukan dalam rencana pengujian dan akan menindaklanjuti kesalahan yang teridentifikasi selama pross pengujian	Dengan tidak dilakukan *final acceptance test*, permasalahan kinerja tidak dapat dideteksi sehingga tidak dapat diperbaiki	Memeriksa apakah kebijakan dan prosedur yang ada mendorong dilakukannya *final acceptance test*	
Promotion to Production			
Memastikan bahwa seluruh manajemen TI mendefinisikan dan mengimplementasikan berbagai prosedur formal untuk mengendalikan pemidahtanganan sistem dari pengembangan ke operasi dengan melakukan pengujian	Apabila tidak dilakukan pengujian terlebih dahulu, tidak diketahui apakah sistem telah sesuai dengan rencana implementasi atau tidak dan tidak disetujui oleh para *stakeholder*	Memeriksa apakah terdapat kebijakan dan prosedur yang mendorong dilakukannya pengujian, dan apakah berjalan efektif atau tidak	

untuk mengawasi operasional sistem apakah telah sesuai dengan rencana implementasi, dan disetujui oleh para *stakeholder* utama, seperti pengguna/user, *system owner* dan manajemen operasional			
Post-implementation Review			
Memastikan adanya prosedur yang mengharuskan dilakukan review setelah pengimplementasian sistem untuk menilai dan melaporkan apakah sistem telah mencapai manfaat yang diharapkan melalui cara yang paling *cost effective*	Manajemen TI tidak dapat mengidentifikasi apakah sistem telah memberikan hasil dan manfaat sesuai dengan yang diharapkan	Memeriksa apakah terdapat prosedur yang mendorong dilakukannya review setelah proses implementasi	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Define and Manage Service Levels (DS1)	Diperiksa oleh Tanggal		**DS1**

Tujuan

1. Memastikan bahwa layanan yang diberikan memenuhi tingkat layanan yang dibutuhkan oleh seluruh *stakeholder* yang disesuaikan dengan kriteria kinerja/performa yang diharapkan oleh organisasi
2. Memastikan bahwa dilakukan pengawasan dan monitoring terhadap tingkat layanan

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Service Level Management Framework (DS1.1)			
Memastikan adanya suatu kerangka layanan dan kerangka operasional yang jelas dan formal yang mendefinisikan kebutuhan dan tingkat layanan yang diberikan pada pemakai/pengguna, ketersediaan, keandalan, kinerja, dan keamanan layanan serta biaya yang dibutuhkan untuk memberikan layanan tersebut	Tidak adanya kerangka yang jelas akan mengakibatkan: adanya gap antara layanan yang diharapkan dan kemampuan sistem yang sebenarnya; biaya yang dikeluarkan menjadi tidak terkontrol; tidak ada kerangka operasional yang jelas; tidak ada pengukuran kinerja yang jelas, dan ; tidak ada pembagian tanggung jawab yang jelas antara pengguna dan pemberi jasa	Melakukan pemahaman terhadap kebijakan, prosedur, metode dan *service level agreement* organisasi, serta memastikan apakah efektif dan dapat mencapai tujuan organisasi atau tidak	
Definition of Services (DS1.2)			
Memastikan bahwa terdapat pendefinisian awal layanan TI berdasarkan karakteristik layanan dan kebutuhan organisasi yang dituangkan dalam suatu portfolio daftar layanan	Tidak adanya pendefinisian awal layanan mengakibatkan: ketidaktepatan layanan yang diberikan; salah dalam	Memastikan bahwa terdapat proses untuk mengembangkan, mereview dan menyesuaikan daftar layanan atau portfolio layanan,	

	memprioritaskan layanan; ketidakpahaman terhadap dampak insiden akan mengakibatkan respon penanganan yang lambat; interpretasi dan pemahaman layanan TI yang berbeda	sehingga tetap efektif dan *up to date*	
Service Level Agreements (DS1.3)			
Mendefinisikan dan menyetujui SLA yang memuat semua layanan TI berdasarkan kemampuan TI, kebutuhan pengguna, komitmen pengguna dan kemampuan TI, dengan memperhatikan aspek-aspek ketersediaan, kehandalan, kinerja, kapasitas untuk berkembang/tumbuh, tingkat dukungan terhadap pengguna, rencana yang berkelanjutan, keamanan dan batasan permintaan.	Tidak adanya pendefinisian layanan dalam bentuk SLA mengakibatkan: tidak terpenuhinya kebutuhan pengguna; sumber daya tidak digunakan secara efektif dan efisien; gagal untuk mengidentifikasi dan merespon insiden penting	Memastikan bahwa para stakeholder menyetujui format dan isi SLA Mereview apakah SLA telah memadai atau belum Memastikan apakah senantiasa dilakukan perbaikan terhadap SLA dengan mempertimbangkan umpan balik dari pengguna	
Operating Level Agreements (DS1.4)			
Mendefinisikan OLAs yang akan menjelaskan teknis layanan yang diberikan untuk mendukung SLA(s) secara optimal	Dengan tidak adanya OLA, mengakibatkan kegagalan dalam memberikan layanan sesuai kebutuhan, timbul gap dalam memahami teknis pelayanan yang mengakibatkan terjadinya insiden, penggunaan sumber daya yang tidak efisien dan menelan banyak biaya	Memastikan bahwa terdapat suatu proses yang akan mengembangkan, mengatur, mereview dan menyesuaikan OLAs Memastikan bahwa OLAs akan mendukung kebutuhan teknis yang dijelaskan di SLAs Memastikan bahwa OLAs mengandung pendefinisian optimal dari layanan yang	

		diberikan	
Monitoring and Reporting of Service Level Achievements (DS1.5)			
Memastikan dilakukan monitoring dan pelaporan secara kontinyu terhadap performa layanan yang diberikan. Laporan monitoring harus dianalisis untuk mengidentifikasi trend negatif dan positif dari layanan yang diberikan	Isu dan permasalahan yang berkaitan dengan layanan tidak dapat diidentifikasi Ketidakpuasan pengguna akibat kurangnya informasi dan buruknya kualitas layanan	Mengetahui sejauh mana performa layanan yang diberikan	
Review of Service Level Agreements and Contracts (DS1.6)			
Mereview SLA dan kontrak dengan penyedia layanan secara reguler untuk menilai apakah layanan yang diberikan telah efektif, *up to date* dan memenuhi kebutuhan pengguna	Ketidaksesuaian SLA dengan keadaan yang dialami oleh organisasi, sehingga operasional organisasi menjadi tidak efektif dan efisien yang mengakibatkan kerugian biaya	Melakukan pemahaman terhadap kebijakan dan prosedur yang ada, melakukan review terhadap keefektifan SLA dan melakukan penilaian apakah manajemen setuju dengan perkembangan selanjutnya dari SLA	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Define and Manage Third Party Services (DS2)	Diperiksa oleh Tanggal		**DS2**

Tujuan

1. Memastikan bahwa tanggung jawab, tugas, peran dan layanan yang diberikan dan dijalankan oleh pihak ketiga (*supplier, vendor* dan *partner*), sesuai dengan kebutuhan organisasi
2. Meminimalkan timbulnya risiko

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref
Identification of All Supplier Relationships (DS2.1)			
Mengidentifikasi seluruh layanan yang diberikan oleh supplier dan mengkategorikannya berdasarkan tipe supplier dan tingkat kepentingannya, serta mengidentifikasi tugas, tanggung jawab, peran, tujuan, dan layanan yang diharapkan dari supplier	Tidak teridentidikasinya supplier yang penting Penggunaan sumber daya supplier yang tidak efisien dan tidak efektif Layanan buruk dan timbulnya biaya tambahan akibat peran dan tanggung jawab supplier yang tidak jelas	Periksa skema pengkategorian supplier Periksa alasan pemilihan supplier Periksa kontrak dengan supplier	
Supplier Relationship Management (DS2.2)			
Memformalkan hubungan dengan setiap supplier dan memastikan bahwa kualitas hubungan tersebut berdasarkan kepercayaan dan keterbukaan (*transparency*)	Supplier tidak responsif dan tidak menjalankan komitmen Isu dan permasalahan tidak terpecahkan Kualitas layanan tidak memenuhi syarat	Memastikan bahwa terdapat dokumentasi formal, kontrak, kebijakan yang berisi tugas dan tanggung jawab supplier, dan memastikan bahwa supplier yang dipilih benar-benar memiliki kemampuan sesuai kebutuhan organisasi	
Supplier Risk Management (DS2.3)			
Mengidentifikasi dan menghilangkan	Supplier tidak	Melakukan	

risiko agar supplier dapat memberikan layanan yang efektif, aman dan berkelanjutan, dengan mempertimbangkan hukum dan peraturan yang berlaku, hal-hal yang tidak boleh diungkap (*nondisclosure agreements* (NDAs)), hukuman, penghargaan, dll	mematuhi peraturan yang berlaku, sehingga mengakibatkan terjadinya insiden serta kerugian biaya dan rusaknya reputasi organisasi	penilaian apakah di dalam organisasi terdapat proses manajemen risiko dan monitoringnya, dan apakah didukung oleh kebijakan yang memadai	
Supplier Performance Monitoring (DS2.4)			
Membangun suatu proses untuk memastikan bahwa performa layanan yang diberikan supplier telah sesuai dengan kebutuhan organisasi yang tertuang dalam kontrak dan SLAs	Dengan tidak adanya proses monitoring, maka penurunan kualitas layanan tidak dapat diidentifikasi sehingga akan memberikan dampak negatif bagi organisasi	Melakukan penilaian apakah terdapat pemantauan terhadap layanan yang diberikan supplier	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Define and Manage Performance and Capacity (DS3)	Diperiksa oleh Tanggal		**DS3**

Tujuan:

Memastikan apakah terdapat perencanaan yang mencakup prediksi kebutuhan di masa mendatang berdasarkan beban kerja yang ada, kebutuhan akan storage dan tindakan untuk menangani hal di luar dugaan dan penilaian terhadap kinerja dan kemampuan sumber daya TI, sehingga memberikan kepastian bahwa sumber daya informasi yang ada mendukung kebutuhan organisasi

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref
Performance and Capacity Planning (DS3.1)			
Membangun suatu rencana untuk melakukan review terhadap kinerja dan kemampuan sumber daya TI untuk memastikan bahwa penggunaan sumber daya tersebut mampu menghemat biaya dan mampu bekerja sesuai dengan beban kerja yang ditentukan dalam SLAs	Terjadi insiden akibat kurangnya kapasitas/kemampuan sumber daya TI Kegagalan sistem dalam mencapai kinerja yang diharapkan	Melakukan pemahaman dan penilaian kecukupan atas rencana penilaian dan pemantauan kinerja dan kemampuan sumber daya TI	
Current Performance and Capacity (DS3.2)			
Melakukan penilaian terhadap kinerja dan kemampuan sumber daya TI yang ada saat ini untuk menentukan apakah terdapat kemampuan dan kinerja memadai untuk memberikan layanan yang sesuai kebutuhan organisasi	Timbulnya gangguan terhadap proses bisnis, tidak terpenuhinya SLA dan kebutuhan organisasi, layanan yang diberikan di bawah atau di atas yang seharusnya aibat tidak adanya ukuran kapasitas sumber daya TI yang jelas	Memastikan telah dikembangkan suatu perangkat lunak untuk monitoring kinerja dan kapasitas sumber daya TI berdasarkan kebutuhan organisasi, ketentuan dalam SLA, dampak bagi operasional/keuangan/peraturan akibat isu kinerja dan kapasitas TI	
Future Performance and Capacity (DS3.3)			
Melakukan prediksi terhadap performance dan kemampuan sumber daya TI untuk meminimumkan risiko	Layanan TI tidak mampu mendukung proses bisnis akibat kemampuan sumber daya TI yang tidak	Periksa apakah sumber daya TI yang ada mampu mendukung proses bisnis organisasi	

terganggunya layanan yang diberikan akibat tidak memadainya kemampuan atau penurunan *performance*	memadai		
IT Resources Availability (DS3.4)			
Menilai ketersediaan sumber daya TI apakah telah memiliki kinerja yang baik yang mampu mendukung proses bisnis organisasi	Sistem tidak dapat bekerja dengan baik akibat tidak tersedianya sumber daya TI yang memadai	Memastikan apakah sumber daya TI yang ada telah memadai	
Monitoring and Reporting (DS3.5)			
Memonitor kinerja dan kapasitas sumber daya TI apakah mampu memberikan layanan yang diharapkan	Layanan yang diberikan tidak sesuai harapan dan penyimpangan yang terjadi dalam layanan yang diberikan tidak dapat dideteksi	Memastikan apakah dilakukan monitoring dan pelaporan terhadap kinerja dan kapasitas sumber daya TI	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Ensure Continues Service (DS4)	Diperiksa oleh Tanggal		**DS4**

Tujuan:

1. Memastikan adanya proses untuk mengembangkan, menjaga dan menguji rencana kontinuitas TI, utilisasi *offsite backup storage* dan menyediakan pelatihan TI secara periodik.
2. Memastikan bahwa organisasi mampu meminimalisir kegagalan atau terhambatnya layanan TI pada fungsi dan proses bisnis yang utama

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
IT Continuity Framework			
Memastikan adanya suatu kerangka kerja yang mendefinisikan peran, tanggung jawab dan tugas dari penyedia layanan, serta peraturan dan struktur untuk mendokumentasikan, menguji dan menjalankan *disaster recovery* dan rencana kontinuitas TI, bagi kelanjutan TI dalam mendukung proses bisnis organisasi	Kontinuitas layanan TI tidak dikelola dengan tepat, dan meningkatnya ketergantungan pada staf utama	Memastikan apakah terdapat kerangka kontinuitas TI yang membantu proses bisnis organisasi, dan lakukan penilaian apakah efektif atau tidak	
IT Continuity Plan			
Memastikan adanya suatu rencana kontinuitas TI berdasarkan kerangka kerja, yang mendefinisikan risiko sehingga akan mengurangi dampak gagalnya proses dan fungsi TI yang utama serta mendefinisikan proses *recovery* untuk menangani seluruh layanan TI yang utama	Kegagalan untuk memulihkan (*recovery*) sistem dan layanan TI secara tepat waktu Gagalnya proses pengambilan keputusan Kurangnya sumber daya yang dibutuhkan untuk pemulihan sistem	Memastikan bahwa terdapat rencana kontinuitas TI dengan kemampuan *recovery* yang sejalan dengan komitmen layanan, untuk semua fungsi dan proses bisnis yang utama/penting	
Critical IT Resources			
Memprioritaskan *recovery* pada item paling penting dalam rencana kontinuitas TI, serta memastikan	Tidak tersedianya sumber daya TI yang penting, meningkatnya biaya	Memastikan bahwa terdapat rencana kontinuitas TI yang konsisten, untuk fungsi TI utama, dan telah sesuai	

bahwa respon dan *recovery* yang dilakukan sejalan dengan kebutuhan organisasi, dengan tetap memperhatikan optimalisasi biaya, serta mematuhi peraturan dan perjanjian kontrak	akibat rencana kontinuitas TI, dan pemrioritasan layanan tidak didasarkan pada kebutuhan organisasi	dengan tujuan organisasi	
Maintenance of the IT Continuity Plan			
Mendukung manajemen TI untuk mendefinisikan dan menjalankan prosedur perubahan pengendalian untuk memastikan bahwa rencana kontinuitas TI tetap *up to date* dan menggambarkan kebutuhan organisasi yang sebenarnya	Rencana kontinuitas yang tidak relevan dan gagal menggambarkan kebutuhan organisasi dan kurangnya prosedur pengendalian terhadap perubahan	Melakukan pemahaman dan penilaian terhadap prosedur yang mendorong pembaharuan rencana kontinuitas TI, dan apakah efektif atau tidak	
Testing of the IT Continuity Plan			
Menilai keefektifan rencana kontinuitas TI apakah dapat menangani kekurangan sistem yang ada, dan menilai keefektifan proses *recovery* terhadap sistem TI	Rencana kontinuitas tidak dapat diterapkan secara efektif, sehingga menyulitkan pada waktu melakukan *recov ery* dan tindakan lain dalam rangka mengatasi keadaan darurat	Menilai apakah terdapat pengujian terhadap rencana kontinuitas TI	
IT Continuity Plan Training			
Melakukan pelatihan bagi semua pihak yang terlibat, yang meliputi pembelajaran terhadap prosedur, tugas dan tanggung jawab apabila terjadi suatu insiden atau kerusakan	Proses bisnis menjadi terganggu/diiterupsi selama periode yang tidak dapat dipastikan, karena tidak didukung oleh staf yang ahli dalam mengatasi insiden/kerusakan yang terjadi	Menilai apakah terdapat pelatihan berkaitan dengan kontinuitas TI	
Distribution of the IT Continuity Plan			
Memastikan terdapat strategi yang aman dan tepat dalam pendistribusian apakah seluruh rencana kontinuitas TI sehingga dapat digunakan oleh seluruh pihak yang berwenang/diotorisasi	Pendistribusian rencana kontinuitas TI yang tidak tepat, mengakibatkan informasi yang bersifat rahasia diberitahukan pada pihak yang tidak berwenang, sehingga	Menilai strategi pendistribusian rencana kontinuitas TI, sehingga hanya dapat diakses oleh pihak yang berwenang/diotorisasi	

	proses *upgrade* terhadap rencana yang ada tidak tepat waktu		
IT Services Recovery and Resumption			
Merencanakan tindakan yang akan diambil ketika dilakukan proses *recovery* TI dan ketika melanjutkan layanan. Tindakan ini meliputi backup, inisiasi untuk alternatif pemrosesan, komunikasi antara pengguna dan *stakeholder* dan *resumption procedures*. Memastikan bahwa manajemen mengerti akan jadwal *recovery* TI ini dan melakukan investasi yang dibutuhkan untuk mendukung proses *recovery* dan *resumption* ini	Langkah dan proses *recovery* tidak tepat sehingga menimbulkan kelemahan proses *recovery* dan kegagalan dalam memulihkan layanan sistem yang penting secara tepat waktu	Menilai rencana *recovery* TI apakah efektif dan telah sesuai dengan kebutuhan organisasi	
Offsite Backup Storage			
Memastikan adanya kebijakan atau prosedur yang mendefinisikan suatu media penyimpanan terhadap *backup data*	Tidak tersedianya media penyimpanan untuk *backup data* yang akan mengakibatkan rusaknya data	Menilai apakah data benar-benar dilindungi di lokasi penyimpanan yang aman, dan apakah media *backup* memuat semua informasi yang dibutuhkan dalam rencana kontinuitas TI	
Post-resumption Review			
Memastikan bahwa manajemen TI telah membangun suatu prosedur untuk menilai ketercukupan rencana kontinuitas TI yang ada yang dilihat dari tetap berjalannya fungsi TI dengan baik, setelah terjadinya kerusakan dan perubahan rencana TI	Rencana *recovery* yang tidak tepat dan tidak mampu memenuhi tujuan dan kebutuhan organisasi	Menilai keefektifan kebijakan atau prosedur operasional TI	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Ensure System Security (DS5)	Diperiksa oleh Tanggal		**DS5**

Tujuan:

Menjaga integritas informasi dan melindungi aset TI melalui proses penanganan keamanan (*security management* process) yang meliputi pembangunan dan pemeliharaan keamanan TI dalam hal tugas dan tanggung jawab, kebijakan, standar dan prosedur, serta mengharuskan dilakukannya monitoring dan pengujian terhadap keamanan yang ada, yang dilakukan secara periodik dan melakukan tindakan korektif terhadap kelemahan dan insiden yang terjadi dalam hal keamanan. Proses penanganan keamanan yang efektif akan melindungi semua aset TI dan meminimalkan dampak yang ditimbulkan oleh insiden dalam hal keamanan.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Management of IT Security			
Memprioritaskan keamanan TI pada level paling tinggi, sehingga penanganan tindakan keamanan TI akan sejalan dengan kebutuhan organisasi	Kurangnya tata kelola keamanan TI mengakibatkan tidak sejalannya TI dengan tujuan organisasi selain itu data dan aset TI juga tidak terlindungi	Melakukan pemahaman dan penilaian apakah terdapat kebijakan atau prosedur yang mendetil dalam mengatur keamanan TI	
IT Security Plan			
Menterjemahkan kebutuhan organisasi, penanganan risiko dan kepatuhan terhadap peraturan ke dalam suatu rencana keamanan TI dengan mempertimbangkan infrastruktur TI dan budaya keamanan yang ada. Pastikan bahwa rencana keamanan TI akan diimplementasikan dalam kebijakan pengamanan dan prosedur pengamanan dengan suatu investasi yang tepat dalam hal layanan, personel, perangkat lunak dan perangkat keras	Rencana keamanan TI tidak sejalan dengan kebutuhan organisasi dan mengakibatkan timbulnya banyak biaya dan menjadi tidak efektif	Melakukan pemahaman dan penilaian apakah terdapat rencana keamanan TI (*IT security plan*) yang mencakup standar, kebijakan dan prosedur keamanan yang lengkap, peran dan tanggung jawab staf terjadap keamanan TI, dan investasi pada keamanan TI (*required security resources*)	
Identity Management			

Memastikan bahwa semua user baik itu user internal, eksternal maupun yang bersifat sementara (*temporary*) beserta aktifitasnya dalam sistem TI, diidentifikasi secara khusus, yang meliputi hak aksesnya	Tidak adanya pendefinisian hak akses mengakibatkan tidak diotorisasinya perubahan terhadap perangkat keras dan perangkat lunak, sehingga keamanan sistem/TI menjadi terganggu	Melakukan pemahaman dan penilaian apakah terdapat kebijakan dan prosedur sehubungan dengan user dan hak aksesnya, keamanan akses pada sistem dan semua sumber daya TI	
User Account Management			
Terdapat prosedur yang tepat berkaitan dengan penanganan permintaan, pembuatan, pengaturan, pembekuan, perubahan dan penutupan *user account* dan hak aksesnya	Pelanggaran keamanan, user tidak mematuhi kebijakan dan prosedur keamanan TI, insiden tidak ditangani tepat waktu, dan kegagalan untuk menutup account yang sudah tidak terpakai	Melakukan pemahaman dan penilaian apakah terdapat pengelolaan *user account*, dan apakah efektif atau tidak	
Security Testing, Surveillance and Monitoring			
Menguji dan memonitor implementasi keamanan TI secara proaktif, untuk mencegah dan atau mendeteksi lebih awal dan kemudian melaporkan kejadian yang abnormal	Penyalahgunaan *user account*, tidak terdeteksinya pelanggaran terhadap keamanan TI, dan ketidakhandalan *security logs*	Melakukan pengamatan apakah terdapat proses pencatatan dan pelaporan yang memadai, terkait dengan pelanggaran keamanan	
Security Incident Definition			
Mendefinisikan karakteristik insiden dalam hal keamanan TI yang mungkin terjadi, sehingga dapat dikelompokkan dan ditangani dengan tepat	Tidak terdeteksinya pelanggaran keamanan dan tidak terdapat pengelompokkan pelanggaran keamanan yang tepat	Melakukan pengamatan apakah terdapat pendeteksian dan pengelompokkan pelanggaran keamanan yang tepat	
Protection of Security Technology			
Membangun sistem keamanan yang mampu melindungi teknologi informasi dalam mengadapi berbagai serangan	Pengungkapan informasi yang tidak seharusnya dan pelanggaran terhadap hukum dan aturan yang berlaku	Melakukan pengamatan dan penilaian apakah terdapat kebijakan atau prosedur untuk melindungi teknologi informasi	
Cryptographic Key Management			
Memastikan apakah terdapat kebijakan dan prosedur untuk	Penggunaan kunci/*password* oleh pihak yang tidak	Melakukan penilaian apakah kebijakan dan prosedur yang terkait dengan *cryptographic*	

mengorganisir penciptaan, perubahan, penarikan kembali (*revocation*), penghancuran, pendistribusian, sertifikasi, penyimpanan, penginputan, penggunaan *cryptographic* untuk melindungi proses perubahan dan pengungkapan data yang tidak seharusnya	berwenang, pengaksesan modul *cryptographic* yang tidak diotorisasi dan registrasi user yang tidak diverifikasi	mampu melindungi informasi dan data yang penting	
Malicious Software Prevention, Detection and Correction			
Memastikan bahwa terdapat perangkat lunak yang mencegah, mendeteksi dan mengoreksi yang melindungi sistem dan teknologi informasi dari serangan *virus, worms, spyware* dan *spam*	Tersebarnya informasi ke pihak yang tidak berwenang, pelanggaran terhadap hukum dan aturan yang berlaku, data dan sistem mudah terserang virus	Melakukan pengamatan apakah perangkat lunak (*malicious software*) mampu melindungi data, sistem dan teknologi informasi dari berbagai serangan	
Network Security			
Menggunakan teknik dan prosedur keamanan seperti *firewalls*, alat-alat keamanan, pemisahan jaringan, pendeteksian terjadinya gangguan untuk mengotorisasi akses dan mengendalikan informasi dari dan ke jaringan	*Firewalls* gagal melindungi informasi organisasi, dilakukannya perubahan yang tidak diotorisasi terhadap aturan *firewalls*, dan pelanggaran keamanan tidak terdeteksi tepat waktu	Memastikan apakah kebijakan atau prosedur keamanan jaringan mencakup seluruh layanan yang diberikan, lalu lintas data, dan tipe koneksi yang diperbolehkan	
Exchange of Sensitive Data			
Pertukaran data yang sensitif hanya dilakukan di jalur yang benar-benar dipercaya	Keamanan fisik yang tidak memadai mengakibatkan penyebaran informasi organisasi yang sensitif kepada pihak-pihak yang tidak berwenang	Melakukan penilaian apakah terdapat pengendalian aplikasi yang akan memvalidasi data yang sensitif sebelum data tersebut diproses dan ditransmisikan	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Identify and Allocate Cost (DS6)	Diperiksa oleh Tanggal		**DS6**

Tujuan:

Memastikan adanya suatu sistem pengalokasian biaya TI yang mampu mencatat, menghitung, mengalokasikan dan melaporkan biaya TI secara tepat dan sesuai dengan kebutuhan organisasi

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Definition of Services			
Mengidentifikasi dan memetakan semua biaya TI terkait dengan layanan yang diberikan, sehingga menjadi transparan	Penghitungan biaya yang tidak tepat, keputusan investasi dilakukan berdasarkan informasi yang salah, para pimpinan memiliki pandangan yang salah terhadap biaya TI yang harus dikeluarkan	Menilai apakah kebijakan dalam mengidentifikasi dan memetakan semua biaya TI terkait dengan layanan yang diberikan, telah tepat	
IT Accounting			
Mengalokasian biaya yang sebenarnya dikeluarkan berdasarkan *enterprise cost model*. Ketidaksesuaian prediksi biaya dan biaya yang sebenarnya dikeluarkan harus dianalisis dan dilaporkan apakah telah sesuai dengan sistem pengukuran keuangan organisasi	Model akutansi yang ada tidak mampu merefleksikan alokasi biaya yang ada, pencatatan biaya tidak mengikuti kebijakan keuangan organisasi, organisasi memiliki pandangan yang salah terhadap biaya TI	Malakukan penilaian terhadap model akuntansi biaya TI yang ada, apakah telah mampu mengalokasikan dan memprediksi anggaran TI yang dibutuhkan dan melaporkan biaya sebenarnya yang dikeluarkan oleh TI	
Cost Modelling and Charging			
Mengimplementasikan dan menggunakan model penentuan biaya TI berdasarkan definisi layanan yang diberikan, sehingga item-item yang dapat dibebankan teridentifikasi dengan jelas,	Model penentuan biaya tidak sejalan dengan prosedur akuntasi secara keseluruhan	Melakukan penilaian apakah terdapat model penentuan biaya yang efektif	

terukur dan terprediksi oleh pengguna			
Cost Model Maintenance			
Mereview dan melakukan *benchmark* biaya secara reguler untuk mejaga kerelevanan biaya tersebut terhadap proses bisnis dan aktifitas TI	Model dan metode pengalokasian biaya tidak mencerminkan biaya yang sesungguhnya terjadi dan tidak mencerminkan kebutuhan organisasi	Melakukan pemahaman bahwa kebijakan atau standar pemodelan alokasi biaya benar-benar efektif dan direview secara reguler	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**DS – Delivery and Support**	Tanggal		
	Educate and Train Users (DS7)	Diperiksa oleh Tanggal		**DS7**

Tujuan:

Memastikan adanya pendidikan yang efektif bagi seluruh pengguna sistem TI mencakup kebutuhan pelatihan bagi setiap kelompok user. Pogram pelatihan yang efektif akan meningkatkan penggunaan teknologi dengan mengurangi kesalahan user, meningkatkan produktifitas dan meningkatkan kepatuhan terhadap pengendalian yang ada

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Identification of Education and Training Needs			
Membuat dan mengupdate kurikulum yang ada secara reguler untuk mengidentifikasi dan mendokumentasikan kebutuhan pelatihan bagi seluruh pegawai	Staf tidak mendapatkan pelatihan yang memadai sehingga tidak dapat menjalankan tugasnya sesuai dengan tuntutas sistem	Melakukan pengamatan apakah terdapat kebijakan atau prosedur sehubungan dengan rencana dan materi pelatihan bagi pegawai, dan apakah efektif atau tidak	
Delivery of Training and Education			
Mengidentifikasi target pengguna yang harus diberi pelatihan, mekanisme pelatihan, serta guru/pelatih yang memberikan pelatihan	Program dan mekanisme pelatihan yang tidak tepat dan tidak efektif, materi pelatihan yang sudah tidak *up to date*	Melakukan pemahaman dan penilaian bahwa jadwal pelatihan telah sesuai kebutuhan dan telah terdapat mekanisme dan materi pelatihan yang memadai	
Evaluation of Training Received			
Mengevaluasi bobot pendidikan dan pelatihan dengan melihat kerelevanan, kualitas, keefektifan, pengetahuan, biaya dan nilai tambah yang diberikan. Hasil evaluasi ini merupakan input bagi kurikulum/materi pelatihan di masa mendatang	Program pelatihan yang tidak tepat dan tidak efektif, materi pelatihan tidak *up to date*, menurunnya kualitas pelatihan, manfaat dan nilai tambah yang diperoleh tidak sebesar biaya pelatihan yang telah dikeluarkan	Melakukan penilaian apakah target pelatihan telah dicapai	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**DS – Delivery and Support**	Tanggal		
	Manage Service Desk and Incidents (DS8)	Diperiksa oleh Tanggal		**DS8**

Tujuan:

Memastikan apakah permintaan user terhadap TI dan permasalahannya direspon dengan cepat, efektif dan tepat waktu, serta disertai dengan pelaporan yang efektif

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Service Desk			
Membangun suatu fungsi layanan berupa *service desk* yang akan menjadi antar muka (*interface*) antara user dan TI, dan dapat membantu untuk mengkomunikasikan, menganalisis semua panggilan, menyelesaikan insiden yang terjadi, memenuhi permintaan layanan dan kebutuhan informasi	Tidak adanya dukungan atau bantuan pada saat user mengalami kesulitan, sehingga akan mempengaruhi aktifitasnya	Melakukan pengamatan apakah terdapat *service desk*, dan apakah berjalan efektif atau tidak	
Registration of Customer Queries			
Memastikan adanya suatu fungsi dan layanan yang melakukan pencatatan permintaan layanan dan kebutuhan informasi dari pengguna	Permintaan pengguna tidak dilayani dengan cepat dan tepat waktu	Melakukan pengamatan apakah terdapat fungsi dan layanan yang demikian dan apakah berjalan efektif atau tidak	
Incident Escalation			
Mengimplementasikan prosedur penanganan insiden untuk memastikan bahwa insiden tersebut dapat ditangani dengan cara yang efisien dan tepat waktu	Tidak adanya panduan yang jelas serta standar untuk menangani insiden	Melakukan pengamatan apakah terdapat prosedur penanganan insiden yang baik, dan apakah efektif atau tidak	
Incident Closure			
Mengimplementasikan suatu prosedur yang mencatat dan melaporkan insiden yang berhasil ditangani, serta langkah penyelesaiannya, dan insiden yang tidak berhasil	Informasi yang salah mengenai insiden yang terjadi sehingga insiden tidak ditangani dengan tepat dan cepat	Melakukan pengamatan apakah prosedur yang ada telah mencatat dan pelaporkan insiden yang terjadi dengan tepat	

ditangani			
Reporting and Trend Analysis			
Terdapat prosedur yang menjamin kecukupan laporan aktifitas layanan TI yang diberikan, untuk mengetahui performa layanan, waktu respon terhadap permintaan layanan dan trend permasalahan yang sering terjadi	Sulit melakukan perbaikan layanan TI	Melakukan pengamatan apakah terdapat prosedur pelaporan yang baik, dan apakah efektif atau tidak	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**DS – Delivery and Support**	Tanggal		
	Manage the Configuration (DS9)	Diperiksa oleh Tanggal		**DS9**

Tujuan:

Memastikan adanya pengendalian yang dapat menjaga integritas konfigurasi perangkat lunak dan perangkat keras

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Configuration Repository and Baseline			
Memastikan adanya suatu alat dukung dan sebuah tempat penyimpanan yang memuat semua informasi yang relevan terkait konfigurasi sistem, serta memastikan bahwa konfigurasi awal (*configuration baseline*) disimpan sebagai *checkpoint* untuk kembali lagi setelah dilakukan perubahan	Tidak adanya dasar untuk kembali setelah terjadi perubahan, sehingga apabila terjadi perubahan yang tidak sesuai, maka akan sulit untuk membatalkannya	Melakukan pengamatan apakah terdapat proses yang demikian, dan apakah efektif atau tidak	
Identification and Maintenance of Configuration Items			
Memastikan adanya prosedur konfigurasi untuk mendukung manajemen dan mencatat semua perubahan pada *configuration repository*, yang terintegrasi dengan prosedur manajemen perubahan dan penanganan masalah serta insiden yang dimiliki organisasi	Informasi yang tidak akurat akibat tidak dicatatnya semua perubahan yang terjadi, dan tidak terkendalinya manajemen perubahan yang mengakibatkan rusaknya proses bisnis organisasi	Melakukan pengamatan apakah prosedur tersebut berjalan efektif atau tidak	
Configuration Integrity Review			
Memastikan adanya proses review terhadap konfigurasi data secara periodik untuk memverifikasi integritas konfigurasi, memastikan adanya proses review perangkat lunak yang telah terinstall secara periodik	Tidak adanya proses review mengakibatkan meningkatnya biaya penanganan masalah dan penyalahgunaan aset TI	Melakukan pengamatan apakah terdapat proses yang demikian, dan apakah efektif atau tidak	

untuk melihat apakah penggunaan perangkat lunak tersebut telah sesuai kebijakan, dan untuk melihat perangkat lunak mana yang tidak berlisensi, dan memastikan apakah kesalahan dan penyimpangan yang terjadi akan dilaporkan, ditindak lanjuti dan dikoreksi			

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	DS – Delivery and Support			
	Manage Problems (DS10)	Diperiksa oleh Tanggal		DS10

Tujuan:

Memastikan adanya proses penanganan masalah secara efektif, yang melakukan identifikasi dan pengelompokkan masalah, analisis penyebab masalah dan pemecahan masalah, memberikan rekomendasi untuk perbaikan; memelihara catatan permasalahan yang ada dan mereview status tindakan korektif yang dilakukan

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Identification and Classification of Problems			
Mengimplementasikan suatu proses untuk melaporkan dan mengklasifikasikan permasalahan yang ada dilihat dari dampak, urgensi dan prioritas pemecahan	Gangguan layanan TI, permasalahan akan terus berulang, permasalahan dan insiden tidak dapat diselesaikan tepat waktu	Melakukan penilaian apakah terdapat proses yang demikian, dan apakah berjalan efektif atau tidak	
Problem Tracking and Resolution			
Memastikan bahwa sistem pengelolaan masalah menyediakan fasilitas jejak audit yang memadai yang membolehkan untuk melakukan pelacakan, analisis dan menentukan penyebab timbulnya masalah	Proses pemecahan masalah menjadi tidak jelas, tidak terstruktur, mengakibatkan hilangnya informasi dan pada akhirnya mengakibatkan pemborosan biaya dan tidak tepat waktu	Melakukan pengamatan apakah terdapat fasilitas jejak audit yang memadai, dan apakah efektif atau tidak	
Problem Closure			
Mengimplementasikan suatu prosedur untuk menutup/menyudahi penyelesaian masalah	Permintaan belum terselesaikan, makin buruknya layanan, insiden yang penting tidak dapat diselesaikan dengan baik	Melakukan pengamatan apakah terdapat prosedur tersebut, dan apakah efektif atau tidak	
Integration of Configuration, Incident and Problem Management			
Mengintegrasikan proses konfigurasi, penanganan masalah dan insiden untuk menjamin penanganan dan perbaikan masalah secara efektif	Kehilangan informasi, insiden tidak dipecahkan dengan tepat, terganggunya proses bisnis, berkurangnya kepuasan terhadap layanan TI	Melakukan penilaian apakah terdapat proses integrasi tersebut	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**DS – Delivery and Support**	Tanggal		
	Manage Data (DS11)	Diperiksa oleh Tanggal		**DS11**

Tujuan:

Memastikan data dikelola dengan baik, efektif dan tersimpan dengan aman, melalui kombinasi antara pengendalian aplikasi dan umum atas berbagai operasi TI, yang meliputi *media library, backup and recovery*, dan pemusnahan media yang tak terpakai.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Business Requirements for Data Management			
Memverifikasi bahwa semua data yang akan diproses telah diterima dan diproses secara lengkap, akurat dan tepat waktu, dan semua output didistribusikan sesuai dengan kebutuhan organisasi	Data tidak dapat memenuhi kebutuhan organisasi, dan terjadinya pelanggaran keamanan	Melakukan pengamatan bahwa terdapat proses tersebut	
Storage and Retention Arrangements			
Memastikan adanya suatu pendefinisian dan pengimplementasian prosedur penyimpanan data yang efektif dan efisien, yang sesuai dengan tujuan, kebijakan keamanan dan peraturan organisasi	Data tidak dilindungi dari penggunaan yang tidak diotorisasi	Melakukan pengamatan apakah terdapat proses tersebut, dan apakah berjalan efektif atau tidak	
Media Library Management System			
Memastikan adanya suatu pendefinisian dan pengimplementasian prosedur untuk memelihara media penyimpanan untuk menjamin penggunaan dan integritasnya	Integritas media penyimpanan tidak terjamin, tidak terdapat *media backup*, pengaksesan data yang tidak diotorisasi, rusaknya *backup*, tidak dapat menentukan lokasi *media backup*	Melakukan pengamatan apakah terdapat prosedur yang demikian dan apakah berjalan efektif atau tidak	
Disposal			
Memastikan adanya pendefinisian dan pengimplementasian prosedur untuk memastikan bahwa	Pengungkapan informasi organisasi, integritas data yang sensitif tidak terjamin, tidak	Melakukan pengamatan apakah terdapat proses yang demikian dan apakah berjalan efektif atau tidak	

terdapat perlindungan terhadap data dan perangkat lunak yang sensitif ketika data dan perangkat keras dihapus atau dipindah	diotorisasinya pengaksesan data		
Backup and Restoration			
Memastikan adanya pendefinisian dan pengimplementasian prosedur untuk *backup* dan pengembalian (*restoration*) sistem, aplikasi, data dan dokumentasi agar sejalan dengan kebutuhan organisasi dan rencana kontinuitas	Penyebaran informasi organisasi yang seharusnya tidak diungkapan, ketidakmampuan untuk me-*recovery backup data* ketika dibutuhkan, prosedur *recovery* tidak bisa memenuhi kebutuhan organisasi, ketidakmampuan untuk me-*restore* data ketika terjadi kerusakan/bencana, ketidakcukupan waktu untuk melakukan *backup*	Melakukan pengamatan apakah terdapat prosedur *backup* dan *restore*, dan apakah berjalan efektif atau tidak	
Security Requirements for Data Management			
Memastikan terdapat proses untuk mendefinisikan dan mengimplementasikan kebijakan dan prosedur pengamanan dalam hal penerimaan, pemrosesan, penyimpanan data dan penggunaan output	Penyalahgunaan dan perusakan data yang sensitif, pengaksesan data yang tidak diotorisasi, ketidaklengkapan dan ketidakakuratan proses transmisi data serta data diubah oleh pihak yang tidak diberikan otorisasi	Melakukan pengamatan apakah dalam pengelolaan data memperhatikan aspek keamanan	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**DS – Delivery and Support**			
	Manage the Physical Environment (DS12)	Diperiksa oleh Tanggal		**DS12**

Tujuan:

Merancang perlindungan terhadap peralatan komputer dan personel serta penanganan fasilitas fisik dengan baik. Proses penanganan lingkungan fisik meliputi penentuan kebutuhan lokasi fisik, memilih fasilitas yang tepat dan merancang proses yang tepat untuk melakukan monitoring terhadap faktor lingkungan dan akses fisik. Penanganan lingkungan fisik yang efektif akan mengurangi interupsi bisnis akibat rusaknya peralatan komputer dan buruknya personel TI.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Site Selection and Layout			
Memastikan adanya pemilihan dan perancangan lokasi fisik penyimpanan peralatan TI, yang memperhitungkan risiko yang ada misalnya bencana	Meningkatkan risiko kemanan akibat tidak teridentifikasinya ancaman terhadap keamanan fisik	Melakukan pengamatan apakah terdapat proses pemilihan dan perancangan lokasi/site dan apakah telah memperhatikan *building codes*; lingkungan, kebakaran, aliran listrik, kesehatan pegawai, aturan keamanan	
Physical Security Measures			
Memastikan adanya perancangan dan pengimplementasian ukuran keamanan fisik agar sejalan dengan kebutuhan organisasi dan memperhitungkan keamanan lokasi serta aset fisik, terkait dengan pencurian, temperature, kebakaran, asap, air, getaran, teror, perusakan, kekuatan berlebih, kimia dan ledakan	Tidak teridentifikasinya keamanan fisik sehingga perangkat keras dapat dicuri atau digunakan oleh orang yang tidak berhak, peralatan TI dikonfigurasi ulang tanpa otorisasi, informasi rahasia diakses oleh orang yang tidak behak	Melakukan pengamatan dan penilaian apakah terdapat proses yang demikian dan apakah berjalan efektif atau tidak	
Physical Acces			
Memastikan adanya perancangan dan pengimplementasian prosedur untuk memberikan jaminan,	Pengunjung yang tidak diotorisasi dapat mengakses peralatan dan informasi TI dan	Melakukan pengamatan apakah terdapat prosedur yang demikian dan apakah efektif atau tidak	

membatasi, memenuhi kebutuhan organisasi mencakup keadaan darurat, akses ke lingkungan kerja, yang harus diotorisasi, dicatat dan dimonitor, dan diberlakukan bagi semua orang yang akan memasuki area kerja, meliputi staf, staf kontrak, klien, vendor, pengunjung dan pihak ketiga lainnya	*secure areas* dimasukin oleh pihak yang tidak diberikan otorisasi		
Protection Against Environmental Factors			
Memastikan adanya ukuran yang mencukupi untuk perlindungan dengan memperhatikan faktor lingkungan seperti debu, api, dan lain-lain	Fasilitas TI menjadi tidak aman dan tidak terlindung dari bahaya/risiko yang ditimbulkan lingkungan	Melakukan pengamatan apakah terdapat kebijakan yang mendukung perlindungan fasilitas TI	
Physical Facilities Management			
Memastikan adanya pengaturan fasilitas TI agar memperhatikan kesehatan dan keamanan lingkungan dan personil TI	Keamanan dan kesehatan fasilitas TI dan personil TI tidak terlindung dengan baik	Melakukan pengamatan apakah terdapat pengaturan yang demikian	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**DS – Delivery and Support**	Tanggal		
	Manage Operations (DS13)	Diperiksa oleh Tanggal		**DS13**

Tujuan:

Memastikan adanya prosedur manajemen pemrosesan data yang efektif dan pemeliharaan perangkat keras yang baik agar data yang diproses lengkap dan akurat. Prosedur ini meliputi penentuan kebijakan operasi dan prosedur untuk pengaturan jadwal pemrosesan yang efektif, perlindungan terhadap output yang sensitif, memonitor kinerja infrastruktur dan menjamin pemeliharaan perangkat keras. Manajemen operasi yang efektif membantu menjaga integritas data dan mengurangi delay dalam proses bisnis dan mengurangi biaya operasi TI

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Operations Procedures and Instructions			
Memastikan adanya prosedur operasional TI, yang mencerminkan tugas staf operasional TI, mampu mengatasi jika staf mengalami perpindahan jadwal kerja dan mengatasi masalah operasional yang ditimbulkan oleh TI	Terjadi kesalahan kerja sehingga memerlukan pengerjaan ulang akibat salah memahami prosedur operasional TI; ketidakefisienan akibat prosedur yang tidak jelas atau tidak standar; ketidakmampuan dalam penanganan masalah operasional akibat adanya perpindahan jadwal kerja atau pergantian staf	Melakukan pengamatan dan penilaian apakah terdapat prosedur operasional TI	
Job Scheduling			
Memastikan adanya jadwal pemrosesan pekerjaan dengan urutan yang sangat efisien	Permasalahan dalam mengatur jadwal jika ada pekerjaan khusus/di luar yang biasa, atau ada pekerjaan yang memerlukan pemrosesan ulang	Melakukan penilaiaan apakah terdapat jadwal pemrosesan pekerjaan yang efektif dan efisien	
IT Infrastructure Monitoring			
Memastikan diimplementasikannya suatu prosedur untuk memonitor infrastruktur TI dan *event-event* yang terkait, dimana kronologis informasi disimpan dalam file *operation*	Tidak terdeteksinya permasalah dan insiden terkait infrastruktur TI yang berdampak terhadap proses bisnis organisasi	Melakukan pengamatan dan penilaian apakah terdapat prosedur monitoring terhadap	

logs sehingga memungkinkan dilakukannya rekonstruksi, review dan pengujian terhadap deretan operasi yang ada		infrastruktur TI yang ada, dan apakah berjalan efektif atau tidak	
Sensitive Documents and Output Devices			
Memastikan adanya suatu perlindungan secara fisik terhadap aset TI yang sensitif salah satunya berupa pencatatan akuntansi dan manajemen *inventory* aset TI dengan baik	Penyalahgunaan aset TI yang sensitif yang mengakibatkan kerugian finansial dan ketidakmampuan untuk mencatat semua aset TI yang sensitif	Melakukan pengamatan dan penilaian bahwa terdapat perlindungan aset TI yang sensitif	
Preventive Maintenance for Hardware			
Memastikan adanya prosedur yang memelihara dan menjaga infrastruktur TI agar dapat mengurangi terjadinya kegagalan proses TI dan menurunnya kinerja TI	Ketidakmampuan mencegah timbulnya masalah infrastruktur	Melakukan pengamatan apakah terdapat prosedur pemeliharaan infrastruktur TI	

PT Bank XYZ		Disiapkan oleh Tanggal		Program Audit
Proses :	**ME – Monitor and Evaluate**			
	Monitor and Evaluate IT Performance (ME1)	Diperiksa oleh Tanggal		**ME1**

Tujuan:

Memastikan adanya monitoring terhadap efektifitas kinerja TI dengan pendefinisian indikator kinerja yang relevan, sistematis dan tepat waktu dan melakukan tindakan untuk mengatasi tindakan penyimpangan yang terjadi, agar didapat suatu kepastian bahwa kinerja TI telah sejalan dengan tujuan dan kebijakan organisasi.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Monitoring Approach			
Memastikan adanya kerangka monitoring yang menyeluruh dengan suatu pendekatan yang mendefinisikan ruang lingkup, metodologi dan proses yang harus diikuti untuk mengukur solusi TI dan *service delivery* dan memonitor kontribusi TI bagi organisasi	Laporan kinerja yang didasarkan pada data yang tidak akurat dan tidak terpercaya, kurangnya pengidentifikasian isu-isu terkait TI dan data hasil monitoring tidak dapat dijadikan dasar dalam menganalisis kinerja TI	Melakukan pengamatan dan penilaian apakah terdapat pendekatan yang demikian dalam melakukan monitoring	
Definition and Collection of Monitoring Data			
Memastikan adanya prosedur yang mendefinisikan dan mengumpulkan data untuk dimonitor berdasarkan target kinerja yang diinginkan dan disetujui oleh seluruh *stakeholder*	Laporan kinerja TI berdasarkan beberapa indikator yang tidak efektif, data yang telah dimonitor tidak dapat mendukung dalam melakukan analisis terhadap kinerja TI	Melakukan pemahaman apakah terdapat prosedur yang demikian, dan apakah berjalan efektif atau tidak	
Monitoring Method			
Memastikan adanya metode monitoring kinerja (misalnya *balance scorecard*), yang meliputi target, ukuran, dan ringkasan kinerja; sudut pandang terhadap kinerja TI	Laporan kinerja TI yang tidak mencerminkan kinerja TI yang sesungguhnya dan pengambilan keputusan yang salah yang didasarkan informasi kinerja yang tidak handal	Melakukan pengamatan apakah terdapat metode monitoring kinerja yang demikian, dan apakah efektif atau tidak	
Performance Assessment			
Memastikan apakah dilakukan review secara periodik untuk:	Lemahnya kinerja TI, tidak ada tindakan	Melakukan penilaian apakah	

menilai apakah kinerja TI telah mencapai target; menganalisis penyebab terjadinya penyimpangan; dan menilai tindakan perbaikan yang dilakukan	perbaikan terhadap kinerja TI yang buruk	terdapat proses review yang demikian dan apakah berjalan efektif atau tidak	
Board and Executive Reporting			
Memastikan adanya laporan mengenai kontribusi TI bagi proses bisnis organisasi, apakah tujuan organisasi berhasil dicapai, anggaran TI berhasil digunakan dengan baik, dan apakah risiko TI berhasil dihilangkan	Pimpinan tidak puas terhadap performa TI, yang dapat diakibatkan pimpinan tidak dapat mengendalikan aktifitas TI	Melakukan penilaian apakah terdapat laporan kontribusi TI bagi para pimpinan	
Remedial Actions			
Memastikan adanya proses untuk mengidentifikasi dan inisiasi tindakan perbaikan yang didasarkan pada hasil monitoring, penilaian (assessment) dan laporan kinerja TI	Timbulnya kesalahan akibat permasalahan yang tidak berhasil dipecahkan, dan kinerja TI yang buruk tidak ditanggapi dengan serius	Melakukan penilaian apakah terdapat proses yang demikian	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**ME – Monitor and Evaluate**	Tanggal		
	Monitor and Evaluate Internal Control (ME2)	Diperiksa oleh Tanggal		**ME2**

Tujuan:

Memastikan adanya proses monitoring dan pelaporan terhadap pengendalian internal TI, untuk menjamin bahwa terdapat proses operasi yang efektif dan efisien yang mematuhi hukum dan aturan yang berlaku

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref
Monitoring of Internal Control Framework			
Memastikan adanya kerangka proses monitoring yang dilakukan secara kontinyu, proses *benchmark* dan perbaikan terhadap lingkungan pengendalian TI dan kerangka pengendalian agar sesuai dengan tujuan organisasi	Meningkatkan dampak buruk bagi organisasi, kelemahan pengendalian mengakibatkan tidak terdeteksinya fungsi TI yang salah	Melakukan pengamatan dan penilaian apakah terdapat kerangka proses monitoring	
Supervisory Review			
Memastikan adanya proses monitoring dan evaluasi terhadap efisiensi dan efektifitas dari review pengendalian internal TI	Pengendalian yang tidak akurat dan tidak lengkap akan menurunkan kualitas data yang mengakibatkan kesalahan dalam pengambilan keputusan yang dilakukan oleh manajemen sehingga akan menghambat proses bisnis	Melakukan pengamatan dan penilaian apakah terdapat proses yang demikian	
Control Exceptions			
Memastikan adanya proses untuk mengidentifikasi dan menganalisis pengendalian terhadap kelainan yang terjadi dan penyebab kelainan tersebut serta tindakan korektifnya	Kekurangan dalam hal pengendalian tidak diketahui oleh manajemen TI dan tidak dapat diidentifikasi secara tepat waktu sehingga membutuhkan waktu lebih lama untuk menyelesaikan isu pengendalian tersebut	Melakukan pemahaman dan penilaian bahwa terdapat proses yang demikian	

	yang akibatnya akan menurunkan kinerja TI		
Control Self-assessment			
Memastikan adanya proses penilaian (*self assessment*) terhadap kelengkapan dan keefektifan pengendalian proses TI serta kebijakan dan kontrak yang telah disepakati	Kelemahan pengendalian tidak dapat diidentifikasi secara tepat waktu sehingga membutuhkan waktu lebih lama untuk menyelesaikan isu pengendalian tersebut yang akibatnya akan menurunkan kinerja TI	Melakukan pengamatan apakah terdapat penilaian terhadap pengendalian yang ada	
Assurance of Internal Control			
Memastikan apakah terdapat kebijakan untuk melakukan *assurance* terhadap kelengkapan dan keefektifan pengendalian internal	Semua proses TI tidak dapat dikendalikan secara efektif yang diakibatkan tidak dipatuhinya peraturan dan kontrak yang berlaku sehingga tujuan organisasi tidak tercapai	Melakukan pengamatan apakah terdapat kebijakan untuk melakukan *assurance* terhadap pengendalian internal	
Internal Control at Third Parties			
Memastikan adanya prosedur pengendalian internal terhadap pihak ketiga yang memadai untuk menjamin bahwa pihak ketiga telah mematuhi peraturan dan hukum yang berlaku serta perjanjian kontrak yang telah disepakati	Tidak memadainya pengendalian terhadap pihak ketiga sehingga layanan TI menjadi menurun dan tidak dapat memenuhi kebutuhan organisasi	Melakukan penilaian ketercukupan pengendalian internal terhadap pihak ketiga	
Remedial Actions			
Memastikan adanya proses identifikasi, inisiasi, pelacakan dan pengimplementasian *remedial action* sebagai tindak lanjut dari penilaian dan pelaporan terhadap pengendalian internal yang ada	Rusaknya reputasi organisasi akibat gagalnya memperbaiki pengendalian terhadap pihak ketiga	Melakukan pengamatan apakah terdapat proses yang demikian	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**ME – Monitor and Evaluate**	Tanggal		**ME3**
	Ensure Compliance with External Requirements (ME3)	Diperiksa oleh Tanggal		

Tujuan:

Memastikan adanya review kepatuhan terhadap hukum, aturan dan kontrak yang berlaku.

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Identification of External Legal, Regulatory and Contractual Compliance Requirement (ME3.1)			
Memastikan adanya proses pengidentifikasian hukum dan peraturan internasional agar sejalan dengan kebijakan, standar, prosedur dan metodologi TI yang berlaku di organisasi	Tidak mematuhi hukum atau peraturan yang berlaku yang berakibat mengurangi kepuasan pengguna	Melakukan penilaian apakah terdapat proses yang demikian	
Optimisation of Response to External Requirements (ME3.2)			
Mereview kebijakan, standar, prosedur dan metodologi TI apakah telah sesuai dengan hukum, peraturan dan kontrak yang telah disepakati	Tidak dipatuhinya hukum, peraturan dan kontrak yang telah disepakati berakibat tidak tercapainya tujuan organisasi	Melakukan pengamatan apakah terdapat proses review yang demikian	
Evaluation of Compliance With External Requirements (ME3.3)			
Memastikan apakah kebijakan, standar, prosedur dan metodologi TI telah mematuhi hukum dan aturan yang berlaku	Mendapat sanksi dan mengalami kerugian finansial, pengguna menjadi tidak puas sehingga berdampak buruk bagi kinerja dan reputasi organisasi	Melakukan penilaian apakah kebijakan, standar, prosedur dan metodologi telah mematuhi hukum dan aturan yang berlaku	
Positive Assurance of Compliance (ME3.4)			
Memastikan adanya proses yang melaporkan hasil penilaian (*assurance*) kepatuhan dan ketaatan terhadap kebijakan, hukum dan peraturan baik dari dalam (internal) maupun dari luar (eksternal)	Ketidakpatuhan terhadap peraturan yang berlaku tidak dilaporkan yang berakibat menurunkan reputasi dan kinerja organisasi serta tidak dilakukannya tindakan korektif secara tepat waktu	Melakukan pengamatan bahwa terdapat proses yang demikian	

Integrated Reporting (ME3.5)			
Memastikan adanya laporan TI yang terintegrasi dengan hukum, dan peraturan yang berlaku serta kontrak yang telah disepakati	Tidak terintegrasinya laporan TI dengan hukum dan peraturan yang berlaku, serta kontrak yang telah disepakati mengakibatkan pimpinan salah dalam mengambil keputusan	Melakukan penilaian apakah laporan TI telah terintegrasi dengan hukum dan peraturan yang berlaku, serta kontrak yang telah disepakati	

PT Bank XYZ		Disiapkan oleh		Program Audit
Proses :	**ME – Monitor and Evaluate**	Tanggal		**ME4**
	Provide IT Governance (ME4)	Diperiksa oleh		
		Tanggal		

Tujuan:

Memastikan adanya suatu kerangka tata kelola TI yang efektif yang mencakup pendefinisian struktur organisasi TI, proses-proses dalam organisasi TI tersebut, kepemimpinan, tugas dan tanggung jawab masing-masing personil TI untuk memastikan bahwa investasi yang dilakukan dalam bidang TI sejalan dengan tujuan dan strategi organisasi

Tujuan Pengendalian	Dampak	Hal yang Dilakukan	Ref.
Establishment of an IT Governance Framework (ME4.1)			
Memastikan adanya pembangunan kerangka tata kelola TI yang sejalan dengan tata kelola organisasi dan lingkungan pengendalian yang ada	Proses TI tidak dapat dipertanggungjawabkan, portfolio TI tidak mampu mendukung tujuan dan strategi organisasi, tidak dilakukan tindakan untuk memperbaiki proses TI, dan pengendalian TI tidak berfungsi sebagaimana mestinya	Melakukan penilaian apakah terdapat kerangka tata kelola TI yang demikian	
Strategic Alignment (ME4.2)			
Memastikan adanya semacam komite strategi TI yang dapat memberikan arahan tentang strategi TI yang baik kepada manajemen agar dapat mendukung tujuan organisasi dan dapat mendapatkan manfaat dari investasi TI yang dilakukan	Investasi TI yang tidak efektif akibat dari gagalnya TI mendukung pencapaian tujuan organisasi dan rencana strategi TI tidak sejalan dengan strategi organisasi	Melakukan penilaian apakah para pimpinan memahami isu strategis TI dan adanya komite strategi TI atau semacamnya	
Value Delivery (ME4.3)			
Memastikan terdapat pengelolaan investasi, aset dan layanan TI, sehingga dapat mendukung strategi dan tujuan organisasi dan memberikan *value*/manfaat bagi organisasi	Aset dan layanan TI tidak dapat memberikan *value* dan manfaat yang diinginkan sehingga mengurangi kepuasan pengguna dan investasi TI menjadi sia-sia	Melakukan penilaian apakah investasi dikelola sedemikian rupa sehingga dapat memberikan *value*/manfaat yang diharapkan	
Resource Management (ME4.4)			
Mengatur investasi, penggunaan dan pengalokasian sumber daya TI dengan melakukan	Kemampuan personil dan tidak memadainya sumber daya sehingga tidak mampu mewujudkan strategi dan	Melakukan penilaian apakah terdapat manajemen sumber daya yang demikian	

assessment secara regular terhadap gagasan-gagasan dan operasi TI	tujuan organisasi		
Risk Management (ME4.5)			
Memastikan bahwa terdapat manajemen risiko, dimana terdapat penilaian risiko TI dan dampaknya bagi organisasi serta penanganannya	Pengidentifikasian dan pengelolaan risiko yang tidak efektif sehingga akan meningkatkan pengeluaran/biaya, gagalnya layanan aplikasti TI yang penting	Melakukan penilaian apakah terdapat manajemen risiko dan apakah berjalan efektif atau tidak	
Performance Measurement (ME4.6)			
Memastikan adanya pengukuran terhadap kinerja TI yang akan dilaporkan ke para pimpinan	Kinerja yang buruk tidak dapat diidentifikasi dan dicari penyelesaiannya secara tepat waktu	Melakukan penilaian apakah terdapat pengukuran terhadap kinerja TI	
Independent Assurance (ME4.7)			
Memastikan adanya *independent assurance* terhadap kesesuaian TI dengan hukum dan aturan yang berlaku; kebijakan, standar dan prosedur organisasi; praktek TI yang biasa dilakukan; dan kinerja TI yang efektif dan efisien	Kegagalan dalam mendeteksi atau mencegah penurunan kinerja layanan TI akibat dari ketidakefektifan tata kelola TI, manajemen risiko dan pengendalian internal, serta perilaku yang tidak etis	Melakikan pengamatan apakah terdapat *independent assurance* yang demikian, dan apakah berjalan efektif atau tidak	

LAMPIRAN 4

Sumber atas Lampiran 4 Kuisioner ini berasal dari Karya Akhir berjudul Audit TI Menggunakan COBIT 4.1 di Direktorat Jenderal Anggaran Departemen Keuangan – oleh Risnawati Kumala Dewi, Program Magister Akuntansi FEUI, Mei 2009, yang sudah disesuaikan dengan kondisi PT Bank XYZ, yang berdasarkan dari IT Assurance Guide, ITGI.

PT Bank XYZ		Disiapkan oleh :		**No Dokumen**
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		**KK-PO1**
Tanggal		Tanggal :		
Proses :	**Define a Strategic Information Technology Plan (PO1)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebijakan dan prosedur Perusahaan atau TI mencakup suatu pendekatan perencanaan yang terstruktur?	√		
2	Apakah terdapat suatu metodologi untuk memformulasikan dan memodifikasi rencana-rencana, yang mencakup:			
	• misi dan tujuan Perusahaan	√		
	• usaha-usaha TI untuk mendukung misi dan tujuan Perusahaan	√		
	• peluang-peluang untuk melakukan aktifitas TI	√		
	• studi kelayakan TI	√		
	• penilaian risiko dari aktifitas TI	√		
	• investasi yang optimal dari investasi TI pada saat ini dan yang akan datang	√		
	• *re-engineering* dari aktifitas TI untuk merefleksikan perubahan-perubahan Perusahaan	√		
	• evaluasi dari strategi alternatif untuk aplikasi, teknologi dan Perusahaan	√		
3	Apakah dipertimbangkan berbagai hal yang meliputi: perubahan-perubahan yang berhubungan dengan organisasi, evolusi teknologi, kebutuhan-kebutuhan peraturan, *business process engineering*, penentuan staf/personil, *in-sourcing* dan *out-sourcing* dan secara memadai tercakup dalam proses perencanaan?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
4	Apakah terdapat rencana jangka panjang dan jangka pendek TI yang memadai mencakup Perusahaan, semua misi, dan fungsi-fungsi bisnis yang penting dan utama?	√		
5	Apakah berbagai proyek TI didukung oleh pendokumentasian yang tepat seperti yang diidentifikasi dalam metodologi perencanaan TI?	√		
6	Apakah terdapat *checkpoint* untuk memastikan bahwa tujuan TI dan rencana jangka panjang serta jangka pendek TI tetap sesuai dengan tujuan Perusahaan dan rencana jangka panjang serta jangka pendek Perusahaan?	√		
7	Apakah terdapat review dan persetujuan atas rencana TI oleh *process owner* atau pimpinan?	√		
8	Apakah rencana TI menilai sistem informasi yang ada saat ini, yang meliputi: tingkat otomatisasi bisnis, fungsionalitas, stabilitas, kompleksitas, biaya, kekuatan dan kelemahan?	√		
9	Terdapat prosedur standar penanganan kasus beserta monitoringnya	√		
10	Selalu dilakukan review terhadap keberhasilan dan kegagalan investasi TI serta analisis kasus terus ditingkatkan seperti yang diinginkan (contoh: data-data sebelumnya harus dianalisis dan diperbaiki dengan mengacu pada *best practice*)	√		
11	Manajemen TI ikut bertanggung jawab (akuntabilitas) dalam mencapai tujuan organisasi, dengan melakukan *what if analyses* serta memiliki komitmen yang tinggi dalam mendukung pencapaian tujuan organisasi.	√		
12	Proses bisnis dan TI pendukungnya memiliki pandangan yang sama terhadap sistem, mencakup pandangan mengenai pentingnya TI, penggunaan TI dan pelaporan TI	√		
13	Kriteria yang tepat, standar dan indikator performa telah dibangun dan digunakan untuk menilai dan melaporkan performa kepada pimpinan dan *stakeholder* utama. Terdapat rencana tindakan yang akan diambil terhadap proses yang menyimpang	√		
14	Terdapat review berkaitan dengan pencapaian target yang sebelumnya dan telah dituangkan dalam suatu strategi TI	√		

No	Pertanyaan	Ya	Tidak	Keterangan
15	Dilakukan *benchmarking* untuk menilai keberadaan dan kemampuan sistem.	√		
16	Adanya suatu proses akan memberikan outcome yang terukur yang digambarkan oleh metrics (apa) dan target (berapa banyak), tujuan TI akan tercapai dan memberikan manfaat bagi organisasi	√		
17	Terdapat review kebijakan dan prosedur yang ada untuk menentukan apakah kebijakan dan prosedur akan mendukung rencana strategi TI	√		
18	Terdapat rencana taktis TI yang terstruktur yang didasarkan pada rencana strategik TI, jika rencana strategik diupdate maka rencana taktis pun akan diupdate	√		
19	Rencana taktis TI berisi definisi project, informasi perencanaan, deliverable, dan manfaat yang dapat diukur, dan telah memperhitungkan risiko yang mungkin terjadi	√		
20	Terdapat suatu proses identifikasi program TI dan proyek-proyek yang mendukung rencana taktis TI	√		
21	Tujuan dan sasaran organisasi yang diharapkan telah didokumentasikan dan terdapat informasi yang tepat terkait dengan anggaran dan usaha yang dilakukan	√		
22	Program dan sasaran project telah dikomunikasikan secara jelas ke semua stakeholder	√		
23	Staf TI mengetahui arah dan tujuan organisasi, tujuan jangka pendek dan jangka panjang, misi dan nilai yang ingin dicapai	√		
24	Laporan sistem informasi yang ada saat ini (mencakup *feedback* sistem, penggunaan sistem yang telah diperbaiki) dipelihara dengan baik.	√		
25	Risiko dan biaya yang timbul akibat penggunaan TI telah terdokumentasi dalam rencana strategis TI	√		
26	*Outcome* yang diperoleh (yang mendatangkan manfaat bagi organisasi) telah diketahui oleh seluruh *stakeholder* dan *feedback* dari stakcholder merupakan suatu hal yang menjadi pertimbangan	√		
27	Rencana strategik TI telah disetujui oleh *IT steering committee*	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO2
Tanggal		Tanggal :		
Proses :	**Define the Information Architecture (PO2)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebijakan dan prosedur TI mencakup pengembangan dan pemeliharaan kamus data (*data dictionary*)?	√		
2	Apakah proses yang digunakan untuk memperbarui model arsitektur informasi didasarkan atas rencana jangka panjang dan jangka pendek?		√	Berdasarkan kebutuhan bisnis.
3	Masih berhubungan dengan pertanyaan sebelumnya, dan apakah proses tersebut mempertimbangkan biaya dan risiko yang mungkin timbul, serta memastikan bahwa persetujuan pimpinan diperoleh sebelum dilakukan perubahan pada arsitektur informasi?	√		
4	Apakah proses yang digunakan untuk memelihara kamus data (*data dictionary*) dan syntax data (*data syntax*) *up to date*?	√		
5	Apakah kebijakan dan prosedur TI mencakup klasifikasi data, yang meliputi berbagai kategori keamanan dan kepemilikan data, serta aturan akses bagi berbagai kelompok data telah didefinisikan secara jelas dan tepat?	√		
6	Apakah terdapat standar-standar yang mendefinisikan klasifikasi yang berlaku (*default*) bagi aset data yang tidak ada/memiliki suatu pengidentifikasi (*identifier*) klasifikasi data?	√		
7	Apakah kebijakan dan prosedur TI mencakup/memenuhi hal-hal berikut: • terdapat proses otorisasi yang mengharuskan pemilik data (seperti yang didefinisikan dalam kebijakan	√ √		

No	Pertanyaan	Ya	Tidak	Keterangan
	kepemilikan data) memberikan otorisasi seluruh akses ke data			
	• tingkat keamanan didefinisikan secara jelas untuk tiap-tiap klasifikasi data	√		
	• tingkat akses didefinisikan secara jelas, dan tepat/sesuai untuk klasifikasi data	√		
8	Organisasi memiliki model informasi dengan standar yang telah ditentukan dan diketahui oleh seluruh pihak dalam organisasi tersebut, termasuk berbagai pihak yang memiliki kepentingan terhadap TI	√		
9	Model informasi tersebut dapat digunakan dan dipelihara secara efektif dan sejalan dengan proses yang menterjemahkan strategi TI menjadi rencana taktis TI dan mengimplementasikan rencana taktis tersebut ke dalam suatu proyek	√		
10	Informasi akan selalu tersedia dan akan bermanfaat untuk mendukung proses pengambilan keputusan	√		
11	Terdapat review terhadap skema klasifikasi data untuk memverifikasi apakah semua komponen telah ada dan lengkap, dan apakah skema tersebut mampu menyeimbangkan biaya dan risiko yang muncul. Skema klasifikasi data ini mencakup kepemilikan data serta penentuan ukuran *security* yang tepat yang didasarkan pada level klasifikasi data	√		
12	Terdapat program yang akan menilai kualitas data, hal ini dilakukan untuk memastikan bahwa integritas dan konsistensi data terjaga dengan baik	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO3
Tanggal		Tanggal :		
Proses :	**Determine Technological Direction (PO3)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat suatu proses penciptaan dan pembaruan secara teratur dari rencana infrastruktur teknologi?	√		
2	Masih berhubungan dengan pertanyaan sebelumnya, dan apakah proses tersebut mengkonfirmasikan bahwa setiap perubahan diusulkan diuji terlebih dahulu untuk menilai biaya dan risikonya, serta perubahan terhadap rencana infrastruktur teknologi dilakukan setelah mendapat persetujuan dari pimpinan?	√		
3	Apakah rencana infrastruktur teknologi diperbandingkan dengan rencana jangka panjang dan jangka pendek TI?	√		
4	Apakah terdapat suatu proses untuk mengevaluasi status teknologi pada saat sekarang, untuk memastikan bahwa teknologi Perusahaan mencakup berbagai aspek seperti: arsitektur sistem, arah teknologi dan strategi migrasi?	√		
5	Apakah kebijakan dan prosedur TI memastikan pemenuhan kebutuhan untuk mengevaluasi dan memantau kecenderungan teknologi pada saat ini dan saat yang akan datang, serta memperhatikan berbagai kondisi peraturan yang ada?	√		
6	Apakah terdapat perencanaan atas pengaruh logistik dan lingkungan dari akuisisi teknologi?	√		
7	Apakah kebijakan dan prosedur TI memastikan dipenuhinya kebutuhan untuk menilai secara sistematik rencana teknologi untuk aspek kontinjensi, seperti: *redundancy*	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	(berhubungan dengan kapasitas yang tidak terpakai), *resilience* (kemampuan untuk pulih kembali), *adequacy* (kecukupan) dan *evolutionary capability* (kemampuan berubah/berevolusi) dari infrastruktur?			
8	Apakah manajemen TI mengevaluasi teknologi yang muncul (*emerging technology*), dan mengambil/memasukkan teknologi yang tepat ke dalam infrastruktur TI yang ada pada saat sekarang?	√		
9	Apakah rencana akuisisi perangkat keras dan perangkat lunak sesuai dengan kebutuhan yang diidentifikasi dalam rencana infrastruktur teknologi?	√		
10	Apakah terdapat standar-standar teknologi bagi berbagai komponen teknologi yang digambarkan dalam infrastruktur teknologi?	√		
11	Perencanaan infrastruktur teknologi didasarkan pada strategi TI dan rencana taktis TI yang telah dibuat	√		
12	Perencanaan infrastruktur teknologi telah menampung teknologi yang terintegrasi, arsitektur sistem dan aspek tak terduga dari komponen infrastruktur, biaya transisi dan biaya lainnya, kompleksitas, risiko teknis, nilai fleksibilitas di masa mendatang, daya tahan produk dan arah akuisisi aset TI	√		
13	Strategi TI dan perencanaan infrastruktur teknologi sejalan dengan pengembangan TI yang dilakukan	√		
14	Terdapat *technology guideline* yang benar-benar mendukung solusi teknologi, dan secara tepat menggambarkan arah perkembangan teknologi organisasi dan secara luas memberikan arahan pemecahan berbagai masalah TI	√		
15	Apakah terdapat bagian yang menangani arsitektur TI yang benar-benar menyadari peran dan tanggung jawabnya?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO4
Tanggal		Tanggal :		
Proses :	**Define the Information Technology Organisation dan Relationship (PO4)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Terdapat suatu kerangka proses TI untuk melaksanakan rencana strategi TI. Kerangka ini memuat struktur dan hubungan antar proses TI	√		
2	Terdapat suatu komite strategi TI untuk memastikan bahwa tata kelola TI merupakan bagian dari tata kelola organisasi yang harus diterapkan dan memberikan arahan strategi TI yang harus dijalankan oleh Perusahaan	√		
3	Semua anggota komite strategi TI telah mengerti dan memahami tanggung jawab, dan peranannya untuk memastikan bahwa mereka tidak menyimpang dari strategi organisasi	√		
4	Apakah keanggotaan dan fungsi dari *IT planning/steering committee* secara jelas didefinisikan, dan tanggung jawabnya juga diidentifikasi?	√		
5	Apakah pernyataan tertulis (*charter)* dari *IT planning/steering committee* menyesuaikan tujuan komite dengan tujuan Perusahaan dan rencana jangka panjang dan jangka pendek, serta dengan tujuan TI baik dalam jangka panjang dan jangka pendek?	√		
6	Apakah terdapat suatu proses untuk meningkatkan kesadaran, pemahaman dan keahlian dalam mengidentifikasi dan memecahkan isu-isu manajemen informasi?	√		
7	Apakah terdapat proses dan indikator kinerja untuk menentukan efektifitas dari fungsi TI?	√		
8	Apakah kebijakan dan komunikasi dari pimpinan sudah memastikan independensi dan otoritas dari fungsi TI	√		

No	Pertanyaan	Ya	Tidak	Keterangan
9	Apakah terdapat kebijakan yang memenuhi kebutuhan akan evaluasi dan modifikasi dari struktur organisasi untuk menyesuaikan dengan tujuan dan keadaan/kondisi yang berubah?	√		
10	Apakah terdapat kebijakan yang menerangkan/menjelaskan peran dan tanggung jawab seluruh personel dalam organisasi, yang berhubungan dengan sistem informasi, pengendalian internal dan keamanan?	√		Sedang dalam proses pengerjaan
11	Apakah pimpinan secara periodik melakukan review terhadap deskripsi peran dan tanggung jawab para personel TI.	√		
12	Apakah pimpinan memastikan bahwa peran dan tanggung jawab dilaksanakan dengan baik oleh para personel TI?	√		
13	Apakah terdapat kampanye/pemberitahuan yang teratur untuk meningkatkan kesadaran pengendalian internal dan keamanan serta disiplin?	√		
14	Apakah terdapat kebijakan dan fungsi untuk melakukan *quality assurance* (jaminan kualitas) terhadap semua aktifitas TI?	√		
15	Apakah fungsi *quality assurance* memiliki independensi yang mencukupi?	√		
16	Apakah dalam melakukan fungsi *quality assurance* terdapat proses untuk menentukan personel yang mempunyai kompetensi dan keahlian memadai dalam menjalankan tanggung jawabnya?	√		
17	Apakah terdapat proses dalam *quality assurance* untuk menentukan program/merencakan sumber daya, dan untuk memastikan penyelesaian dari pengujian dan persetujuan *quality assurance* sebelum sistem baru atau sistem yang mengalami perubahan diimplementasikan?	√		
18	Apakah DTI secara formal memberikan tanggung jawab tingkat organisasi untuk memformulasikan pengendalian internal dan kebijakan serta prosedur keamanan (logika dan fisik) kepada *security officer*?	√		
19	Apakah kebijakan keamanan Perusahaan secara jelas mendefinisikan tanggung jawab bagi keamanan informasi, dan tiap-tiap	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	pemilik (*owner*) aset informasi diharuskan untuk melaksanakannya?			
20	Apakah terdapat kebijakan dan prosedur yang mencakup kepemilikan data dan sistem bagi seluruh sumber data utama dan sistem?	√		Sedang dalam proses pengerjaan
21	Apakah terdapat prosedur untuk melakukan review dan memelihara berbagai perubahan pada kepemilikan data dan sistem secara teratur?	√		
22	Apakah terdapat kebijakan dan prosedur yang menggambarkan praktik-praktik pengawasan terhadap fungsi TI, untuk memastikan bahwa peran dan tanggung jawab secara tepat dilaksanakan?	√		
23	Apakah hasil temuan dari proses pengawasan dibicarakan dan di- *followed up?*	√		
24	Apakah seluruh personel memiliki otoritas dan sumber daya yang mencukupi untuk melaksanakan peran dan tanggung jawab mereka?	√		
25	Apakah terdapat pemisahan tugas antara: • pengembangan sistem dan pemeliharaan • pengembangan sistem dan operasi • pengembangan sistem/pemeliharaan dan keamanan informasi • operasi dan pengendalian data • operasi dan pemakai (user) • operasi dan keamanan informasi	 √ √ √ √ √ √		
26	Apakah penentuan personel TI dan kompetensi dipelihara untuk memastikan kemampuannya dalam memberikan solusi-solusi teknologi yang efektif?	√		
27	Apakah terdapat kebijakan dan prosedur untuk melakukan evaluasi kembali dari deskripsi posisi (pekerjaan) TI?	√		Sedang dalam proses pengerjaan
28	Apakah terdapat suatu metodologi untuk mengukur performa personel TI?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
29	Apakah DTI Sedang dalam proses pengerjaan memiliki prosedur formal dalam menangani proses TI, yang meliputi perumusan tindakan-tindakan untuk menghadapi kejadian di luar dugaan, pendokumentasian pengetahuan yang penting, pelatihan bagi personel TI, transfer tanggung jawab, dsb, sehingga jika personel yang bertanggung jawab terhadap suatu proses/personel utama berhalangan hadir, maka personel lain dapat menggantikannya?	√		Sedang dalam proses pengerjaan
30	Apakah terdapat peran dan tanggung jawab yang tepat bagi proses-proses penting, termasuk aktifitas-aktifitas siklus hidup pengembangan sistem (*system development life cycle*), keamanan informasi, akuisisi dan perencanaan kapasitas?	√		
31	Apakah terdapat KPI (*Key Performance Indicator*) dan KSF (*Key Success Factor*) yang tepat dan efektif dalam mengukur hasil-hasil dari fungsi TI dalam mencapai tujuan Perusahaan?	√		Sedang dalam proses pengerjaan
32	Apakah terdapat kebijakan dan prosedur TI untuk mengendalikan berbagai aktifitas konsultan dan personel kontrak untuk memastikan perlindungan dari aset Perusahaan?	√		Sedang dalam proses pengerjaan
33	Apakah terdapat prosedur-prosedur yang dapat diterapkan pada jasa TI kontrakan untuk kecukupan dan konsistensi dengan kebijakan akuisisi yang dimiliki oleh Perusahaan?	√		Sedang dalam proses pengerjaan
34	Apakah terdapat proses-proses untuk mengkoordinasikan, mengkomunikasikan dan mendokumentasikan berbagai kepentingan baik pihak dalam maupun pihak luar dari fungsi TI?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO5
Tanggal		Tanggal :		
Proses :	**Manage the Information Technology Investment (PO5)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Terdapat suatu *financial framework* atau semacamnya untuk mengendalikan investasi dan biaya yang ditimbulkan oleh aset TI dan layanannya	√		
2	Apakah terdapat kebijakan dan prosedur untuk memastikan persiapan dan persetujuan dari sebuah anggaran operasi TI tahunan Perusahaan serta rencana jangka panjang dan jangka pendek Perusahaan?	√		Sedang dalam proses pengerjaan
3	Apakah terdapat kebijakan dan prosedur untuk memastikan bahwa anggaran operasi TI tahunan konsisten/sesuai dengan rencana jangka panjang dan jangka pendek TI?	√		
4	Apakah proses dari sebuah anggaran melibatkan partisipasi manajemen dari unit-unit utama fungsi TI, khususnya dalam persiapannya?	√		
5	Apakah terdapat kebijakan dan prosedur untuk secara teratur mengawasi biaya aktual dan membandingkannya dengan biaya yang diproyeksikan?	√		
6	Masih berhubungan dengan pertanyaan sebelumnya, apakah penentuan/perhitungan biaya aktual tadi didasarkan atas sistem akuntansi biaya Perusahaan?	√		
7	Apakah terdapat kebijakan dan prosedur untuk menjamin bahwa jasa yang diberikan oleh fungsi TI dijelaskan/dibuktikan dalam hal biaya, dan memiliki kesesuaian dengan biaya rata-rata pada umumnya?	√		Sedang dalam proses pengerjaan
8	Apakah terdapat dukungan yang memadai dalam anggaran TI, dalam menjelaskan/membuktikan rencana operasi	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	tahunan TI?			
9	Apakah kategori pengeluaran TI bersifat komprehensif, sesuai dan dikelompokkan secara tepat?	√		
10	Apakah terdapat suatu praktek untuk menyiapkan suatu anggaran yang menggambarkan prioritas investasi TI yang harus dilakukan yang mencakup biaya operasional dan pemeliharaan infrastruktur saat ini? Praktek ini mendukung pengembangan seluruh anggaran TI seperti anggaran untuk program-program individu dengan penekanan pada komponen TI?	√		
11	Apakah terdapat sistem yang memadai dalam hal pencatatan secara rutin, pemrosesan, dan pelaporan atas biaya yang berhubungan dengan aktifitas-aktifitas dari fungsi TI?	√		
12	Apakah terdapat suatu metode untuk menganalisis dan mengumpulkan data-data yang menyimpang?	√		
13	Apakah terdapat suatu analisis biaya yang akan memberikan informasi untuk mengidentifikasi, menghitung dan menilai manfaat dari solusi TI yang diambil, memberikan layanan TI dan mengatur aset TI?	√		
14	Apakah terdapat proses perbaikan untuk mengidentifikasi penyimpangan manfaat yang terjadi?	√		
15	Apakah proses penganggaran dimonitor untuk melihat apakah berjalan efektif atau tidak (alokasi biaya, alokasi biaya layanan dan analisis keragaman anggaran), dan terdapat review laporan yang ada untuk memverifikasi bahwa ada pelajaran yang bisa dicatat untuk membuat penganggaran di masa mendatang lebih akurat dan handal?	√		
16	Apakah terdapat alat (*tools*) yang digunakan untuk memantau biaya?	√		
17	Masih berhubungan dengan pertanyaan sebelumnya, apakah alat (*tools*) tadi digunakan secara tepat?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO6
Tanggal		Tanggal :		
Proses :	Communicate Management Aims and Direction (PO6)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebijakan dan prosedur Perusahaan menciptakan suatu kerangka (*framework*) yang memberikan perhatian tertentu atas TI, memacu terbentuknya suatu lingkungan pengendalian positif dan memenuhi aspek-aspek: • Integritas • nilai-nilai etika • standar-standar profesional dalam bertindak (*code of conduct*) • keamanan dan pengendalian internal • kompetensi dari personel • latar belakang personel • filosofi di DTI • akuntabilitas, perhatian dan arah yang diberikan oleh pimpinan	√ √ √ √ √ √ √ √ √		
2	Apakah Perusahaan mempromosikan suatu lingkungan pengendalian yang positif?	√		
3	Apakah para pimpinan yang ada di Perusahaan telah menerima secara penuh tanggung jawab untuk memformulasikan, mengembangkan, mendokumentasikan, menyebarkan, mengendalikan, dan secara teratur mereview kebijakan-kebijakan yang mengarah pada tujuan dan aturan umum?	√		
4	Apakah terdapat program yang formal, untuk mendorong komunikasi dan pelatihan berkesinambungan yang berhubungan dengan lingkungan pengendalian yang positif?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
5	Apakah terdapat kebijakan dan prosedur untuk memastikan bahwa sumber daya yang tepat dan memadai diberikan dalam rangka mengimplementasikan kebijakan Perusahaan secara tepat waktu?	√		
6	Apakah terdapat prosedur yang tepat untuk memastikan bahwa personil memahami kebijakan dan prosedur yang diimplementasikan, serta kebijakan dan prosedur tersebut dipatuhi?	√		
7	Apakah kebijakan dan prosedur TI sudah mendefinisikan, mendokumentasikan dan memelihara kebijakan dan tujuan filosofi formal yang mengarahkan kepada kualitas dari sistem dan jasa yang diberikan konsisten dengan filosofi, kebijakan dan tujuan Perusahaan?	√		
8	Para pimpinan di DTI memastikan bahwa filosofi, kebijakan, tujuan kualitas dipahami, diimplementasikan, dan dipelihara pada seluruh tingkatan dalam fungsi TI?	√		
9	Apakah terdapat prosedur yang memenuhi kebutuhan dilakukannya review secara periodik dan persetujuan kembali terhadap standar-standar, aturan, kebijakan, dan prosedur utama/pokok yang berhubungan dengan TI?	√		Sedang dalam proses pengerjaan
10	Apakah para direktur di Perusahaan telah menerima tanggung jawab penuh untuk mengembangkan sebuah kerangka bagi pendekatan menyeluruh atas keamanan dan pengendalian internal?	√		
11	Apakah dokumen kerangka keamanan dan pengendalian internal menspesifikasikan kebijakan keamanan dan pengendalian internal, maksud dan tujuan, struktur organisasi, ruang lingkup dalam organisasi, pemberian tanggung jawab, dan definisi dari pinalti serta tindakan disiplin lainnya yang berhubungan dengan kegagalan untuk mematuhi kebijakan keamanan dan pengendalian internal?	√		Sedang dalam proses pengerjaan
12	Apakah kebijakan keamanan dan pengendalian internal yang formal mengidentifikasi proses pengendalian organisasi dan mencakup komponen-	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	komponen pengendalian berikut:			
	• lingkungan pengendalian	√		
	• penilaian risiko	√		
	• aktifitas-aktifitas pengendalian	√		
	• informasi dan komunikasi	√		
	• Pemantauan	√		
13	Apakah terdapat kebijakan untuk isu-isu khusus/tertentu dengan mendokumentasikan keputusan-keputusan manajemen dalam memenuhi atau menangani aktivitas tertentu, aplikasi, sistem dan teknologinya?	√		
14	Dilakukan penilaian untuk melihat apakah risiko TI dan kerangka pengendalian sejalan dengan risiko dan kerangka pengendalian organisasi dengan mempertimbangkan level toleransi terhadap risiko organisasi	√		
15	Apakah manajemen TI menentukan ruang lingkup, tujuan dan harapan terhadap pengendalian TI?	√		
16	Apakah struktur risiko TI dan kerangka pengendalian telah didefinisikan dengan baik dan tanggung jawab yang ada telah diberikan pada individu yang tepat?	√		
17	Apakah terdapat sekumpulan kebijakan, standar dan prosedur yang sejalan dengan strategi TI dan lingkungan pengendalian?	√		Sedang dalam proses pengerjaan

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO7
Tanggal		Tanggal :		
Proses :	**Manage IT Human Resources (PO7)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat penggunaan kriteria untuk merekrut dan memilih staf TI?	√		
2	Apakah dilakukan pemeliharaan terhadap proses rekruitmen staf TI agar sejalan dengan kebijakan dan prosedur perekrutan staf di Perusahaan?	√		
3	Apakah spesifikasi dari kualifikasi yang diperlukan/diinginkan untuk posisi staf disesuaikan atau diperbandingkan dengan kebutuhan dari badan/asosiasi profesional yang relevan?	√		
4	Apakah para pimpinan dan pegawai menerima proses kompetensi pekerjaan (*job competency process*)?	√		
5	Apakah program pelatihan sesuai atau konsisten dengan kebutuhan minimum yang didokumentasikan organisasi mengenai pendidikan dan kesadaran umum yang mencakup isu-isu keamanan?	√		
6	Apakah Divisi TI memiliki komitmen untuk pelatihan dan pengembangan karir para pegawainya?	√		
7	Apakah ketidaksesuaian/celah antara keahlian teknis dan keahlian manajemen diidentifikasi dan tindakan yang tepat diambil untuk mengatasi ketidaksesuaian/celah tersebut?	√		
8	Apakah terdapat pelatihan lintas bagian atau fungsi (*cross training*) yang terus menerus?	√		
9	Apakah program pelatihan tersebut telah menyertakan semua kerangka pengendalian internal dan syarat keamanan berdasarkan kebijakan keamanan dan pengendalian	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	internal, yang mencakup: keamanan, penggunaan sumber daya dan fasilitas organisasi secara tepat, penanganan insiden, tanggung jawab pegawai terhadap keamanan informasi)?			
10	Apakah dilakukan review terhadap materi dan program pelatihan, secara reguler?	√		
11	Apakah terdapat personil atau staf cadangan (*back-up staff*) untuk fungsi pekerjaan atau bagian yang penting, dengan tujuan meminimalkan ketergantungan terhadap satu individu/staf?	√		
12	Apakah terdapat dokumentasi fungsi pekerjaan atau tugas utama TI?	√		
13	Apakah proses *security clearance* terhadap semua pegawai, kontraktor dan vendor di Perusahaan telah memadai/mencukupi?	√		Sedang dalam proses pengerjaan
14	Apakah pegawai dievaluasi berdasarkan serangkaian standar profil kompetensi dan dilakukan evaluasi secara periodik, serta menyertakan rencana rekruitmen khusus untuk menempatkan kebutuhan pegawai di masa sekarang dan masa yang akan datang?	√		
15	Apakah proses perubahan dan pengakhiran pekerjaan memastikan perlindungan terhadap sumber daya organisasi?	√		
16	Apakah Divisi TI melakukan identifikasi kemampuan/keahlian apa yang dibutuhkan dari pegawai TI yang mencakup, pendidikan, pelatihan dan sertifikasi yang dibutuhkan bagi pegawai TI di Perusahaan?	√		
17	Apakah proses rekruitmen pegawai dan penghentian pegawai TI telah didokumentasikan sehingga mampu memberikan gambaran akan kebutuhan pegawai TI?	√		
18	Apakah divisi sumber daya manusia di Perusahaan melakukan review dan menyetujui proses rekruitmen pegawai TI serta penghentian pegawai TI yang sejalan dengan kebijakan organisasi?	√		
19	Apakah terdapat pemeriksaan terhadap latar belakang pegawai (*background check*) pada proses rekruitmen pegawai TI?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
20	Apakah telah dilakukan penilaian terhadap performa kerja pegawai untuk melihat kompetensi pegawai dalam menjalankan tugasnya?	√		
21	Apakah proses remunerasi (penggajian)/penghargaan telah sejalan dengan performa yang dicapai pegawai dan kebijakan yang ada di Perusahaan?	√		
22	Apakah terdapat dokumentasi mengenai prosedur perubahan tugas kerja yang memuat seluruh elemen untuk meminimalkan gangguan proses bisnis?	√		
23	Apakah user yang sudah tidak terdaftar sebagai pegawai di Perusahaan telah dihapuskan hak aksesnya terhadap seluruh informasi yang ada di Perusahaan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO8
Tanggal		Tanggal :		
Proses :	Manage Quality (PO8)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat suatu *Quality Management System* (QMS) atau semacamnya (jika ada, sebutkan namanya) yang mengidentifikasi kebutuhan kualitas dan kriteria TI di Perusahaan; proses TI yang penting; kebijakan, kriteria dan metode untuk mendefinisikan, mendeteksi, mengkoreksi dan mencegah terjadinya pelanggaran?	√		Sedang dalam proses pengerjaan
2	Apakah QMS dibangun dengan mendapatkan input dari manajemen TI, *stakeholder* lain dan kerangka organisasi yang relevan?	√		
3	Apakah hasil temuan dari *quality review* yang dilakukan telah dikomunikasikan pada DTI dan *stakeholder* lain secara tepat waktu untuk merencanakan pengambilan tindakan yang diperlukan?	√		
4	Apakah standar dan kerangka kerja TI yang ada telah sesuai dengan sistem, data dan informasi yang ada di Perusahaan?	√		
5	Apakah rencana kualitas (*quality plan*) TI: • didasarkan atas *quality plan* Perusahaan serta rencana jangka panjang dan jangka pendek TI • mendukung/mempromosikan filosofi perbaikan terus menerus (*continous improvement*) dan menjawab pertanyaan mendasar seperti apa, siapa dan bagaimana • lengkap dan tidak usang	√ √ √		
6	Apakah terdapat pendekatan standar terhadap *quality assurance* (kepastian kualitas)?	√		
7	Jika jawaban pada pertanyaan nomor 6 adalah "ya" apakah pendekatan itu: • dapat diterapkan pada aktifitas-aktifitas kepastian kualitas untuk projek yang	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	bersifat umum dan bersifat spesifik • dapat ditingkatkan/ditinggikan, dan tentunya dapat diterapkan pada seluruh proyek • dipahami oleh seluruh individual yang terlibat dalam proyek dan aktifitas-aktifitas kepastian kualitas • diterapkan menyeluruh di seluruh fase dari sebuah proyek	√ √ √		
8	Jika jawaban pada pertanyaan nomor 6 adalah "ya" apakah pendekatan standar untuk *quality assurance* menginstruksikan tipe dari aktifitas-aktifitas *quality assurance* (yaitu *specific review, audit, inspection* dan lain-lain) yang harus dijalankan untuk mencapai tujuan dari rencana kualitas?	√		
9	Apakah pimpinan mendefinisikan dan mengimplementasikan standar, kebijakan dan prosedur TI?	√		
10	Apakah metodologi siklus hidup pengembangan sistem (*system development life cycle*): • mengarahkan/mengatur proses pengembangan, pengakuisisian, pengimplementasian, dan pemeliharaan sistem informasi terkomputerisasi dan teknologi yang berhubungan dengannya • mendukung dan mendorong usaha pengembangan/modifikasi yang sesuai dengan rencana jangka panjang dan jangka pendek TI • mengharuskan adanya proses pengembangan atau modifikasi yang terstruktur, dan proses otorisasi untuk memulai suatu proyek • bersikap lengkap dan tidak usang • memiliki kemampuan untuk disesuaikan atau ditingkatkan dalam mengakomodir seluruh tipe pengembangan • dapat diterapkan bagi penciptaan/pengadaan dan pemeliharaan perangkat lunak yang dikembangkan sendiri maupun yang dibeli jadi • telah mendokumentasikan persiapan bagi perubahan yang berhubungan dengan	√ √ √ √ √ √		

No	Pertanyaan	Ya	Tidak	Keterangan
	teknologi			
	• telah mengembangkan suatu kerangka umum mengenai akuisisi dan pemeliharaan dari infrastruktur teknologi	√		
	• memiliki serangkaian langkah-langkah yang harus diikuti yang meliputi pengakuisisian dan pengujian, dan sesuai dengan kerangka akuisisi dan pemeliharaan infrastruktur teknologi	√		
	• mengharuskan adanya persiapan (untuk di masa yang akan datang) yang menjelaskan perihal kriteria penerimaan implementor pihak ketiga, standar dan prosedur penanganan perubahan, dan penanganan masalah	√		
	• mengharuskan adanya pemeliharaan dari program yang didetilkan dan dokumentasi sistem (bisa berupa *flowchart*, *data flow diagram*, narasi/penjelasan program tertulis)	√		
	• mengharuskan dokumentasi tersebut diperbarui begitu terjadinya perubahan	√		
	• mengharuskan diterapkannya pengujian (sistem/program) yang detil/memadai	√		
	• mendefinisikan keadaan-keadaan yang akan menentukan jenis pengujian (*parallel testing* atau *pilot testing*) yang akan dilakukan terhadap sistem yang baru atau yang dimodifikasi	√		
	• mengharuskan bahwa pengujian tersebut (sebagai bagian dari proyek pengembangan sistem, implementasi, atau modifikasi) secara independen diverifikasi, didokumentasi, dan disimpan	√		
	• mengharuskan adanya otorisasi dalam menjalankan proyek	√		
	• mengharuskan dibuatnya analisis biaya dan manfaat untuk mengembangkan sistem yang baru atau memodifikasi sistem yang ada	√		
11	Apakah pendekatan kepastian kualitas Perusahaan:			

No	Pertanyaan	Ya	Tidak	Keterangan
	• mengharuskan dibuatnya review sesudah dilakukan implementasi (*post-implementation review*) untuk memastikan sistem yang baru atau yang dimodifikasi sesuai dengan metodologi siklus hidup • mengharuskan dibuatnya review agar dapat menerangkan sejauh mana sistem yang baru atau yang dimodifikasi telah mencapai tujuannya	√ √		
	• menghasilkan laporan, yang membuat/memberikan rekomendasi pengembangan sistem dan efektifitas kepada manajemen TI (pengguna dan fungsi TI) • memiliki rekomendasi yang secara periodik ditindaklanjuti dan dilaporkan kepada para pimpinan	√ √		
12	Apakah pimpinan TI mereview dan memperbarui secara tepat metodologi siklus hidup pengembangan sistem untuk menyelidiki kecukupannya bagi pengembangan/modifikasi yang baru dan teknologi yang baru?	√		
13	Apakah terdapat pencapaian koordinasi dan komunikasi yang dekat antara pengguna jasa fungsi TI dan implementor sistem di seluruh siklus hidup pengembangan sistem?	√		
14	Apakah pihak lain yang berkepentingan terhadap TI Perusahan stakeholder puas terhadap proses QMS yang ada di Perusahaan ?	√		
15	Apakah umpan balik dari pihak lain yang berkepentingan terhadap TI Perusahaan ditindaklanjuti?	√		
16	Apakah aktifitas perbaikan dilakukan secara kontinyu, diatur secara efektif dan diimplementasikan sesuai standar kualitas, kebijakan, praktek dan prosedur yang berlaku di Perusahaan?	√		
17	Apakah terdapat penggunaan matrik untuk mengukur hasil berbagai aktifitas, yang berguna untuk menilai apakah kualitas yang diinginkan telah tercapai?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO9
Tanggal		Tanggal :		
Proses :	**Assess and Manage IT Risks (PO9)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kerangka penilaian risiko yang sistematik, yang mengikutkan risiko-risiko informasi relevan dan yang membentuk suatu dasar untuk menentukan bagaimana risiko harus diatur ke tingkat yang dapat diterima?	√		
2	Apakah pendekatan penilaian risiko memberikan adanya atau membuat suatu penilaian risiko yang diperbarui secara teratur pada tingkat global dan sistem khusus/tertentu?	√		
3	Apakah terdapat prosedur penilaian risiko untuk menentukan bahwa risiko yang teridentifikasi mencakup faktor-faktor eksternal dan internal, dan mempertimbangkan hasil audit, inspeksi dan insiden teridentifikasi lainnya?	√		
4	Apakah tujuan tingkat organisasi (*organization wide objective*) dimasukkan ke dalam proses identifikasi risiko?	√		
5	Apakah prosedur untuk memantau perubahan dalam aktifitas pemrosesan sistem, menentukan bahwa risiko dan *exposure* (pembongkaran) sistem disesuaikan secara tepat waktu?	√		
6	Apakah terdapat prosedur untuk pemantauan dan perbaikan terus menerus dari penilaian risiko?	√		
7	Apakah dokumentasi penilaian risiko mencakup: • sebuah deskripsi dari metodologi penilaian risiko • identifikasi dari *exposure* signifikan dan apa risikonya • risiko dan *exposure* yang ditangani	√ √ √		

No	Pertanyaan	Ya	Tidak	Keterangan
8	Apakah digunakan teknik analisis kemungkinan, frekuensi dan ancaman dalam pengidentifikasian risiko?	√		
9	Apakah staf penilaian risiko memiliki kualifikasi yang memadai?	√		
10	Penerimaan dari risiko residual mencakup dan mempertimbangkan: • kebijakan organisasi • identifikasi dan pengukuran risiko • ketidakpastian diikutkan/dipertimbangkan dalam pendekatan penilaian risiko • biaya dan efektivitas dari implementasi perlindungan dan pengendalian	 √ √ √ √		
11	Apakah terdapat pendekatan kuantitatif dan/atau kualitatif formal untuk memilih ukuran-ukuran pengendalian yang memaksimalkan *return on investment* (ROI)?	√		
12	Apakah terdapat keseimbangan antara penggunaan ukuran-ukuran deteksi, pencegahan, koreksi, dan pemulihan?	√		
13	Apakah terdapat prosedur formal untuk mengkomunikasikan maksud dan tujuan dari ukuran-ukuran pengendalian?	√		
14	Apakah risiko yang ada telah diidentifikasi dan dicatat/didokumentasikan secara formal dalam suatu rencana penanganan risiko?	√		
15	Apakah semua penyimpangan yang terjadi disampaikan pada para pimpinan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-PO10
Tanggal		Tanggal :		
Proses :	Manage Projects (PO10)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kerangka manajemen proyek: • mendefinisikan ruang lingkup dan batasan untuk menangani proyek	√		
	• mereview permohonan proyek dalam hal konsistensi dengan rencana operasional yang telah disetujui dan proyek yang diprioritaskan dalam rencana itu	√		
	• mendefinisikan metodologi manajemen proyek yang diadopsi dan diterapkan pada tiap-tiap proyek, yang mencakup: perencanaan proyek, penentuan staf, alokasi tanggung jawab dan otoritas, pemecahan tugas, anggaran waktu dan sumber daya, milestone, checkpoint dan persetujuan	√		
	• bersifat lengkap/menyeluruh dan tidak usang	√		
	• memberikan peluang peran aktif atau partisipasi dari manjemen departemen pengguna yang dipengaruhi dalam pendefinisian dan otorisasi dari proyek	√		
	• menspesifikasikan dasar untuk pemilihan anggota staf yang akan ditugaskan dalam proyek	√		
	• mendefinisikan tanggung jawab dan otoritas dari anggota tim proyek	√		
	• membuat suatu pernyataan tertulis yang jelas, yang mendefinisikan sifat dan ruang lingkup proyek sebelum pekerjaan atas proyek itu dimulai	√		
	• mencakup penjelasan atau alasan mengapa proyek harus dijalankan, seperti: adanya masalah atau proses harus diperbaiki, untuk meningkatkan	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	kemampuan perusahaan, adanya defisiensi pada sistem yang ada sekarang, adanya peluang, dan adanya kebutuhan keamanan dan pengendalian internal			
	• menjelaskan cara bagaimana studi kelayakan proyek yang diusulkan disiapkan, direview dan disetujui oleh pimpinan	√		
	• menjelaskan cara yang mana setiap tahapan dari proses pengembangan yang meliputi: studi kelayakan, definisi kebutuhan, dan perancangan sistem, disetujui sebelum melanjutkan ke tahapan berikutnya, yaitu tahapan pemrograman, pengujian sistem, pengujian transaksi, dan pengujian parallel	√		
	• mengharuskan dibuatnya suatu *Software Project Master Plan* (SPMP) untuk tiap-tiap proyek	√		
	• sesuai dengan standar organisasi untuk SPMP, atau jika tidak ada, digunakan standar tepat lainnya	√		
	• Mengharuskan dibuatnya suatu *Software Quality Assurance Plan* (SQAP) untuk tiap-tiap proyek dan terintegrasi dengan SPMP	√		
	• mengharuskan baik SQAP dan SPMP direview secara formal dan disetujui oleh seluruh pihak yang terlibat	√		
	• menjelaskan cara program manajemen risiko proyek yang formal itu mengeliminasi atau meminimalkan risiko-risiko yang berhubungan dengan proyek	√		
	• mengharuskan dibuatnya sebuah rencana pengujian (*test plan*) untuk setiap proyek	√		
	• mengharuskan dibuatnya rencana yang memadai untuk melatih staf pemilik dan staf TI untuk setiap proyek	√		
2	Apakah studi kelayakan proyek mencakup: • lingkungan dari proyek yaitu: perangkat keras, perangkat lunak, dan telekomunikasi	√		
	• ruang lingkup dari proyek	√		
	• hambatan dari proyek	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	• manfaat dan biaya yang direalisasi			
3	Apakah *milestone* dan biaya proyek aktual dan yang dianggarkan, dipantau dan dilaporkan ke pimpinan pada setiap fase utama dari proyek?	√		
4	Apakah *milestone* dan biaya proyek yang melebihi *timeframe* dan jumlah yang dianggarkan, membutuhkan persetujuan oleh pimpinan yang bersangkutan?	√		
5	Apakah SQAP sesuai dengan standar organisasi untuk SQAP, atau jika tidak ada, sesuai dengan kriteria tertentu yang telah ditetapkan	√		
6	Apakah tugas-tugas kepastian (*assurance*) SQAP mendukung akreditasi dari sistem yang baru atau yang sedang dimodifikasi serta menyelidiki apakah pengendalian internal dan keamanan sudah memenuhi kebutuhan?	√		
7	Apakah seluruh pemilik proyek memberikan masukan dalam SPMP dan SQAP?	√		
8	Apakah terdapat proses sesudah implementasi untuk memastikan bahwa sistem yang baru atau yang dimodifikasi memenuhi manfaat yang diharapkan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI1
Tanggal		Tanggal :		
Proses :	**Identify Automated Solution (AI1)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kebijakan dan prosedur yang mengharuskan bahwa : • didefinisikannya kebutuhan pengguna yang dipenuhi oleh sistem yang ada sekarang atau yang akan dipenuhi oleh sistem baru/modifikasi, dan memerlukan persetujuan	√		
	• dokumentasi berisikan kebutuhan pengguna yang meliputi kebutuhan teknis dan fungsional, direview dan disetujui secara tertulis oleh pihak yang berwenang sebelum proses pengembangan, implementasi, atau modifikasi disetujui	√		
	• kebutuhan operasional dan fungsional solusi dipenuhi, termasuk performa, *safety*, *reliabilitas*, *compability*, keamanan, dan aspek hukum	√		
	• alternatif solusi bagi kebutuhan pengguna dipelajari dan dianalisis sebelum dilakukannya pemilihan solusi perangkat lunak	√		
	• diidentifikasinya paket perangkat lunak yang memenuhi kebutuhan pengguna bagi pengembangan atau modifikasi sistem tertentu, sebelum keputusan pemilihan akhir dibuat	√		
	• berbagai alternatif untuk akuisisi produk perangkat lunak didefinisikan secara jelas dalam hal apakah dibeli jadi, dibuat sendiri, melalui kontrak, atau dengan mengembangkan sistem yang sudah ada sekarang, atau dengan kombinasi dari semua tadi	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	• dibuatnya studi kelayakan teknis terhadap pengembangan/modifikasi sistem baru, yang memerlukan analisis dan persetujuan dari pihak yang berwenang	√		
	• dilakukan analisis biaya dan manfaat dalam proses pengembangan, implementasi, dan modifikasi sistem, dari masing-masing alternatif	√		
	• dibuatnya studi kelayakan ekonomis, yang dianalisis dan disetujui oleh pemilik yang berwenang, sebelum diambil suatu keputusan	√		
	• pengidentifikasian solusi dan analisa kelayakannya memperhatikan model data yang terdapat di Perusahaan	√		
	• dilakukan analisa dan pendokumentasian pada waktu melakukan tahapan pengembangan, implementasi, dan modifikasi sistem dengan memperhatikan ancaman/resiko keamanan, kelemahan yang mungkin terjadi berikut pengaruhnya, keamanan dan pengendalian internal yang memungkinkan untuk mengeliminasi resiko yang teridentifikasi	√		
	• biaya dan manfaat yang diperoleh terutama dalam hal keamanan diuji secara hati-hati untuk memastikan bahwa biaya pengendalian tidak melebihi manfaatnya	√		
	• adanya tanda tangan/persetujuan yang formal dari pimpinan atau pihak yang berwenang atas studi biaya/manfaat	√		
	• diperlukan adanya jejak audit (*audit trails*) dan pengendalian yang tepat ke dalam seluruh sistem baru atau usulan modifikasi selama fase perancangan	√		
	• jejak audit dan pengendaliaan memberikan kemungkinan untuk melindungi dari penggunaan yang dilakukan oleh pihak yang tidak berwenang	√		
	• Divisi TI mengidentifikasi seluruh program perangkat lunak sistem yang potensial, yang akan memenuhi	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	kebutuhan-kebutuhan operasional Perusahaan			
	• berbagai produk/aplikasi direview dan diuji sebelum digunakan oleh staf TI dan pihak-pihak yang terlibat	√		
	• akuisisi produk perangkat lunak mengikuti kebijakan *procurement* Perusahaan	√		
	• untuk perangkat lunak lisensi yang diperoleh dari pihak ketiga, pihak ketiga harus memberikan prosedur-prosedur yang tepat untuk melakukan validasi, melindungi, dan memelihara hak integritas produk perangkat lunak	√		
	• terdapat kontrak atau permintaan tertulis dalam hal melakukan proses *procurement* jasa dari fungsi TI	√		
	• rencana penerimaan atas fasilitas disetujui/disepakati bersama-sama dengan *supplier* sesuai kontrak	√		
	• rencana penerimaan atas teknologi khusus/spesifik disetujui/disepakati bersama dengan supplier sesuai kontrak	√		
2	Apakah analisis resiko mengenai ancaman keamanan, dampaknya, dan pengendalian internal yang layak untuk mengurangi atau mengeliminasi resiko-resiko yang ada, dilaksanakan sesuai dengan kerangka penilaian resiko secara keseluruhan	√		
3	Dalam mengimplementasikan *automated solution*, resiko yang mungkin timbul telah dibicarakan dan disetujui oleh pimpinan di Perusahaan dan telah mempertimbangkan seluruh pengendalian terhadap resiko tersebut	√		
4	Apakah terdapat mekanisme untuk menangani dan memelihara atribut keamanan bagi data yang diekspor dan diimpor, serta menginterpretasikan data tersebut secara tepat?	√		
5	Apakah Divisi TI telah mengembangkan dan mengimplementasikan suatu pendekatan *procurement* pusat, yang menggambarkan serangkaian prosedur dan standar yang harus diikuti dalam mendapatkan perangkat keras TI, perangkat lunak, dan jasa lainnya?	√		Sedang dalam proses pengerjaan

No	Pertanyaan	Ya	Tidak	Keterangan
6	Apakah kontrak-kontrak yang ada menyatakan bahwa perangkat lunak, dokumentasi, atau jasa lainnya harus mengalami pengujian dan review terlebih dahulu sebelum penerimaan?	√		
7	Apakah pengujian yang dinyatakan dalam spesifikasi kontrak meliputi:			
	• pengujian sistem	√		
	• pengujian integritas data	√		
	• pengujian perangkat keras dan komponen	√		
	• pengujian prosedur	√		
	• pengujian daya/beban (load) dan tekanan (stress)	√		
	• pengujian kinerja sistem	√		
	• pengujian penyimpangan sistem	√		
	• pengujian penerimaan pengguna	√		
	• pengujian pilot dari seluruh sistem	√		
8	Seluruh kebutuhan teknis aplikasi dan infrastruktur TI di Perusahaan telah memenuhi standar arsitektur informasi Perusahaan	√		
9	Rancangan sistem yang *user friendly* untuk meningkatkan keahlian pemakai/pengguna akhir telah dipertimbangkan selama perancangan sistem	√		
10	Isu-isu performa pemakai/pengguna (waktu respon sistem, kemampuan download/upload) telah dimasukkan dalam spesifikasi kebutuhan sistem sebelum perancangan dan pengembangan sistem	√		
11	Produk yang dibeli direviu dan diuji sebelum penggunaannya dan penyelesaian pembayarannya.	√		
12	Apakah Divisi TI dalam menjalankan fungsinya, mematuhi serangkaian prosedur dan standar untuk mendapatkan perangkat keras, perangkat lunak dan layanan yang berhubungan dengan TI?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI2
Tanggal		Tanggal :		
Proses :	**Acquire and Maintain Application Software (AI2)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebijakan dan prosedur yang ada memastikan bahwa :			
	• terdapat hubungan/koordinasi yang dekat dengan pemakai dalam menciptakan/membuat spesifikasi rancangan, dan memverifikasinya dengan kebutuhan pengguna	√		
	• pada saat terjadi perubahan yang besar pada sistem yang ada sekarang, dilaksanakan proses pengembangan sistem yang sama seperti halnya dalam pengembangan sistem yang baru	√		
	• spesifikasi rancangan diketahui dan disetujui oleh para pimpinan di Perusahaan dan pengguna yang berkepentingan	√		
	• diterapkannya proses yang tepat untuk mendefinisikan format dokumen (file) yang akan digunakan untuk menyimpan data untuk masing-masing proyek pengembangan sistem baru atau modifikasi sistem	√		
	• dibuatnya spesifikasi program tertulis yang detil untuk masing-masing proyek pengembangan dan modifikasi, dan spesifikasi program tesebut sesuai dengan spesifikasi rancangan	√		
	• adanya mekanisme yang memadai untuk mendefinisikan dan mendokumentasikan kebutuhan input untuk masing-masing proyek pengembangan sistem baru dan modifikasi sistem	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	• adanya pengembangan antar muka (*interface*) antara pemakai dan mesin, yang mudah untuk digunakan dan terdapat fungsi *online help*	√		
	• adanya mekanisme yang memadai untuk mendefinisikan dan mendokumentasikan kebutuhan pemrosesan untuk masing-masing proyek pengembangan sistem baru dan modifikasi sistem	√		
	• adanya mekanisme yang memadai untuk mendefinisikan dan mendokumentasikan kebutuhan output untuk masing-masing proyek pengembangan sistem baru dan modifikasi sistem	√		
	• adanya mekanisme yang memadai untuk memastikan dispesifikasikannya kebutuhan pengendalian internal dan keamanan untuk masing-masing proyek pengembangan sistem baru dan modifikasi sistem	√		
	• kebutuhan pengendalian internal dan keamanan mencakup pengendalian aplikasi, yang menjamin ketepatan, kelengkapan, ketepatwaktuan, dan otorisasi dari input dan output	√		
	• program aplikasi memiliki kemampuan untuk secara rutin memverifikasi tugas-tugas yang dijalankan oleh perangkat lunak, dan mengembalikan integritas melalui *rollback* atau cara-cara lainnya	√		
	• perangkat lunak aplikasi diuji sesuai dengan rencana uji/tes proyek dan standar pengujian yang telah dibuat, sebelum disetujui oleh pengguna	√		
	• dibuatnya referensi pemakai dan *support manuals* yang memadai (biasanya dalam bentuk elektronik)	√		
	• dilakukan penilaian kembali terhadap rancangan sistem pada saat terjadinya penyimpangan teknologi atau logika yang signifikan selama pengembangan dan pemeliharaan sistem	√		
2	Apakah metodologi pengembangan sistem memastikan bahwa referensi dan *support materials* diperbarui secara tepat dan tepat waktu?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
3	Apakah metodologi pengembangan sistem mengharuskan dilaksanakannya penilaian sensitivitas (*sensitivity assessment*) selama permulaan pengembangan sistem baru atau modifikasi?	√		
4	Apakah metodologi pengembangan sistem mengharuskan aspek keamanan dan pengendalian internal dinilai bersama-sama dengan rancangan konseptual sistem agar dalam rancangan sistem memperhitungkan aspek keamanan?	√		
5	Apakah metodologi pengembangan sistem mengharuskan dipertimbangkannya isu-isu keamanan logika dan aplikasi yang bersifat pencegahan atau pendeteksian, dan disertakan ke dalam rancangan sistem baru atau modifikasi sistem?	√		
6	Apakah penilaian aspek keamanan dan pengendalian internal didasarkan pada suatu kerangka yang memadai (masuk akal/logis)?	√		
7	Apakah telah memanfaatkan *artificial intelligence system* dalam interaksi atau pengendalian dengan operator manusia, untuk memastikan pengambilan keputusan yang penting telah disetujui?		√	
8	Apakah terdapat pembatasan akses yang kuat atau dipersonilisasi (*depersonalization*) dari data historis untuk melindungi informasi sensitif yang digunakan selama pengujian aplikasi?	√		
9	Apakah spesifikasi rancangan untuk akuisisi perangkat lunak memperhatikan kebutuhan organisasi (Perusahaan) ?	√		
10	Apakah terdapat *failure recovery* dan *backup arrangements* dalam detil spesifikasi rancangan perangkat lunak?	√		
11	Apakah dalam dokumentasi proyek pengembangan sistem terdapat informasi mengenai ketersediaan data, pengendalian data, keamanan data dan kebutuhan jaringan?	√		
12	Apakah sistem aplikasi dikonfigurasi sesuai kebutuhan organisasi (Perusahaan) dan pengguna?	√		
13	Apakah terdapat dokumentasi formal yang mengatur mengenai *upgrade system?*	√		

No	Pertanyaan	Ya	Tidak	Keterangan
14	Apabila pengembangan sistem dilakukan oleh pihak ketiga, apakah terdapat perjanjian/kesepakatan selama proses perancangan, pengembangan dan implementasi sistem?	√		
15	Apakah terdapat suatu strategi dan perencanaan untuk pemeliharaan aplikasi perangkat lunak?	√		
16	Apakah terdapat proses untuk pemeliharaan aplikasi perangkat lunak yang juga mengikutsertakan proses *updating user*, *system* dan *operational documentation?*	√		
17	Apakah seluruh perubahan proses pemeliharaan sistem telah mengikuti prosedur formal yang ada dan memperhitungkan dampak bagi aplikasi dan infrastruktur yang ada?	√		
18	Apakah dilakukan penilaian secara periodik terhadap pemeliharaan sistem?	√		
19	Apakah seluruh permasalahan yang berkaitan dengan performa sistem telah dianalisa dan dilaporkan ke pimpinan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI3
Tanggal		Tanggal :		
Proses :	**Acquire and Maintain Technology Infrastructure (AI3)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kebijakan dan prosedur yang memastikan bahwa : • dibuatnya suatu rencana evaluasi formal untuk menilai pengaruh/dampak perangkat keras dan perangkat lunak baru terhadap performa keseluruhan sistem	√ √		Masih dalam proses pengerjaan
	• dibatasinya kemampuan untuk melakukan akses perangkat lunak sistem	√		Masih dalam proses pengerjaan
	• proses set-up, instalasi dan pemeliharaan perangkat lunak sistem tidak membahayakan keamanan data dan program yang sedang disimpan dalam sistem	√		Masih dalam proses pengerjaan
	• dipilihnya parameter perangkat lunak sistem untuk memastikan integritas data dan program dalam sistem	√		Masih dalam proses pengerjaan
	• perangkat lunak sistem diinstal dan dipelihara sesuai dengan kerangka akuisisi dan pemeliharaan infrastruktur teknologi	√		Masih dalam proses pengerjaan
	• pemasok (*vendor*) perangkat lunak sistem memberikan kepastian integritas akan perangkat lunak mereka dan modifikasi pada perangkat lunak mereka	√		Masih dalam proses pengerjaan
	• dilaksanakannya pengujian yang menyeluruh dari perangkat lunak sistem sebelum digunakan dalam lingkungan yang sebenarnya, yang meliputi pengujian terhadap *functionality, security, availability,* dan *integrity condition*	√		Masih dalam proses pengerjaan
	• diubahnya kata sandi (*password*) instalasi perangkat lunak yang diberikan oleh pemasok pada saat dilakukannya instalasi	√		Masih dalam proses pengerjaan

No	Pertanyaan	Ya	Tidak	Keterangan
	• dikendalikannya perubahan-perubahan perangkat lunak sistem agar sesuai dengan prosedur manajemen perubahan yang dimiliki oleh organisasi			Masih dalam proses pengerjaan
2	Apakah terrdapat kebijakan dan prosedur untuk pemeliharaan preventif dari perangkat keras (yang dioperasikan oleh fungsi TI dan fungsi pengguna) untuk mengurangi frekuensi dan dampak kegagalan performa sistem?	√		Masih dalam proses pengerjaan
3	Apakah pemasok (*vendor*) memberikan dan menganjurkan langkah-langkah pemeliharaan preventif atas perangkat keras yang dipasoknya?	√		
4	Apakah tanggung jawab untuk menggunakan berbagai utilitas perangkat keras sensitif secara jelas didefinisikan dan dipahami oleh programmer?	√		
5	Masih berhubungan dengan pertanyaan sebelumnya, apakah penggunaan berbagai utilitas tersebut dipantau dan dicatat?	√		
6	Apakah terdapat perencanaan akuisisi, implementasi dan perubahan (*upgrade*) infrastruktur teknologi yang sesuai kebutuhan organisasi dan memperhitungkan semua aspek penting seperti resiko yang mungkin timbul dari proses transisi dan migrasi?	√		
7	Apakah sebelum proses instalasi dan atau pemeliharaan, telah dilakukan proses *back up* terlebih dahulu?	√		
8	Apakah terdapat prosedur penerimaan (*acceptance procedur*) dengan menggunakan kriteria penerimaan (*acceptance criteria*) untuk menilai apakah performa produk telah konsisten dan sesuai dengan kebutuhan?	√		
9	Apakah kegiatan pemeliharaan pada komponen infrastruktur teknologi yang sensitif direview secara reguler oleh staf yang berkompeten?	√		
10	Apakah sering terjadi penyimpangan proses perubahan infrastruktur teknologi dari proses perubahan yang normal (yg sesuai dengan arahan *vendor* dan *guideline* yang ada)	√		
11	Apakah dokumentasi perangkat lunak sistem dipelihara, dijaga ke-*up to date*-annya, dan dijaga agar tetap sesuai dengan dokumentasi yang dimiliki vendor?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
12	Apakah seluruh penyimpangan yang terjadi atau suatu perlakuan khusus didokumentasikan secara formal?	√		
13	Apakah terdapat review secara teratur terhadap tindakan pemeliharaan yang telah dilakukan, untuk melihat serangan terhadap infrastruktur yang tidak didukung oleh TI dan resiko TI di masa yang akan datang serta serangan dalam hal keamanan TI?	√		
14	Apakah terdapat semacam *maintenance tracking logs* dan *feedback tools* untuk memastikan bahwa hasil review telah dibicarakan ke semua pihak yang berkepentingan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI4
Tanggal		Tanggal :		
Proses :	**Enable Operation and Use (AI4)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebutuhan operasional ditentukan dengan/berdasarkan statistik performa historis yang ada dan masukan dari pengguna?	√		
2	Apakah terdapat prosedur operasional dan dokumentasi sistem (mencakup *online assistance*) yang harus diikuti sebelum mengimplementasikan/meng-*update utomated system* atau infrastruktur yang ada	√		
3	Apakah setiap pengguna yang ingin menggunakan sistem harus mendapat persetujuan untuk mengakses sistem terlebih dahulu (*access approval*)?	√		
4	Apakah terdapat pengaturan hak akses (*privilege management*) ke sistem?	√		
5	Apakah bagian TI Perusahaan menerapkan suatu pemisahan tugas (*segregation of duties*), sehingga tugas-tugas penting yang terkait dengan sistem dipegang oleh staf yang berbeda?	√		
6	Apakah bagian TI Perusahaan Perusahaan menjalankan proses *backup* terhadap semua data yang penting, sehingga, jika terjadi suatu hal yang tidak diinginkan dapat dilakukan *recovery* berdasarkan data yang telah di-*backup*?	√		
7	Apakah bagian TI Perusahaan menerapkan keamanan fisik (*physical security*) yang memadai terhadap sistem dan infrastruktur TI yang ada di DJA?	√		
8	Apakah bagian TI Perusahaan melakukan penyimpanan/pengarsipan memadai terhadap dokumen sumber (*source document*	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	archival)?			
9	Apakah staf operasi dan teknis memiliki kepedulian dan pengetahuan memadai agar dapat memberikan layanan, melakukan *supporting*, *maintain* sistem aplikasi dan infrastruktur TI yang ada secara efektif dan efisien?	√		
10	Apakah prosedur manual pengguna, manual operasi, *online help* dan bahan pelatihan dikembangkan sebagai bagian dari setiap proyek pengembangan sistem, implementasi atau modifikasi, dan dijaga supaya tetap *up to date*?	√		
11	Apakah terdapat kebutuhan operasional yang benar-benar merefleksikan harapan/kebutuhan pengguna dan operasi?	√		
12	Apakah kinerja/performa operasional diukur, dikomunikasikan, dan diperbaiki, terlebih pada saat terjadi penurunan kinerja?	√		
13	Apakah staf operasi, staf teknis dan pengguna memiliki kepedulian terhadap kinerja yang diinginkan?	√		
14	Masih berhubungan dengan pertanyaan sebelumnya, apakah staf operasi, staf teknis dan pengguna dapat memberikan umpan balik untuk menilai kecukupan manual prosedur pengguna, manual operasi, *online help* dan materi pelatihan?	√		
15	Apakah staf operasi memiliki manual operasi untuk seluruh sistem dan pemrosesan yang berada dalam tanggung jawab mereka?	√		
16	Apakah seluruh perpindahan program dari proses/tahap pengembangan aplikasi untuk digunakan dalam lingkungan yang sebenarnya diikuti dengan pembaruan atau pembuatan manual operasi?	√		
17	Apakah terdapat manual pelatihan bagi pengguna untuk seluruh sistem/aplikasi yang ada?	√		
18	Masih berhubungan dengan pertanyaan sebelumnya, apakah manual pelatihan bagi pengguna tersebut merefleksikan fungsionalitas dari aplikasi yang	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	bersangkutan?			
19	Apakah manual pelatihan tersebut dapat memudahkan dan memuaskan pengguna dalam menggunakan sistem/aplikasi yang ada?	√		
20	Masih berhubungan dengan pertanyaan sebelumnya, apakah manual untuk sistem tadi merefleksikan penggunaan sistem dalam praktik sehari-hari, sehingga mencerminkan adanya suatu transfer pengetahuan terhadap seluruh pengguna?	√		
21	Apakah manual pelatihan bagi pengguna memberikan: • gambaran umum dari sistem dan lingkungan sistem	√		
	• penjelasan dari seluruh input sistem, program, output, dan integrasi dengan sistem yang lain	√		
	• penjelasan dari seluruh layar entri data dan layar tampilan data	√		
	• penjelasan dari seluruh pesan-pesan kesalahan (*error*) dan respon yang tepat untuk menangani kesalahan tersebut	√		
22	Apakah manual operasi memberikan penjelasan/konfirmasi yang mencakup : • nama sistem, nama program, urutan/tahapan dalam menjalankannya	√		
	• definisi dari seluruh nama file input, yang diproses, output, dan format media	√		
	• jadwal untuk bekerja/dijalankan secara harian, mingguan, bulanan, per tiga bulanan, per akhir tahun, dan lain-lain	√		
	• prosedur *backup, restart*, dan *restore* pada berbagai titik atau pada saat terjadi keabnormalan	√		
	• bentuk output yang khusus atau prosedurnya, dan pendistribusian laporan/output tersebut	√		
	• prosedur-prosedur darurat yang tetap	√		
23	Apakah terdapat pemeliharaan yang berkesinambungan terhadap dokumentasi aplikasi, manual pengguna dan operasi, serta manual pelatihan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI5
Tanggal		Tanggal :		
Proses :	**Procure IT Resources (AI5)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kebijakan dan prosedur yang berhubungan dengan proses pengadaan dan akuisisi infrastruktur, fasilitas, perangkat keras, perangkat lunak dan layanan TI yang sesuai dengan tujuan Perusahaan?	√		
2	Apakah proses pengadaan TI dan strategi akuisisi sejalan dengan kebijakan dan prosedur pengadaan yang ada di Perusahaan hal ini bisa dilihat, misalnya dari peraturan yang ada, kepatuhan terhadap kebijakan akuisisi TI yang dimiliki Perusahaan, syarat *lisensi dan leasing*, ketentuan dalam melakukan *technology upgrade*, rencana akuisisi, dsb?	√		
3	Apakah terdapat prosedur atau kebijakan untuk membuat, memodifikasi, mengakhiri kontrak dengan semua *supplier*?	√		
4	Masih berhubungan dengan pertanyaan sebelumnya, apakah prosedur kontrak tersebut mencakup tanggung jawab *supplier*, aturan transisi sistem, standar keamanan sistem, dan memperhatikan masalah hukum, keuangan, kinerja, keamanan, hak intelektual, dan hukuman jika terjadi pelanggaran (mencakup *penalty clauses*)?	√		
5	Apakah kontrak yang dilakukan tidak melenceng dari kebijakan dan standar yang dimiliki oleh Perusahaan?	√		
6	Apakah kontrak menyertakan hak dan kewajiban semua pihak dalam melakukan akuisisi infrastruktur, fasilitas dan layanan TI terkait?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
7	Masih berhubungan dengan pertanyaan sebelumnya, apakah kontrak yang ada mencakup tanggung jawab supplier-klien, *Service Level Agreement* dari supplier, monitoring dan pelaporan, aturan transisi, prosedur yang harus diperhatikan, standar keamanan, kebutuhan pengendalian, *quality assurance* terhadap supplier, dan memperhatikan aspek legal, keuangan, organisasi, performa organisasi, *intellectual property*, dan tanggung jawab (*responsibility dan liability*)?	√		
8	Apakah supplier dipilih berdasarkan praktek yang wajar (*fair*) dan formal dan dengan kriteria yang sesuai kebutuhan organisasi?	√		
9	Apakah perjanjian kontrak sesuai dengan kebijakan organisasi sehingga kepentingan organisasi akan dilindungi pada waktu melakukan akuisisi sumber daya TI?	√		
10	Apakah proses akuisisi sumber daya TI telah direview dan disetujui oleh personel yang tepat dan telah dilakukan berdasarkan aturan yang ada?	√		
11	Apakah terdapat perlindungan terhadap hak dan kewajiban semua pihak pada waktu melakukan proses akuisisi sumber daya TI. Hak dan kewajiban ini mencakup:			
	• persetujuan	√		
	• tingkat layanan (*service level*)	√		
	• prosedur pemeliharaan	√		
	• pengendalian terhadap akses yang ada	√		
	• Keamanan	√		
	• review kinerja sistem	√		
	• dasar pembayaran	√		
12	Apakah seluruh proses akuisisi telah mempertimbangkan seluruh hak dan kewajiban yang relevan mencakup:			
	• kepemilikan dan lisensi dari hak intelektual	√		
	• pemeliharaan	√		
	• Garansi	√		
	• masa upgrade	√		
	• maksud dan tujuan yang jelas termasuk dalam hal *security*	√		
	• hak akses	√		

No	Pertanyaan	Ya	Tidak	Keterangan
13	Apakah terdapat suatu proses penilaian kualitas dan *acceptance process* untuk seluruh akuisisi sumber daya TI yang dilakukan?	√		
14	Apakah seluruh proses akuisisi perangkat lunak dan perangkat keras didokumentasikan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI6
Tanggal		Tanggal :		
Proses :	Manage Changes (AI6)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat prosedur perubahan yang formal agar seluruh permintaan yang mencakup perubahan aplikasi, proses, sistem dan layanan dan *platform*, ditangani sesuai standar yang berlaku.	√		Sedang dalam proses pengerjaan
2	Prosedur perubahan yang meliputi:			
	• definisi tugas dan tanggung jawab	√		
	• pengelompokkan dan prioritas semua perubahan	√		
	• penilaian dampak perubahan, otorisasi dan persetujuan dilakukannya perubahan	√		
	• pelacakan perubahan	√		
	• mekanisme pengendalian	√		
	• dampak perubahan terhadap integritas data (mencakup semua perubahan file data yang dilakukan oleh sistem)	√		
	• prosedur *rollback*	√		
	• penggunaan proses perubahan yang dilakukan secara darurat	√		
	• penggunaan *record management system*	√		
	• jejak audit	√		
	• pemisahan tugas	√		
3	Apakah terdapat (dan sedang digunakan) suatu metodologi untuk memprioritaskan permohonan-permohonan perubahan sistem dari pengguna?	√		
4	Apakah permintaan untuk melakukan perubahan dirangking terlebih dahulu berdasarkan kriteria yang telah didefinisikan sebelumnya untuk menentukan prioritas perubahan?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
5	Apakah setiap permintaan perubahan disetujui secara formal oleh para pimpinan dan pihak yang berkepentingan terhadap TI (*IT technical stakeholder*)?	√		
6	Apakah prosedur-prosedur perubahan darurat dinyatakan/dipenuhi/terdapat dalam manual operasi?	√		
7	Apakah perubahan darurat yang dilakukan telah diotorisasi oleh pihak yang berwenang?	√		
8	Apakah terdapat suatu sistem yang melacak dan melaporkan jika terjadi penolakan terhadap perubahan yang diinginkan, dan juga akan mencatat dan memonitor perubahan yang telah disetujui untuk dilakukan/diproses, disetujui tapi tidak dimulai untuk diproses, sedang dalam proses atau telah selesai dilakukan?	√		
9	Apakah dilakukan review dan monitor terhadap setiap perubahan yang dilakukan?	√		
10	Apakah terdapat proses *update* terhadap sistem, dokumen dan prosedur, ketika mengimplementasikan perubahan, sehingga prosedur operasional, informasi konfigurasi, dokumen aplikasi, *help screens*, materi pelatihan, selalu *up to date?*	√		
11	Apakah seluruh perubahan yang dilakukan/ditunjukkan benar-benar merupakan hasil keputusan pimpinan dan Divisi TI?	√		
12	Apakah perubahan yang dilakukan membawa dampak perubahan pada dokumentasi program dan operasi?	√		
13	Apakah dokumentasi yang ada sekarang mencerminkan lingkungan yang telah mengalami perubahan?	√		
14	Apakah proses perubahan dipantau/diawasi untuk memperbaiki/meningkatkan waktu respon, efektivitas respon, dan kepuasan pengguna?	√		
15	Apakah terdapat analisis tipe-tipe perubahan yang dibuat pada sistem untuk identifikasi kecenderungan perubahan yang terjadi?	√		
16	Apakah pengguna (user) sadar dan peduli serta memahami kebutuhan akan prosedur pengendalian perubahan formal?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-AI7
Tanggal		Tanggal :		
Proses :	**Install and Accredit Solutions and Changes (AI7)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kebijakan dan prosedur yang berhubungan dengan proses siklus pengembangan sistem?	√		
2	Apakah terdapat suatu metodologi siklus pengembangan sistem yang formal untuk instalasi sistem dan akreditasi, yang meliputi di antaranya, pendekatan dalam bentuk fase (*phased approach*) dari :			
	• pelatihan	√		
	• penentuan ukuran kinerja sistem	√		
	• Rencana konversi	√		
	• pengujian program-program	√		
	• berbagai grup program dan sistem keseluruhan	√		
	• Rencana pengujian paralel dan prototipe	√		
	• pengujian penerimaan sistem	√		
	• pengujian keamanan dan akreditasi	√		
	• pengujian operasional sistem	√		
	• pengendalian perubahan	√		
	• implementasi dan review sesudah implementasi	√		
	• modifikasi	√		
3	Apakah terdapat pelatihan bagi pengguna yang merupakan bagian dari setiap usaha pengembangan sistem?	√		
4	Apakah staf TI sadar dan peduli serta memahami kebutuhan pengendalian terhadap pengembangan sistem dan pelatihan bagi pengguna?	√		
5	Apakah terdapat proses monitoring terhadap pelatihan, untuk memperoleh *feedback* yang dapat memperbaiki sistem yang ada?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
6	Apakah berbagai pengendalian program/sistem konsisten dengan standar keamanan di Perusahaan?	√		
7	Apakah berbagai pengendalian program/sistem sesuai dengan standar, kebijakan, dan prosedur TI?	√		
8	Apakah terdapat berbagai macam pengembangan dan pengujian untuk berbagai proses dalam sistem (*in process system*)?	√		
9	Apakah terdapat kriteria-kriteria yang telah ditentukan sebelumnya bagi keberhasilan pengujian, kegagalan, dan penghentian dari usaha/tindakan yang lebih jauh?	√		
10	Apakah rencana pengujian sistem untuk menilai resiko proyek telah mencakup semua kebutuhan pengujian secara fungsional dan teknis?	√		
11	Apakah rencana pengujian untuk simulasi volume, interval pemrosesan, ketersediaan output, instalasi dan akreditasi merupakan bagian dari proses pengujian itu sendiri?	√		
12	Apakah ada kebijakan, prosedur yang mengatur rencana mitigasi infrastruktur dan konversi data serta mempertimbangkan, perangkat keras, jaringan, sistem operasi, perangkat lunak, data transaksi, file master, *backup* dan *archive*, antarmuka dengan system intern dan ekstern, prosedur, dokumentasi sistem dll?	√		
13	Apakah dilakukan pengujian terhadap lingkup produksi, yang mencakup beban kerja, sistem operasi, aplikasi perangkat lunak yang dibutuhkan, sistem manajemen database, dan infrastruktur jaringan?	√		
14	Terdapat rencana untuk melakukan proses *fallback* dan *recovery* apabila terjadi kegagalan dalam proses implementasi	√		
15	Terdapat suatu lingkungan TI yang *secure*, dengan memperhatikan *security, internal control, operational practices*, kualitas data, kebutuhan *privacy* dan beban kerja	√		
16	Terdapat perlindungan terhadap data pada waktu melakukan pengujian	√		

No	Pertanyaan	Ya	Tidak	Keterangan
17	Apakah pada waktu melakukan konversi data perangkat keras, jaringan, sistem operasi, perangkat lunak, transaksi data, *file master, backup dan archives, interface* dengan sistem internal dan eksternal, prosedur, dan dokumentasi sistem dilindungi?	√		
18	Apakah sebelum dilakukan konversi, data yang ada di-*back up* terlebih dahulu agar dapat dilakukan proses *fallback* and *recovery*?	√		
19	Apakah terdapat pengujian yang dilakukan secara independen terhadap perubahan yang terjadi sesuai dengan rencana pengujian yang telah didefinisikan sebelumnya dan telah mempertimbangkan keamanan dan kinerja sistem?	√		
20	Apakah dilakukan evaluasi terhadap hasil pengujian, apabila ada kesalahan yang berhasil diidentifikasi akan dilakukan suatu proses/tindakan korektif?	√		
21	Adanya perbandingan kepuasan pemakai/pengguna antara produk/layanan vendor dengan produk *in-house*	√		
22	Apakah digunakan alat-alat yang terotomatisasi dalam mengoptimalkan sistem yang dikembangkan dengan tujuan efisiensi?	√		
23	Apakah dalam memperbaharui *source program* atau penghentian penggunaan aplikasi versi lama, mengikuti prosedur yang ada?	√		
24	Apakah terdapat prosedur untuk melakukan *post implementation review*, dengan tujuan melihat apakah ada isu-isu yang perlu diperhatikan dan ditangani setelah dilakukan implementasi sistem?	√		
25	Terdapat pengendalian terhadap distribusi perangkat lunak yang terotomasi untuk melakukan verifikasi bahwa proses distribusi menuju ke tujuan yang memang diberikan wewenang dan telah diidentifikasi dengan benar	√		
26	Meskipun perangkat lunak telah didistribusikan, tetap terdapat *formal log* yang mencatat perangkat lunak didistribusikan kemana, kapan diimplementasikan dan kapan dilakukan proses *update* terhadap masing-masing perangkat lunak tersebut.	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS1
Tanggal		Tanggal :		
Proses :	**Define and Manage Service Levels (DS1)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah proses persetujuan tingkat jasa/layanan (*service level agreement*) diidentifikasi dengan kebijakan?	√		SLA antara DTI dengan user
2	Apakah ada partisipasi dari pengguna (user) dalam membuat dan memodifikasi *agreement*?	√		
3	Apakah kewajiban dari pengguna dan provider didefinisikan dengan jelas?	√		
4	Apakah terdapat suatu proses perbaikan dan penyesuaian tingkat jasa/layanan (*service level agreement*) yang didasarkan pada *performance feedback* dari pihak yang diberi layanan dan kebutuhan bisnis?	√		
5	Apakah DTI memantau dan melaporkan pencapaian dari kriteria performa jasa tertentu?	√		
6	Apakah DTI memantau dan melaporkan seluruh masalah yang dihadapi?	√		
7	Apakah manajemen melakukan review teratur secara periodik terhadap proses TI?	√		
8	Apakah terdapat proses untuk mengidentifikasi sehubungan dengan hal-hal yang tidak tercapai (*non-performance*)?	√		
9	Apakah persetujuan tingkat jasa (*service level agreement*) mencakup diantaranya hal-hal berikut:			
	• definisi jasa	√		
	• biaya jasa	√		
	• tingkat jasa minimum yang dapat diukur/dikuantifikasi	√		
	• tingkat dukungan dari fungsi TI	√		
	• ketersediaan, kehandalan, kapasitas untuk pertumbuhan	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	• rencana kontinuitas	√		
	• kebutuhan-kebutuhan keamanan	√		
	• prosedur perubahan bagi setiap persetujuan	√		
	• persetujuan tertulis dan formal disetujui antara provider dan pengguna jasa	√		
	• review periode efektif dan periode baru	√		
	• isi dan frekuensi pelaporan performa dan pembayaran atas jasa	√		
	• biaya yang dibebankan adalah realistis dibandingkan terhadap sejarah dan praktik-praktik terbaik	√		
	• kalkulasi dari biaya yang dibebankan	√		
	• komitmen perbaikan/peningkatan jasa	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS2
Tanggal		Tanggal :		
Proses :	Manage Third Party Services (DS2)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah tugas dan tanggung jawab pihak ketiga telah didokumentasikan dalam bentuk formal?	√		
2	Apakah terdapat kebijakan dan prosedur TI mengenai hubungan dengan pihak ketiga (*third party relationship*)?	√		Sedang dalam proses pengerjaan
3	Masih berhubungan dengan pertanyaan sebelumnya, apakah hal tersebut di atas konsisten dengan kebijakan umum perusahaan (*organisational general policies*)?	√		
4	Apakah terdapat kebijakan yang secara khusus mengatur kebutuhan akan kontrak, dan definisi isi kontrak?	√		
5	Apakah terdapat *relationship manager* atau semacamnya yang bertanggung jawab terhadap kontrak, termasuk pengawasannya?	√		
6	Apakah kontrak yang dibuat mewakili catatan/penjelasan yang lengkap dan menyeluruh dari hubungan dengan pihak ketiga?	√		
7	Apakah terdapat suatu daftar yang berisikan hubungan pihak ketiga, dan apakah daftar tersebut selalu diperbaharui, dikelompokkan dengan tepat dan rinci, agar memudahkan sewaktu melakukan monitoring terhadap pihak ketiga?	√		
8	Apakah dibentuk suatu kontrak untuk kontinuitas jasa?	√		
9	Masih berhubungan dengan pertanyaan sebelumnya, apakah kontrak tersebut mencakup rencana kontinuitas oleh *supplier* untuk memastikan adanya jasa yang	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	kontinu?			
10	Apakah kontrak yang ada mencakup hal-hal: • persetujuan manajemen formal dan hukum	√		
	• entitas hukum yang memberikan jasa	√		
	• jasa-jasa yang diberikan/disediakan	√		
	• persetujuan tingkat jasa (*service level agreement*) baik kualitatif maupun kuantitatif	√		
	• biaya jasa/layanan dan frekuensi pembayaran atas jasa	√		
	• solusi dari masalah yang ada	√		
	• pemberian pinalti apabila hal-hal yang disepakati tidak tercapai (*non-performance*)	√		
	• proses penghentian	√		
	• proses modifikasi	√		
	• pelaporan jasa/layanan, mencakup isi, frekuensi, dan distribusi	√		
	• peran antara pihak-pihak yang terlibat dalam kontrak	√		
	• kapasitas kontinuitas, bahwa jasa akan diberikan/disediakan oleh pemasok	√		
	• proses komunikasi antara pengguna dan provider	√		
	• jangka waktu kontrak	√		
	• tingkat akses yang diberikan/disediakan oleh *supplier* (vendor)	√		
	• kebutuhan-kebutuhan keamanan	√		
	• jaminan kerahasiaan (tidak diungkap kepada pihak yang tidak berwenang)	√		
	• hak untuk melakukan akses dan melakukan audit	√		
11	Apakah pihak ketiga yang potensial dikualifikasikan (dinyatakan lulus) melalui penilaian atas kemampuan mereka (*due dilligence*) yang disesuaikan dengan kebutuhan PT Bank XYZ?	√		
12	Apakah dilakukan monitoring terhadap layanan/kinerja yang diberikan oleh pihak ketiga?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
13	Apakah pihak ketiga secara reguler memberikan laporan kinerja kepada manajemen, untuk melihat apakah layanan yang diberikan telah sesuai dengan kontrak dan yang telah ditentukan dalam SLA?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS3
Tanggal		Tanggal :		
Proses :	Manage Performance and Capacity (DS3)			

No		Ya	Tidak	Keterangan
1	Apakah terdapat suatu proses *benchmark* terhadap kemampuan/kinerja TI yang ada untuk mengidentifikasi perbaikan yang perlu dilakukan, baik secara internal maupun eksternal?	√		
2	Apakah kerangka waktu dan tingkat layanan (*level of service*) didefinisikan untuk semua layanan yang diberikan/disediakan oleh fungsi TI?	√		
3	Apakah kerangka waktu dan tingkat layanan (*level of service*) merefleksikan kebutuhan para pengguna?	√		
4	Apakah kerangka waktu dan tingkat layanan (*level of service*) konsisten dengan harapan/ekspektasi kinerja dari peralatan TI?	√		
5	Apakah terdapat suatu *performance* dan *capacity plan*, yang merefleksikan kebutuhan pengguna?	√		
6	Apakah staf TI mengetahui dan memahami *capacity plan* yang ada, sehingga mereka dapat menerapkannya pada waktu melakukan perubahan terhadap aplikasi, server dan sumber daya TI lainnya?	√		Hanya staf tertentu saja yang memiliki kewenangan
7	Apakah terdapat rencana ketersediaan (*availability plan*) dan merefleksikan kebutuhan pengguna?	√		
8	Apakah terdapat suatu cara untuk melakukan identifikasi dan pelacakan bila terjadi insiden dan kinerja yang	√		

No		Ya	Tidak	Keterangan
	buruk? Jika ya, sebutkan caranya di kolom keterangan.			
9	Apakah dalam *performance* dan *capacity planning*, juga memperhitungkan tindakan yang harus dilakukan dalam menghadapi kondisi-kondisi yang tidak terduga?	√		
10	Apakah terdapat pemantauan yang terus menerus terhadap seluruh peralatan, sumber daya dan kapasitas TI?	√		
11	Apakah *lack of performance* diperhatikan oleh pihak Divisi TI?	√		
12	Apakah peluang perbaikan/peningkatan kinerja diperhatikan atau dipenuhi oleh Divisi TI?	√		
13	Apakah performa konfigurasi yang optimal diawasi melalui alat-alat pemodelan, teknik dan proses untuk memaksimalkan performa dan dengan mengurangi kapasitas TI sesuai dengan kebutuhan?	√		
14	Apakah pengguna secara proaktif melakukan review terhadap kinerja dan kemampuan TI serta memodifikasi/menyesuaikan dengan beban kerja yang ada?	√		
15	Apakah dalam melakukan penilaian beban kerja mengikutsertakan masukan dari pengguna (perubahan permintaan) dan dari supplier (teknologi baru/produk baru)?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS2
Tanggal		Tanggal :		
Proses :	Ensure Continuous Service (DS4)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah kebijakan organisasi mengharuskan sebuah kerangka dan rencana kontinuitas menjadi bagian kebutuhan operasional yang normal bagi fungsi TI dan semua organisasi?	√		
2	Apakah kebijakan dan prosedur TI mengharuskan adanya filosofi dan kerangka yang konsisten yang berhubungan dengan pengembangan rencana kontinuitas (*continuity plan*)?	√		
3	Apakah kebijakan dan prosedur TI mengharuskan adanya suatu penanganan kerusakan sistem (*disaster recovery)* dan kejadian yang tak terduga?	√		
4	Apakah kebijakan dan prosedur TI mengharuskan adanya pemrioritasan aplikasi dan ketepatan waktu pemulihan dan pengembalian?	√		
5	Apakah kebijakan dan prosedur TI mengharuskan adanya penjelasan peran dan tanggung jawab khusus/spesifik mengenai perencanaan kontinuitas dengan pengujian tertentu, pemeliharaan, dan kebutuhan pembaruan (*updating*)?	√		
6	Apakah kebijakan dan prosedur TI mengharuskan adanya kontrak formal dengan pemasok (vendor) untuk memberikan/menyediakan jasa pemulihan (*recovery*) termasuk fasilitas *back-up*?	√		
7	Apakah telah dilakukan pengujian secara reguler untuk memastikan kualitas *backup* dan media *backup*?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
8	Apakah kebijakan dan prosedur TI mengharuskan dalam setiap rencana kontinuitas isinya mencakup:			
	• prosedur-prosedur darurat untuk memastikan keselamatan dari seluruh anggota staf yang terkena dampaknya	√		
	• peran dan tanggung jawab fungsi TI, pemasok (vendor) yang memberikan jasa pemulihan, pengguna jasa, personil administrasi pendukung	√		
	• sebuah kerangka pemulihan (*recovery framework*) yang konsisten dengan kelangsungan rencana jangka panjang	√		
	• penjabaran dengan menuliskan suatu daftar yang berisi sumber daya alternatif meliputi *hardware, peripherals*, dan *software*	√		
	• penjabaran dengan menuliskan suatu daftar yang berisi aplikasi yang mendapat prioritas paling tinggi sampai paling rendah dan waktu pemulihan yang dibutuhkan oleh aplikasi tersebut	√		
	• fungsi-fungsi administrasi untuk berkomunikasi dan memberikan jasa pendukung seperti *benefit, payroll, external communication, cost tracking* dan lain-lain	√		
	• berbagai skenario pemulihan dari hilangnya kemampuan mulai dari yang sedikit hingga hilang seluruhnya	√		
	• peralatan tertentu dan berbagai kebutuhan *supply*	√		
	• pelatihan dan kepedulian dari peran individual maupun kelompok	√		
	• jadwal pengujian, hasil pengujian terakhir dan tindakan korektif yang diambil dari pengujian sebelumnya	√		
	• alternatif pengujian jika pengujian sebelumnya tidak layak	√		
	• keharusan untuk mengukur dan melaporkan keberhasilan atau kegagalan suatu pengujian	√		
	• nama, alamat, dan nomor telepon dari *key personnel*	√		
	• rencana rekonstruksi untuk melakukan pemulihan	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	• alternatif-alternatif untuk memulai kembali proses bisnis (misalnya setelah gedung/tempat terbakar)	√		
9	Apakah rencana kontinuitas pengguna dibuat berdasarkan ketersediaan sumber daya fisik untuk menjalankan pemrosesan yang penting (manual dan terkomputerisasi)?	√		
10	Apakah terdapat pelatihan bagi semua pihak yang terlibat, yang meliputi pembelajaran terhadap prosedur, tugas dan tanggung jawab apabila terjadi suatu insiden atau kerusakan?	√		
11	Apakah dapat dipastikan bahwa seluruh layanan TI telah didistribusikan secara tepat dan aman dan dapat digunakan oleh seluruh pihak berwenang?	√		
12	Apakah dilakukan review terhadap rencana *recovery* TI untuk memastikan bahwa rencana *recovery* tersebut telah sesuai dengan kebutuhan organisasi?	√		
13	Apakah kelemahan TI yang ada telah menjadi perhatian manajemen TI dan telah dilakukan suatu usaha perbaikan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS5
Tanggal		Tanggal :		
Proses :	Ensure Systems Security (DS5)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat struktur organisasi memadai dan terdapat laporan mengenai sistem keamanan informasi yang ada dan apakah *security management* dan *administration function* memiliki kewenangan memadai?	√		
2	Apakah rencana keamanan stratejik berada pada tempatnya, yang memberikan arah dan pengendalian tersentralisir atas keamanan sistem informasi, bersama-sama dengan kebutuhan keamanan pengguna (untuk/supaya konsisten)?	√		
3	Pastikan bahwa terdapat kebijakan, standar dan prosedur yang mendetil dalam hal keamanan, yang meliputi:	√		Sedang dalam proses pengerjaan
	• Kepatuhan terhadap kebijakan dalam hal keamanan	√		Sedang dalam proses pengerjaan
	• Manajemen resiko	√		Sedang dalam proses pengerjaan
	• Komunikasi eksternal dalam hal kebijakan keamanan	√		Sedang dalam proses pengerjaan
	• Kebijakan dalam hal firewall	√		Sedang dalam proses pengerjaan
	• Kebijakan dalam hal keamanan e-mail	√		Sedang dalam proses pengerjaan
	• Kesepakatan untuk mematuhi kebijakan sistem informasi yang ada	√		Sedang dalam proses pengerjaan
	• Kebijakan pengamanan dalam hal laptop/desktop	√		Sedang dalam proses pengerjaan

No	Pertanyaan	Ya	Tidak	Keterangan
	• Kebijakan dalam hal penggunaan internet	√		Sedang dalam proses pengerjaan
4	Apakah *IT security plan* mempertimbangkan *IT tactical plans*, klasifikasi data, standar teknologi, keamanan dan kebijakan pengendalian, manajemen resiko dan syarat kepatuhan dari pihak eksternal?	√		Sedang dalam proses pengerjaan
5	Apakah terdapat suatu proses yang secara periodik akan mengupdate *IT security plan*, dan proses update tersebut direview dan disetujui oleh manajemen?	√		Sedang dalam proses pengerjaan
6	Tentukan apakah *IT security plan* mencakup: • Kebijakan keamanan yang lengkap dan standar yang sejalan dengan kerangka kebijakan keamanan informasi yang dikembangkan	√		Sedang dalam proses pengerjaan
	• Prosedur untuk mengimplementasikan kebijakan dan standar	√		Sedang dalam proses pengerjaan
	• Peran dan tanggung jawab staf	√		Sedang dalam proses pengerjaan
	• Kebutuhan staf	√		Sedang dalam proses pengerjaan
	• Kepedulian terhadap keamanan dan pelatihan	√		Sedang dalam proses pengerjaan
	• Praktek pelaksanaan keamanan	√		Sedang dalam proses pengerjaan
	• Investasi pada sumber daya keamanan yang dibutuhkan (*required security resources*)	√		Sedang dalam proses pengerjaan
7	Apakah terdapat suatu proses yang mengintegrasikan kebutuhan keamanan informasi dalam *IT security plan* yang mencakup pengembangan *Service Level Agreement* dan *Operational Level Agreement*, *automated solution requirements*, *application software*, dan komponen infrastruktur TI?	√		Sedang dalam proses pengerjaan
8	Apakah keamanan yang tersentralisir berada pada tempatnya, untuk memastikan akses yang tepat/sesuai terhadap sumber daya sistem?	√		Sedang dalam proses pengerjaan

No	Pertanyaan	Ya	Tidak	Keterangan
9	Apakah skema klasifikasi data berada pada tempatnya dan sedang digunakan, untuk memastikan bahwa semua sumber daya sistem memiliki seorang pemilik yang bertanggung jawab atas keamanan dan isinya?	√		Sedang dalam proses pengerjaan
10	Apakah *information security system* cukup responsif terhadap perubahan yang terjadi akibat kebutuhan organisasi?	√		Sedang dalam proses pengerjaan
11	Apakah profil keamanan pengguna berada pada tempatnya, yang mewakili "*least access as required*" dan secara reguler direview oleh pihak manajemen untuk akreditasi kembali?	√		Sedang dalam proses pengerjaan
12	Apakah terdapat penyuluhan (*indoctrination*) kepada pegawai mengenai keamanan sistem, tanggung jawab kepemilikan dan kebutuhan proteksi virus?	√		Sedang dalam proses pengerjaan
13	Apakah terdapat pelaporan sehubungan dengan berbagai usaha pengrusakan/penerobosan terhadap sistem keamanan?	√		Sedang dalam proses pengerjaan
14	Apakah terdapat prosedur yang berhubungan dengan pemeliharaan kunci dan modul *cryptographic?*	√		Sedang dalam proses pengerjaan
15	Masih berhubungan dengan pertanyaan sebelumnya, apakah prosedur tersebut diatur/dikendalikan secara terpusat dan digunakan untuk seluruh aktivitas akses eksternal dan trasmisi data?	√		
16	Apakah terdapat standar manajemen kunci *cryptographic* untuk aktifitas tersentralisir dan aktifitas pengguna?	√		
17	Apakah pengendalian perubahan atas perangkat lunak keamanan bersifat formal dan konsisten dengan standar normal dari pemeliharaan dan pengembangan sistem?	√		
18	Apakah terdapat kebijakan terhadap penetapan user, standar dan prosedur bagi semua user dan proses yang meliputi vendor, penyedia jasa layanan dan partner bisnisnya?	√		
19	Apakah mekanisme otentikasi (*authentication mechanism*) yang sedang digunakan memberikan fitur berikut ini: • *single-use of authentication data* (misalnya kata sandi tidak pernah		√	

No	Pertanyaan	Ya	Tidak	Keterangan
	digunakan kembali)			
	• *multiple authentication* (digunakan dua atau lebih mekanisme otentifikasi yang berbeda)	√		
	• *policy based authentication* (kemampuan untuk menspesifikasi prosedur-prosedur otentifikasi yang terpisah untuk kejadian khusus/spesifik)	√		
	• *on-demand authentication* (kemampuan untuk melakukan otentifikasi kembali pengguna setelah otentifikasi awal)	√		
20	Apakah terdapat pembatasan terhadap jumlah akses atau sesi yang terjadi secara bersamaan dari seorang pengguna?	√		
21	Pada saat akan menyelesaikan *log-on* apakah terdapat pemberitahuan (*warning*) untuk menginformasikan bahwa akses yang tidak berwenang bisa mengakibatkan timbulnya tuntutan (*prosecution*)?	√		
22	Pada saat *log-on*, apakah terdapat pesan pemberitahuan kepada pengguna mengenai penggunaan yang tepat dari perangkat keras, perangkat lunak, atau koneksi/hubungan?	√		
23	Atas berbagai akses yang terjadi, apakah terdapat pelaporan mengenai kegagalan maupun keberhasilan akses kepada pengguna?	√		
24	Apakah kebijakan mengenai kata sandi (*password*) mencakup:			
	• mendorong diubahnya kata sandi yang diperoleh pertama kali	√		
	• panjangnya kata sandi minimum yang tepat/memadai	√		
	• mendorong seringnya perubahan kata sandi	√		
	• perlindungan/proteksi yang cukup atas kata sandi darurat	√		
25	Apakah terdapat prosedur penanganan atau resolusi masalah yang formal, misalnya, mengnonaktifkan user ID setelah lima kali gagal melakukan log-on; waktu otentifikasi dibatasi selama lima menit; pengguna diberitahu mengenai peng-nonaktifan (suspensi), tetapi tidak perlu memberitahukan alasannya?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
26	Apakah terdapat *firewall* perangkat lunak dan perangkat keras untuk membatasi akses terhadap aset informasi?	√		
27	Apakah terdapat peng-nonaktifan kata sandi dari pegawai yang sudah tidak bekerja lagi?	√		
28	Apakah terdapat pembatasan akses ke lokasi tertentu/khusus yang berhubungan dengan TI?	√		
29	Apakah terdapat rotasi personil (yang tidak diumumkan terlebih dahulu) untuk aktifitas-aktifitas penting/sensitif yang dilakukan secara berkelanjutan?		√	
30	Apakah perangkat keras dan perangkat lunak yang berhubungan dengan keamanan mendapat perlindungan yang cukup, dan terdapat pembatasan akses?	√		
31	Apakah terdapat pembatasan akses terhadap data, seperti manajemen keamanan, kata sandi, kunci *cryptographic*?	√		
32	Apakah terdapat kebijakan mengenai keamanan jaringan meliputi layanan yang diberikan, lalu lintas data, tipe koneksi yang diperbolehkan?	√		Sedang dalam proses pengerjaan
33	Apakah terdapat prosedur atau *guidelines* untuk mengatur semua komponen jaringan yang penting misalnya *router, DMZ, VPN switches* yang diperbaharui secara reguler dan perubahan tersebut didokumentasikan dengan baik?	√		Sedang dalam proses pengerjaan
34	Apakah terdapat penggunaan jalur yang benar-benar aman dalam mentransmisikan informasi sensitif yang belum dienkripsi (*non-encrypted*)?	√		
35	Apakah terdapat pembatasan terhadap penyebaran alamat email ke pihak luar, untuk melindungi sistem dari *junk mail*?	√	-	
36	Apakah terdapat ukuran (*measure*) pengendalian pencegahan dan deteksi yang dibuat oleh manajemen yang berhubungan dengan virus komputer?	√		
37	Apakah terdapat prosedur yang mendorong terjaganya integritas dari *electronic value*, seperti fasilitas *card reader* dilindungi dari pengrusakan, informasi kartu (PIN dan informasi lainnya) dilindungi dan pencegahan terhadap pemalsuan kartu?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
38	Apakah aspek keamanan dapat diterapkan di seluruh aspek TI dalam organisasi?	√		
39	Apakah semua aset organisasi yang penting dan jaringan yang beresiko tinggi dimonitor secara rutin?	√		
40	Apakah terdapat *Computer Emergency Response Team* (CERT) yang mampu mengendalikan keadaan darurat dari kejadian yang berkaitan dengan keamanan. Hal berikut harus menjadi bagian penting dari proses CERT:			Sedang dalam proses pengerjaan
	• Penanganan insiden - Terdapat prosedur umum dan khusus untuk menangani insiden secara efektif dan melaporkan bila terjadi serangan/ancaman dari luar	√		Sedang dalam proses pengerjaan
	• *Vendor relation* - Tugas dan tanggung jawab vendor dalam mencegah dan menindaklanjuti insiden yang terjadi, melakukan koreksi terhadap kesalahan perangkat lunak dan area TI lainnya	√		Sedang dalam proses pengerjaan
	• Komunikasi - Kebutuhan, implementasi dan penanganan keadaan darurat dikomunikasikan ke manajemen	√		Sedang dalam proses pengerjaan
	• Investigasi terhadap isu hukum dan kriminal - Isu dipicu oleh pertimbangan hukum dan kebutuhan atau batasan yang dihasilkan akibat investigasi kriminal selama terjadinya insiden	√		Sedang dalam proses pengerjaan
	• *Constituency relation - respon centre* akan memberikan dukungan terhadap pemberian layanan dan metode pelatihan, kepedulian, manajemen konfigurasi dan autentifikasi	√		Sedang dalam proses pengerjaan
	• Agenda riset dan interaksi - identifikasi terhadap kegiatan riset yang ada dan riset yang perlu dilakukan dalam hubungannya dengan kegiatan *response centre*	√		Sedang dalam proses pengerjaan
	• *Model of the threat* - Pembangunan suatu pemodelan yang mengkarakteristikkan ancaman dan resiko yang mungkin timbul untuk membantu mengurangi kegiatan yang beresiko	√		Sedang dalam proses pengerjaan
	• Isu eksternal - Faktor-faktor yang berada di luar pengendalian dan pengawasan organisasi (contoh hukum, kebijakan,	√		Sedang dalam proses pengerjaan

No	Pertanyaan	Ya	Tidak	Keterangan
	syarat prosedural)			
41	Apakah pengendalian terhadap akses file dan data secara fisik maupun logik direview secara tahunan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS6
Tanggal		Tanggal :		
Proses :	Identify and Allocate Costs (DS6)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat prosedur, yang mendorong dibuatnya rencana pemeliharaan dan pengembangan rutin dengan memperhatikan prioritas dari pengguna?	√		
2	Apakah terdapat prosedur, dimana pengguna memiliki keterlibatan yang cukup tinggi dalam menentukan penggunaan sumber daya TI?	√		
3	Apakah terdapat prosedur yang mendorong dibuatnya anggaran TI tahunan yang sesuai dengan kebutuhan organisasi?	√		
4	Apakah terdapat prosedur yang mendorong dibuatnya anggaran TI tahunan yang memperhatikan biaya-biaya di masa lampau serta beberapa asumsi, agar dapat memberikan pemahaman kepada pengguna?	√		
5	Apakah terdapat prosedur yang mendorong dibuatnya anggaran TI tahunan berisi alokasi biaya bagi fungsi/layanan TI, yang memerlukan persetujuan pengguna terlebih dahulu?	√		
6	Apakah terdapat prosedur yang mendorong dibuatnya anggaran TI tahunan yang mencakup pelaporan dan pembebanan aktual (yang terjadi sebenarnya)?	√		
7	Apakah terdapat prosedur yang memantau/melacak biaya-biaya yang dialokasikan atas berbagai sumber daya TI?	√		
8	Apakah terdapat prosedur yang mendorong pelaporan secara teratur kepada pengguna atas kinerja untuk berbagai kategori biaya?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
9	Apakah terdapat prosedur yang mendorong pelaporan kepada pengguna mengenai perbandingan dengan pihak luar (*benchmarking*) mengenai efektifitas biaya?	√		
10	Apakah terdapat prosedur yang mendorong dilakukannya modifikasi tepat waktu terhadap alokasi biaya untuk mencerminkan kebutuhan organisasi yang berubah-ubah?	√		Masih dalam proses pengerjaan
11	Apakah terdapat prosedur yang secara formal menyetujui dan menerima biaya/beban seperti yang diterima?	√		
12	Apakah terdapat prosedur yang mengidentifikasi peluang perbaikan/peningkatan TI untuk mengurangi biaya/beban atau mendapatkan nilai yang lebih dengan jumlah biaya/beban yang sama?	√		
13	Apakah terdapat laporan yang merekam dan menggambarkan/menjelaskan berbagai perubahan dari komponen-komponen biaya dan prosedur perhitungan alokasi?	√		
14	Apakah dilakukan review secara reguler (tahunan atau semi tahunan) terhadap alokasi biaya yang mencakup kebutuhan Perusahaan dan perubahan layanan TI di Perusahaan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS7
Tanggal		Tanggal :		
Proses :	Educate and Train Users (DS7)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat kebijakan dan prosedur yang berhubungan dengan kesadaran akan keamanan dan pengendalian yang berkelanjutan?	√		
2	Apakah terdapat program pelatihan dan pendidikan yang memfokuskan pada keamanan sistem informasi dan prinsip-prinsip pengendalian, bagi staf TI?	√		
3	Apakah setiap pegawai menyadari tanggung jawab akan pentingnya keamanan dalam penggunaan dan penjagaan sumber daya TI?	√		
4	Apakah terdapat kebijakan dan prosedur yang berhubungan dengan pelatihan dan sesuai dengan konfigurasi teknis dari sumber daya TI saat ini?	√		
5	Apakah terdapat peluang pelatihan *in-house*, dan sering diikuti oleh pegawai?	√		
6	Apakah terdapat peluang pelatihan teknis TI dari luar yang sering diikuti oleh pegawai?	√		
7	Apakah terdapat fungsi pelatihan yang bertugas menilai kebutuhan pelatihan personil mengenai keamanan dan pengendalian?	√		
8	Apakah semua pegawai diharuskan untuk menghadiri pelatihan akan pentingnya keamanan TI, misalnya mengenai prinsip keamanan sistem secara umum, kode etik dalam TI dan lain-lain?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
9	Apakah pelatihan kesadaran keamanan telah mencakup kebijakan untuk mencegah pengungkapan informasi penting/sensitif melalui percakapan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS8
Tanggal		Tanggal :		
Proses :	Manage Service Desk and Incidents (DS8)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah telah dilakukan analisa untuk menentukan model bagian pelayanan TI, staf, alat TI yang terintegrasi dengan proses lain?	√		
2	Apakah sifat fungsi *help desk* (yaitu bagaimana permintaan bantuan/asistensi diproses dan diberikan) berjalan efektif?	√		
3	Apakah tindakan dokumentasi untuk kegiatan *help desk* dinilai cukup/memadai?	√		
4	Apakah terdapat instruksi untuk menangani permintaan yang tidak dapat segera diselesaikan oleh staf bagian layanan TI, dengan mencari alternatif solusi lain?	√		
5	Apakah terdapat proses aktual untuk mencatat/memasukkan dan mandaftar permintaan jasa/layanan?	√		
6	Apakah terdapat suatu proses dan atau *tools* untuk mencatat permintaan pelanggan, status permintaan tersebut dan tindakan untuk mengatasi permintaan tersebut?	√		
7	Apakah catatan yang berisi terjadinya kesalahan selalu di-*update*, untuk menunjukkan tanggal dan waktu penugasan personel TI terhadap penyelesaian permintaan yang ada?	√		
8	Apakah terdapat proses yang cukup/memadai untuk pengajuan pertanyaan dan intervensi pimpinan dalam memecahkan masalah?	√		
9	Apakah terdapat jangka waktu yang cukup/memadai dalam menangani/menjawab setiap pertanyaan yang diajukan?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
10	Apakah terdapat prosedur untuk memantau/melacak perkembangan dan pelaporan atas kegiatan *help desk*?	√		
11	Apakah tindakan/inisiatif perbaikan/peningkatan kinerja secara formal diidentifikasi dan dilaksanakan secara kontinyu?	√		
12	Apakah terdapat kesesuaian antara *service level agreement* dengan standar kinerja/performa?	√		
13	Apakah tingkat kepuasan pengguna secara periodik ditentukan/diukur dan dilaporkan?	√		
14	Apakah telah dilakukan suatu analisa *trend* permintaan untuk mengidentifikasi pola kesalahan yang sering terjadi?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS9
Tanggal		Tanggal :		
Proses :	Manage the Configuration (DS9)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah proses untuk menciptakan dan mengendalikan *configuration baseline* (titik *cut-off* dalam perancangan dan pengembangan dari suatu item konfigurasi, dan evolusi tidak terjadi tanpa adanya pengendalian konfigurasi yang ketat) tepat?	√		
2	Apakah terdapat fungsi-fungsi untuk memelihara *configuration baseline*?	√		
3	Apakah prosedur pengendalian konfigurasi mencakup integritas *configuration baseline*?	√		
4	Apakah prosedur pengendalian konfigurasi mencakup pengendalian otorisasi akses terprogram terhadap perubahan sistem?	√		
5	Apakah prosedur pengendalian konfigurasi mencakup pemulihan (*recovery*) dari item-item konfigurasi?	√		
6	Apakah prosedur pengendalian konfigurasi mencakup penyelesaian konfigurasi dan laporan yang menilai kecukupan dari prosedur pencatatan konfigurasi?	√		
7	Apakah prosedur pengendalian konfigurasi mencakup individu-individu (yang bertanggung jawab untuk melakukan review pengendalian konfigurasi) yang memiliki pengetahuan, keahlian dan kemampuan yang sesuai?	√		
8	Apakah prosedur pengendalian konfigurasi mencakup adanya prosedur-prosedur untuk melakukan review akses ke *software baseline*?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
9	Apakah prosedur pengendalian konfigurasi mencakup hasil dari review yang diberikan kepada pimpinan untuk tindakan perbaikan?	√		
10	Apakah dilakukan review periodik terhadap konfigurasi sistem?	√		
11	Apakah *configuration baseline* memiliki sejarah/historis yang cukup/memadai untuk melacak berbagai perubahan?	√		
12	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk membuat dan memelihara program aplikasi yang dilisensi?	√		
13	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk memastikan program aplikasi yang dilisensi dikendalikan secara memadai?	√		
14	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk memastikan kehandalan dan integritas perangkat lunak?	√		
15	Apakah terdapat prosedur pengendalian terhadap perubahan perangkat lunak untuk memastikan kehandalan dan integritas dari *authorised software* yang digunakan, dan untuk memeriksa *unauthorised software*?	√		
16	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk memberikan tanggung jawab dalam pengendalian *unauthorised software* kepada staf tertentu?	√		
17	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk mencatat pemakaian *unauthorised software* dan pelaporan kepada DTI untuk tindakan perbaikan yang dilakukan?	√		
18	Apakah terdapat prosedur pengendalian perubahan perangkat lunak untuk menentukan apakah manajemen mengambil tindakan perbaikan atas penyimpangan yang terjadi atau tidak?	√		
19	Apakah proses untuk memindahkan (migrasi) aplikasi yang sedang dalam pengembangan ke lingkungan pengujian, dan akhirnya ke dalam status produksi, akan mengakibatkan perubahan pada laporan konfigurasi?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
20	Apakah proses penyimpanan perangkat lunak mencakup pendefinisian area penyimpanan file yang aman untuk semua perangkat lunak yang berlaku dalam tahap yang tepat dari siklus hidup pengembangan sistem?	√		
21	Apakah proses penyimpanan perangkat lunak mencakup diharuskannya pemisahan tempat penyimpanan perangkat lunak yang satu dengan perangkat lunak yang lain?	√		
22	Apakah proses penyimpanan perangkat lunak mencakup pendefinisian pengendalian akses logika dan fisik?	√		
23	Apakah proses penyimpanan perangkat lunak memperhatikan akuntabilitas perangkat lunak?	√		
24	Apakah proses penyimpanan perangkat lunak mencakup pembuatan/penetapan jejak audit?	√		
25	Apakah proses penyimpanan perangkat lunak mencakup pendeteksian, pendokumentasian, dan pelaporan kepada Divisi TI semua kejadian yang tidak sesuai dengan prosedur yang telah ditetapkan?	√		
26	Apakah proses penyimpanan perangkat lunak mencakup penentuan apakah Divisi TI mengambil tindakan perbaikan atau tidak?	√		
27	Apakah terdapat koordinasi di antara pengembangan aplikasi, kepastian kualitas, dan operasi mengenai pembaharuan (updating) dari *configuration baseline* atas perubahan yang terjadi?	√		
28	Apakah perangkat lunak diberi label (identitas) secara periodik dan diinvetarisir?	√		
29	Apakah terdapat penggunaan *library management software* untuk menghasilkan jejak audit dari perubahan-perubahan program?	√		
30	Apakah terdapat penggunaan *library management software* untuk memelihara jumlah/banyaknya versi program?	√		
31	Apakah terdapat penggunaan *library management software* untuk mencatat dan melaporkan perubahan-perubahan program?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
32	Apakah terdapat penggunaan *library management software* untuk memelihara informasi tanggal/pembuatan program?	√		
33	Apakah terdapat penggunaan *library management software* untuk memelihara *copy* dari versi program sebelumnya?	√		
34	Apakah terdapat penggunaan *library management software* untuk mengendalikan pembaharuan-pembaharuan (*updating*) yang terjadi secara bersamaan?	√		
35	Apakah setiap aset yang baru selalu dicatat?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS2
Tanggal		Tanggal :		
Proses :	Manage Problems (DS10)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah terdapat proses manajemen/pengelolaan masalah yang memastikan bahwa semua kejadian operasional yang bukan merupakan bagian dari operasi standar dicatat, dianalisa dan dicari penyelesaiannya secara tepat waktu?	√		
2	Apakah terdapat proses manajemen/pengelolaan masalah yang mendorong dibuatnya laporan atas masalah-masalah yang signifikan?	√		
3	Apakah terdapat prosedur pengelolaan masalah untuk mendefinisikan dan mengimplementasikan sistem manajemen/pengelolaan masalah?	√		
4	Apakah terdapat prosedur pengelolaan masalah untuk mencatat, menganalisa, dan mencari penyelesaian secara tepat waktu untuk semua peristiwa yang tidak sesuai standar/non standar?	√		
5	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk membuat laporan berbagai kejadian penting dan melaporkannya kepada pengguna (user)?	√		
6	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk mengidentifikasikan tipe-tipe permasalahan dan metodologi prioritisasi yang membolehkan berbagai usaha pemecahan masalah berdasarkan resiko?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
7	Apakah terdapat prosedur manajemen/pengelolaan masalah pendistribusikan keluaran (output) kepada pihak-pihak yang tidak berwenang?	√		
8	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk melacak/menelusuri kecenderungan permasalahan?	√		
9	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk mengumpulkan data permasalahan yang terjadi dengan tepat, akurat dan konsisten demi mendukung proses pelaporan?	√		
10	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk menentukan apakah manajemen secara periodik mengevaluasi proses manajemen/pengelolaan masalah, untuk meningkatkan efisiensi dan efektivitas?	√		
11	Apakah terdapat prosedur manajemen/pengelolaan masalah untuk mendorong kecukupan jejak audit bagi permasalahan sistem?	√		
12	Apakah terdapat prioritas dalam pemrosesan masalah yang darurat?	√		
13	Masih berhubungan dengan pertanyaan sebelumnya, apakah pemrosesan tersebut telah didokumentasikan?	√		
14	Masih berhubungan dengan pertanyaan sebelumnya, apakah pemrosesan tersebut membutuhkan persetujuan dari DTI?	√		
15	Apakah terdapat prosedur otorisasi akses yang bersifat sementara dan darurat yang mengharuskan adanya pendokumentasian akses dan dipelihara/disimpan dalam suatu file?	√		
16	Apakah terdapat prosedur otorisasi akses sementara dan darurat yang mengharuskan adanya persetujuan dari Divisi TI?	√		
17	Apakah terdapat prosedur otorisasi terhadap akses sementara dan darurat dengan memperhitungkan fungsi keamanan?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS11
Tanggal		Tanggal :		
Proses :	Manage Data (DS11)			

No	Pertanyaan	Ya	Tidak	Keterangan
For Data Preparation				
1	Apakah terdapat prosedur persiapan data yang memastikan kelengkapan, ketepatan, dan validitas data?	√		Sedang dalam proses pengerjaan
2	Apakah terdapat prosedur otorisasi untuk semua dokumen sumber?	√		Sedang dalam proses pengerjaan
3	Apakah terdapat pemisahan tugas antara pihak yang menghasilkan, yang menyetujui, dan yang mengkonversi dokumen sumber menjadi sebuah data?	√		
4	Apakah data ditransmisikan secara tepat waktu?	√		
5	Apakah terdapat review secara periodik terhadap dokumen sumber mengenai penyelesaian dan persetujuannya?	√		
6	Apakah terdapat penanganan yang tepat/sesuai apabila dokumen sumber mengandung kesalahan?	√		
7	Apakah terdapat pengendalian yang cukup untuk melindungi informasi yang penting/sensitif pada dokumen sumber?	√		
8	Apakah terdapat prosedur yang memastikan kelengkapan dan ketepatan dokumen sumber dan konversi dokumen sumber yang tepat waktu?	√		Sedang dalam proses pengerjaan
9	Apakah terdapat penyimpanan/penahanan dokumen yang memadai (cukup lama) untuk membolehkan rekonstruksi pada saat terjadi kehilangan, ketersediaan untuk review dan audit, dan kebutuhan penyelidikan?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
For Data Input				
10	Apakah diperlukan persetujuan terlebih dahulu sebelum dilakukan input (entri) data?	√		
11	Apakah terdapat pemisahan tugas yang memadai di antara: bagian yang menyajikan, bagian yang menyetujui, bagian yang mengotorisasi dan fungsi entri data?	√		
12	Apakah terdapat terminal yang unik, dan identifikasi operator yang aman dalam melakukan proses input data?	√		
13	Apakah terdapat penggunaan, pemeliharaan, dan pengendalian dari terminal input data dan identitas (ID) operator?	√		
14	Apakah terdapat jejak audit untuk mengidentifikasi sumber masukan?	√		
15	Apakah terdapat verifikasi rutin atau pemeriksaan terhadap data yang dimasukkan, sesegera mungkin?	√		
16	Apakah terdapat penanganan yang tepat terhadap kesalahan dalam pemasukkan data?	√		
17	Apakah terdapat pemberian tanggung jawab yang jelas untuk mendorong otorisasi yang tepat atas data?	√		
For Data Processing				
18	Apakah terdapat program yang mampu menguji input yang mengandung kesalahan (misalnya program validasi dan editing)?	√		
19	Apakah terdapat program yang mampu memeriksa dan memvalidasi semua transaksi?	√		
20	Apakah terdapat program yang tidak membolehkan dibiarkannya kondisi-kondisi yang mengandung kesalahan (error)?	√		
21	Apakah terdapat prosedur penanganan kesalahan yang mencakup pengoreksian dan memerlukan persetujuan kembali?	√		
22	Apakah terdapat prosedur penanganan kesalahan yang mencakup didefinisikannya tanggung jawab individu atas file tunda/non aktif/suspen?	√		
23	Apakah terdapat prosedur penanganan kesalahan yang mencakup diperlukannya laporan atas kesalahan yang belum diselesaikan dari file tunda/non aktif/suspen?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
24	Apakah terdapat prosedur penanganan kesalahan yang mencakup ketersediaan rencana prioritisasi file tunda/non aktif/suspen atas dasar umur dan tipe?	√		
25	Apakah terdapat catatan dari program yang dijalankan dan transaksi yang diproses atau ditolak untuk keperluan jejak audit?	√		
26	Apakah terdapat kelompok pengendalian untuk mengawasi kegiatan input/entri dan menyelidiki kejadian-kejadian non-standar?	√		
27	Apakah terdapat prosedur tertulis untuk mengoreksi dan menyajikan kembali data yang mengandung kesalahan, termasuk solusinya (yang bersifat tidak menghambat pemrosesan yang lain) untuk dilakukan pemrosesan kembali?	√		
28	Apakah penyajian/peng-inputan kembali transaksi diproses sama seperti sebelumnya?	√		
29	Apakah terdapat tanggung jawab untuk mengoreksi kesalahan (error) pada proses input data?	√		
30	Apakah sistem *artificial intelligence* berada pada tempatnya dalam suatu kerangka pengendalian interaktif dengan operator manusia untuk memastikan bahwa keputusan-keputusan yang vital diproses dan disetujui?	√		
	For Output, Interfacing and Distribution			
31	Apakah akses ke keluaran (output) dibatasi secara fisik dan logika dan hanya boleh dilakukan oleh pihak yang berwenang?	√		
32	Apakah terdapat review yang berkelanjutan terhadap output?	√		
33	Apakah terdapat jejak audit untuk memfasilitasi pelacakan/penelusuran pemrosesan transaksi dan rekonsiliasi data?	√		
34	Apakah ketepatan laporan keluaran diperiksa, dan kesalahan (*error*) yang terdapat di dalam keluaran dikendalikan oleh personil yang ahli?	√		
35	Apakah terdapat definisi yang jelas dari isu-isu keamanan terhadap proses keluaran, *interfacing* (antar muka) dan distribusi?	√		
36	Apakah dilakukan komunikasi terhadap Divisi TI apabila terjadi pelanggaran	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	keamanan?			
37	Apakah terdapat metodologi standar untuk menindaklanjuti tindakan pelanggaran keamanan tersebut?	√		
38	Apakah terdapat pendefinisian yang jelas mengenai proses dan pihak yang bertanggung jawab terhadap pemusnahan (*disposal*) keluaran/output?	√		
39	Apakah proses pemusnahan material yang sudah tidak terpakai disaksikan oleh pihak yang berwenang?	√		
40	Apakah semua media masukan dan keluaran disimpan di lokasi yang terpisah?	√		
41	Apakah informasi yang telah dihapus, diatur sedemikian rupa sehingga benar-benar tidak bisa diambil kembali oleh pihak yang tidak berwenang?	√		
42	Apakah infrastruktur fisik yang ada akan mencegah data agar tidak hilang karena kebakaran, gangguan, serangan eksternal atau akses yang tidak diotorisasi?	√		
	For Media Library			
43	Apakah isi dari media *library* secara sistematik dicatat sebagai inventaris?	√		
44	Apakah penyimpangan yang terjadi diperbaiki tepat waktu?	√		
45	Apakah digunakan berbagai ukuran untuk memelihara integritas dari *magnetic media*?	√		
46	Apakah terdapat prosedur penjagaan untuk menjaga isi media library?	√		
47	Apakah tanggung jawab terhadap pengelolaan *media library* diberikan kepada staf TI tertentu?	√		
48	Apakah terdapat strategi pengembalian ke kondisi awal (*restoration*) dan media *back-up*?	√		
49	Apakah media *back-up* dipilih sesuai dengan strategi *back up*yang telah didefinisikan dan apakah dilakukan verifikasi secara reguler untuk menilai kegunaan media *back up* tersebut?	√		
50	Apakah media *back-up* tersimpan secara aman, dan lokasi penyimpanannya direview secara periodik dalam hal keamanan akses	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	fisik dan keamanan data file?			
51	Apakah periode penahanan/pemilikan dan ketentuan penyimpanan didefinisikan secara jelas untuk berbagai dokumen, data, program, laporan dan pesan?	√		
52	Apakah setiap percakapan dan setiap transaksi melalui telepon atau *email* dicatat, direkam dan disimpan (sepanjang tidak melanggar peraturan/hukum)?	√		
53	Apakah terdapat prosedur yang sesuai dengan kebutuhan/ketentuan proses bisnis dan peraturan yang berlaku, untuk mengarsipkan informasi?	√		
For Information Authentication and Integrity				
54	Apakah integritas data file diperiksa secara periodik?	√		
55	Apakah dilakukan verifikasi terhadap permohonan/permintaan yang diterima dari luar PT Bank XYZ baik itu melalui telepon atau voicemail atau *email* dengan cara melakukan telepon balik, balasan *email* atau melalui cara lainnya?	√		
56	Apakah metode yang telah diatur sebelumnya digunakan untuk verifikasi independen dari keabsahan/keaslian sumber dan isi transaksi yang diminta, yang diterima melalui fax, *email* atau *image system*?	√		
57	Apakah digunakan sertifikasi atau tanda tangan elektronik dalam meverifikasi integritas dan keabsahan/keaslian dari dokumen elektronik yang masuk?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS12
Tanggal		Tanggal :		
Proses :	**Manage the Physical Environment (DS12)**			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah lokasi fasilitas tidak terlihat secara jelas dari luar, dan berada di area yang memiliki tingkat akses yang paling sedikit, serta dibatasi hanya untuk orang-orang tertentu saja?	√		
2	Apakah prosedur akses fisik dan logika cukup/memadai, termasuk akses keamanan bagi pegawai, pemasok (vendor), dan staf yang memelihara fasilitas dan peralatan?	√		
3	Apakah praktik dan prosedur pengelolaan/penanganan kunci (*key*) dan *card reader* dinilai memadai, termasuk pembaruan yang berkelanjutan?	√		
4	Apakah kebijakan otorisasi dan akses dalam memasuki/meninggalkan, melindungi, registrasi, tanda/kartu masuk sementara, kamera pengintai di daerah yang sensitif, dinilai memadai?	√		
5	Apakah terdapat proses pembatalan, respon, dan eskalasi pada saat terjadi pelanggaran/penerobosan keamanan?	√		
6	Apakah terdapat review periodik dan berkelanjutan atas berbagai profil akses?	√		
7	Apakah terdapat berbagai ukuran pengendalian keamanan dan akses, yang mencakup peralatan informasi yang *portable* dan/atau *off-site*?	√		
8	Apakah terdapat review registrasi pengunjung, pemberian tanda/kartu masuk, perlindungan (*escort*), orang yang bertanggung jawab atas pengunjung, dan buku pencatatan, untuk memastikan terdapatnya *check in* dan *out* dan	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	pemahaman resepsionis atas berbagai prosedur keamanan?			
9	Apakah akses ke lokasi TI yang sensitif, akan dibatasi misalkan dengan cara memagari/membentengi gedung dan menaruh alat keamanan di dalam dan di luar gedung. Alat keamanan tersebut akan mencatat siapa saja yang memasuki wilayah dan akan membunyikan alarm jika ada pihak yang tidak berwenang masuk ke lokasi TI tersebut. Alat keamanan ini bisa berupa *badges* atau *key card, key pad, closed circuit television* dan *biometric scanner*?	√		
10	Apakah terdapat review atas prosedur pemberitahuan (*warning*) kebakaran, cuaca, elektrikal dan alarm?	√		
11	Masih berhubungan dengan pertanyaan sebelumnya, apakah terdapat review dari skenario-skenario respon yang diharapkan pada saat terjadi berbagai tingkat keadaan darurat yang berhubungan dengan lingkungan?	√		
12	Apakah terdapat review dari prosedur pengendalian terhadap kelembaban, ventilasi, jaringan listrik dan AC?	√		
13	Masih berhubungan dengan pertanyaan sebelumnya, apakah terdapat review dari skenario-skenario respon yang diharapkan pada saat terjadi kehilangan atau keadaan/sesuatu hal ekstrim yang tidak diantisipasi?	√		
14	Apakah terdapat review dari proses alarm akibat pelanggaran/penerobosan keamanan yang mencakup:			
	• definisi dari prioritas alarm	√		
	• skenario-skenario respon atas tiap-tiap prioritas alarm	√		
	• tanggung jawab dari personil PT Bank XYZ versus personil keamanan dari vendor	√		
	• interaksi dengan pihak yang berwenang di PT Bank XYZ	√		
	• review atas prosedur alarm yang terbaru	√		
15	Apakah PT Bank XYZ bertanggung jawab atas akses fisik dalam fungsi TI yang	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	mencakup: • pengembangan, pemeliharaan dan review berkelanjutan dari kebijakan dan prosedur keamanan	√		
	• dibuatnya hubungan dengan vendor yang berorientasi pada keamanan	√		
	• Penanganan atas isu-isu teknologi yang berhubungan dengan keamanan	√		
	• pengkoordinasian kesadaran dan pelatihan keamanan untuk pegawai PT Bank XYZ	√		
	• pengkoordinasian aktifitas-aktifitas yang mempengaruhi pengendalian akses logika melalui aplikasi tersentralisir	√		
	• pemberian kesadaran dan pelatihan keamanan tidak hanya dalam fungsi TI tetapi untuk semua pengguna	√		
16	Apakah terdapat negosiasi dan pembaharuan (*updating*) dari isi kontrak jasa/layanan keamanan?	√		
17	Apakah dalam merancang lokasi TI telah memperhatikan kabel telekomunikasi secara fisik, aliran air, dan kekuatan listrik?	√		
18	Apakah terdapat kepatuhan/kesesuaian terhadap peraturan kesehatan, keselamatan dan lingkungan?	√		
19	Apakah keamanan fisik dinyatakan/dipenuhi dalam rencana kontinuitas, dan memastikan diterapkannya keamanan fisik yang sama untuk fasilitas yang berasal dari supplier?	√		
20	Apakah terdapat penggunaan *Uninterruptible Power Source (UPS)* sebagai infrastruktur alternatif untuk mengimplementasikan keamanan?	√		
21	Apakah terdapat penggunaan jalur telekomunikasi alternatif sebagai infrastruktur alternatif untuk mengimplementasikan keamanan?	√		
22	Apakah pemusnahan peralatan penyimpanan yang mengandung informasi sensitif berlangsung dengan aman?	√		
23	Apakah lokasi TI yang sensitif diperiksa dengan frekuensi tertentu (termasuk hari akhir dan libur) oleh staf yang menangani masalah *security*?	√		

PT Bank XYZ		Disiapkan oleh :		No Dokumen
Responden :		Tanggal :		
Jabatan :		Diperiksa oleh :		KK-DS13
Tanggal		Tanggal :		
Proses :	Manage Operation (DS13)			

No	Pertanyaan	Ya	Tidak	Keterangan
1	Apakah seluruh pemrosesan yang dilakukan, termasuk *restart* dan *recovery* telah lengkap?	√		
2	Apakah terdapat prosedur *shut down* dan *Initial Programme Load* (IPL) yang memadai?	√		
3	Apakah digunakan statistika penyelesaian jadwal untuk mengkonfirmasikan penyelesaian yang berhasil dari seluruh kebutuhan/ketentuan?	√		
4	Apakah terdapat pemisahan fisik dan logika dari sumber dan objek, perpustakaan (*library*) pengujian/tes-pengembangan-produksi, prosedur pengendalian perubahan untuk memindahkan program di antara perpustakaan tadi?	√		
5	Apakah digunakan statistika kinerja/performa untuk kegiatan-kegiatan operasional, yang mencakup kapasitas, utilisasi, dan performa perangkat keras dan *peripherals*?	√		
6	Apakah digunakan statistika kinerja/performa untuk kegiatan-kegiatan operasional, yang mencakup utilisasi, dan performa memory?	√		
7	Apakah digunakan statistika kinerja/performa untuk kegiatan-kegiatan operasional, yang mencakup utilisasi, dan performa segala sesuatu yang berhubungan dengan telekomunikasi?	√		
8	Apakah terdapat suatu keyakinan bahwa performa operasional sesuai dengan	√		

No	Pertanyaan	Ya	Tidak	Keterangan
	standar/ketentuan performa produk, standar performa yang didefinisikan secara internal dan komitmen persetujuan tingkat jasa/layanan?			
9	Apakah dokumen/catatan pengoperasian dipelihara, disimpan/ditahan, dan direview secara berkelanjutan?	√		
10	Apakah terdapat pemeliharaan atas semua peralatan yang dilaksanakan secara tepat waktu?	√		
11	Apakah terdapat prosedur dan kebijakan untuk menangani hal-hal di luar kebiasaan?	√		Sedang dalam proses pengerjaan
12	Apakah para operator mengalami pergantian (*shifting*), memiliki kesempatan cuti, dan memelihara kompetensinya?	√		
13	Apakah terdapat suatu prosedur yang mencakup jadwal pekerjaan sehari-hari, penunjukkan seseorang apabila terjadi kegagalan pekerjaan dan menjalankan sederetan kode jika terjadi kegagalan proses/pekerjaan?	√		
14	Apakah terdapat kebijakan atau prosedur yang memonitor infrastruktur TI dan *event-event* terkait?	√		
15	Apakah terdapat deskripsi tugas dan pekerjaan yang berkaitan dengan pemisahan tugas? Sebagai contoh, operator komputer seharusnya tidak memiliki akses ke program dan programmer seharusnya tidak memiliki akses ke produksi data, dsb	√		
16	Apakah kronologis informasi disimpan dalam suatu file *operation logs* atau semacamnya, sehingga memungkinkan dilakukannya rekonstruksi, review dan pengujian terhadap waktu dilakukannya deretan operasi atau aktifitas yang mendukung operasi?	√		
17	Apakah terdapat penjagaan fisik yang tepat, praktek akuntasi dan manajemen inventory terhadap aset TI yang sensitif seperti form khusus dan *security tokens*?	√		

No	Pertanyaan	Ya	Tidak	Keterangan
18	Apakah terdapat prosedur dan kebijakan untuk memperoleh, mengubah dan memindahkan akses terhadap aset yang sensitif?	√		
19	Apakah terdapat prosedur dan kebijakan untuk memindahkan dan memusnahkan dokumen output?	√		
20	Apakah *maintenance* bagi seluruh perangkat keras yang penting dirancang dengan memperhatikan analisis *cost-benefit*, rekomendasi vendor, risiko, personel yang cakap dan faktor relevan lainnya?	√		