Analisis Risiko Terhadap Business Continuity di PT.X

Andrew Hartanto Susilo, Adi Wibowo, Alexander Setiawan
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) - 8417658
E-mail: andrewsusilo92@gmail.com,adiw@petra.ac.id,alexander@petra.ac.id

ABSTRAK: PT. X merupakan suatu perusahaan yang bergerak dibidang *retail (Penjualan besi beton).* Dalam menjalankan proses bisnisnya perusahaan ini menggunakan *software*, *hardware*, jaringan, dan lain-lain. Melihat dari kondisi di PT. X tidak menutup kemungkinan terjadinya risiko akibat masalah-masalah dalam hal *data security*, *data integrity*, kerusakan *hard disk*, kesenimbangunan proses bisnis IT dan lain-lain.

Pada penelitian ini dilakukan analisis risiko terhadap seluruh area IT dan proses bisnis yang ada di PT. X. Area-area yang akan dianalisis tersebut didapatkan dengan cara melakukan penganalisisan pada *business continuity* berdasarkan Standard ISO 27002 : 2005 chapter 14 kemudian melakukan penganalisisan IT Domain dan berikutnya melakukan risk assessment maupun risk mitigation.

Adapun risiko-risiko 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 maupun framework. Hasil analisis risiko ini membantu perusahaan menyadari risiko-risiko apa yang mungkin terjadi dan dapat membahayakan kelangsungan bisnis perusahaan sehingga perusahaan dapat mengambil tindakan untuk mencegah atau menangani risiko tersebut.
Kata kunci :

Analisis Business Continuity, Analisis Risiko, *Risk Assessment,Risk Mitigation*.

ABSTRACT: PT. X is a retail company that is located in Surabaya. In order to meet its objectives and customers' satisfaction, PT. X uses softwares, hardwares, networks, people, et cetera. 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 research 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 business continuity with standard ISO/IEC 27002:2005 chapter 14 into IT *domain* and after that doing risk assessment and also risk mitigation.

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.

Key words :

Business continuity analysis, IT domain analysis, Risk Assessment and Risk Mitigation.

1. PENDAHULUAN

PT. X adalah sebuah perusahaan yang bergerak di bidang penjualan besi beton. PT. X telah menjadi salah satu supplier besi beton yang sudah terkemuka di kawasan Surabaya. PT. X memiliki visi, yaitu menjadi perusahaan yang memiliki tipe barang terlengkap dan menjadi supplier besi beton terbesar. PT. X juga memiliki misi, yaitu ekspansi gudang, menyiapkan dana dalam jumlah besar untuk penanaman modal di pabrik dan menambah armada.

PT. X telah memiliki ratusan konsumen tetap yang tiap harinya mengambil besi beton dalam jumlah yang besar. Untuk dapat memberikan pelayanan yang terbaik bagi para konsumen dan membantu keefektifan kinerja perusahaan PT. X. Maka PT. X menerapkan solusi yang berbasis IT yaitu sebuah *software* pada perusahaannya. *Software* yang digunakan PT. X adalah sebuah *software* yang berbasis *Visual Basic*. *Software* tersebut membantu setiap divisi yang ada pada perusahaan PT. X untuk memberikan pelayanan yang terbaik dan kinerja perusahaan yang lebih efektif dan efisien, contoh seperti:

- Bagian penjualan:
  Mencatat *order* / *sales order* (menginputkan nama konsumen, alamat untuk kiriman barang, jenis barang yang diminta, jumlah barang yang diminta dan total pembayaran).
- Bagian pembelian:
  Mencatat pemesanan / *purchase order* (menginputkan nama supplier, alamat supplier, nomor faktur, nomor surat jalan, jenis barang, jumlah barang, harga beli dan total pembayaran).
- Bagian stok barang:
  Mencatat keluar masuk barang (menginputkan jenis barang, jumlah barang dan harga pokok maupun harga jual).
- Bagian *accounting*:
  Mencatat segala bentuk transaksi (menginputkan jenis pembayaran dan menginputkan waktu pembayaran)

Software tersebut sangatlah penting dalam jalannya kinerja di dalam perusahaan. Apabila terjadi gangguan atau permasalahan pada *software* tersebut dapat sangat merugikan PT. X sehingga akibatnya kinerja perusahaan tidak dapat berjalan secara maksimal.

Berdasarkan tinjauan dan informasi yang didapat ternyata PT. X pada tahun 2012 pernah mengalami gangguan pada *software* yang dimilikinya yang mengakibatkan pihak PT. X harus melakukan sistem manual dalam proses kinerjanya. Dengan terjadinya gangguan tersebut keseluruhan data yang telah diinputkan sebelumnya juga menghilang atau tidak ada sama sekali. Dengan adanya gangguan tersebut yang berlangsung hanya dua hari sudah membuat kerugian yang cukup besar bagi PT. X. Selain itu juga ada beberapa permasalahan yang sering terjadi di PT. X tersebut antara lain pada saat terjadi kesalahan penginputan pada program dapat membuat keseluruhan data yang diterima di keseluruhan divisi juga salah. Dengan adanya sedikit kesalahan sudah berakibat fatal dan merugikan pihak perusahaan tersebut. Selain itu PT. X pernah mengalami juga gangguan pada jaringannya. Pada tahun 2001-2011, PT. X menggunakan kabel *LAN* dan pada tahun 2012 PT. X mengganti proses jaringannya dengan menggunakan *WI-FI* dan saat penggunaan jaringan *WI-FI* tersebut PT. X mengalami *trouble* dan membuat sistem komputerisasinya *error*.

2. Risk Management Process

2.1 Pengertian Risk Management Process

Risiko dalam teknologi informasi juga memiliki dua *domain* yakni *risk assessment* dan *risk mitigation. Risk assessment* adalah untuk dapat mengetahui risiko yang ada dan mengetahui seberapa besarkah risiko tersebut. *Risk mitigation* adalah proses mengidentifikasi risiko, mengestimasi biaya dan bagaimanakah langkah yang harus diambil dalam menanggapi risiko tersebut agar dapat berkurang. Pilihan yang ada pada *risk mitigation* adalah *assume, avoid, transfer,* dan *lessen*. *Assume* adalah menerima risiko dan tetap bisa melanjutkan kegiatan operasi bisnis. *Avoid* adalah menghentikan pengerjaan atau kegiatan operasional perusahaan dan menghindari risiko. *Transfer* adalah proses mitigasi dimana risiko ditanggung oleh pihak ketiga, atau pihak lain yang bersedia menanggung contohnya seperti asuransi. *Lessen* adalah mengimplementasikan penanganan agar sekalipun risiko tersebut diterima dampaknya dapat diperkecil atau kemungkinan terjadinya dapat dikurangi

2.2 NIST (National Institute of Standard and Technology)

NIST adalah badan federal non-regulasi dengan misi mengembangkan dan mempromosikan pengukuran, standar dan teknologi untuk meningkatkan produktivitas dan meningkatkan kualitas hidup. NIST memiliki beberapa standard antara lain:

- SP 800-12: *An Introduction to Computer Security: The NIST Handbook*
- SP 800-18: *Guide for Developing Security Plans for Information Technology Systems*
- SP 800-26: *Security Self-Assessment Guide for Information Technology System*
- SP 800-30: *Risk Management Guide for Information Technology Systems*

Standard NIST yang sangat membantu dalam memberikan konsep dan petunjuk dalam pembuatan proyek dan analisis risiko adalah SP 800-30 dikarenakan pada SP 800-30 ini ada beberapa langkah dalam pembuatan *risk management* yang benar dan sesuai dengan standard bagaimana dan juga ada beberapa metode yang dapat menunjang pembuatan *risk management*.

Pada SP 800-30 ini berisi mengenai langkah-langkah dalam penganalisisan risiko. Mulai dari *risk assessment* kemudian *risk mitigation* dan yang terakhir *risk evaluation*. Akan tetapi langkah-langkah yang akan digunakan dalam membantu penganalisisaan risiko untuk business continuity pada perusahaan tersebut hanya sampai pada langkah *risk assessment* dan *risk mitigation*.

3. Spesifikasi software dan hardware

NO	Divisi	Software	Deskripsi
1	Stock / *Inventory*	*Microsoft Access* dan *Microsoft Visual Basic*	Melihat, menginputkan dan mengganti data.
2	Penjualan (*Marketing*)	*Microsoft Word* dan *Microsoft Access* maupun *Microsoft Visual Basic*	Melakukan kegiatan penjualan seperti membuat laporan untuk tender, menelpon pihak konsumen menanyakan dan mencatat orderan dan lain-lain.
3	Pembelian	*Microsoft Word* dan *Microsoft Access* maupun *Microsoft Visual Basic*	Meminta barang pada *supplier*.
4	*Accounting*	*Microsoft Excel* dan *Microsoft Access* maupun *Microsoft Visual Basic*	Melakukan pencatatan dan penghitungan transaksi pada perusahaan
5	*Finance*	*Microsoft Excel*	Mengatur keuangan.
6	Pengiriman	*Microsoft Word*	Menginputkan dan mencatat data yang diperlukan.

Hardware: Menggunakan komputer standard. Terdapat 12 komputer yang digunakan untuk menjalankan *operational* perusahaan tersebut

4. Risk Factor from threat and vulnerability identification

Dari Faktor-faktor yang tidak menjadi risiko dan tidak terlalu berpengaruh bagi perusahaan akan dieliminasi (P17, P18,P19, P23, P25, P31, P32, P33) sesuai temuan-temuan yang didapatkan dari hasil observasi. Berdasarkan hasil analisis tersebut, dapat disimpulkan faktor-faktor risiko yang dapat terjadi di perusahaan selama proses bisnis berlangsung.

P01,P04,P07	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.
P01,P20	Tidak ada proses evaluasi dari sistem IT yang ada
P01,P03	Tidak ada perencanaan strategis untuk IT
PO1, PO4, PO9, P13, P27	Tidak pernah dilakukan *Risk Assessment* dalam bidang IT sehingga belum begitu memahami risiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan).
PO2, P12	Tidak ada struktur *database*, permodelan arsitektur, DFD, *data dictionary*, *low level design*, dan *high level design*.
PO2, PO4, PO8, P12	Kekurangan dari sistem IT saat ini adalah *software* yang digunakan belum bisa mencakup semua proses bisnis dalam perusahaan dan belum bisa mengikuti perkembangan teknologi yang ada, dan jaringan yang sering terputus-putus
PO2, P21, P28, P14	*Backup* data hanya secara fisik dan *on site* saja, dan tidak pernah dilakukan pengecekan hasil *backup* atau *refresh* data, sehingga sistem IT tidak aman
PO3, P13, P16	Tidak ada perkiraan dan pencatatan mengenai perubahan kebijakan.
PO3, PO4, PO6, P21, P30	Tidak ada standar, *framework*, atau SOP untuk teknologi, sistem IT dan proses yang cocok menggunakan IT.
P05	Tidak ada investasi untuk IT, hanya memenuhi kebutuhan perusahaan saja, apabila tidak butuh maka perusahaan tidak akan mengeluarkan biaya untuk itu.
P06	*Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT.
P07	Tidak ada perjanjian tertulis antara perusahaan dengan pegawai yang sudah berhenti terkait keamanan informasi dan data perusahaan.
P08	Tidak ada sistem manajemen kualitas yang mengukur kesesuaian IT dengan kebutuhan bisnis perusahaan meliputi kriteria kualitas, proses-proses IT yang penting, kebijakan, dan proses-proses untuk mengatasi ketidaksesuaian dengan kriteria dan standar.
PO5, PO10, P11, P12, P15, P23, P29	Tidak ada standar, *framework*, manajemen proyek dan manajemen risiko dalam melakukan proyek, sehingga tidak ada anggaran khusus untuk IT dan proyek yang ada tidak berjalan sesuai perjanjian awal.
P12	*Software* perusahaan tidak dikembangkan sesuai perubahan zaman karena kapasitas dan kemampuan yang tidak mencukupi, dan tidak ada standar atau spesifikasi tertentu.
P14, P21	Tidak dilakukan perencanaan pembaharuan sistem secara terus menerus dan tidak ada IT c*ontinuity plan*.
P21, P22	Tidak ada dan belum pernah ada penerapan d*isaster recovery* p*lan* dan IT s*ecurity* p*lan*.
P22	Tidak ada prosedur khusus dalam pembuatan hak akses atau *account* dan tidak pernah ada evaluasi atau pergantian secara berkala.
P25	Tidak ada s*ervice desk* untuk *customer* khusus di perusahaan, hanya dari bagian operasional, *manager*. *Service* d*esk* untuk IT yaitu *bagian staff* IT.
P29	Tidak ada *training* atau zona aman terkait keaamanan dan insiden dalam perusahaan.
P32	Tidak pernah dilakukan audit mekanisme kerja oleh pihak luar perusahaan yang mengawasi proses-proses dalam perusahaan.

5. Risiko tertinggi

5.1 Penghitungan risiko tertinggi

5.2 Risk Response Planning

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

1. *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: *Limitation*
   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.
2. Tidak pernah dilakukan *risk assessment* dalam bidang IT sehingga belum begitu memahami risiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan).
   Response: *Limitation*
   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 yang ada seperti ISO 27002:2005 *chapter* 14 *point* 5 membahas *business contiuity* dan menggunakan NIST SP 800:30 melakukan penganalisisan risiko.
3. *Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT.
   Response: *Limitation*
   Dampak dari risiko 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.
4. Tidak ada perjanjian tertulis antara perusahaan dengan pegawai yang sudah berhenti terkait keamanan informasi dan data perusahaan.
   Response : Limitation
   Dampak dari risiko tersebut adalah bocornya data penting perusahaan dapat dikurangi dengan membuat surat – surat perjanjian yang tertulis maupun dapat mengikuti dengan standard ISO/IEC 27002:2005 terkait *confidentiality agreement*.
5. Tidak ada *training* atau zona aman terkait keamanan dan insiden dalam perusahaan.

No	Risk Factor	Likelihood	Impact	Hasil	Level
1.	*Backup* data hanya secara fisik dan *on site* saja, dan tidak pernah dilakukan pengecekan hasil *backup* atau *refresh* data, sehingga sistem IT tidak aman	6	4,66	27,96	Critical
2.	Tidak pernah dilakukan Risk Assessment dalam bidang IT sehingga belum begitu memahami risiko IT dengan baik. Proses *maintenance* hanya dilakukan saat masalah terjadi (penanganan bukan pencegahan).	8	3,33	26,64	Critical
3.	*Staff* yang mengontrol IT merupakan pihak di luar perusahaan (*outsource programmer*) yang berperan sebagai konsultan IT.	9	2,66	23,94	Critical
4.	Tidak ada perjanjian tertulis antara perusahaan dengan pegawai yang sudah berhenti terkait keamanan informasi dan data perusahaan.	8	2,33	18,64	Serious
5.	Tidak ada *training* atau zona aman terkait keaamanan dan insiden dalam perusahaan.	8	2,33	18,64	Serious
6.	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.	6	3	18	Serious
7.	Tidak ada proses evaluasi dari sistem IT yang ada	5	3,33	16,65	Serious

Response: *Avoid*
untuk masalah tidak adanya zona aman terkait keamanan dan insiden dalam perusahaan. *Lessen* untuk masalah tidak adanya training terkait keamanan dan insiden dalam perusahaan.
Risiko 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 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.

6. 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: *Limitation*
   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.
7. Tidak ada proses evaluasi dari sistem IT yang ada.
   Response: Limitation
   Dampak apabila proses evaluasi dari sistem IT tidak ada dapat membuat sistem IT kedepannya kurang baik karena apabila pihak perusahaan mau melakuka perubahan seperti pembaruan atau pengupgradean pihak perusahaan tidak dapat mengetahui secara pasti dan tepat yang diperlukan.

6. KESIMPULAN

Berdasarkan analisis dan observasi yang telah dilakukan, dapat disimpulkan bahwa 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 stok/ *inventory*, proses pembelian dan proses *accounting*.

7. DAFTAR PUSTAKA

- Gary Stoneburner, Alice Goguen, and Alexis Feringa, (2013). Risk Management Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Diakses pada tanggal 05 Mei 2013.
- Senfit Sandra, Gallegos Frederick, and Davis Aleksandra, (2013). Information Technology Control and Audit (Fourth Edition). Broken Sound Parkway NW,Suite 300 : Taylor & Francis Group.
- Moeller Robert R. (2010). IT Audit, Control and Security. New Jersey : John Wiley & Sons, Inc .
- PMBOK. *4thProject Management Knowledge Area*. USA: PMBOK. Rehage, Steve Hunt, Fernando N. (2008). *Developing IT Audit Plan.* USA: The Institute of Internal Auditors.
- Tim PPM Manajemen. (2012). *Business Model Canvas Penerapan di Indonesia.* Indonesia :Penerbit PPM.
- Information technology, Security techniques , Code of practice for information security management, (http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf), diakses 30 Mei 2013.
- Bridgeland, David dan Zahavi, Ron.(2009).Business Modelling: A Practical Guide to Realizing Business Value. US : Elsevier Inc.
- Rappa,M. Managing Digital Enterprise. 2000. <http://digitalenterprise.org>.
- Osterwalder, A., dan Pigenur, Y.(2010) Business Model Generation. USA: John Wiley and Sons
- Rehage, Steven Hunt dan Fernando N. (2008). Developing IT Audit Plan. USA: The Institute of Internal Auditors.