Analisa Risiko Teknologi Informasi di Divisi Produksi PT.X

Stevie Pramudita[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
Email : steve02_05@yahoo.co.id[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK

PT. X merupakan suatu perusahaan yang bergerak di industri rokok. Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *software*, *hardware*, jaringan, dan mesin yang digunakan untuk proses produksi. Tetapi perusahaan kurang melakukan monitoring terhadap alat-alat IT di perusahaan sehingga bila terjadi masalah, proses perbaikan masalah tersebut menjadi terlambat, dan perusahaan tidak memiliki rencana bila terjadi bencana.

Pada skripsi ini dilakukan analisa risiko terhadap IT di perusahaan dan proses bisnis yang ada di perusahaan. Langkah-langkah dalam melakukan analisa risiko tersebut yaitu dengan menggunakan COBIT 4.1, ISO 31000 dan untuk perhitungan menggunakan *Risk Rating Methodology OWASP*.
Risiko-risiko yang ditemukan di perusahaan dari skala *Critical-High* yaitu tidak adanya *Disaster* Recovery *Plan* (DRP), hasil *backup* data disimpan diruangan yang sama dengan server utama, tidak adanya monitoring dalam mem-backup data, *backup* data hanya dilakukan secara *onsite*, tidak adanya pencatatat data yang di *backup*.

Respon yang akan diberikan kepada perusahaan yaitu perusahaan sebaiknya membuat *DRP* sehingga bila terjadi bencana data penting perusahaan tidak hilang, tempat untuk menyimpan hasil backup sebaiknya berbeda dengan server utama, perusahaan sebaiknya melakukan monitoring sewaktu mem-*backup* data, *backup* juga harus dilakukan secara *offsite*, dan seharusnya terdapat pencatatan data yang di *backup* sehingga bila data tersebut hilang maka data tersebut dapat dengan mudah di *restore*.

Kata Kunci: Analisa Risiko, COBIT 4.1, ISO 31000, *OWASP*

ABSTRACT

PT. X is a tobacco company. In order to support its business processes, this company uses software, hardware, network and machines for production process. However, this company is lack of monitoring of IT tools so that when problems occur, the problem solving can be delayed, and it has no plans if disaster might happen.

This thesis assess IT risks and company's business processes. This assessment uses COBIT 4.1 standard, ISO 31000, and for the calculation used Risk Rating Methodology OWASP.

Risks that have Critical-High scale are no Disaster Recovery Plan, backup result is stored in the same room with the main server, no monitoring in data backing up, data backup is just done in onsite technique, no backup data recording.

The responses to the company's risk factors are that company should make DRP so that when any disaster occurs, company's important data is not lost, backup storage should located, at different place than main server, company should backup process, and backup should be done by offsite technique, so when any data is lost, it can be easily restored.

Keywords: *Risk Analysis, COBIT 4.1, ISO 31000, OWASP*

1. PENDAHULUAN

PT. X merupakan suatu perusahaan yang bergerak di industri rokok. Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *software*, *hardware*, jaringan, dan mesin yang digunakan untuk proses produksi. Tetapi perusahaan kurang melakukan monitoring terhadap alat-alat IT di perusahaan sehingga bila terjadi masalah, proses perbaikan masalah tersebut menjadi terlambat, dan perusahaan tidak memiliki rencana bila terjadi bencana.

Divisi Produksi di PT. X khususnya dalam mengatasi risiko IT belum pernah dilakukannnya analisa risiko yang dapat mengetahui risiko-risiko IT apa saja yang mungkin terjadi di perusahaan sehingga risiko-risiko tersebut dapat menghambat proses bisnis yang terjadi di perusahaan.

Dalam skripsi ini dilakukannya analisa risiko IT perusahaan. Dengan menggunakan beberapa teori penunjang. Teori-teori yang dipakai yaitu ISO 31000 untuk mengetahui langkah-langkah dalam menganalisa risiko, COBIT 4.1. untuk memilih proses yang akan digunakan dalam menganalisa risiko di perusahaan, dan OWASP untuk melakukan analisa perhitungan *score* yang dapat mengetahui faktor risiko yang paling berbahaya atau berisiko yang akan dialami oleh perusahaan.

Dari teori-teori yang digunakan sehingga dapat menghasilkan faktor risiko yang paling berisiko untuk perusahaan dan respon-respon dalam mengatasi setiap risiko yang mungkin akan dialami oleh perusahaan.

2. LANDASAN TEORI

2.1 ISO 31000

ISO 31000 merupakan standart international pedoman penerapan manajemen risiko yang diterbitkan oleh *International Organization for Standardization*. Di dalam ISO 31000 terdapat 11 prinsip, 4 *components* dan 6 proses [2].

6 proses yang terdapat dalam ISO 31000 yaitu:

- *Communication and Consultation*
  Harus adanya konsultasi yang membahas tentang manajemen risiko agar mereka mempunyai tanggung jawab dalam melaksanakan manajemen risiko, dan mereka harus mempunyai dasar di mana keputusan dibuat dan alasan mereka mengapa tindakan tersebut harus dilakukan
- *Establishing the context*
  Saat membuat konteks untuk proses manajemen risiko, mereka perlu dipertimbangkan secara lebih rinci dan jelas khususnya bagaimana mereka berhubungan dengan lingkup proses manajemen risiko tertentu.
- *Risk Assessment*
  Proses dalam *Risk Assessment* yaitu*:*
  - *Risk Identification*
    Tahap awal dimana seorang analis harus bisa menghasilkan daftar lengkap risiko – risiko yang dialami sebuah perusahaan yang mungkin nantinya risiko tersebut dapat terulang kembali. Pada tahap ini risiko tersebut haruslah jelas karena risiko tersebut harus bisa dipilah apakah risiko tersebut dapat terus meningkat, apakah risiko tersebut dapat dicegah, dan apakah risiko tersebut dapat diatasi dengan segera atau risiko tersebut dapat diturunkan tingkat keseriusan risiko tersebut. Karena pada tahap ini, risiko tersebut bila setelah selesai di tahap identifikasi maka risiko tersebut akan dibawa ketahap analisis, maka dari itu informasi yang di dapat haruslah informasi yang relevan dan informasi tersebut harus *up-to-date.*
  - *Risk Analysis*
    Tahapan kedua dalam *Risk Assessment*, pada tahapan ini adalah tahap pengembangan dari risiko – risiko yag telah ada di tahap *Risk Identification*. Pada tahap pengembangan ini perlu dilakukan evaluasi risiko apakah risiko ini perlu ditangani dengan segera atau bisa ditangani berikutnya. Dengan membuat tabel *likelihood* dan *impact* dari semua risiko yang ada.
  - *Risk Evaluation*
    Tahap risiko untuk membantu dalam membuat keputusan, berdasarkan hasil analisis risiko, tentang risiko yang membutuhkan penanganan dengan segera atau risiko tersebut bisa ditangani berikutnya, jadi pada tahapan ini seorang analis risiko akan memprioritaskan risiko mana yang harus didahulukan penangannya dan risiko mana yang nantinya bisa ditangani.
- *Risk Treatment*
  Risk Treatment adalah tahapan pemilihan apakah risiko dapat diterima atau ditolak, bila risiko tersebut diterima apakah ada penanganan yang secara mendalam lagi, bila risiko tersebut ditolak apakah ada risiko baru yang akan datang.
- *Monitoring and Review*
  Kemajuan aktual dalam melaksanakan rencana perlakuan resiko memberikan ukuran kinerja dan dapat dimasukkan ke dalam manajemen kinerja organisasi, pengukuran dan pelaporan kegiatan internal dan eksternal. Pemantauan dan *review* dapat melibatkan pemeriksaan biasa atau pengawasan dari apa yang sudah ada atau bisa periodik.
- *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

Control Objective for Information and Related Technology (*CobiT*). *CobiT* 4.1 adalah model standart pengelolahan *IT* yang mendapatkan pengakuan luas, dikembangkan oleh *Information Technology Governance Institute* (*ITGI*) dari *Information System Audit and Control Association* (ISACA). Dalam *CobiT* 4.1 terdapat 4 *domain* dan terdapat 34 proses. 4 domain yang terdapat dalam CobiT yaitu : (1). *Plan and Organize*, (2). *Acquisition and Implementation*, (3). *Delivery and Support*, (4). *Monitoring and Evaluation* [5].

Dari proses di Cobit 4.1. proses yang diambil oleh penulis yaitu *Delivery and Support* (DS) 3 dan *Delivery and Support* (DS) 4.

Dalam *DS* 3 terdapat 5 *Control Objective* yaitu:

- *Performance and Capacity Planning*
- *Future Performance and Capacity*
- *IT Resources Availability*
- *Monitoring and Reporting*

Dalam *DS* 4 terdapat 10 *Control Objective* yaitu:

- *IT Continuity Framework*
- *IT Continuity Plans*
- *Critical IT Resources*
- *Maintanance of the IT Continuity Plan*
- *Testing of the IT Continuity Plan*
- *IT Continuity Plan Training*
- *Distribution of the IT Continuity Plan*
- *Service Recovery and Resumption*
- *Offsite Backup Storage*
- *Post Resumption Review*

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

Penilaian risiko didapatkan dari hasil perkalian nilai *likelihood* dan nilai *impact*. Untuk mendapatkan nilai *likelihood* dan *impact* dari setiap faktor risiko, maka dibutuhkan kriteria-kriteria untuk menilai nilai dari setiap risiko yang ada [1]. Kriteria yang digunakan untuk menilai *likelihood* yaitu :

1. *Skill Level*
   Skill Level dapat menjadi ukuran dalam terjadinya suatu risiko yang terjadi di perusahaan. Hal ini digunakan untuk mengukur seberapa tinggi yang dimiliki oleh *staff IT* jika adanya *threat agent* yang mencoba untuk menerobos sistem keamanan yang ada.
2. *Management and Stakeholder Support*
   Dukungan dari beberapa pihak agar pengetahuan terhadap risiko agar dapat diaplikasikan.
3. *Teamwork*
   Teamwork mengukur seberapa solid tim tersebut dalam melakukan pencegahan risiko bila risiko tersebut terjadi.
4. *Project Management*
   Project Management diukur seberapa mampuhkah *project management* untuk menangani risiko yang ada.

5. *Awareness*

Adanya kesadaran dengan semua pihak terhadap risiko yang terjadi dan adanya tindakan untuk meminimalkan risiko tersebut agar risiko tersebut tidak terjadi lagi.

Kriteria yang digunakan untuk menilai *impact* yaitu :

1. *Confidentiality*

Confidentiality yaitu jika terjadi masalah banyak layanan yang mengalami gangguan. Gangguan-gangguan yang mungkin bisa terjadi yaitu data rusak, kerahasiaan data tidak terjaga bahkan data yang dimiliki oleh perusahaan bisa hilang.

2. *Integrity*

Adanya kesinambungan antara alat-alat IT dengan keperluan bisnis yang ada. Semakin tidak cocoknya alat-alat IT dengan kepentingan bisnis, semakin tinggi risiko yang harus di tanggung oleh perusahaan.

3. *Availability*

Availability yaitu mengukur seberapa banyak layanan yang tidak tersedia akibat terjadinya risiko tersebut bila risiko tersebut terjadi di perusahaan

4. *Accountability*

Accountability yaitu mengukur seberapa jauh pihak-pihak yang bertanggung jawab dalam meminimalkan risiko tersebut.

5. Layanan

Mengukur seberapa parah dampak terhadap layanan ketika risiko tersebut terjadi. Bila layanan menjadi lebih buruk maka dampak yang diterima perusahaan menjadi lebih besar.

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

2.4 Kriteria Penilaian Risiko Berdasarkan OWASP

Berikut merupakan salah satu kriteria *impact* berdasarkan OWASP [6]. Berikut kriteria impact yang digunakan.

1. *Financial Damage*

Mengukur seberapa parah dampak risiko karena adanya kerugian keuangan perusahaan yang nantinya akan berdampak pada profit perusahaan

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Gambar 1 *Overall Likelihood* [6].

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	5	1	2	1	5
Overall technical impact=6.25 (MEDIUM)				Overall business impact=2.25 (LOW)			

Gambar 2 *Overall Impact* [6].

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Gambar 3 *Likelihood and Impact Levels* [6].

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Gambar 4 *Overall Risk Severity* [6].

3. PENILAIAN RISIKO

3.1 Penentuan Kriteria Penilaian Risiko

Tabel 1. Penentuan Kriteria Penilaian Risiko

Kriteria	Sumber	Keterangan*
Skill Level	Analisa Perpustakaan Universitas Kristen Petra.	Sesuai dengan sumber.
Management and Stakeholder Support	Pengembangan analisa berdasarkan *ITRISK ASSESSMENT DI PERPUSTAKAN UNIVERSITAS KRISTEN PETRA.*	Definisi : Dukungan dari beberapa pihak agar pengetahuan terhadap risiko agar dapat diaplikaskan - *Management and Stakeholder Support* mendukung dan menyetuji adanya kebijakan penanganan suatu risiko yang terjadi (1). - *Management and Stakeholder Support* mendukung adanya pencegahan risko tetapi management hanya menganggap sebagian kecil pentingnya penanganan suatu risiko yang terjadi (4). - *Management and Stakeholder Support* mendukung adanya pencegahan risiko tetapi management kurang menganggap pentingnya

		penanganan suatu risiko yang terjadi. (6) - *Management and Stakeholder Support* tidak mendukung dan menyetujui bahkan mempersulit untuk dilakukannya pencegahan penanganan suatu risiko (9). *(1), (4), (6), (9) yaitu *score* di tiap-tiap kriteria.
Teamwork	Analisa Perpustakaan Universitas Kristen Petra.	Sama dengan sumber.
Project Management	Analisa Perpustakaan Universitas Kristen Petra.	Sama dengan sumber.
Awareness	Pengembangan analisa berdasarkan *IT RISK ASSESSMENT DI PERPUSTAKAN UNIVERSITAS KRISTEN PETRA.*	Definisi : Adanya kesadaran dengan semua pihak terhadap risiko yang terjadi dan adanya tindakan untuk meminimalkan risiko tersebut agar risiko tersebut tidak terjadi lagi. - Adanya kesadaran untuk melakukan tindakan pencegahan agar risiko tersebut berkurang (1). - Adanya kesadaran akan tetapi minimnya tindakan untuk mencegah risiko tersebut terjadi (3). - Kecilnya kesadaran dan minimnya tindakan yang dilakukan untuk mencegah

		risiko tersebut terjadi (5). - Tidak adanya kesadaran dan dorongan untuk meminimalkan risiko tersebut (9). *(1), (3), (5), (9) yaitu *score* di tiap-tiap kriteria.
Integrity	Analisa Perpustakaan Universitas Kristen Petra.	Sesuai dengan sumber.
Confidentiality	Analisa Perpustakaan Universitas Kristen Petra.	Sesuai dengan sumber.
Availability	Pengembangan analisa berdasarkan *IT RISK ASSESSMENT DI PERPUSTAKAN UNIVERSITAS KRISTEN PETRA*.	Definisi : mengukur seberapa banyak layanan yang tersedia akibat terjadinya risiko tersebut bila risiko tersebut terjadi di perusahaan. - Semua layanan tetap tersedia sekalipun risiko tersebut terjadi (1). - Semua kecil layanan saja yang tidak berfungsi akibat dari risiko tersebut (5). - Sebagian besar layanan yang tidak dapat berfungsi bila risiko tersebut terjadi. (7). - Hampir sebagian besar layanan tersebut tidak berfungsi ketika risiko tersebut terjadi (9). *(1), (5), (7), (9) yaitu *score* di tiap-tiap kriteria.
Accountability	Analisa Perpustakaan Universitas Kristen Petra.	Sesuai dengan sumber.

Layanan / *Service*	Pengembangan analisa berdasarkan *IT RISK ASSESSMENT DI PERPUSTAKAN UNIVERSITAS KRISTEN PETRA.*	Mengukur seberapa parah dampak terhadap layanan ketika risiko tersebut terjadi. Bila layanan menjadi lebih buruk maka dampak yang diterima perusahaan menjadi lebih besar. - Tidak adanya dampak terhadap layanan bila risiko tersebut terjadi (1). - Hanya sebagian kecil saja layanan yang terganggu atau terkena dampak bila risiko tersebut terjadi (7). - Hampir semua layanan yang terganggu sehingga fungsi kerja menjadi menurun (9). *(1), (7), (9) yaitu *score* di tiap-tiap kriteria.
Financial Damage	Pengembangan analisa berdasarkan *OWASP*	Mengukur seberapa parah dampak risiko karena adanya kerugian keuangan perusahaan yang nantinya akan berdampak pada profit perusahaan. - Kerugian yang diterima perusahaan tidak berdampak pada perusahaan (1). - Kerugian yang diterima perusahaan berdampak kecil pada profit perusahaan (4). - Kerugian yang diterima perusahaan berdampak besar pada profit perusahaan (6). - Kerugian yang diterima perusahaan dapat menyebabkan perusahaan bangkrut (9). *(1), (4), (6), (9) yaitu *score* di tiap-tiap kriteria.

3.2 *Risk Severity*

Pada Risk Severity akan diambil 10 tertinggi dari Risk Factors berdasarkan nilai dari Risk Severity yang tertinggi.

Tabel 2. *Risk Severity* berdasarkan urutan

Rank	No.	Risiko	Risk Severity	Level	Overall Level
1.	13.	Tidak adanya monitoring dalam mem-*backup* data.	31.886	MH	High
2.	14.	Hasil backup data disimpan di ruangan yang sama dengan server utama.	30.346	MH	High
3.	7.	Tidak adanya Disaster Recovery Plan.	27.152	MH	High
4.	12.	Proses backup hanya disimpan di pita tape dan harddisk lain.	22.830	MH	High
5.	15.	Tidak adanya pencatatan data yang di backup, hanya dilakukannya proses backup.	22.310	MH	*High*
6.	2.	Proses *monitoring* hanya dilakukan setiap pagi hari sewaktu memasuki jam kerja	17.788	MM	*Medium*
7.	5.	Tidak adanya pelaporan secara rutin tentang performa dan kapasitas *IT*	16.745	MM	*Medium*
8.	3.	Tidak adanya *aplikasi* dalam menanggulangi kinerja *bandwidth* bila terjadi lonjakan kapasitas.	16.075	MM	*Medium*
9.	4.	Divisi *IT* tidak menghitungkan kerugian finansial akibat alat-alat *IT* tidak sesuai	14.574	HL	*Medium*
10.	11.	Tidak adanya pencegahan masalah agar masalah tersebut tidak berlanjut.	14.184	MM	*Medium*

3.3 *Risk Respose Planning*

Risk Response Planning merupakan bagaimana cara perusaahaan harus beraksi terhadap risiko tersebut. Dari risiko yang ada, maka dapat disimpulkan R*isk* R*esponse* P*lanning* yang disarankan, Berikut adalah 10 contoh *Risk Response*

- Tidak adanya *monitoring* dalam mem-*backup* data.
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Sesuai standart ISO 22313 sebaiknya perusahaan melakukan *monitoring* terhadap setiap proses yang ada berada di perusahaan.
- Hasil *backup* data disimpan di ruangan yang sama dengan server utama.
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk faktor risiko tersebut yaitu sebaiknya hasil *backup* disimpan di ruangan yang berbeda dengan server utama. Minimal di tiga tempat yang berbeda sehingga bila terjadi gangguan seperti kebakaran, maka data-data penting perusahaan dapat terselamatkan sehingga proses bisnis dapat berjalan dengan lancar.
  Sesuai dengan standart NIST 800-34 dikatakan tempat penyimpanan hasil backup harus berada di ruangan yang berbeda dengan server utama sehingga data-data penting perusahaan dapat lebih aman.
- Tidak adanya *Disaster Recovery Plan*.
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk menghadapi perusahaan karena tidak adanya *Disaster Recovery Plan* yaitu seharusnya perusahaan membuat rencana bila terjadi gangguan-gangguan seperti kebakaran, gempa bumi, banjir, tsunami sehingga bila bencana tersebut terjadi perusahaan mempunyai respon yang tanggap dalam mengatasi bencana tersebut.
  Sesuai standart NIST 800-34 perusahaan harus membuat rencana untuk mengatasi bencana yang ada seperti kebakaran, gempa bumi, tsunami, banjir dan perusahaan harus mempunyai rencana *recovery* bila bencana tersebut selesai sehingga proses bisnis yang terjadi di perusahaan dapat berlangsung secara terus-menerus.
- Proses *backup* hanya disimpan di pita tape dan *harddisk* lain.
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Proses *backup* hanya dilakukan secara *onsite* data-data penting perusahaan disimpan di media *harddisk* dan pita tape, seharusnya proses *backup* juga terjadi secara *offsite* yaitu proses penyimpanan data-data penting perusahaan di dalam *cloud* seperti *dropbox, google drive*, sehingga data-data penting perusahaan menjadi lebih aman dan proses bisnis dapat berjalan dengan lancar.
  Sesuai dengan standart ISO 22313 proses backup juga harus dilakukan secara *offsite* sehingga data-data penting perusahaan tersebut menjadi lebih aman dari masalah yang ada seperti kebakaran, banjir, tsunami, gempa bumi.
- Tidak adanya pencatatan data yang di *backup*, hanya dilakukannya proses *backup*
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk mengatasi risiko tersebut adalah sebaiknya perusahaan melakukan pencatatan data-data penting apa saja perusahaan yang di backup, sehingga bila terjadi masalah maka data tersebut dapat dengan mudah ditemukan, sehingga data penting tersebut dapat dengan mudah di *restore*.
  Sesuai dengan standart ISO 22313 perusahaan sebaiknya melakukan pencatatan data setelah dilakukannya *monitoring* sehingga data tersebut menjadi lebih aman.
- Proses *monitoring* hanya dilakukan setiap pagi hari sewaktu memasuki jam kerja
  Risk Severity : *Medium*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon terhadap risiko ini proses *monitoring* hanya dilakukan pagi hari tidak menjadi masalah, akan tetapi sebaiknya jika proses *monitoring* hanya dilakukan pada pagi hari maka perusahaan sebaiknya mempunyai aplikasi yang dapat memberikan pesan kepada staff *IT* jika terjadi kerusakan atau gangguan pada alat-alat *IT* sehingga masalah tersebut dapat terselesaikan dengan cepat.
  Sesuai dengan standard NIST 800-34 perusahaan dapat mengintall suatu *software* yang dapat mengatasi masalah lonjakan kapasitas dengan cara memberikan peringatan kepada staff *IT* bila terjadinya lonjakan seperti mengirimkan email kepada staff *IT*.
- Tidak adanya pelaporan secara rutin tentang performa dan kapasitas *IT*
  Risk Severity : M*edium*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk risiko ini adalah divisi IT haruslah memberikan pelaporan secara rutin dengan management tentang performa dan kapasitas *IT*.
  Sesuai dengan standart ISO 22313 setiap karyawan sebaiknya memberikan pelaporan kepada management tertinggi tentang performa dan kapasitas *IT*.
- Tidak adanya *aplikasi* dalam menanggulangi kinerja *bandwidth* bila terjadi lonjakan kapasitas.
  Risk Severity : *Medium*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk risiko tersebut yaitu perusahaan sebaiknya menambahkan suatu aplikasi yang dapat mengetahui bila terjadi lonjakan kapasitas bandwidth sehingga karyawan atau staff *IT* dapat mengetahui lonjakan kapasitas tersebut.
  Sesuai dengan standard NIST 800-34 perusahaan dapat mengintall suatu *software* yang dapat mengatasi masalah lonjakan kapasitas dengan cara memberikan peringatan kepada staff *IT* bila terjadinya lonjakan seperti mengirimkan email kepada staff *IT*.
- Divisi *IT* tidak menghitungkan kerugian finansial akibat alat-alat *IT* tidak sesuai
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk menghadapi risiko tersebut yaitu perusahaan harus memperhitungkan setiap kerugian akibat alat-alat *IT* tidak sesuai.
  Sesuai standart ISO 22313 setiap perusahaan sebaiknya menghitungkan kerugian finansial akibat alat-alat *IT* tidak sesuai..

- Tidak adanya pencegahan masalah agar masalah tersebut tidak berlanjut.
  Risk Severity : *High*
  Risk Response : *Lessen*
  Latar Belakang Pemilihan *Risk Response* :
  Respon untuk mengatasi masalah ini yaitu sebaiknya perusahaan memberikan pencegahan terhadap respon yang terjadi sehingga masalah yang di timbulkan tidak terjadi secara terus-menerus.
  Sesuai dengan ISO 22313 suatu organisasi harus meminimalisir risiko yang ada sehingga risiko tersebut tidak terjadi secara terus-menerus.

4. KESIMPULAN

4.1 Kesimpulan

Risiko-risiko dalam bidang IT yang mungkin terjadi selama berjalannya proses bisnis dan tindakan mitigasi yang dapat dilakukan oleh PT. X adalah :

- Tidak adanya monitoring dalam mem-*backup* data.
  Response: *Lessen* dengan menggunakan standard ISO 22313 sebaiknya perusahaan melakukan *monitoring* terhadap setiap proses yang ada di perusahaan.
- Hasil Backup data disimpan di ruangan yang sama dengan server utama.
  Response: *Lessen* dengan menggunakan standard NIST SP 800-34 setiap karyawan harus mempunyai peran dan tanggung jawab dalam memberikan respon yang baik dalam setiap masalah yang ada, sehingga jika dengan adanya respon yang baik, masalah tersebut dapat terselesaikan.
- Tidak adanya *Disaster Recovery Plan*
  Response: *Lessen* sesuai standard NIST 800-34 perusahaan harus membuat rencana untuk mengatasi bencana yang ada seperti kebakaran, gempa bumi, banjir, tsunami dan perusahaan harus mempunyai rencana *recovery* bila bencana tersebut selesai sehingga proses bisnis yang terjadi di perusahaan dapat berlangsung secara terus-menerus.
- Proses b*ackup* hanya disimpan di pita tape dan *harddisk* lain.
  Response: *Lessen* sesuai standard ISO 22313 proses *backup* juga harus dilakukan secara *offsite* sehingga data penting perusahaan menjadi lebih aman bila terjadi masalah seperti kebakaran, banjir, gempa bumi.
- Tidak adanya pencatatan data yang di *backup*, hanya dilakukannya proses *backup*
  Response: *Lessen*, sesuai standard ISO 22313 perusahaan harus melakukan pencatatan data setelah dilakukannya *monitoring* sehingga data tersebut menjadi lebih aman.
- Proses *monitoring* hanya dilakukan setiap pagi hari sewaktu memasuki jam kerja.
  Response: *Lessen*, proses *monitoring* hanya dilakukan pada pagi hari tidak menimbulkan masalah akan tetapi sesuai standard NIST SP 800-34 perusahaan dapat meng-*install* software yang dapat mengatasi masalah dengan cara memberikan peringatan kepada staff IT bila terjadi masalah dengan cara mengirimkan *email* kepada staff IT.
- Tidak adanya pelaporan secara rutin tentang performa dan kapasitas IT.
  Response: *Lessen*, sesuai standard ISO 22313 setiap karyawan sebaiknya memberikan pelaporan kepada managemen tertinggi tentang performa dan kapasitas IT.
- Tidak adanya *aplikasi* dalam menanggulangi kinerja bandwidth bila terjadi lonjakan kapasitas.
  Response: *Lessen* dengan memilih standar NIST 800-34 perusahaan dapat menginstall suatu *software* yang dapat mengatasi masalah lonjakan kapasitas dengan cara memberikan peringatan kepada staff IT bila terjadi masalah dengan cara mengirimkan email kepada staff IT.
- Divisi IT tidak menghitungkan nominal kerugian finansial akibat alat-alat IT tidak sesuai.
  Response : Lessen, dengan memilih standard ISO 22313 setiap perusahaan sebaiknya menghitungkan kerugian finansial akibat alat-alat IT tidak sesuai.
- Tidak adanya pencegahan masalah agar masalah tersebut tidak berlanjut.
  Response : Lessen, sesuai standard ISO 22313 suatu organisasi harus meminimalisir risiko yang ada sehingga risiko tersebut tidak terjadi secara terus-menerus.
- Terlambatnya respon yang ditunjukkan bila divisi-divisi lain mengalami gangguan.
  Response: Lessen, sesuai dengan standard NIST 800-34 setiap karyawan harus mempunyai peran dan tanggung jawab dalam memberikan respon yang baik dalam setiap masalah yang ada, sehingga jika dengan adanya respon yang baik, masalah tersebut dapat dengan selesai terselesaikan
- Tidak adanya pelatihan karyawan tentang alat-alat IT yang baru.
  Response : Lessen, sesuai standart ISO 22313 perusahaan harus memberikan pelatihan dalam bentuk apapun kepada karyawan sehingga dengan adanya pelatihan tersebut dapat meminimalkan risiko tersebut terjadi.
- Tidak adanya *framework* dalam menyusun tentang perencanaan teknologi informasi
  Response: Lessen, sesuai dengan standard ISO 38500 dijelaskan bahwa perusahaan harus menerapkan 6 prinsip agar bisnis tetap berlangsung. 6 prinsip yang harus dimiliki perusahaan yaitu *responsibility*, *strategy*, *acquisition*, *performance*, *conformance*, *human behaviour*.
- Tidak adanya *framework* dalam menyusun teknologi informasi untuk meningkatkan performa dan kapasitas *IT*
  Response: Lessen, sesuai dengan standard ISO 38500 dijelaskan bahwa perusahaan harus menerapkan 6 prinsip agar bisnis tetap berlangsung. 6 prinsip yang harus dimiliki perusahaan yaitu responsibility, *strategy*, *acquisition*, *performance*, *conformance*, *human behaviour*.

5. DAFTAR PUSTAKA

[1] Chrisdiyanto, I (2013). *IT Risk Assessment di perpustakaan Universitas Kristen Petra*. Surabaya.

[2] Draft International Standard. (2008). ISO/DIS 31000 : Risk Management-Principles and Guidelines on Implementation.

[3] Draft International Standard (2011). ISO/DIS 22313 : *Societal security – Business continuity management system – Guidance.*

[4] International Standard (2008). ISO/IEC 38500: *Corporate governance of information technology.*

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

[6] OWASP Risk Rating Methodology. (2008). The OWASP Risk Rating Methodology. Retrieved Sept. 17, 2013, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology