**TUGAS PAPER**

**M0214 – TOPIK-TOPIK LANJUTAN SISTEM INFORMASI**

**IT Risk Assessment Pada PT. X**

**Dibuat oleh :**

**Ambrosius Adimas W (1501167645)**

**Eggy Alfian Susanto (1501195402)**

**Octavion Tjia (1501171522)**

**Prisilia Rinita (1501187325)**

**Rizky Firstiana Putri (1501192836)**

**Yoga Pratama (1501169783)**

**06PKM**

****

**Binus University**

**Jakarta**

**2014**

**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.

**BAB 1**

**PENDAHULUAN**

**LATAR BELAKANG**

Seiring dengan perkembangan teknologi informasi dan komunikasi, tingkat persaingan antar perusahaan pun semakin tinggi dan karena itu semakin dibutuhkan suatu sistem informasi yang dapat meningkatkan efektifitas dan efisiensi perusahaan di dalam mencapai tujuan atau goal nya, selain itu juga dibutuhkan suatu review atau IT Assessment untuk dapat memahami hal-hal apa saja yang dapat menjadi peluang atau pun dapat menjadi resiko bagi perusahaan di kemudian hari.

Dengan adanya suatu assessment atas resiko maka dapat membantu perusahaan dalam menentukan langkah atau tindakan apa yang dapat diambil oleh perusahaan untuk dapat mengurangi dampak buruk yang dapat terjadi atau pun sebaliknya dapat membantu perusahaan dalam mencapai tujuannya.

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.

**RUANG LINGKUP**

 Di dalam tulisan ini akan dijelaskan mengenai risk assessment terhadap sistem informasi dari PT.X dan keuntungan dari pembuatan risk assement ini.

**TUJUAN DAN MANFAAT**

Tujuan dari penulisan ini adalah untuk menganalisa mengenai risk assessment dari PT.X dan keuntungan yang didapatkan oleh PT.X setelah membuat risk assessment ini. Sedangkan manfaat dari penulisan ini yaitu dapat membantu perusahaan dalam mengambil keputusan sehingga resiko-resiko yang ada dapat dicegah atau diatasi untuk mengurangi dampak dari resiko tersebut dan mengubahnya menjadi peluang bagi perusahaan.

**METODE PENULISAN**

Metode yang digunakan dalam melakukan penelitian dan penulisan adalah dengan melakukan pengumpulan data melalui studi pustaka atas jurnal-jurnal dan analisis terhadap data yang dikumpulkan serta identifikasi kebutuhan informasi dan identifikasi persyaratan sistem.

**BAB 2**

**LANDASAN TEORI**

**2.1 Pengertian Sistem Informasi**

Menurut Satzinger, Jackson, dan Burd (2002, p7) sistem Informasi adalah sekumpulan komponen yang saling terkait yang mengumpulkan, memproses, menyimpan dan menyediakan sebagai hasil berupa informasi yang dibutuhkan untuk menyelesaikan tugas bisnis..

Dan pengertian lain dari sistem informasi menurut Whitten (2004, p10) adalah susunan dari orang-orang, data, proses, dan teknologi informasi yang berinteraksi untuk mengumpulkan, menyimpan, menyediakan output sebagai informasi yang dapat mendukung sebuah organisasi.

Dari definisi diatas, dapat disimpulkan bahwa sistem informasi adalah Kumpulan – Kumpulan komponen yang saling berhubungan, yang menyediakan, menyimpan, mengumpulkan, dan memproses informasi terhadap sebuah organisasi untuk membantu organisasi dalam pengambilan keputusan.

**2.2 Pengertian Risk**

 Menurut Kamus Besar Bahasa Indonesia, Risk (Dalam Kamus Besar Bahasa Indonesia bertuliskan Resiko) adalah Kemungkinan terjadinya peristiwa yang dapat merugikan perusahaan.

Dan pengertian lain dari Risk (Resiko) Menurut Vaughan, Risk adalah *Chance of loss*. Chance Of Loss berhubungan dengan suatu exposure (keterbukaan) terhadap kemungkinan kerugian. Dalam ilmu statistik, chance dipergunakan untuk menunjukkan tingkat probabilitas akan munculnya situasi tertentu. Sebagian penulis menolak definisi ini karena terdapat perbedaan antara tingkat risiko dengan tingkat kerugian. Dalam hal chance of loss 100%, berarti kerugian adalah pasti sehingga risiko tidak ada. Istilah selanjutnya adalah Risk is the possibility of loss (Risiko adalah kemungkinan kerugian). Istilah possibility berarti bahwa probabilitas sesuatu peristiwa berada diantara nol dan satu. Namun, definisi ini kurang cocok dipakai dalam analisis secara kuantitatif. Pengertian selanjutnya adalah Risk is uncertainty (Risiko adalah ketidakpastian). Uncertainty dapat bersifat subjective dan objective. Subjective uncertainty merupakan penilaian individu terhadap situasi risiko yang didasarkan pada pengetahuan dan sikap individu yang bersangkutan. Objective uncertainty akan dijelaskan pada dua definisi risiko berikut.

**2.2.1 Jenis-jenis resiko**

Menurut Gondodiyoto (2009, p110), risiko dapat dibedakan dalam beberapa jenis, yaitu :

1. Risiko Bisnis (Business Risks)

Risiko Bisnis adalah risiko yang dapat disebabkan oleh factor-faktor intern (permasalahan kepegawaian,berkaitan dengan mesin-mesin, dll) maupun ekstern(perubahan kondisiperekonomian, tingkat kurs yang berubah mendadak, dll) yang berakibat kemungkinan tidak tercapainya tujuan organisasi.

1. Risiko Bawaan (Inherent Risks)

Risiko Bawaan adalah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian intern. Contohnya kegiatan kampus, jika tidak ada absensi akan banyak mahasiswa yang tidak hadir.

1. Risiko Pengendalian (Control Risks)

Risiko pengendalian adalah masih adanya risko meskipun sudah ada pengendaluan. Contohnya meskipun sudah ada absensi tetapi tetap saja beberapa mahasiswa yang menitip absen.

1. Risiko Deteksi (Detection Risks)

Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya error yang cukup atau materialitas atau adanya kemungkinan fraud.

1. Risiko Audit (Audit Risks)

Risiko audit adalah risiko risiko bahwa hasil pemeriksaan auditor ternyata belum mencerminkan keadaan sesungguhnya.

**2.3 Pengertian Risk Assessment**

*Risk Assessment*adakah proses identifikasi ancaman-ancaman yang mungkin terjadi, baik yang berasal dari dalam, maupun dari luar. Bencana yang dianalisa termasuk bencana alam, bencana kegagalan teknis, maupun ancaman-ancaman faktor manusia. Risk Assessment berperan penting untuk keberlangsungan pembangunan keseluruhan *Disaster Recovery Planning* karena dapat dianggap sebagai landasan awal yang akan mempengaruhi tahapan-tahapan selanjutnya. *Risk Assessment* biasanya diikuti dengan Impact Analysis, dimana kemungkinan-kemungkinan bencana yang sudah teridentifikasi kemudian dianalisis dampaknya.

**2.4 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.

**2.5 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 2.1 di bawah ini.



Gambar 2.1 Tahap – tahap IT *Audit Plan*

Sumber: GTAG*: Developing IT Audit Plan* (2008)

**2.6 Cobit**

 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, 1. Deliver and Support, dan Monitor and Evaluate.

****

**2.7 Pengertian Jaringan**

 Jaringan komputer menurut Andrew S. Tanenbaum (1997, p1) adalah sekumpulan computer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. Ada dua model koneksi dalam jaringan yaitu:

1. Internet

Pengertian internet memiliki arti yang cukup luas dimana kata internet itu sendiri merupakan singkatan kata dari interconnection-networking, bila dijabarkan secara sistem global maka internet merupakan jaringan komputer diseluruh penjuru dunia yang saling terhubung satu sama lain dengan menggunakan standar Internet Protocol Suite(TCP/IP) sehingga antara komputer dapat saling mengakses informasi dan bertukar data. Internet mencangkup segala sesuatu secara luas baik itu komputerisasi maupun telekomunikasi

1. Protokol

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

**BAB 3**

**PEMBAHASAN**

**3.1 Model Bisnis Perusahaan**

 Setiap perusahaan memiliki model bisnis yang berbeda-beda, tergantung pada jenis bisnis yang dijalaninya. Pada perusahaan X ini model bisnis yang dijalankan dapat dideskripsikan melalui Sembilan pilar utama (*Nine Building Block*) yang diambil pada sebuah buku “Business Model Canvas” yang penerapannya di Indonesia diterapkan oleh Tim PPM Manajemen tahun 2012 [4]. Adapun Sembilan Pilar Utama pada PT X ini adalah sebagai berikut :

1. *Value Proposition*
	1. Swalayan

Makanan segar, makanan cepat saji, makanan ringan local, makanan ringan import, bumbu dapur dan saos kemasan, berbagai jenis minuman, keperluan rumah tangga, perlengkapan bayi dan anak, peralatan mandi dan pembersih badan, kebutuhan pokok, obat dan kosmetik.

* 1. Bakery

Kue kering, kue basah, roti, cake, pudding, agar agar, kue tradisional dan tart.

* 1. Restoran

Masakan Indonesia dan masakan *International* (*Chinese Food*).

1. *Target Konsumen*
	1. Kalangan menengah yang berdomisili di sekitar Surabaya.
	2. Kalangan atas yang berdomisili di sekitar Surabaya
2. *Relationship*

Pada bisnis swalayan A menyediakan fitur Privilage Card untuk konsumen yang setia pada swalayan ini dimana kartu ini memiliki banyak keuntungan. Yaitu pada setiap pembelian dengan kelipatan lima ratus ribu rupiah akan mendapatkan tambahan satu poin, dimana poin tersebut akan digunakan untuk menukar dengan *voucher* atau mendapatkan diskon jika poin yang terkumpul sudah mencapai 100 poin.

1. *Value Configuration*

Pada divisi *Procurement* melakukan pemesanan dengan membuatkan PO (*Purchase* *Order*) yang sudah disetujui oleh Manager Procurement terhadap Supplier. Maka setelah proses Procurement disetujui selanjutnya PO akjan dibawa oleh sales dan ketika barang dating maka sales akan membawa barang beserta invoice-nya menuju gudang untuk dilakukan good receipt.

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 r

oti, 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.

1. *Partner Network*
	1. Pada hal ini rekan bisnis atau mitra bisnis yang bekerja sama dengan perusahaan ini, seperti perusahaan PT. Segarman, Unilever, Wings, dan ribuan supplier lainnya.

**3.2 Strategi Bisnis Perusahaan**

Tujuan utama bisnis dalam perusahaan ini adalah mendapat keuntungan (*revenue*) yang sebesar-besarnya. Setiap tahun akan ada target dan tujuan 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 3.1 Proses bisnis Swalayan A

* 1. **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.

1. Aplikasi

Aplikasi yang diterapkan pada perusahaan ini yaitu berbeda beda pada tiap jenis bisnisnya, yuitu :

1. Swalayan
* 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-End System dan* POS (*Point of Sales*).
* Program kasir untuk swalayan A.
* Tim Viewer digunaan untuk mengkontrol dan mengakses program diluar progam perusahaan, dibatasii dengan menggunakan username dan password.
1. Bakery
	* FoxPro digunakan untuk program kasir.
	* Ms. Excel yang digunakan untuk membuat laporan penjualan.
2. Restoran
* Sejenis program SIPOS untuk mengatur data masakan dan harga, serta data member, stok barang, penjualan, nota, dan membuat laporan penjualan.
1. Personalia
* Program FoxPro untuk mengatur data pegawai, absensi dan penggajian (*Payroll*).
* Ms. Excel yang digunakan untuk mencatat penggajian pegawai.
1. 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 terdapat 14 komputer dengan sembilan computer berbasis Windows 98 dan lima computer berbasis Windows XP. Pada Restoran terdapat tiga computer dengan 1 komputer berbasis Windows 98, dan dua computer berbasis Windows XP. Pada Bakery 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. 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.

**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.

1. *Management and Stakeholder Support*

Resiko dapat terjadi karena kurangnya dukungan dari pihak manajemen yang dapat berupa jumlah staff, kebijakan yang ditetapkan dan biaya yang disediakan. Sedangkan dukungan dari stakeholder dapat berupa saran atau permintaan akan kebutuhan terhadap IT.

1. *Awareness*

Resiko dapat terjadi karena kurangnya kesadaran dari pihak perusahaan mengenai resiko tersebut.

 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.

* 1. *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.

* 1. *Loss of Availability*

Dampak dari suatu resiko seperti adanya layanan atau proses yang tidak bisa berfungsi dengan baik.

* 1. *Loss of Accountability*

Dampak dari suatu resiko seperti tidak adanya orang-orang yang dapat ditunjuk untuk mempertanggung jawabkan atau mengatasi resiko tersebut.

* 1. *Financial*

Dampak dari suatu resiko seperti adanya kerugian dalam bentuk keuangan yang akan berdampak terhadap profit yang didapatkan perusahaan.

* 1. *Service*

Dampak dari suatu resiko seperti adanya hal-hal yang mengganggu layanan yang dapat diberikan kepada *customer* sehingga berpengaruh terhadap kepuasan *customer*.

* 1. *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 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.

7. 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.

**BAB 4**

**PENUTUP**

**KESIMPULAN**

Dengan melakukan implementasi IT dan Sistem Informasi yang mendukung PT. X memperoleh kemudahan dalam pengolahan dan pengiriman data. Dan dengan hal ini proses penjualan, proses penerimaan, pengeluaran barang lalu penerimaan dan pengeluaran uang menjadi lebih efisien dan efektif dikarenakan IT yang ada sangat mendukung proses pertukaran informasi yang terjadi di perusahaan.

 Pemberlakukan pengimplementasian Audit dan juga risk response planning di dalam perusahaan akan sangat mengurangi kesalahan kesalahan yang terjadi didalam perusahaan di karenakan sistem lama ataupun secara manual, dengan memperlakukan hal ini pengecekan untuk Audit dan risk response akan menjadi lebih efektif dan juga efisien, mengingat teknologi IT yang lebih baik dan proses struktur yang lebih baik setelah melakukan analisis dapat di perbaiki dan lebih dimajukan lagi. Proses proses transaksi yang meliputi bagian bagian divisi perusahaan juga menjadi lebih terarah dan lebih efisien.

**SARAN**

Diperlukan proses analisa lebih lanjut untuk penelitian selanjutnya yang bertujuan untuk meningkatkan proses IT dan Sistem Informasi Audit dan juga Risk response planning yang ada di dalam perusahaan X sehingga bisa dikembangkan kembali.

**DAFTAR PUSTAKA**

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

OWASP Risk Rating Methodology. (2008). The OWASP Risk Rating Methodology. Retrieved Apr. 27, 2013, from https://www.owasp.org/index.php/OWASP\_Risk\_Rating\_M ethodology

Tim PPM Manajemen. (2012). *Business Model Canvas Penerapan di Indonesia. Indonesia* :Penerbit PPM
 IT Governance Institute. (2007). *Cobit* 4.1. USA: ISACA

**LAMPIRAN**

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Ambrosius Adimas W |
| NIM | **:** | 1501167645 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | Taman Permata Cipunir, Jl Koala XVII Blok A9 No. 64,Bekasi |
| No. HP  | **:** | 081932865152 |
| E-mail  | **:** | ambrosiusadimas@gmail.com |

Riwayat pendidikan :

* Tahun 1998 – 2004 : SD Kristen 1 BPK Penabur, Cirebon
* Tahun 2004 – 2007 : SMP Kristen 1 BPK Penabur, Cirebon
* Tahun 2007 – 2010 : SMAK 1 BPK Penabur, Cirebon
* Tahun 2010 – sekarang : Binus University, Jakarta

Jakarta, 1 Maret 2014

Hormat saya,

Ambrosius Adimas W

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Eggy Alfian Susanto |
| NIM | **:** | 1501195402 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | - |
| No. HP  | **:** | 081294641024 |
| E-mail  | **:** | eggyalfian@ymail.com |

Riwayat pendidikan :

* Tahun 1998 – 2004 : SDN Sukadanau 02
* Tahun 2004 – 2007 : MTs N Daar El-Qolam
* Tahun 2007 – 2010 : SMA Daar El-Qolam
* Tahun 2010 – sekarang : Binus University, Jakarta

Jakarta, 8 Maret 2014

Hormat saya,

Eggy Alfian Susanto

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Octavion Tjia |
| NIM | **:** | 1501171522 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | Jalan K.H. Syahdan, Gg. Keluarga no 37, Kost Apple, Kecamatan Palmerah, Jakarta Barat 11480  |
| No. HP  | **:** | 08994505150 / 085365993535 |
| E-mail  | **:** | octaviontjia@gmail.com |

Riwayat pendidikan :

* Tahun 1999 – 2005 : SDK Yos Sudarso, Batam
* Tahun 2005 – 2008 : SMPK Yos Sudarso, Batam
* Tahun 2008 – 2011 : SMAK Yos Sudarso, Batam
* Tahun 2011 – sekarang : Binus University, Jakarta

Jakarta, 1 Maret 2014

Hormat saya,

Octavion Tjia

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Prisilia Rinita |
| NIM | **:** | 1501187325 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | Jl.Srigading 4 Blok A5/5 Puspita Loka, BSD |
| No. HP  | **:** | 081285319091 |
| E-mail  | **:** | Prisilia.rinita@gmail.com |

Riwayat pendidikan :

* Tahun 1999 – 2005 : SDK Ora et Labora BSD
* Tahun 2005 – 2008 : SMP Ora et Labora BSD
* Tahun 2008 – 2011 : SMA Binus International School
* Tahun 2011 – sekarang : Binus University, Jakarta

Jakarta, 1 Maret 2014

Hormat saya,

Prisilia Rinita

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Rizky Firstiana Putri |
| NIM | **:** | 1501192836 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | Jln Tanah Merdeka No.22A rt 08/05 Kel.Susukan Kec.Ciracas Jakarta Timur |
| No. HP  | **:** | 089601130039 |
| E-mail  | **:** | firstianaputrii@gmail.com |

Riwayat pendidikan :

* Tahun 1999 – 2005 : SD Kartika XI-I, Jakarta
* Tahun 2005 – 2008 : SMPI PB Soedirman, Jakarta
* Tahun 2008 – 2011 : SMAN 42, Jakarta
* Tahun 2011 – sekarang : Binus University, Jakarta

Jakarta, 1 Maret 2014

Hormat saya,

Rizky Firstiana Putri

**DAFTAR RIWAYAT HIDUP**

|  |  |  |
| --- | --- | --- |
| Nama  | **:** | Yoga Pratama |
| NIM | **:** | 1501169783 |
| Tahun Angkatan | **:** | 2011 |
| Jurusan  | **:** | Sistem Informasi |
| Universitas | **:** | Bina Nusantara University |
| Alamat Universitas | **:** | Jln.Kebon Jeruk Raya No.27 , Kebon Jeruk, Jakarta Barat |
| Alamat Rumah | **:** | Jalan K.H. Syahdan No 19A, Kecamatan Palmerah, Jakarta Barat 11480  |
| No. HP  | **:** | 081317750745 |
| E-mail  | **:** | yogamadness@gmail.com |

Riwayat pendidikan :

* Tahun 1999 – 2005 : SD Mujahidin, Pontianak
* Tahun 2005 – 2008 : SMP N 10, Pontianak
* Tahun 2008 – 2011 : SMA N 9, Pontianak
* Tahun 2011 – sekarang : Binus University, Jakarta

Jakarta, 1 Maret 2014

Hormat saya,

Yoga Pratama