Analisa Manajemen Risiko Pada Perusahaan Real Estate X

Anthony Loana Weol[1], Adi Wibowo[2], Lily Puspa Dewi[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: anthonyweol@yahoo.com[1], adiw@petra.ac.id[2], lily@petra.ac.id[3]

ABSTRAK

Perusahaan *Real Estate* X memiliki divisi *IT* yang memberikan support dan layanan kepada divisi – divisi lain yang menjadi *customer* bagi divisi *IT*. Divisi *IT* memberikan layanan seperti pengadaan *software*, perakitan *hardware*, dan layanan *helpdesc* bagi divisi yang membutuhkan. Permasalahan yang pernah terjadi pada perusahaan adalah jaringan terputus, yang diakibatkan adanya titik jenuh pada kabel yang mengakibatkan data yang dimasukkan ke dalam komputer tidak bisa ditransfer ke *server*, *server full*, karena setiap data yang ada didalam perusahaan akan dimasukkan kedalam *memory* pada *server*, dan seringkali kapasitas *memory* pada *server* sudah tidak cukup lagi untuk menampung data yang ada, dan kerusakan – kerusakan *hardware* yang diakibatkan oleh kelalaian *user*.

Pada skripsi ini, dilakukan proses *risk assessment* terhadap manajemen kualitas dan manajemen risiko dalam layanan *IT*. Penulis menggunakan beberapa sumber untuk membantu memahami dan melakukan penilaian terhadap faktor – faktor risiko yang ada, yaitu *COBIT 4.1*, *ISO 31000*, dan *Risk Rating Metodhology by OWASP*. Berdasarkan penelitian dan wawancara yang dilakukan, ditemukan beberapa faktor risiko seperti tidak adanya *Quality Management System* yang digunakan untuk pedoman divisi *IT*, tidak adanya manajemen risiko yang terstruktur pada perusahaan, dan tidak adanya kriteria untuk menentukan *likelihood* dan *impact* bagi risiko – risiko yang ditemukan.

Respon yang seharusnya dilakukan oleh perusahaan adalah membuat suatu *Quality Management System* yang dapat digunakan untuk memberikan panduan dan pedoman bagi divisi *IT* untuk melaksanakan tugas dan kewajiban, serta menerapkan suatu manajemen risiko yang digunakan untuk mengetahui, menganalisa, dan mengidentifikasi cara – cara mencegah dan menghindari risiko – risiko terjadi.

Kata Kunci : Analisa Risiko *IT*, *Risk Assessment*, *COBIT*, Metode Kualitatif

ABSTRACT

Real Estate company X has the IT division that provides support and services to another divisions which became a customer for the IT division. IT division provides services such as procurement of software, hardware assembly, and service divisions helpdesc for the needy. The problems that have occurred on the company network is lost, which caused the saturation point in the cable resulting data is entered into a computer can not be transferred to the server, the server is full, because any existing data within the company will be put into memory on the server, and often memory capacity in the server is no longer enough to accommodate the existing data, and the damage - hardware damage caused by the negligence of the user. That requires a risk analysis of quality management and risk management to cope with risks that exist.

In this thesis, risk assessments of the quality management and risk management in IT services was carried out. The author uses several sources to help understand and assess the factors - existing risk factors, namely COBIT 4.1, ISO 31000, and Risk Rating Metodhology by OWASP. Based on research and interviews conducted, it was found several risk factors such as lack of Quality Management System that is used to guide the IT division, the absence of a structured risk management at the company, and the absence of criteria for determining the likelihood and impact for risks that were found.

Responses should be done by the company is making a Quality Management System that can be used to provide guidance and guidance for IT divisions to carry out the duties and obligations, and implement a risk management used to identify, analyze, and identify ways how to prevent and avoid risks occurs.

Keywords*: IT Risk Analysis, Risk Assessment, COBIT, Qualitative Methods*

1. PENDAHULUAN

Di jaman era globalisasi saat ini teknologi sangat berkembang dengan pesat. Hampir seluruh kegiatan yang terjadi di kehidupan sehari – hari tidak lepas dengan teknologi yang ada. Banyak proses bisnis telah memanfaatkan teknologi tidak hanya di bidang industri namun juga di bidang – bidang yang lain.

Perusahaan *Real Estate* X adalah sebuah perusahaan yang bergerak di bidang properti. Dalam proses bisnis yang dijalankan oleh Perusahaan *Real Estate* X, penggunaan *Information Technology* (*IT*) menjadi salah satu faktor pendukung untuk memperlancar proses bisnis yang ada. *Penggunaan Information Technology* (*IT*) pada perusahaan *Real Estate* X sangat mempengaruhi setiap proses bisnis yang ada, termasuk dalam pengolahan data, pencatatan keuangan, penyimpanan desain bangunan dan properti, oleh karena itu kualitas dari *Information Technology* (*IT*) yang menopang setiap proses yang ada harus selalu dinilai dan diukur kualitasnya, serta meninjau setiap risiko yang dapat memunculkan kendala bagi perusahaan.

Melalui *Risk Assessement*, perusahaan dapat mengetahui risiko – risiko apa saja yang mungkin terjadi, mengukur seberapa besar risiko tersebut terjadi, tingkat keseringan risiko itu terjadi dan apa dampak yang ditimbulkan dalam proses bisnis bila risiko tersebut terjadi. Dari analisa *Risk Assessment* ini akan ditunjukkan hasil perhitungan risiko manakah yang paling tinggi untuk dapat dilakukan tindakan penanganan. Lebih lanjut, diharapkan perusahaan tersebut dapat menggunakan *Risk Assessment* untuk mengambil keputusan yang bisa bermanfaat untuk perusahaan, sehingga segala risiko tersebut dapat dijadikan sebuah kesempatan untuk meningkatkan proses bisnis yang terjadi di perusahaan tersebut.

2. LANDASAN TEORI

2.1 ISO 31000

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh *International Organization for Standarization*. Standar ini ditujukan untuk dapat diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko. Menurut *ISO 31000* ada 6 proses yang dilakukan dalam mengelola risiko, yaitu[1]:

1.Communication and Consultation

Adanya konsultasi untuk membahas tentang manajemen risiko agar memiliki tanggung jawab dalam melaksanakan manajemen risiko, dan memiliki dasar di mana keputusan dibuat dan alasan mengapa tindakan tersebut harus dilakukan.

2.Establishing The Context

Saat membuat konteks untuk proses manajemen risiko, diperlukan pertimbangan secara rinci dan jelas khususnya bagaimana hubungan dengan lingkup proses manajemen risiko tertentu.

3.Risk Assessment

Proses – proses dalam *Risk Assessment* yaitu

a. Risk Identification

Pada tahap ini risiko akan digolongkan kedalam risiko yang dapat terus meningkat, risiko yang dapat dicegah, dan risiko yang dapat diatasi dengan segera atau risiko tersebut dapat diturunkan tingkat keseriusan risiko tersebut.

b. Risk Analysis

Pada tahap pengembangan ini perlu dilakukan evaluasi risiko yang akan ditangani terlebih dahulu dan yang ditangani sesudahnya, dengan cara membuat tabel *likelihood* dan *impact* dari semua risiko yang ada.

c. Risk Evaluation

Pada tahap ini analis risiko akan memprioritaskan risiko mana yang harus didahulukan penangannya dan risiko mana yang nantinya bisa ditangani.

4.Risk Treatment

Tahap ini adalah tahap pemilihan apakah risiko dapat diterima atau ditolak, apabila risiko diterima, maka ditinjau terlebih lagi penanganan yang lebih dalam, sedangkan apabila risiko ditolak, maka akan dipertimbangkan apakah akan memunculkan risiko baru.

5.Monitoring and Review

Kemajuan aktual dalam melaksanakan rencana tindakan untuk resiko memberikan ukuran kinerja dan dapat dimasukkan ke dalam manajemen kinerja perusahaan, pengukuran dan pelaporan kegiatan *internal* dan *external*. Pemantauan dan *review* dapat melibatkan pemeriksaan biasa atau pengawasan dari apa yang sudah ada atau bisa periodik.

6. Recording the risk management process

Aktivitas manajemen risiko harus dicatat, sehingga dari catatan tersebut dapat dijadikan perbaikan dari risiko – risiko yang ada

2.2 COBIT 4.1

CobiT 4.1 adalah model standar pengelolahan *IT* yang mendapatkan pengakuan luas, dikembangkan oleh *Information Technology Governance Institute* (*ITGI*) dari *Information System Audit and Control Association* (*ISACA*). COBIT digunakan sebagai standar dalam menilai dan mengukur proses dalam manajemen untuk memastikan bahwa proses *IT* dapat berlangsung dengan baik.[4]

Proses COBIT untuk perusahaan *Real Estate* X :

- PO 8 (*Manage Quality*)

  PO8 manage quality akan berfokus kepada kinerja yang dilakukan saat ini, apakah sudah mencapai tujuan yang diinginkan, dan implementasi dari program – program yang digunakan untuk meningkatkan kinerja *IT*. Tujuan dari proses ini adalah memenuhi kepuasan terhadap kebutuhan bisnis untuk *IT* dan memastikan adanya perbaikan serta peningkatan terhadap kualitas pelayanan *IT*. Dalam analisa risiko berdasarkan PO 8 terdapat 6 *control objective* yang akan dianalisa berdasarkan pertanyaan-pertanyaan wawancara berdasarkan *control practices*. 6 *control objective* tersebut yaitu:
  - *Quality Management System*
  - *IT Standards and Quality Practices*
  - *Development and Acquisition Standards*
  - *Customer Focus*
  - *Continuous Improvement*
  - *Quality Measurement, monitoring, and Review*
- PO 9 (*Assess and Manage IT Risks*)

  PO9 Assess and Manage IT Risks adalah proses yang digunakan untuk mengelola resiko – resiko yang terjadi. Dengan berfokus pada pengembangan kerangka manajemen resiko yang diterapkan pada perusahaan, resiko – resiko akan ditemukan dan dilihat dampak terhadap proses bisnis maupun tujuan perusahaan. Pada *PO9* ini terdapat 6 *control objectives* yang akan dianalisa berdasarkan pertanyaan – pertanyaan wawancara berdasarkan *control practices*. 6 *control objective* tersebut yaitu :
  - *IT Risk Management Framework*
  - *Extabilish the Risk Context*
  - *Event Identification*
  - *Risk Assessmemt*
  - *Risk Response*
  - *Maintenance and Monitoring of a Risk Action Plan*

2.3 Kriteria Penilaian Risiko Berdasarkan Analisa Risiko di Perpustakaan Universitas Kristen Petra

Teori analisa pemberian nilai untuk setiap *likelihood* dan *impact* juga mengacu berdasarkan *IT Risk Assessment* pada tahun 2013 di Perpustakaan Universitas Kristen Petra. Berikut kriteria *likelihood*[2]:

a. Skill Level

Skill level adalah keahlian yang mempengaruhi terjadinya risiko. *Skill level* menilai pengetahuan (*knowledge*) yang dimiliki oleh pelaku. semakin tinggi pengetahuan pelaku, maka risiko akan semakin rendah. Penilaian dihitung dari tingkat pengetahuan dalam menangani risiko.

b. Management and Stakeholder Support

Management and stakeholder support menilai tentang kebijakan yang dibuat oleh manajemen terkait penanganan risiko. Penilaian didasarkan kepada tingkat dukungan dari manajemen dan stakeholder dalam menangani risiko yang ada.

c. Teamwork

Teamwork menilai bagaimana kerja sama tim dalam melakukan penanganan risiko. *Teamwork* meliputi pembagian kerja, penanganan risiko, dan komunikasi pihak

didalamnya. Penilaian didasarkan kepada tingkat kerja sama dan inisiatif tim dalam perusahaan dalam menangani risiko.

d. ***Project Management***
Project management mengukur seberapa siap *project management* menangani risiko yang ada. *project management* mengukur *requirement*, jangka waktu, biaya, ruang lingkup, dan target yang ingin dicapai. Penilaian didasarkan pada adanya *requirement*, jangka waktu, biaya, ruang lingkup, dan target yang ada.

e. ***Awareness***
Awareness mengukur seberapa tinggi kesadaran semua pihak terhadap risiko yang mungkin terjadi, dan kesadaran terhadap tindakan yang harus diambil dalam menghadapi risiko. Penilaian didasarkan kepada tingkat kesadaran dan penanganan terhadap risiko.

Kriteria penilaian *likelihood* risiko diatas berdasarkan Analisa Risiko di Perpustakaan Universitas Kristen Petra. Berikut kriteria *impact* berdasarkan OWASP dan Analisa Risiko di Perpustakaan Universitas Kristen Petra.

2.4 Kriteria Penilaian Risiko Berdasarkan OWASP

Dalam OWASP[7], *likelihood* dan *impact* dihitung dan dinilai berdasarkan pemberian nilai yang ada. Dalam perhitungan *likelihood* dan *impact*, terdapat level risiko terdapat 3 jenjang, yaitu *low* (0 to <3), *medium* (3 to<6), dan *high* (6 to <9). Perhitungan dilakukan dengan memberikan nilai pada masing – masing faktor yang kemudian akan dirata – rata.

Terdapat dua macam dampak yang ditimbulkan apabila proses penyerangan berhasil dilakukan. Dampak pertama adalah dampak teknis yang terjadi pada sisi aplikasi. Dampak kedua adalah dampak bisnis yang terjadi pada sisi bisnis dan operasional perusahaan. Faktor untuk memperkirakan dampak yang terjadi diantaranya *technical impact factor* dan *business impact factor*[8].

A. ***Technical Impact Factors***

a. ***Loss of confidentiality***
Loss of Confidientality mengukur seberapa banyak data yang dapat diperlihatkan dan seberapa sensitif data tersebut. Penilaian didasarkan kepada sensitifitas dan kepentingan data.

b. ***Loss of integrity***
Seberapa banyak data yang dapat dikorupsi dan bagaimana tingkat kerusakannya. Penilaian didasarkan kepada jenis data dan ruang lingkup data yang mengalami gangguan.

c. ***Loss of availability***
Seberapa besar layanan yang hilang dan seberapa vital hal tersebut terjadi. Penilaian didasarkan kepada jenis layanan data yang terganggu.

d. ***Loss of accountability***
Apakah aksi yang dilakukan oleh seorang *attacker* dapat ditelusuri. Penilaian didasarkan kepada mudah atau tidaknya penelusuran *attacker*.

B. ***Business Impact Factor***

a. ***Financial Damage***
Mengukur seberapa besar dampak keuangan yang akan diterima. Peniaian didasarkan kepada tingkat kerugian yang dialami perusahaan.

b. ***Reputation Damage***
Dampak risiko terhadap reputasi yang akan diterima oleh suatu perusahaan atau organisasi. Penilaian didasarkan terhadap rusaknya reputasi yang dialami oleh perusahaan.

c. ***Non-Compliance***
Seberapa besar tingkat kepatuhan yang dimiliki, yang berdampak kepada suatu pelanggaran terhadap hukum atau undang – undang. Penilaian didasarkan kepada tingkat pelanggaran yang dilakukan.

d. ***Privacy Violation***
Berapa banyak informasi yang terungkap melalui risiko tersebut, penilaian didasarkan kepada banyaknya individu yang mengetahui informasi yang terungkap.

Threat Agent Factor			
Skill level	Motive	Opportunity	Size
5	2	7	1
Overall Threat Agent Factor : 3.75 (medium)			

Gambar 1. Overall Threat Agent Factor

Vulnerability Factor			
Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
3	6	9	2
Overall Vulnerability factor : 5 (Medium)			

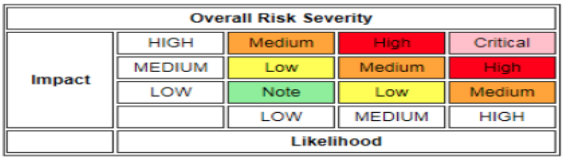
Gambar 2. Overall Vulnerability Factor

Technical Impact			
Loss of Confidie-ntality	Loss of Integrity	Loss of Availability	Loss of Accountability
9	7	5	8
Overall techincal impact : 7.25 (High)			

Gambar 3. Overall Technical Impact Factor

Business Impact			
Financial Damage	Reputation Damage	Non – Compliance	Privacy Violation
1	2	1	5
Overall business impact : 2.25 (Low)			

Gambar 4. Overall Bussiness Impact Factor



Gambar 5. Overall Risk Severity

2.5 Kriteria Penilaian Risiko Berdasarkan Analisa Risiko di Perpustakaan Universitas Kristen Petra

Dalam penentuan *impact* terdapat beberapa kriteria yang dapat digunakan untuk menghitung nilai yang ada. Berikut adalah kriteria – kriteria yang digunakan untuk menghitung *impact* yang ada :

a. ***Confidientality***
Dampak yang disebabkan oleh adanya risiko, seperti hilangnya data, data rusak atau *corrupt*, kerahasiaannya bocor. Penilaian didasarkan kepada banyaknya data yang rusak.

b. ***Integrity***
Mengukur seberapa besar dampak risiko pada perusahaan. Semakin tinggi pengaruh risiko terhadap layanan *IT* yang berdampak pada perusahaan, maka nilai akan semakin

tinggi. Penilaian didasarkan kepada terganggunya konsistensi layanan yang dilakukan oleh divisi IT.

c. Avalability

Avalability mengukur seberapa banyak layanan yang menjadi tidak tersedia akibat terjadinya risiko. Semakin banyak layanan yang menjadi hilang akibat risiko, maka semakin besar nilai yang diberikan. Penilaian didasarkan kepada banyak atau tidaknya layanan yang tidak bisa diberikan.

d. Acountability

Mengukur pihak – pihak yang bertanggung jawab terhadap risiko. Penilaian didasarkan kepada kemudahan untuk menemukan pihak – pihak yang bertanggung jawab.

e. Service

Mengukur seberapa parah layanan yang terganggu akibat adanya risiko yang terjadi dan mempengaruhi kepuasan pengguna. Penilaian didasarkan kepada tingkat kepuasan yang dimiliki oleh customer.

f. Privacy Violation

Mengukur seberapa besar jumlah orang yang terganggu privasinya akibat adanya risiko yang terjadi. Penilaian didasarkan kepada banyaknya privasi orang yang terganggu.

3. PENILAIAN RISIKO

3.1 Kriteria Penilaian Risiko yang Dipakai

Kriteria penilaian untuk aspek *likelihood* dan *impact* penulis risiko menggunakan penilaian berdasarkan OWASP dan Analisa Risiko di Universitas Kristen Petra. Namun ada beberapa kriteria likelihood dan impact yang dikembangkan sesuai dengan kondisi yang ada dalam perusahaan. Kriteria penilaian risiko yang telah dikembangkan dapat dilihat di Tabel 1.

Tabel 1. Kriteria Penilaian Risiko

Kriteria	Sumber	Keterangan
Skill Level	Chrisdiyanto, 2013	Sesuai dengan sumber
Management and Stakeholder Support	Chrisdiyanto, 2013	Sesuai dengan sumber
Integrity	Chrisdayanto, 2013	Sesuai dengan sumber
Teamwork	Chrisdiyanto, 2013	Sesuai dengan sumber
Project Manageme-nt	Chrisdiyanto, 2013	Sesuai dengan sumber
Awareness	Chrisdiyanto, 2013	Sesuai dengan sumber
Avalability	Chrisdayanto, 2013	Sesuai dengan Sumber

Tabel 1. Kriteria Penilaian Risiko (lanjutan)

Kriteria	Sumber	Keterangan
Reputation Damage	Pengembangan analisa OWASP	merupakan dampak terhadap baik atau buruknya reputasi yang diterima oleh divisi *IT* terkait risiko – risiko yang terjadi. Jika risiko yang diterima semakin mencoreng reputasi yang dimiliki oleh divisi *IT*, maka semakin besar skenario risiko yang terjadi. • Dampak risiko sangat kecil bagi reputasi (1) • Dampak risiko sedikit besar bagi reputasi (4) • Dampak risiko begitu besar bagi reputasi (5) • Dampak risiko menghilangkan reputasi (9)
Service	Pengembangan analisa Chrisdiyanto	mengukur seberapa dalam terganggunya layanan yang diakibatkan oleh timbulnya risiko yang terjadi, sehingga mempengaruhi kepuasan yang dimiliki oleh pengguna. Semakin besar pengaruh risiko terhadap kepuasan yang diterima oleh divisi *IT*, maka semakin besar skenario risiko yang ada. • Sebagian kecil layanan yang ada terganggu dan kepuasan masih stabil (1) • Layanan yang bersifat vital kinerjanya tidak maksimal, sehingga kepuasan menurun (5) • Sebagian besar bahkan hampir semua layanan tidak berjalan, sehingga kepuasan sangat rendah (9)

3.2 Risk Severity

Berdasarkan hasil penilaian *likelihood* dan *impact*, dilakukan perhitungan untuk mendapatkan *risk severity* dengan mengalikan tiap-tiap aspek *likelihood* dan *impact*. Melalui hasil perhitungan *risk severity*. Setelah itu maka dapat ditentukan prioritas untuk masing-masing risiko. Hasil perhitungan *risk severity* ditampilkan pada Tabel 2. Risiko dirurutkan dari risiko tertinggi ke risiko terendah berdasarkan risk severity.

Tabel 2. Risk Severity

No.	Risiko	Risk Sever-ity	Level	Overall Level
17	Tidak ada rencana untuk mengembang-kan *risk action* dan *risk assessment*	36.585	HM	*High*
8	Tidak ada rencana mengembang-kan *QMS*/*SOP*	36.456	HM	*High*
14	Tidak ada proses perhitungan *likelihood* pada perusahaan	27.56	HM	*High*
16	Tidak ada *risk action* yang terstruktur	27.795	MM	*Medium*
3	Tidak adanya standar *IT* yang mengatur teknologi informasi secara keseluruhan	21.28	MM	*Medium*
15	Tidak ada rencana untuk pertimbangan risiko residual	20.79	MM	*Medium*
12	tidak adanya kriteria khusus yang digunakan untuk menghitung *likelihood* dan *impact*	20.125	MM	*Medium*
4	Tidak adanya proses dokumentasi tentang model *SDLC* dan proses – proses dalam pembuatan *software*	18.26	MM	*Medium*
1	Tidak ada *QMS* yang mengatur pedoman *IT* dalam melaksanakan tugas dan kewajiban	16.488	MM	*Medium*
2	Divisi *IT* tidak bisa mengikuti keseluruhan *SOP*	16.333	MM	*Medium*

3.3 Risk Response

Risk response merupakan cara perusahaan sebaiknya bereaksi terhadap risiko tersebut. Dari 11 risiko tertinggi, maka dapat disimpulkan *risk response planning* yang disarankan adalah sebagai berikut:

1. Tidak ada pengembangan berkelanjutan untuk *risk acton*/*risk assessment* untuk kedepannya.
   Risk severity: *High*
   Risk Response: *Avoid*
   Perusahaan dianjurkan untuk merencanakan dan membuat suatu pengembangan *risk action* dan *risk assessment* untuk menangani risiko menurut panduan *ISO* 31000 atau *NIST* 800-30[5].
2. Tidak adanya rencana pengembangan berkelanjutan terhadap *QMS*/*SOP* untuk pedoman bagi divisi *IT* untuk kedepannya
   Risk severity: *High*
   Risk Response: *Lessen*
   Perusahaan dianjurkan membuat suatu struktur *QMS*/*SOP* yang dikembangkan lebih lagi sebagai pedoman divisi *IT*, dengan menggunakan panduan *ISO* 9001[3].
3. Tidak adanya proses perhitungan *likelihood* pada perusahaan
   Risk severity: *High*
   Risk Response: *Avoid*
   Perusahaan dianjurkan memiliki suatu proses perhitungan terhadap *likelihood* dan *impact* sehingga perusahaan dapat mengetahui secara pasti risiko mana yang memiliki pengaruh besar bagi perusahaan. Perhitungan *likelihood* dan *impact* dapat melihat bantuan *risk rating methodology by OWASP*.
4. Tidak ada *risk action* terstruktur berdasarkan biaya, prioritas, manfaat, dan tanggung jawab
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Sesuai standar *ISO* 31000 mengenai manajemen risiko, perusahaan harus memiliki suatu *risk action* yang terstruktur, dan dapat dipertanggungjawabkan. Oleh karena itu, perusahaan bisa membuat *risk action* yang berpedoman pada *NIST* 800-30 tentang alur pembuatan *risk action*.
5. Tidak ada standar IT yang mengatur sistem teknologi informasi secara keseluruhan.
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Perusahaan dianjurkan mengimplementasikan berbagai macam contoh *framework* yang dapat digunakan untuk mengatur teknologi informasi yang ada. Beberapa contoh *framework* yang dapat digunakan adalah *ISO* 29110 untuk *software*, *ISO* 27001 untuk *security*, *ISO* 22301 untuk *Business Continuity and Management System*, dan *ISO* 31000 untuk *Risk Management*.
6. Tidak adanya rencana untuk pertimbangan risiko residual.
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Perusahaan dianjurkan untuk mempertimbangkan kemungkinan terjadinya risiko residual terkait penanganan risiko yang ada. Analisa terkait risiko residual yang dapat diacu sesuai dengan *ISO* 31000 atau *NIST* SP800-30.
7. Tidak ada kriteria khusus untuk lakukan perhitungan likelihood dan impact.
   Risk severity: *Medium*
   Risk Response: *Avoid*
   Penentuan kriteria likelihood dan impact yang jelas sangat dibutuhkan untuk mengetahui tingkat kategori risiko yang ada. Perusahaan dapat menggunakan panduan *risk rating metodhology by OWASP* untuk menerapkan dan melakukan perhitungan *likelihood* dan *impact*.

8. Tidak adanya proses dokumentasi tentang model *SDLC* dan proses – proses dalam pembuatan *software*, baik *software* dari pihak *vendor* dan *software* dari *programmer* divisi *IT* itu sendiri
   Risk severity: *Mediun*
   Risk Response: *Lessen*
   Dalam mengatur pendokumentasian model *SDLC* dari suatu *software*, perusahaan bisa menggunakan contoh *framework*, yaitu ISO 12207 yang menjelaskan tentang *SDLC* dan jenis – jenisnya.
9. Tidak ada *QMS* yang mengatur pedoman *IT* dalam melaksanakan tugas dan kewajiban.
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Pembuatan *QMS* yang digunakan untuk memberikan panduan kepada divisi *IT* untuk melakukan tugas dan kewajiban sebagai divisi *support* bagi perusahaan dapat mengacu *ISO* 9001.
10. Divisi *IT* tidak bisa mengikuti keseluruhan *SOP*.
    Risk severity: *Medium*
    Risk Response: *Lessen*
    Perusahaan dianjurkan untuk melakukan pengamatan dan penyesuaian kembali *SOP* dengan tugas dan kewajiban yang dimiliki oleh divisi *IT*, sehingga *SOP* bisa ditaati dan diikuti dengan baik oleh divisi *IT*. Untuk mengidentifikasi dan mencari penyebab mengapa divisi *IT* tidak bisa mengikuti SOP yang ada, perusahaan bisa menggunakan bantuan COBIT pada aspek *Delivery and Support* (*DS*) yaitu *DS* 9 (*manage configuration*) dan *DS* 10 (*manage problems*).

4. KESIMPULAN

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

1. Peran divisi *IT* pada perusahaan cukup besar. Meskipun divisi *IT* adalah divisi *support*, namun proses bisnis yang dimiliki oleh perusahaan bergantung pada kelancaran dan pelayanan yang diberikan oleh divisi *IT*.
2. Dalam analisa yang dilakukan mengacu pada *CobiT Control Practices* dan berfokus pada *PO* (*Plan and Organize*) yaitu *PO8* dan *PO9*, ditemukan 3 risiko tertinggi dengan *risk severity high*. Risiko – risiko yang memiliki kategori *high* adalah sebagai berikut :
   a. Risiko dengan prioritas 1 :
      i. Nomor Risiko : 18
      ii. Tidak adanya pengembangan *risk action* dan *risk assessment*
   b. Risiko dengan prioritas 2 :
      i. Nomor risiko : 9
      ii. Tidak adanya rencana pengembangan *SOP*/*QMS* untuk membantu pedoman bagi divisi *IT*
   c. Risiko dengan prioritas 3 :
      i. Nomor risiko : 15
      ii. Tidak ada proses perhitungan *likelihood* pada perusahaan
3. Untuk risiko-risiko dalam bidang IT yang ditemukan pada perusaaan *Real Estate* X , pencegahan yang mungkin dapat dilakukan oleh perusahaan adalah dengan menggunakan standar *ISO* 27001, *ISO* 31000, *ISO* 29110, *ISO* 9001[3], *COBIT* 4.1, *risk rating methodology by OWASP*, *NIST* 800-30, *GTAG* 3[6] dan *GTAG* 11.

5. DAFTAR PUSTAKA

[1] Bureau of Indian Standard. 2011. *IS*/*ISO* 31000(2009): *Risk Management*. India : Manak Bhavan

[2] Chrisdiyanto, I. 2013. *IT Risk Assessment di Perpustakaan Universitas Kristen Petra*. Surabaya: Universitas Kristen Petra.

[3] International Organization for Standardization.2008. *Quality Management System – Requirements(ISO 9001)*. USA: ISO.

[4] IT Governance Institute. 2007. *COBIT 4.1*. USA: ISACA.

[5] National Institute of Standards and Technology. 2002. *Computer Security(NIST 800-30).* USA: NIST.

[6] The Institute of internal Auditors. 2005. *Global Technology Audit Guide*. USA : The IIA

[7] The OWASP Risk Rating Methodology. 2012. URI=https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology