IT RISK ASSESSMENT DI PT. X

Celia Wanarta[1], Adi Wibowo[2], Ibnu Gunawan[3]
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131
Surabaya 60236
Telp. (031) – 2983455
Fax. (031) - 8417658
E-mail: celiawanarta@hotmail.com[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK: PT. X merupakan suatu perusahaan yang bergerak dibidang *food industry.* Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *software*, *hardware*, jaringan, dan lain-lain. Tetapi *software* yang digunakan belum bisa mengintegrasikan semua proses bisnis dalam perusahaan. Melihat situasi dan kondisi dari PT. X, tidak menutup kemungkinan terjadinya resiko akibat masalah-masalah seperti *data security*, *data integrity*, kerusakan *hard disk*, kesenimbangunan proses bisnis IT dan lain- lain.

Pada skripsi ini dilakukan analisa resiko terhadap seluruh area IT dan proses bisnis yang ada di PT. X. Area-area yang akan dianalisa tersebut didapatkan dengan cara memetakan COBIT 4.1 ke dalam IT *domain*. Analisa resiko dilakukan dengan menerapkan tiga langkah-langkah dalam metode *Global Technology Audit Guide*.

Adapun resiko-resiko yang ditemukan adalah adanya ketergantungan terhadap outsource programmer yang berperan sebagai konsultan IT, tidak pernah dilakukan *Risk Assessment* dalam bidang IT di perusahaan, tidak ada *Disaster Recovery Plan* dan IT *Security Plan*, tidak ada evaluasi terhadap hak akses, tidak ada orang khusus yang ditunjuk untuk mengelola IT, tidak adanya *training* atau zona aman terkait keamanan dan insiden dalam perusahaan, dan tidak adanya standar, framework, atau SOP untuk teknologi, sistem IT dan proses yang cocok menggunakan IT. Hasil analisa resiko ini membantu perusahaan menyadari resiko-resiko apa yang mungkin terjadi dan dapat membahayakan kelangsungan bisnis perusahaan sehingga perusahaan dapat mengambil tindakan untuk mencegah atau menangani resiko tersebut.

Kata kunci: Analisa resiko, *IT Domain,* GTAG, COBIT, metode kualitatif.

ABSTRACT: *PT. X is a retail company that is located in Surabaya. It operates in three business segments. In order to meet its objectives and customers' satisfaction, PT. X uses softwares, hardwares, networks, people, et cetera. PT. X has a system that has not been able to integrate all components and business processes into one coherent system. Based on the situation and condition in PT. X, there are chances of risk rising caused by data security, data integrity, hard disk, business process sustainability problems, and many more.*

This thesis is about to assess risks that might have happened in all information technology areas and during business processes that are continuisly running. The analized areas are the result of mapping COBIT 4.1 into IT domain. Risk assessment is performed based on three steps of Global Technology Audit Guide method.

Risks that have been found are dependence on outsource programmer as an IT consultant, no IT Risk Assessment, no Disaster Recovery Plan, no IT Security Plan, no access right evaluation, no people that are responsible to manage IT, no training or secure area related to security incident, no standard, framework, and SOP for technology and IT system. The result of risk assessment helps the management of the company realize what risks may occur and could have put the company in a danger situation so that the company could take actions to mitigate and to prevent those risks from happening.

Keywords*: Risk assessment, IT Domain, GTAG, COBIT, qualitative research method.*

1. PENDAHULUAN

PT. X merupakan suatu perusahaan yang bergerak dibidang *food industry*. Perusahaan ini berlokasi di kawasan Surabaya Timur. Perusahaan ini terbagi menjadi tiga bagian usaha yaitu Swalayan A, Bakery B, dan Restoran C. Bagian usaha yang pertama kali didirikan adalah Swalayan A, selanjutnya Restoran C, dan yang terakhir Bakery B.

Saat ini, PT. X telah memiliki sistem informasi yang terintegrasi, tetapi hanya pada bagian Swalayan A. Bakery B dan Restoran C belum memiliki sistem yang terintegrasi sehingga harus menginputkan data secara manual. Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *software*, *hardware*, jaringan, dan lain-lain. Data penjualan pada Bakery B dan Restoran C disimpan dalam komputer menggunakan *software* sederhana yaitu Microsoft Excel. Sedangkan *software* utama yang digunakan saat ini merupakan *software* yang dibuat khusus untuk Swalayan A menggunakan *outsource programmer*. *Maintenance software* tersebut dilakukan oleh divisi IT sendiri selama masih bisa ditangani.

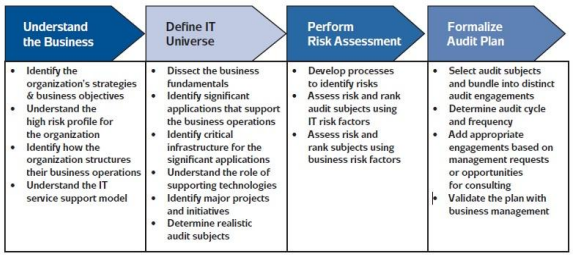
Melihat situasi dan kondisi dari PT. X, tidak menutup kemungkinan terjadinya resiko akibat masalah-masalah seperti *data security*, *data integrity*, kerusakan *hard disk*, kesinambungan proses bisnis IT dan lain- lain. Untuk itu, diperlukan adanya analisa resiko yang mungkin terjadi selama berjalannya proses bisnis dalam perusahaan.

Selama ini belum pernah ada *Risk Assessment* dalam bentuk apapun di dalam perusahaan. *Risk Assessment* membantu perusahaan mengetahui resiko-resiko apa yang dapat terjadi dan seberapa besar dampaknya, resiko mana yang paling mempengaruhi tercapainya tujuan perusahaan. Dengan *Risk Assessment*, perusahaan dapat mengambil langkah-langkah pencegahan sehingga resiko tersebut dapat dicegah atau diatasi untuk meminimalisasi dampak yang terjadi dan mengambil keuntungan dari resiko tersebut.

2. LANDASAN TEORI

2.1 *Global Technology Audit Guidelines*

GTAG (*Global Technology Audit Guide*) merupakan sekumpulan seri buku yang disusun oleh beberapa peneliti dari IIA (*The Institute of Internal Auditors*). GTAG berisi panduan mengaudit teknologi informasi yang ditujukan untuk Kepala Auditor, Panitia Auditor dan Manajemen Eksekutif. Sampai saat ini terdapat beberapa seri GTAG yang sudah dipublikasikan. Dalam seri GTAG yang kesebelas, untuk mengembangkan IT *Audit Plan,* terdapat beberapa tahap yang dapat dilihat pada Gambar 1 di bawah ini. [1]



Gambar 1 Tahap-tahap IT *Audit Plan*
Sumber: GTAG: Developing IT *Audit Plan (2008)*

2.2 COBIT 4.1

COBIT adalah *framework* untuk membantu menjembatani perbedaan dan cara melakukan komunikasi sehubungan dengan kontrol *requirements*, masalah teknis, dan resiko bisnis kepada semua orang yang ada di perusahaan. COBIT memungkinkan pengembangan kebijakan yang jelas dan baik untuk proses-proses IT di perusahaan. COBIT selalu dikembangkan seiring berjalannya waktu dan diselaraskan dengan standar dan pedoman lain. COBIT merupakan kerangka yang baik untuk membantu memahami dan mengelola resiko dan manfaat yang terkait dengan IT.

COBIT mendefinisikan kegiatan IT dalam empat *domain* yaitu *Plan and Organise*, *Acquire and Implement*, *Deliver and Support*, dan *Monitor and Evaluate*.

• *Plan and Organise* (PO)
Memberikan arahan untuk solusi (AI) dan pelayanan (DS). Mencakup strategi dan perencanaan IT terkait dengan infrastruktur IT sehingga dapat berkontribusi dalam pencapaian tujuan bisnis.

• *Acquire and Implement* (AI)
Memberikan solusi dan mengubah mereka menjadi layanan dengan mengidentifikasi, mengembangkan dan mengimplementasikan solusi IT tersebut ke dalam proses bisnis. Selain itu, perubahan dan pemeliharaan sistem yang ada juga dilakukan untuk memastikan solusi tersebut tetap sesuai untuk pencapaian tujuan bisnis.

• *Deliver and Support* (DS)
Menerima solusi dan menyampaikan mereka kepada pengguna meliputi pelayanan, pengelolaan keamanan, dukungan layanan, manajemen data dan fasilitas operasional bagi pengguna.

• *Monitor and Evaluate* (ME)
Mengawasi semua proses untuk memastikan bahwa arahan yang diberikan sudah dijalankan. Semua proses IT perlu dinilai secara berkala dari waktu ke waktu untuk menjaga kualitas. Domain ini menyangkut pengendalian internal dan kepatuhan terhadap kebijakan.[2]

2.3 *Risk Rating Methodology*

Risk Rating merupakan proses penentuan nilai resiko atau ancaman menurut kondisi dan situasi yang ada. Penilaian dilakukan dengan menganalisa kemungkinan terjadinya resiko (*likelihood scale*) dan besar dampak yang ditimbulkan oleh resiko tersebut (*impact scale*). Salah satu metode untuk melakukan penilaian adalah dengan menggunakan kriteria-kriteria yang diambil dari metode OWASP. Menurut OWASP, faktor-faktor yang dapat mempengaruhi terjadinya suatu resiko (*likelihood*) yaitu faktor *threat agent* dan faktor *vulnerability*.

Dalam menentukan besar *impact* dari resiko terhadap perusahaan, dapat digolongkan terlebih dahulu *impact* tersebut menjadi dua yaitu *technical impact* dan *business impact*. Faktor-faktor yang dapat digunakan untuk menilai seberapa besar *technical impact* yang terjadi adalah *loss of confidentiality*, *loss of integrity*, *loss of availability*, dan *loss of accountability*. Faktor-faktor yang dapat digunakan untuk menilai seberapa besar *business impact* yang terjadi adalah *financial damage*, *reputation damage*, *non-compliance*, dan *privacy violation*.

Setelah mendapatkan nilai untuk tiap kriteria yang ada, maka tahap selanjutnya adalah merata-rata nilai *likelihood* dan nilai *impact*, kemudian mengalikannya. Hasil perkalian tersebut merupakan hasil akhir penilaian suatu resiko yang nantinya akan digunakan untuk menggolongkan resiko.[3]

3. MODEL DAN STRATEGI BISNIS PERUSAHAAN

3.1 Model Bisnis Perusahaan

Model bisnis perusahaan dapat dideskripsikan melalui sembilan pilar utama atau yang biasa disebut *Nine Building Blocks* yang diambil dari buku *Business Model Canvas* Penerapan di Indonesia oleh Tim PPM Manajemen tahun 2012[4]. Sembilan pilar utama dalam perusahaan PT. X yaitu:

1. *Value Proposition*
   - Swalayan A
     Makanan segar, makanan cepat saji, makanan ringan lokal maupun impor, bumbu dapur dan saos, berbagai jenis minuman, keperluan rumah tangga seperti pembersih rumah, perlengkapan bayi, peralatan mandi dan pembersih badan, bahan-bahan pokok, obat dan kosmetik.
   - Bakery B
     Roti, kue kering, kue basah, *cake*, dan *pudding*.
   - Restoran C
     Masakan *Chinese* dan Masakan Indonesia
2. *Target Customer*
   Kalangan menengah keatas yang berdomisili di Surabaya.
3. *Relationship*
   Swalayan A menyediakan *Privilege Card* untuk consumen setia yang memiliki banyak keuntungan. Setiap pembelanjaan dengan kelipatan lima ratus ribu rupiah akan mendapatkan tambahan satu poin. Apabila poin yang terkumpul sudah mencapai 100, maka pemegang kartu dapat menukarkannya dengan *voucher* atau mendapat diskon.
4. *Value Configuration*
   Divisi *Purchasing* melakukan *order* dengan membuat *purchase order* (PO) yang sudah disetujui oleh *manager*

Purchasing ke *supplier*. Setelah *Purchase Order* disetujui maka akan dibawa oleh *sales*. Ketika barang datang maka *sales* akan membawa barang dan *invoice* menuju gudang.

Divisi Gudang menerima barang yang dikirim oleh *sales*. Setelah itu barang-barang tersebut akan dicek kuantitas dan kualitasnya sesuai dengan pesanan dan *invoice* yang ada. Data yang ada tersebut akan diserahkan kepada bagian administrasi untuk dimasukkan ke dalam sistem.

Divisi *Accounting* akan mencatat hutang sesuai dengan pesanan yang telah dikirim ke *supplier*. Divisi Operasional berhak meminta barang-barang yang diperlukan sesuai kebutuhan kepada Divisi Gudang. Setelah ada persetujuan dari divisi gudang, maka perpindahan barang akan dilakukan dari gudang ke divisi yang memerlukan.

Pada Swalayan A, setelah barang-barang yang diminta telah dikirim pada divisi Operasional, maka barang-barang tersebut langsung akan didisplay dan siap dijual.

Pada Bakery B, bahan baku yang diminta tersebut akan diolah terlebih dahulu di pabrik menjadi roti, kue, *cake* atau *pudding*. Setelah jadi dan dikemas, maka roti-roti itu akan dijual melalui stand di Swalayan A atau melalui penjual keliling menggunakan sepeda motor.

Pada Restoran C, setelah itu bahan-bahan tersebut disimpan di gudang atau kulkas Restoran C. Bahan-bahan itu akan diolah sesuai pesanan pembeli yang mengunjungi Restoran C.

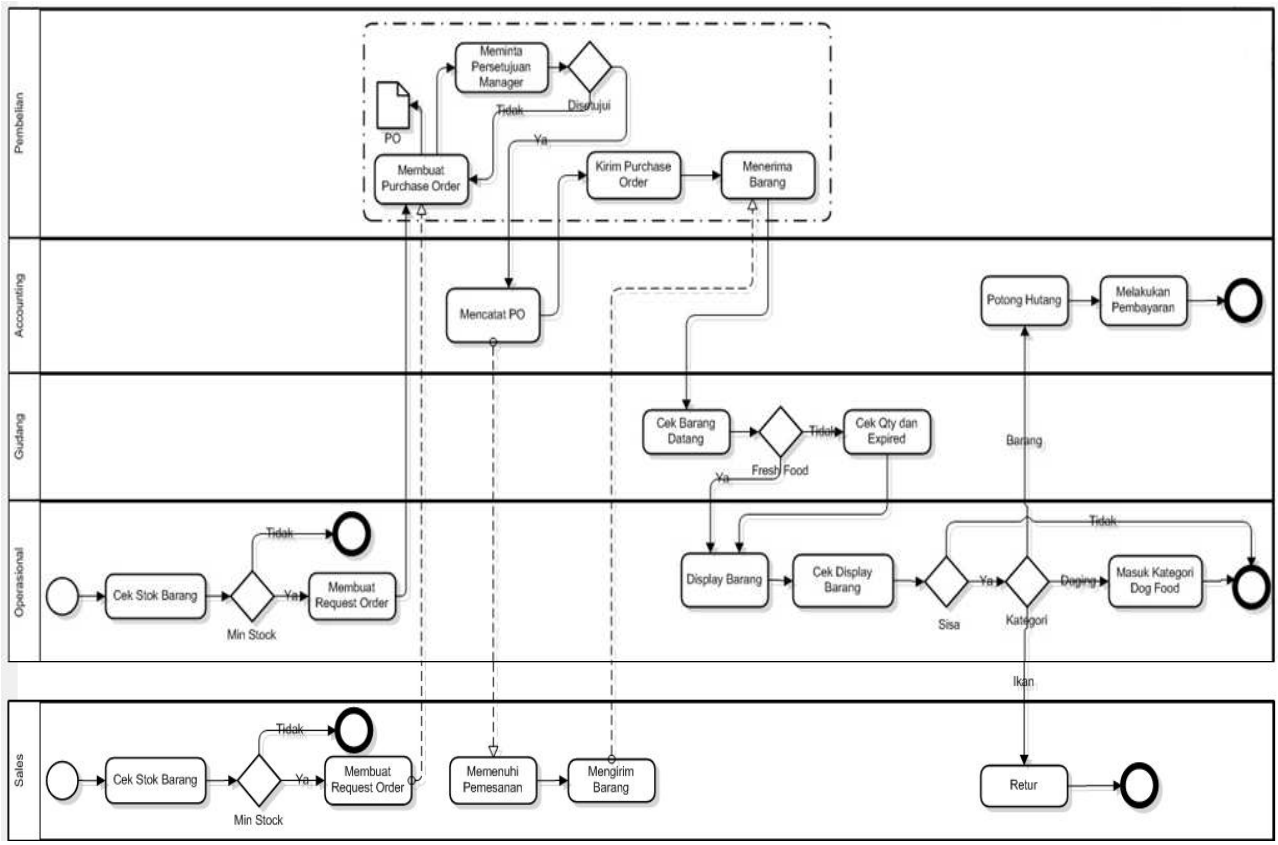
5. *Partner Network*
   Rekan kerja atau *supplier* yang bekerja sama dengan perusahaan ini seperti PT. Segarmas, Unilever, Wings, dan ribuan *supplier* lain.

3.2 Strategi Bisnis Perusahaan

Tujuan bisnis utama dalam perusahaan ini yaitu mendapat keuntungan yang sebesar-besarnya. Setiap tahun aka nada target untuk pencapaian omzet tertentu yang berbeda pada masing-masing unit bisnis. Strategi bisnis yang dilakukan untuk mencapai tujuan tersebut ditentukan oleh divisi dari masing-masing unit bisnis yang ada yaitu divisi operasional dan divisi *Purchasing*. Strategi jangka pendek yang dilakukan oleh divisi operasional dan *Purchasing* dari Swalayan A seperti mengadakan pasar murah, mengadakan promo-promo tertentu, dan. Strategi bisnis jangka panjang dari Swalayan A adalah penggantian aplikasi SIPOS yang berbasis DOS menjadi sebuah aplikasi berbasis *Delphi* atau *Visual Basic*. Strategi bisnis jangka pendek dari Bakery B adalah mengadakan inovasi produk baru hamper setiap bulannya, sedangkan strategi jangka panjangnya adalah dengan mengusahakan penambahan rombong motor untuk meningkatkan penjualan keliling. Strategi bisnis dari Resstoran adalah dengan adanya menu-menu baru dan promosi-promosi tertentu.

3.3 Proses Bisnis Perusahaan

Proses bisnis dalam PT. X salah satunya pada unit bisnis Swalayan A dapat dilihat pada gambar di bawah ini.



Gambar 2 Business Process Modeling Notation Swalayan A

3.4 Kondisi *Information Technology* di Perusahaan

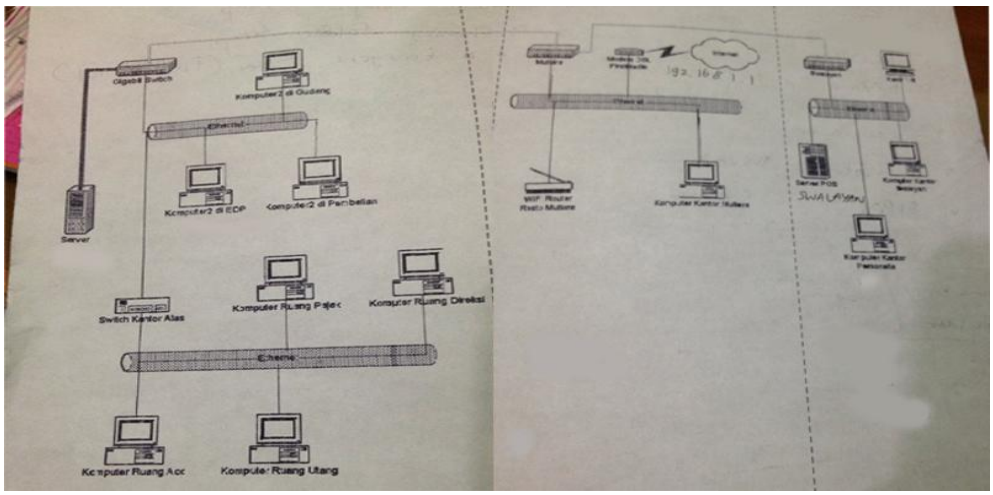
1. Data
   PT. X memiliki satu *database server* yang digunakan untuk menyimpan data yang digunakan untuk beberapa aplikasi yang ada. *Database* yang disimpan menggunakan aplikasi SQL Server 2000.
2. Aplikasi
   Aplikasi yang digunakan dalam perusahaan ini yaitu:
   - Swalayan A
   - Win Solution digunakan untuk mengatur data kas/bank, data *supplier*, data utang dan piutang, data giro keluar, pembelian, penjualan, proses perubahan barang, persediaan, *stock opname*, membuat *form*, dan membuat laporan.
   - SIPOS digunakan sebagai *Back Office* dan *Point of Sales.*
   - Program Kasir digunakan untuk kasir di Swalayan A
   - Team Viewer digunakan untuk memantau dan mengakses program di luar perusahaan, dibatasi dengan menggunakan *password*.
   - Bakery B
   - FoxPro digunakan untuk kasir.
   - Microsoft Excel digunakan untuk membuat laporan penjualan.
   - Restoran C
   - Sejenis SIPOS untuk mengatur data masakan dan harga, data *member*, stok barang, penjualan nota, nota *pending*, dan membuat laporan penjualan.
   - Personalia
   - Program FoxPro untuk mengatur data pegawai, absensi, dan penggajian.
   - Microsoft Excel digunakan untuk mencatat penggajian pegawai.
3. Teknologi
   PT. X memiliki total komputer sebanyak 47 *unit* yang tersebar di berbagai departemen. Sebanyak 29 komputer terletak di kantor PT. X dengan 16 komputer berbasis Windows 2000, satu computer berbasis Windows Vista dan 12 komputer berbasis Windows XP. Pada Swalayan A terdapat 14 komputer dengan sembilan computer berbasis Windows 98 dan lima computer berbasis Windows XP. Pada Restoran C terdapat tiga computer dengan 1 komputer berbasis Windows 98, dan dua computer berbasis Windows XP. Pada Bakery B hanya terdapat satu computer berbasis Windows 2000 sebagai komputer kasir. PT. X juga mempunyai dua buah *server,* satu terletak di gedung kantor dan satu terletak di Swalayan A. Untuk setiap unit kasir dan *server* yang ada disediakan *Uninterruptible Power Supply* yang bertujuan menjaga komputer tetap menyala apabila listrik padam. *Untuk* menangani masalah lampu mati, perusahaan menyediakan *genset* sehingga seluruh proses yang membutuhkan tenaga listrik tetap dapat berjalan.

4. PENENTUAN IT *AUDIT UNIVERSE*

4.1 IT *Audit Universe*

IT *Audit Universe* merupakan ruang lingkup dalam perusahaan yang akan dianalisa dan diteliti. IT *Audit Universe* di PT. X meliputi:

- Penentuan tujuan dan strategi bisnis perusahaan
  Penyusunan strategi yang dibuat oleh perusahaan untuk mencapai tujuan perusahaan dan dengan melihat model bisnis perusahaan.
- Sistem IT dalam perusahaan
  Sistem IT dalam perusahaan meliputi aplikasi yang digunakan, infrastruktur IT, jaringan, dan orang-orang yang terlibat dalam pemeliharaan, penggunaan dan pemanfaatan IT.
- Proses-proses yang ada pada Swalayan A meliputi proses pembelian, penerimaan barang, perpindahan barang, penjualan, retur barang, pemilihan *supplier,* dan proses perencanaan.
- Proses-proses yang ada pada Bakery B dan Restoran C meliputi proses pembelian, penerimaan barang, perpindahan barang, produksi, penjualan, pemilihan *supplier,* dan proses perencanaan.
- Proses-proses yang ada pada Personalia meliputi proses perekrutan pegawai, penggajian, dan pencatatan absensi.
- Proses-proses yang ada pada *Accounting* dan *Finance* meliputi proses penerimaan dan pengeluaran kas, pencatatan hutang dan piutang.



Gambar 3 Struktur Jaringan di PT. X

4.2 IT *Audit Domain*

Menurut ISACA (2005) [5], dalam COBIT 4.1, terdapat 34 *control objectives* yang berfokus pada area-area dalam IT *Governance*. *Control objectives* tersebut merupakan kebijakan atau standar yang digunakan untuk mengontrol dan analisa setiap proses-proses yang ada di perusahaan. Setiap proses yang ada di PT. X yaitu IT *audit universe*, dari COBIT 4.1 akan dipetakan ke IT *domain* sehingga akan menghasilkan bagian-bagian yang akan dianalisa pada setiap *control objectives* yang disebut IT *audit domain.*

5. PENILAIAN RESIKO

5.1 Kriteria Penilaian Resiko

Penilaian resiko didapatkan dari hasil perkalian nilai *likelihood* dan nilai *impact*. Untuk mendapatkan nilai *likelihood* dan nilai *impact* dari setiap resiko, maka dibutuhkan beberapa kriteria untuk menilai skalanya. Kriteria yang digunakan untuk menilai *likelihood* antara lain:

1. *Skill*
   Resiko dapat terjadi karena keterbatasan kemampuan dari *staff* atau dari pihak manajemen.
2. *Management and Stakeholder Support*
   Resiko dapat terjadi karena kurangnya dukungan dari pihak manajemen yang dapat berupa jumlah *staff*, kebijakan yang ditetapkan dan biaya disediakan. Sedangkan dukungan dari *stakeholder* dapat berupa saran atau permintaan akan kebutuhan terhadap IT.
3. *Awareness*
   Resiko dapat terjadi karena kurangnya kesadaran dari pihak perusahaan mengenai resiko tersebut.

Kriteria yang digunakan untuk menilai *impact* antara lain:

1. *Loss of Confidentiality*
   Dampak dari suatu resiko seperti adanya hal-hal yang seharusnya bersifat tertutup menjadi terbongkar atau diketahui banyak orang, contohnya data perusahaan.
2. *Loss of Integrity*
   Dampak dari suatu resiko seperti adanya data yang tidak konsisten. Data yang ada di suatu tempat dapat berbeda dengan data yang sama tetapi berada di tempat lain.
3. *Loss of Availability*
   Dampak dari suatu resiko seperti adanya layanan atau proses yang tidak bisa berfungsi dengan baik.
4. *Loss of Accountability*
   Dampak dari suatu resiko seperti tidak adanya orang-orang yang dapat ditunjuk untuk mempertanggung jawabkan atau mengatasi resiko tersebut.
5. *Financial*
   Dampak dari suatu resiko seperti adanya kerugian dalam bentuk keuangan yang akan berdampak terhadap profit yang didapatkan perusahaan.
6. *Service*
   Dampak dari suatu resiko seperti adanya hal-hal yang mengganggu layanan yang dapat diberikan kepada *customer* sehingga berpengaruh terhadap kepuasan *customer*.
7. *Privacy*
   Dampak dari suatu resiko seperti adanya gangguan kepentingan banyak orang. Misalnya data pribadi orang-orang yang terbongkar atau hal-hal lainnya yang mengganggu kepentingan suatu individu.

5.2 *Risk Severity*

Tabel 5.1 Resiko Tertinggi

No	*Risk Factors*	*Risk* Severity	*Level*	*Overall Level*
1	*Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT	21,32	HM	*High*
2	Tidak ada dan belum pernah ada penerapan d*isaster recovery plan* dan IT s*ecurity* p*lan*	19,46	MM	*Medium*
3	Tidak ada orang khusus yang ditunjuk untuk mengelola IT, hanya seorang *staff* IT saja sehingga adanya ketergantungan terhadap *staff* tersebut. *Staff* IT tersebut juga hanya berperan melakukan *maintenance* dan memberi usulan mengenai kondisi IT yang ada	16,70	MM	*Medium*
4	Tidak pernah dilakukan *risk assessment* dalam bidang IT sehingga belum begitu memahami resiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan)	16,38	HL	*Medium*
5	*Backup* data hanya secara fisik dan *on site* saja, dan tidak pernah dilakukan pengecekan hasil *backup* atau *refresh* data, sehingga sistem IT tidak aman	11,88	ML	*Low*
6	Tidak ada prosedur khusus dalam pembuatan hak akses atau *account* dan tidak pernah ada evaluasi atau pergantian secara berkala	10,58	ML	*Low*
7	Tidak ada *training* atau zona aman terkait keaamanan dan insiden dalam perusahaan	8,88	HL	*Medium*
8	Tidak ada standar, *framework*, atau SOP untuk teknologi, sistem IT dan proses yang cocok menggunakan IT.	2,57	HL	*Medium*

5.3 Risk Response Planning

Risk response planning merupakan bagaimana cara perusahaan harus bereaksi terhadap resiko tersebut. Dari resiko tertinggi yang ada, maka dapat disimpulkan *risk response planning* yang disarankan adalah sebagai berikut:

1. *Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT
   Response: *Reduce*
   Dampak dari resiko tersebut yaitu bocornya data penting perusahaan dapat dikurangi dengan membuat *non-disclosure agreement* dengan *outsource programmer* terkait keamanan data perusahaan sesuai dengan standar ISO/IEC 27002:2005 terkait *confidentiality agreement*. Bisa juga dengan menggunakan *internal programmer* untuk menangani data yang sensitif dan tidak boleh diketahui banyak orang. Sehingga data sensitif tersebut tidak dapat diakses oleh pihak di luar perusahaan.
2. Tidak ada dan belum pernah ada penerapan *disaster recovery plan* dan IT *security plan*.
   Response: *Reduce* atau *Transfer*
   Dampak dari resiko tidak adanya *disaster recovery plan* dan IT *security plan* dapat diperkecil dengan membuat *disaster recovery plan* dan IT *security plan*. Jika tidak memungkinkan disarankan untuk melakukan audit terhadap perusahaan oleh pihak di luar perusahaan. Dengan begitu hasil dari audit adalah auditor membuatkan *disaster recovery plan* dan IT *security plan.* Dampak dari tidak adanya *disaster recovery plan* juga dapat dialihkan dengan mengasuransikan perusahaan sehingga kerugian yang dialami akibat bencana akan ditanggung oleh pihak asuransi. *Disaster recovery plan* adalah sebuah perencanaan sistem informasi yang dirancang untuk mengembalikan operasional, aplikasi, dan infrastruktur setelah terjadinya keadaan darurat yang dampaknya berkepanjangan seperti yang tertulis dalam NIST SP 800-34 dan mengacu pada COBIT 4.1 *control objective Delivery* and *Support* 4. Perusahaan harus terlebih dahulu menentukan insiden-insiden apa yang tergolong ke dalam bencana. *Disaster recovery plan* dan IT *security plan* dapat dibuat berdasarkan standar keamanan ISO 27002:2005 seperti membuat *non-disclosure agreement* dengan pihak eksternal maupun internal perusahaan, kontrol untuk perlindungan dari *software* yang tidak terjamin otoritasnya, *backup* secara *off site* yaitu membuat media *backup* data di luar jangkauan perusahaan, perlindungan data *backup* dengan adanya enkripsi, pengecekan data *backup* secara berkala untuk menjamin konsistensi data, dan penghapusan data penting pada media yang sudah tidak terpakai.
3. Tidak ada orang khusus yang ditunjuk untuk mengelola IT, hanya seorang *staff* IT saja sehingga adanya ketergantungan terhadap *staff* tersebut. *Staff* IT tersebut juga hanya berperan melakukan *maintenance* dan memberi usulan mengenai kondisi IT yang ada.
   Response: *Reduce*
   Dampak ketergantungan terhadap *staff* IT dapat dikurangi dengan menambah *staff* IT untuk mengelola dan melakukan pengawasan secara berkala terhadap sistem IT di perusahaan. Hal tersebut dilakukan agar satu orang *staff* tidak memegang kunci penting terlalu banyak dan mengantisipasi apabila suatu saat *staff* IT tidak ada pada keadaan darurat.
4. Tidak pernah dilakukan *risk assessment* dalam bidang IT sehingga belum begitu memahami resiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan)
   Response: *Reduce*
   Dampak dari tidak adanya *risk assessment* dalam bidang IT dapat diperkecil dengan melakukan *risk assessment* di perusahaan oleh pihak di luar perusahaan yang sudah berpengalaman dan dapat menggunakan metode-metode atau panduan seperti *Global Technology Audit Guidelines* atau ISO/IEC 31010:2009 dengan IT *audit domain* yang dapat ditentukan dengan panduan COBIT 4.1. *Global Technology Audit Guidelines* berisi tahap melakukan *risk assessment* mulai dari pemahaman bisnis, penentuan area-area IT yang akan diaudit, penentuan faktor-faktor resiko, dan penilaian resiko. ISO/IEC 31010:2009 berisi tentang konsep, proses, dan pemilihan teknik *risk assessment* yang dapat digunakan di perusahaan.
5. *Backup* data hanya secara fisik dan *on site* saja, dan tidak pernah dilakukan pengecekan hasil *backup* atau *refresh* data, sehingga sistem IT tidak aman
   Response: *Reduce*
   Dampak dari risiko ini dapat diperkecil dengan melakukan *backup* sesuai dengan standar NIST 800-34. *Backup* dapat dilakukan secara *off site*. Backup dilakukan dengan menyimpan data pada *hard disk* atau dapat juga secara *cloud backup* sehingga data disimpan mengunakan internet. Perusahaan bisa mengakses data backup kapan saja dan dimana saja apabila menggunakan *cloud backup.* Hasil dari *backup* juga sebaiknya di-*restore* secara berkala untuk mengecek apakah data *backup* sesuai dengan data yang ada dan proses *restore* sudah berjalan dengan baik.
6. Tidak ada prosedur khusus dalam pembuatan hak akses atau *account* dan tidak pernah ada evaluasi atau pergantian secara berkala.
   Response: *Avoid*
   Mengacu pada ISO/IEC 27002:2005, dampak dari resiko ini dapat dihindari dengan mengevaluasi dan melakukan pergantian hak akses secara berkala, pencabutan hak akses pegawai yang telah berhenti bekerja atau mutasi jabatan. Hal ini dilakukan untuk menghindari adanya pengaksesan data penting oleh pegawai yang sudah berhenti. Untuk kriteria pembuatan *password* yang baik dapat mengacu pada standar NIST 100-118.
   Tidak ada *training* atau zona aman terkait keamanan dan insiden dalam perusahaan.
   Response: *Avoid* untuk masalah tidak adanya zona aman terkait keamanan dan insiden dalam perusahaan. *Reduce* untuk masalah tidak adanya training terkait keamanan dan insiden dalam perusahaan.
   Resiko tidak adanya *training* atau zona aman terkait keamanan dan insiden dalam perusahaan dapat dihindari dengan mengadakan *training* cara penanganan insiden-insiden terkait keamanan kepada *staff* IT sesuai standar NIST SP 800-34, pembatasan dan pencatatan akses terhadap area-area yang penting dalam perusahaan, pemenuhan standar ruang server yang baik, dan kontrol terhadap bencana fisik terhadap fasilitas dan sistem informasi sesuai standar ISO/IEC 27002:2005.
8. Tidak ada standar, *framework*, atau SOP untuk teknologi, sistem IT dan proses yang cocok menggunakan IT.

Response: *Reduce*

Dampak dari resiko tersebut dapat dikurangi dengan mencari standar atau *framework* yang sesuai. Standar untuk teknologi dan sistem IT terkait keamanan dapat menggunakan NIST. Standar untuk layanan IT dapat menggunakan ITIL. Standar yang dapat digunakan untuk IT *Governance* adalah COBIT. *Framework* yang dapat diadopsi untuk perencanaan sistem IT yaitu EAP, Zachman *Framework*, dan TOGAF. Standar yang dapat digunakan untuk pembuatan SOP adalah ISO 9001. SOP terkait IT yang dapat dibuat oleh perusahaan seperti SOP perencanaan sumber daya IT, SOP pengarsipan data, SOP untuk proses *backup*, SOP untuk *disaster recovery*, SOP untuk pemeliharaan *hardware* dan *software*, SOP mengenai sistem informasi kualitas, dan sebagainya.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan analisa dan observasi yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. PT. X dalam mencapai tujuan bisnisnya menggunakan IT sebagai pendukung jalannya proses bisnis di perusahaan. Dengan penggunaan IT tersebut, perusahaan dapat memperoleh kemudahan dalam pengolahan dan pengiriman data. Proses bisnis yang paling banyak menggunakan IT adalah proses penjualan, proses penerimaan dan pengeluaran barang, penerimaan dan pengeluaran uang.
2. Resiko-resiko dalam bidang IT yang mungkin terjadi selama berjalannya proses bisnis PT. X adalah :
   - *Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT.
   - Tidak ada dan belum pernah ada penerapan *Disaster Recovery Plan* dan IT *Security Plan*.
   - Tidak ada orang khusus yang ditunjuk untuk mengelola IT, hanya seorang *staff* IT saja sehingga adanya ketergantungan terhadap *staff* tersebut. *Staff* IT tersebut juga hanya berperan melakukan *maintenance* dan memberi usulan mengenai kondisi IT yang ada.
   - Tidak pernah dilakukan *Risk Assessment* dalam bidang IT sehingga belum begitu memahami resiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan).
   - *Backup* data hanya secara fisik dan *on site* saja, dan tidak pernah dilakukan pengecekan hasil *backup* atau *refresh* data, sehingga sistem IT tidak aman.
   - Tidak ada prosedur khusus dalam pembuatan hak akses atau *account* dan tidak pernah ada evaluasi atau pergantian secara berkala.
   - Tidak ada *training* atau zona aman terkait keamanan dan insiden dalam perusahaan.
   - Tidak ada standar, *framework*, atau SOP untuk teknologi, sistem IT dan proses yang cocok menggunakan IT.

Kesulitan yang dihadapi penulis selama pengerjaan skripsi ini adalah kesulitan mengatur waktu untuk wawancara dengan narasumber, dan kesulitan menyesuaikan pemahaman atau menjelaskan hal-hal yang belum begitu dimengerti oleh narasumber.

6.2 Saran

Adapun beberapa hal yang dapat dijadikan sebagai saran dalam proses pengembangan selanjutnya yaitu melanjutkan proses analisa resiko ini ke proses audit untuk menilai kinerja dan kondisi IT di perusahaan.

7. DAFTAR PUSTAKA

[1] Rehage, Steve Hunt, Fernando N. (2008). *Developing IT Audit Plan.* USA: The Institute of Internal Auditors

[2] IT Governance Institute. (2007). *Cobit 4.1*. USA: ISACA

[3] OWASP Risk Rating Methodology. (2008). The OWASP Risk Rating Methodology. Retrieved Apr. 27, 2013, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[4] Tim PPM Manajemen. (2012). *Business Model Canvas Penerapan di Indonesia.* Indonesia :Penerbit PPM

[5] IT Governance Institute. (2007). *Cobit 4.1*. USA: ISACA