Analisa Risiko Kelangsungan Bisnis, Pengawasan dan Evaluasi Teknologi Informasi di PT ABC

Raymond Adrian Hardha[1], Adi Wibowo[2], Agustinus Noertjahyana[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: raymondadrianh@live.com[1], adiw@petra.ac.id[2], agust@petra.ac.id[3]

ABSTRAK

PT ABC merupakan perusahaan yang bergerak dibidang produksi besi beton. Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *server*, jaringan, *software*, *hardware*, perangkat PC. Dengan terganggunya salah satu sistem tersebut maka proses pengolahan data akan terganggu karena harus mengolah data secara manual dan melakukan input ke *database* setelah sistem dapat berjalan dengan normal kembali. Melihat situasi dan kondisi dari PT ABC, tidak menutup kemungkinan terjadinya risiko seperti kerusakan *data integrity* dan terganggunya kesinambungan proses bisnis.

Pada skripsi ini dilakukan analisa risiko terhadap IT continuity dan monitoring di PT ABC. Analisa risiko menggunakan *framework* dari ISO 31000, untuk proses analisa menggunakan COBIT 4.1 beserta *control practices*, dan menggunakan *risk rating methodology* (OWASP) untuk penghitungan nilai risiko.

Dari hasil analisa, terdapat 7 risiko yang ditemukan yaitu 1 risiko dengan *risk severity high adalah* tidak mempunyai pihak yang bertanggung jawab terhadap penyimpangan, 2 risiko dengan *risk severity medium adalah* tidak mempunyai *business continuity plan* yang cocok, tidak mempunyai *framework* untuk membuat *business continuity plan,* 4 risiko dengan *risk severity low adalah* tidak mempunyai *offsite backup*, tidak mempunyai prioritas *plan*, tidak ada pelatihan untuk memperdalam *skill* analisa data, tidak melakukan *update IT continuity*. Hasil analisa risiko ini dapat membantu perusahaan untuk menyadari risiko-risiko yang mungkin terjadi sehingga perusahaan dapat mengambil tindakan untuk mencegah atau mengatasi risiko tersebut.

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

ABSTRACT

PT ABC is a company engaged in the production of reinforced concrete. In carrying out its business processes, the company is using the server, network, software, hardware, PC software. With the disruption of one of these systems, the data processing will be annoyed at having to manually process data and perform the input to the database after the system can run normally again. Looking at the situation and condition of PT ABC, did not rule out the occurrence of risks such as damage to data integrity and continuity disruption of business processes.

In this thesis conducted a risk analysis of the IT continuity and monitoring of PT ABC. Risk analysis using the framework of ISO 31000, for process analysis and its use COBIT 4.1 control practices, and use risk rating methodology (OWASP) for calculating the value of risk.

There are 7 risks found from analysis. One risk that has high severity is the company did not have those who has responsibility to monitor irregularities. Two medium risks are the company did not have business continuity plan, and also a framework to build that plan. Four risks with low severity are the company did not have an offsite backup, did not have a priority plan, no training for employees to upgrade analysis skills, and never update IT continuity plan.

Keywords: *Analisa Risiko, ISO 31000, COBIT 4.1, COBIT Control Practices, OWASP*

1. PENDAHULUAN

Perkembangan teknologi kian cepat dan sangat berpengaruh dalam dunia bisnis di berbagai macam perusahaan. Persaingan antar perusahaan, tidak pernah lepas dalam dunia bisnis, juga dipengaruhi perkembangan teknologi. Penerapan sistem komputerisasi sudah mulai diterapkan pada banyak bidang dan berkembang dengan pesatnya. Berbagai sistem dikembangkan dengan menggunakan media komputer dan pendukungnya dan hal ini membuat sebagian besar sektor mulai mengembangkan sistem informasi pada proses bisnis yang dilaksanakan. Salah satu aspek penting dalam sistem informasi adalah aspek keamanan dan manajemen risiko. Dengan berkembangnya sistem informasi pada saat ini beberapa hal penting yang menjadi faktor penentu agar sistem yang berjalan dapat berfungsi dengan baik dan benar. Selain efek positif dari berkembangnya sistem informasi maka permasalahan keamanan dan pengelolaan sumber daya Teknologi Informasi juga terjadi.

PT ABC sebagai salah satu produsen besi beton telah menerapkan teknologi informasi untuk mempermudah pemrosesan data. Untuk itu teknologi informasi di perusahaan merupakan bagian yang sangat penting. Penggunaan sistem *server* untuk jaringan, *database* untuk penyimpanan informasi, perangkat PC dan berbagai macam peranan TI di perusahaan. Dengan terganggunya salah satu sistem tersebut maka proses pengolahan data akan terganggu dan tidak efisien karena harus mencatat data secara manual dan melakukan input ke *database* setelah sistem dapat berjalan dengan normal kembali. Tidak menutup kemungkinan bahwa kesalahan dalam pengambilan keputusan dalam mengatasi resiko, dan dampak yang terjadi dapat menyebabkan meningkatnya biaya operasional. Contoh tersebut merupakan bentuk risiko yang dapat menyebabkan tidak maksimalnya kinerja perusahaan atau lebih buruknya risiko ini dapat berpengaruh terhadap perusahaan di waktu yang akan datang. Sampai saat ini belum pernah dilakukan *risk management* untuk mengidentifikasi risiko-risiko yang dapat terjadi dalam penggunaan TI di perusahaan tersebut.

Mengingat pentingnya peranan TI di PT ABC untuk mendukung proses bisnis, maka diperlukan *risk management* terhadap segala risiko yang berdapak pada perusahaan. Melalui analisis *risk management*, perusahaan dapat mengetahui risiko-risiko yang dapat terjadi dan seberapa parah dampaknya terhadap perusahaan. Perusahaan juga dapat mengerti cara menangani risiko-risiko dan menentukan prioritas yang harus ditangani segera. Oleh karena itu diharapkan perusahaan menggunakan hasil dari *risk management* untuk mengambil kebijakan dalam mengatasi risiko-risiko dengan penanganan yang benar. Risiko-risiko yang ditangani dengan baik dan benar dapat menjadi kesempatan bagi perusahaan untuk meningkatkan kinerja perusahaan.

2. LANDASAN TEORI

2.1 ISO 31000

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh *International Organization for Standardization* pada tanggal 13 November 2009. 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 [2].

- ***Process for managing risk:***

1. Komunikasi dan konsultasi

   Komunikasi dan konsultasi dilakukan dengan pihak internal maupun eskternal perusahaan yang terkait dengan proyek manajemen risiko.

2. Konteks

   Elemen ini berkaitan dengan penentuan parameter dalam manajemen risiko yang harus memperhatikan faktor PEST, yaitu politik, ekonomi, sosial, dan teknologi. Hasil analisis PEST tersebut digunakan manajer untuk membangun konteks manajemen risiko yang meliputi kebijakan, proses metodologi, kriteria *rating* risiko, pelatihan, serta pelaporan setiap proses yang dilakukan.

3. Identifikasi Risiko

   Identifikasi tempat, waktu, alasan dan bagaimana suatu kejadian atau risiko bisa terjadi.

4. Analisis Risiko

   Identifikasi dan evaluasi proses control yang saat ini dilakukan untuk menentukan konsekuensi dan kemungkinan tingkat risiko.

5. Evaluasi Risiko

   Pada elemen ini dilakukan perbandingan antara perkiraan tingkat risiko terhadap *pre-established criteria* dan mempertimbangkan potensi manfaat serta kerugian yang ditimbulkan. Perbandingan tersebut membantu pembuatan keputusan terkait perawatan, pemeliharaan, tindakan tentang prioritas.

6. Perlakuan terhadap risiko

   Pengembangan dan implementasi strategi efektivitas biaya dan rencana peningkatan potensi manfaat dengan mengurangi biaya.

7. Monitor dan *review*

   Proses-proses manajemen risiko perlu dimonitor dan ditinjau untuk kontinuitas peningkatannya.

2.2 OWASP (Open Web Application Security Project)

OWASP merupakan metode untuk melakukan penilaian dengan menggunakan kriteria-kriteria. Penilaian dilakukan dengan menganalisa kemungkinan terjadinya risiko (*likelihood scale*) dan besar dampak yang ditimbulkan oleh risiko tersebut (*impact scale*). Berdasarkan metode OWASP, faktor-faktor yang dapat mempengaruhi terjadinya risiko yaitu *threat agent* dan *vulnerability*. [7]

Tujuan dari threat agent adalah untuk memperkirakan kemungkinan serangan berasal dari agent tersebut. Ancaman tersebut harus dilihat dari keadaan *threat agent* berdasarkan *skill level, motive, opportunity,* dan *size*.

Tujuan dari vulnerability adalah untuk memperkirakan kerentanan yang dapat di eksploitasi oleh threat agent. Ancaman tersebut harus dilihat dari kerentanan (vulnerability) berdasarkan *ease of discovery, ease of explot, awareness, dan intrusion detection.*

Dalam memperkirakan dampak dari sebuah serangan, sangat penting untuk menyadari bahwa ada 2 macam dampak. Pertama adalah dampak teknis (*technical impact*) pada aplikasi, data yang digunakan, dan fungsi yang disediakan. Kedua adalah dampak bisnis (*business impact*) pada bisnis dan perusahaan.

Tujuan dari *technical impact* adalah untuk memperkirakan besarnya dampak pada sistem jika kerentanan di eksploitasi. Point-point untuk menilai seberapa besar technical *impact* yang terjadi adalah *loss of confidentiality, loss of integrity, loss of availability, dan loss of accountability*.

Tujuan dari *Business impact* adalah memperkirakan besarnya dampak terhadap perusahaan dan untuk meningkatkan kesadaran untuk meningkatkan investasi untuk meningkatkan keamanan terhadap kerentanan. Poin-poin untuk menilai seberapa besar *business impact* yang terjadi adalah *financial damage, reputation damage, non-compliance, dan privacy violation*. Perhitungan likelihood pada dilihat pada Gambar 1.

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

Gambar 1. *Likelihood* dan *Impact Levels* [7]

Hasil dari perkalian tersebut merupakan hasil akhir penilaian suatu risiko yang nantinya akan digunakan untuk penggolongan risiko. Berikut contoh penilaian menggunakan *OWASP risk rating methodology* dapat dilihat pada Gambar 2 untuk perhitungan *likelihood* dan Gambar 3 untuk perhitungan *impact*. Untuk menentukan tingkat *Risk Severity* sesuai dengan Gambar 4.

Thread Agent Factor				Vulnerability Factor			
Skill Level	Motive	Opportunity	Size	Ease Of Discovery	Ease Of Exploit	Awarness	Intrusion Detection
5	2	7	1	3	6	9	2
Overall Likelihood = 4.375 (MEDIUM)							

Gambar 2. *Overall Likelihood* [7]

Technical Impact				Business Impact			
Lost Of Confidentiality	Lost Of Integrity	Lost Of Availability	Lost Of Accountability	Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
9	7	5	8	1	2	1	5
Overall Technical Impact = 7.25 (HIGH)				Overall Business Impact = 2.25 (LOW)			

Gambar 3. *Overall Technical Impact dan Business Impact* [7]

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* [7]

2.3 Risk Rating Berdasarkan Analisa IT Risk Assessment Di PT. X

Dari hasil perkalian nilai likelihood dan nilai *impact*, dianalisa sesuai dengan situasi dan kondisi di perusahaan sehingga hanya digunakan beberapa kriteria saja. Kriteria yang digunakan untuk menilai likelihood adalah kriteria yang merupakan penyebab munculnya risiko tersebut, PT X pernah melakukan *risk assessment* yang menghasilkan kriteria untuk penilaian *likelihood* antara lain: [9]

- *Skill*
  Risiko terjadi karena keteratasan kemampuan dari *staff* atau pihak manajemen [9].
  - Staff atau manajemen cukup memiliki pemahaman dan memiliki kemampuan untuk melakukan (1)
  - Staff atau manajemen memiliki pemahaman tetapi tidak memiliki kemampuan untuk melakukan (5)
  - Staff atau manajemen seharusnya memiliki kemampuan yang cukup tetapi tidak ada pemahaman (7)
  - Staff atau manajemen tidak memiliki pemahaman dan tidak memiliki kemampuan untuk melakukan (9)
- *Management and stakeholder support*
  Risiko dapat terjadi karena kurangnya dukungan dari manajemen berupa *staff* dan dukungan dari *stakeholder* berupa permintaan atau kebutuhan terhadap IT [9].
  - Adanya dukungan penuh dari sebagian besar manajemen dan stakeholder (1)
  - Ada kebijakan yang mengatur tetapi jumlah staff tidak memadai dan tidak ada biaya yang disediakan (3)
  - Tidak ada kebijakan yang mengatur tetapi seharusnya jumlah staff dan biaya mencukupi (5)
  - Tidak ada dukungan dari manajemen maupun stakeholder (9)
- *Awareness*
  Risiko dapat terjadi akibat kurangnya kesadaran dari pihak manajemen maupun *staff* [8].
  - Ada cukup kesadaran akan adanya suatu risiko dan ada upaya untuk menghentikan risiko tersebut (1)
  - Ada kesadaran akan adanya suatu risiko tetapi tidak ada upaya untuk menghentikan risiko tersebut karena dianggap tidak terlalu berbahaya (5)
  - Tidak ada kesadaran akan adanya suatu risiko dan tidak ada upaya untuk menghentikan (9)

Kriteria yang untuk *impact* adalah kriteria yang merupakan dampak yang ditimbulkan dari suatu risiko [9]. Antara lain:

- *Loss of Confidentiality*
  Dampak dari suatu risiko, yang seharusnya bersifat tertutup menjadi terbongkar atau diketahui publik [9].
  - Sebagian besar data terlindungi dan aman (1)
  - Sedikit data yang bisa terbongkar (3)
  - Banyak data yang bisa terbongkar (7)
  - Semua data bisa terbongkar (9)
- *Lost of integrity*
  Dampak dari suatu risiko seperti adanya data yang tidak konsisten. Data di tempat satu berbeda dengan data di tempat lain [9].
  - Hampir seluruh data yang ada sudah konsisten (1)
  - Ada beberapa data yang menjadi tidak konsisten (3)
  - Cukup banyak data yang tidak konsisten (5)
  - Banyak data yang tidak konsisten (9)
- *Loss of Availability*
  Dampak dari suatu risiko yang menyebabkan layanan tidak berfungsi dengan baik [9].
  - Sebagian besar layanan dan proses dapat berjalan dengan baik (1)
  - Ada beberapa layanan dan proses yang terhambat atau tidak bisa berjalan (4)
  - Banyak layanan dan proses yang tidak bisa berjalan dengan baik (6)
  - Semua layanan tidak bisa berjalan (9)
- *Loss of Accountability*
  Dampak dari suatu risiko seperti tidak adanya orang-orang yang dapat ditunjuk untuk bertanggung jawab mengatasi risiko [9].
  - Adanya cukup kejelasan pihak yang bertanggung jawab terhadap suatu risiko dan dapat mengatasi (1)
  - Adanya kejelasan pihak yang bertanggung jawab terhadap suatu risiko tetapi memerlukan bantuan orang lain untuk mengatasi (5)
  - Tidak adanya kejelasan pihak yang bertanggung jawab terhadap suatu risiko (9)
- *Financial Damage*
  Dampak dari suatu risiko seperti kerugian keuangan yang nantinya berdampak terhadap profit yang didapatkan perusahaan [9].
  - Kerugian tidak mencapai 3% dari total profit perusahaan (1)
  - Kerugian 5% dari total profit perusahaan (3)
  - Kerugian 10% dari total profit perusahaan (5)
  - Kerugian 20% dari total profit perusahaan (7)
  - Kerugian 40% dari total profit perusahaan (9)
- *Service*
  Dampak dari suatu risiko yang berpengaruh terhadap layanan yang diberikan terhadap pelanggan [9].
  - Hampir tidak ada layanan yang terganggu (1)
  - Ada sedikit layanan kecil yang tidak maksimal (3)
  - Banyak layanan kecil yang tidak bisa terpenuhi (6)
  - Layanan yang penting tidak bisa terpenuhi (9)
- *Privacy Violation*

Dampak dari suatu risiko seperti adanya data pribadi orang yang terbongkar atau hal-hal yang mengganggu kepentingan suatu individu [9].

- Hampir tidak ada gangguan terhadap kepentingan individu (1)
- Sedikit gangguan terhadap kepentingan individu (3)
- Cukup banyak gangguan terhadap kepentingan individu (5)
- Banyak gangguan terhadap kepentingan individu (9)

2.4 COBIT (*Control Objectives for Information and Related Technology*)

COBIT merupakan standar yang dikeluarkan oleh ITGI (*The IT Governance Institute*). COBIT adalah sebuah proses model yang dikembangkan untuk membantu perusahaan dalam pengelolaan sumber daya teknologi informasi. Proses model ini difokuskan pada pengendalian terhadap masing-masing dari 34 proses TI, meningkatkan tingkatan kemapanan proses dalam IT dan memenuhi ekspektasi bisnis dari TI. COBIT menciptakan sebuah jembatan antara manajemen TI dan para eksekutif bisnis. COBIT mampu menyediakan bahasa yang umum sehingga dapat dipahami oleh semua pihak. Penggunaan COBIT di seluruh dunia dapat dikaitkan dengan semakin besarnya perhatian yang diberikan terhadap *corporate governance* dan kebutuhan perusahaan agar mampu berbuat lebih dengan sumber daya yang sedikit meskipun ketika terjadi kondisi ekonomi yang sulit. Fokus utama dari COBIT ini adalah harapan bahwa melaui penggunaan COBIT ini, perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi risiko-risiko *inheren* yang teridentifikasi didalamnya. Risiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuannya [6].

Berikut penjelasan dari COBIT 4.1 DS 4 dan ME 1:

- DS 4 *Ensure Continuous Service*

Pemeliharaan dan pengujian TI secara kontinuitas, memanfaatkan *offsite backup storage*. Sebuah proses yang berfungsi untuk meminimalkan risiko-risiko dan dampak pada TI yang merupakan gangguan besar bagi perusahaan untuk menjalankan proses bisnisnya. Berikut penjelasan tiap poin dari DS 4 [6].

  - DS 4.1 *IT Continuity Framework*
  - DS 4.2 *IT Continuity Plans*
  - DS 4.3 *Critical IT Resources*
  - DS 4.4 *Maintenance of the IT Continuity Plan*
  - DS 4.5 *Testing of the IT Continuity Plan*
  - DS 4.6 *IT Continuity Plan Training*
  - DS 4.7 *Distribution of the IT Continuity Plan*
  - DS 4.8 *IT Services Recovery and Resumption*
  - DS 4.9 *Offsite Backup Storage*
  - DS 4.10 *Post-resumption Review*
- ME 1 *Monitor and Evaluate IT Performance*

Performance management TI yang efektif memerlukan proses pemantauan. Proses ini termasuk menentukan indikator yang bersangkutan dengan kinerja, pelaporan yang sistematis dan tepat waktu terhadap kinerja, dan cepat bertindak atas penyimpangan. Pemantauan diperlukan untuk memastikan bahwa hal yang benar dilakukan dan sejalan dengan arah dan kebijakan yang ditetapkan. Berikut penjelasan tiap poin dari ME 1 [6].

  - ME 1.1 *Monitoring Approach*
  - ME 1.2 *Definition and Collection of Monitoring Data*
  - ME 1.3 *Monitoring Method*
  - ME 1.4 *Performance Assessment*
  - ME 1.5 *Board and Executive Reporting*
  - ME 1.6 *Remedial Actions*

3. PENILAIAN RISIKO

3.1 Penentuan Kriteria Penilaian *Likelihood* dan *Impact*

penelitian penilaian likelihood dan impact yang digunakan dalam penelitian ini terdapat pada Tabel 1.

Tabel 1. Penentuan Kriteria Penilaian likelihood dan impact

Kriteria	Sumber	Keterangan
Skill Level	Pengembangan analisa berdasarkan Inge Chrisdiyanto, 2013	- *Staff* memiliki pengetahuan secara detail untuk melakukan tindakan pencegahan risiko (1) - *Staff* memiliki pengetahuan tetapi tidak memiliki kemampuan untuk melakukan (5) - *Staff* memiliki kemampuan tetapi tidak memiliki pengetahuan yang cukup (7) - *Staff* tidak memiliki pengetahuan dan kemampuan untuk mencegah terjadinya risiko (9)
Management and Stakeholder Support	Celia Wanarta, 2013	Sesuai dengan sumber
Awareness	Celia Wanarta, 2013	Sesuai dengan sumber
Teamwork	Inge Chrisdiyanto, 2013	Sesuai dengan sumber
Project Management	Pengembangan analisa berdasarkan Inge Chrisdiyanto, 2013	- Memiliki waktu, biaya, ruang lingkup, dan target yang jelas (1) - Memiliki waktu, ruang lingkup dan target yang jelas tetapi tidak memiliki biaya yang jelas (3) - Memiliki ruang lingkup dan target yang jelas tetapi tidak memiliki biaya dan waktu yang jelas (5) - Tidak memiliki waktu, biaya, ruang lingkup, dan target yang jelas untuk menangani risiko di perusahaan (9)
Loss of Confidentiality	Pengembangan analisa berdasarkan Celia Wanarta, 2013	- Sebagian besar data terlindungi dan aman (1) - Sedikit data yang bisa terbongkar atau rusak (3) - Banyak data yang bisa terbongkar atau rusak (7) - Semua data bisa terbongkar atau rusak (9)
Loss of Integrity	Celia Wanarta, 2013	Sesuai dengan sumber

Tabel 1. Penentuan Kriteria Penilaian likelihood dan impact (Sambungan)

Kriteria	Sumber	Keterangan
Loss of Availability	Inge Chrisdiyanto, 2013	Sesuai dengan sumber
Service	Pengembangan analisa berdasarkan Celia Wanarta, 2013	- Hampir tidak ada layanan yang terganggu (1) - Sebagian kecil layanan yang tidak maksimal (3) - Sebagian besar layanan yang tidak maksimal (7) - Layanan yang penting tidak bisa terpenuhi (9)
Loss of Accountability	*Celia Wanarta, 2013*	Sesuai dengan sumber
Financial Damage	Pengembangan analisa berdasarkan Celia Wanarta, 2013	- Hampir tidak ada dampak pada keuangan perusahaan (1) - Berdampak kecil pada keuangan perusahaan (5) - Berdampak besar pada keuangan perusahaan (9)

3.2 Penilaian *Risk Severity*

Dari hasil rata-rata yang didapat dari aspek *likelihood* dan aspek *impact*, maka akan didapat nilai *Risk Severity* dan level untuk *likelihood* dan *impact* untuk tiap risiko. Hasil *Risk Severity* dan *Level* dapat dilihat pada Tabel 2.

Tabel 2. Risk Severity

No.	Risiko	Likelihood	Impact	Risk Severity	Level
1	Tidak mempunyai *framework* untuk membuat *business continuity plan*	3,8	4,662	17,716	MM
2	Tidak mempunyai *business continuity plan* yang cocok	2,8	6,839	19,149	LH
3	Tidak mempunyai prioritas *plan*	4,8	2,606	12,509	ML
4	Tidak melakukan *update IT continuity*	3,2	0,648	2,074	ML
5	Tidak mempunyai *offsite backup*	3,8	3,507	13,327	MM

Tabel 2. Risk Severity (Sambungan)

No.	Risiko	Likelihood	Impact	Risk Severity	Level
6	Tidak mempunyai pihak yang bertanggung jawab terhadap penyimpangan	3,4	6,85	23,29	MH
7	Tidak ada pelatihan untuk memperdalam *skill* analisa data	2	3,631	7,262	LM

3.3 Risk Response

Setelah risiko tersebut diurutkan mulai dari tertinggi sampai terendah, maka selanjutnya adalah menentukan pemberian *response* terhadap setiap risiko berdasarkan urutan risiko yang paling tinggi. Prioritas pemberian *response* berdasarkan *Risk Severity* pada Tabel 2. Respon yang diberikan dapat berupa *assume*, *avoid*, *transfer*, dan *lessen*. Dari risiko tertinggi yang ada, maka dapat disimpulkan *risk response planning* yang disarankan adalah sebagai berikut:

1. Tidak mempunyai pihak yang bertanggung jawab terhadap penyimpangan
   Risk severity: *High*
   Risk Response: Lessen
   Perusahaan menganggap selama ini belum pernah ada penyimpangan yang terjadi di IT, sehingga pencalonan *staff* untuk menangani penyimpangan IT di perusahaan masih belum didefinisikan.
   Respon terhadap risiko ini adalah perusahaan harus mencalonkan karyawan yang bertanggung jawab untuk mengatasi penyimpangan di perusahaan. Sesuai dengan standar ISO 22313 (halaman 16 bagian 7.1.3).
   Organisasi harus mencalonkan personil untuk melakukan respon terhadap insiden dengan tanggung jawab yang diperlukan, kewenangan dan kompetensi untuk mengelola insiden [3]. Tim respon harus memiliki prosedur seperti:
   1. Deteksi insiden dan eskalasi
   2. Penilaian Insiden dan tingkat insiden
   3. Menganut dari respons yang tepat
   4. Aktivasi
   5. Evakuasi
   6. Pertolongan pertama

   Semua personil yang berada dalam kelompok ini harus jelas tanggung jawab dan wewenang yang berlaku sebelum, selama dan setelah kejadian.
2. Tidak mempunyai *business continuity plan* yang cocok
   Risk severity: Medium
   Risk response: Lessen
   Perusahaan membuat *business continuity plan* sendiri tanpa menggunakan standar yang cocok seperti COBIT 4.1 DS 4 dikarenakan kurangnya pengetahuan tentang standar *business continuity plan*.
   Respon terhadap risiko ini adalah dengan membuat business continuity plan yang sesuai dengan kebutuhan perusahaan dan

disesuaikan dengan standar *COBIT Control Practices 2nd Edition* (DS 4.2).

Mengembangkan *IT continuity plan* berdasarkan *framework* dan dirancang untuk mengurangi dampak dari gangguan besar pada fungsi bisnis utama. Rencana harus didasarkan pada pemahaman risiko dampak bisnis dan persyaratan ketahanan, pengolahan alternatif dan kemampuan pemulihan semua layanan IT kritis. Mereka juga harus mencakup pedoman penggunaan, peran dan tanggung jawab, prosedur, proses komunikasi, dan pengujian [5]. Buat rencana kesinambungan IT, termasuk:

- Kondisi dan tanggung jawab untuk mengaktifkan rencana
- Prioritaskan strategi pemulihan, termasuk urutan kegiatan jika diperlukan
- persyaratan pemulihan Minimum untuk mempertahankan operasi bisnis yang memadai dan tingkat layanan dengan sumber daya berkurang
- Prosedur darurat

3. Tidak mempunyai *framework* untuk membuat *business continuity plan*

   Risk Severity: Medium

   Risk Response: Lessen

   Dalam pembuatan *business continuity plan*, perusahaan tidak menggunakan *framework.*

   Respon terhadap risiko ini adalah membuat *business continuity plan* dengan menggunakan *framework* dari *Business Continuity Management Framework* 2014-18 *Queensland Government* (halaman 4).

   Menerapkan *framework business continuity plan* untuk membangun ketahanan tingkat tinggi di semua layanan departemen dan situs ketika menghadapi gangguan atau bencana [8].

   - Identifikasi risiko dan analisa dampak bisnis
   - Identifikasi respon
   - Mengembangkan business continuity plan
   - Training, Testing, and Maintenance

4. Tidak mempunyai *offsite backup*

   Risk Severity: Low

   Risk Response: Lessen

   Belum adanya kebijakan dari manajemen untuk melakukan *offsite backup*.

   Respon terhadap risiko ini adalah menyimpan media *backup* di lokasi yang berbeda dengan jarak yang cukup jauh untuk mencegah terjadinya kerusakan media *backup* ketika terjadi bencana di perusahaan [1]. Sesuai dengan standar ISO 27002 (Halaman 44 Bagian 10.5.1 Point D).

5. Tidak mempunyai prioritas *plan*

   Risk Severity: Low

   Risk Response: Lessen

   Belum adanya kebijakan dari manajemen untuk membuat rencana prioritas ketika terjadi bencana seperti kebakaran dan banjir yang terjadi bersamaan.

   Respon terhadap risiko ini adalah dengan membuat rencana prioritas untuk mengatasi kerancuan jika terjadi lebih dari satu bencana yang menimpa perusahaan. Sesuai dengan standar ISO 27001 (Halaman 4 Bagian 6.1.2 Point E). dan *Business Continuity Management Framework* 2014-18 (Halaman 4)[4].

6. Tidak ada pelatihan untuk memperdalam *skill* analisa data

   Risk Severity: Low

   Risk Response: Lessen

   Perusahaan melakukan tes terhadap karyawan baru dan menjelaskan apa saja yang harus dilakukan sehingga rencana untuk melakukan pelatihan tidak ada.

   Respon terhadap risiko ini adalah dengan melakukan pelatihan terhadap karyawan untuk memperdalam keterampilan dalam menganalisa data. Sesuai dengan standar ISO 22313 (Halaman 17 Bagian 7.2)

   Organisasi harus memiliki proses untuk mengidentifikasi dan memberikan persyaratan pelatihan kepada seluruh karyawan[3].

   Jenis pelatihan untuk peran tertentu adalah :

   1. Perencanaan dan pelaksanaan kontinuitas bisnis
      - Pengelolaan program kontinuitas bisnis
      - Melakukan analisis dampak bisnis
      - Mengembangkan dan menerapkan dokumentasi kelangsungan usaha
      - Menjalankan program latihan
      - *Risk assessment*
      - *Communications skills*
   2. Insiden respon dan pemulihan bisnis
      - Manajemen evakuasi
      - *Shelter-in-place*
      - *Check-in* proses untuk memperhitungkan karyawan
      - Pengaturan di tempat kerja alternatif
      - Penanganan pertanyaan media oleh perusahaan

   Keterampilan respon dan kompetensi seluruh organisasi harus dikembangkan dengan pelatihan praktis, termasuk partisipasi aktif dalam latihan.

7. Tidak melakukan *update IT continuity*

   Risk Severity: Low

   Risk Response: Lessen

   IT continuity di perusahaan dibuat tidak berdasarkan *standar* sehingga tidak terdapat pembaharuan oleh perusahaan.

   Respon terhadap risiko ini adalah perusahaan harus melakukan evaluasi terhadap *IT Continuity plan* dan memastikan rencana tersebut harus dalam keadaan up-to-date [3]. Sesuai dengan standar ISO 22313 (Halaman 51 Bagian 9.1.2).

4. KESIMPULAN

Dari analisa dan observasi yang dilakukan di PT ABC, dapat disimpulkan beberapa risiko dalam bidang IT di perusahaan yang mungkin terjadi selama berjalannya proses bisnis perusahaan, terdapat 7 risiko dengan 1 risiko memiliki *risk severity high*, 2 risiko memiliki *risk severity medium*, 4 risiko memiliki *risk severity low*. Berikut 7 risiko berdasarkan ranking tingkat *impact* yang mungkin terjadi beserta tindakan pencegehan atau penanganan risiko.

- Tidak mempunyai pihak yang bertanggung jawab terhadap penyimpangan.

  Response: Lessen dengan menggunakan standar ISO 22313. Organisasi harus mencalonkan personil untuk melakukan respon terhadap insiden dengan tanggung jawab yang diperlukan, kewenangan dan kompetensi untuk mengelola insiden [3].

- Tidak mempunyai *business continuity plan* yang cocok.

  Response: Lessen dengan menggunakan standar *COBIT Control Practices 2nd Edition DS 4.2.* Mengembangkan IT continuity plan berdasarkan framework dan dirancang untuk mengurangi dampak dari gangguan besar pada fungsi bisnis utama. Rencana harus didasarkan pada pemahaman risiko dampak bisnis dan persyaratan ketahanan, pengolahan alternatif dan kemampuan pemulihan semua layanan IT kritis [5].

- Tidak mempunyai *framework* untuk membuat *business continuity plan*

Response: Lessen menggunakan standar Business Continuity Management Framework 2014-18. Menerapkan framework business continuity plan untuk membangun ketahanan tingkat tinggi di semua layanan departemen dan situs ketika menghadapi gangguang atau bencana [8].

- Tidak mempunyai *offsite backup*
  Response: Lessen dengan menggunakan standar ISO 27002. Backup harus disimpan di lokasi terpisah, pada jarak yang cukup untuk mencegah terjadinya kerusakan akibat bencana di situs utama [1].
- Tidak mempunyai prioritas *plan*
  Response: Lessen dengan menggunakan standar ISO 27001. Prioritaskan risiko yang sudah dianalisa untuk pengolahan risiko [4].
- Tidak ada pelatihan untuk memperdalam *skill* analisa data
  Response: Lessen dengan menggunakan standar ISO 22313. Organisasi harus memiliki proses untuk mengidentifikasi dan memberikan persyaratan pelatihan kepada seluruh karyawan [3].
- Tidak melakukan *update IT continuity*
  Response: Lessen dengan menggunakan standar ISO 22313. Evaluasi program kelangsungan bisnis organisasi harus memastikan bahwa solusi kontinuitas bisnis organisasi yang efektif, up-to-date, cocok untuk tujuan, dan sesuai dengan tingkat risiko yang dihadapi oleh perusahaan [3].

5. DAFTAR PUSTAKA

[1] International Organizasion for Standarization. 2005. *Information technology – Security techniques – Code of practice for information security management.* USA: International Organizasion for Standarization

[2] International Organizasion for Standarization. 2008. *Risk management - Principles and guidelines on implementation.* Case Postale: International Organizasion for Standarization

[3] International Organizasion for Standarization. 2011. *Societal security - Business continuity management systems.* Case Postale: International Organizasion for Standarization

[4] International Organizasion for Standarization. 2013. *Information technology – Security techniques – Information security management systems - Requirements.* Case Postale: International Organizasion for Standarization

[5] IT Governance Institute. 2007. *CobiT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition.* Rolling Meadows: IT Governance Institute

[6] IT Governance Institute. 2007. *CobiT 4.1.* Rolling Meadows: IT Governance Institute

[7] The OWASP Risk Rating Methodology. Retrieved May 23, 2014, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[8] Queensland government. *Business Continuity Management Framework*. Queensland Government

[9] Wanarta, C. 2013. *IT Risk Assessment di PT X*. Surabaya: Universitas Kristen Petra.