IT RISK ASSESSMENT DI BIRO ADMINISTRASI KEMAHASISWAAN DAN ALUMNI (BAKA) UNIVERSITAS KRISTEN PETRA

Helen Puspa Ratna[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
E-mail:helen.puspa@yahoo.com[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK : Universitas Kristen Petra memiliki Biro Administrasi Kemahasiswaan dan Alumni (BAKA) yang membantu mahasiswa dalam bidang kesejahteraan mahasiswa dan pembinaan softksill mahasiswa, dan juga menjalin relasi dengan para alumni. Dalam menjalankan proses bisnisnya BAKA membutuhkan dukungan IT dan juga website yang berisi informasi. Fungsi BAKA cukup penting untuk Universitas Kristen Petra, tetapi selama berjalannya proses bisnis di BAKA tidak pernah dilakukan penilaian terhadap risiko yang mungkin saja terjadi.

Pada skripsi ini, dilakukan penilaian risiko terhadap BAKA menggunakan metode *GTAG*, *OWASP Testing Guide*, dan *A Guide to the Project Management of Body Knowledge 4th Edition*.

Berdasarkan analisis, metode ini membantu dalam penilaian risiko yang ada di BAKA dan bagaimana cara penanganan terhadap risiko yang ada.

Kata kunci : Penilaian Risiko, GTAG, OWASP

ABSTRACT *: Petra Christian University has a Bureau of Student and Alumni (BAKA) that assist students in the areas of student welfare and development softksill students, and also establish relationships with alumni. BAKA in running business processes require IT support and also a website that contains information. BAKA function is quite important for Petra Christian University, but during the course of business processes in BAKA never done an assessment of the risks that may occur.*

In this thesis, the risk assessment method GTAG BAKA, the OWASP Testing Guide, and A Guide to the Project Management Body of Knowledge 4th Edition.

Based on the analysis, this method helps in the assessment of the risks that exist in BAKA and how the handling of risk.

Keywords: Risk assessment, GTAG, OWASP

1. PENDAHULUAN

Biro Administrasi Kemahasiswaan dan Alumni (BAKA) adalah salah satu biro di Universitas Kristen Petra yang dibentuk sebagai bagian dari wakil rektor bidang kemahasiswaan yang menangani bidang kemahasiswaan dan alumni. Secara spesifik BAKA bergerak di bidang pembinaan-pengembangan mahasiswa, pelayanan kesejahteraan mahasiswa dan alumni. Proses bisnis yang ada di BAKA adalah proses administrasi realisasi kegiatan, proses realisasi anggaran kegiatan, satuan Kredit Kegiatan Kemahasiswaan (SKKK), administrasi kemahasiswaan, Pelatihan pendamping kemahasiwaan, beasiswa mahasiswa, angsuran / pinjaman mahasiswa, asuransi mahasiswa, santunan mahasiswa.

BAKA dalam menjalankan fungsi atau layanan di atas menggunakan *software* yang dibuat sendiri oleh *staff* BAKA berbasis Visual Basic dan SQL Server. *Software* tersebut sangat penting dalam proses operasi BAKA setiap hari, gangguan terhadap sistem ini dapat mengganggu layanan BAKA untuk bekerja secara maksimal. Fungsi BAKA bagi kemahasiswaan dan alumni sangatlah penting, oleh karena itu tidak diharapkan adanya gangguan terhadap kinerja di BAKA.

Selama ini belum pernah dilakukan *risk assessment* terhadap dukungan TI di BAKA, sedangkan *risk assessment* di BAKA sangatlah penting agar mengetahui apa saja risiko yang mungkin terjadi di BAKA. Oleh karena itu perlu dilakukan tindakan *risk assessment* terhadap layanan TI di BAKA Universitas Kristen Petra agar mengetahui apa saja risiko yang mungkin terjadi yang dapat menghalangi BAKA menjalankan fungsinya

2. DASAR TEORI

2.1 GTAG (Global Technology Audit Guide)

GTAG disusun oleh panduan yang disusun oleh beberapa peneliti dari IIA (Institute of Internal Auditors) dalam rangka merumuskan suatu tahapan perencanaan pengembangan audit terhadap suatu organisasi, dimana pada *risk assessment* merupakan satu bagian penting melakukan suatu proses audit. [1] ada 4 langkah dalam penggunaan GTAG :

a. Mengerti bisnis perusahaan
b. Menjabarkan *IT Audit Universe*
c. Melakukan *risk assessment*
d. Membuat perencanaan audit

2.2 COBIT 4.1

Control Objective for Information and related Technology (COBIT) adalah sekumpulan dokumentasi *best practices* untuk IT *Governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani jarak antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. [2] COBIT memiliki 4 cakupan domain, yaitu :

a. Perencanaan dan organisasi (*Plan and Organise*)
b. Pengadaan dan implementasi (*Acquire and Implement*)
c. Pengantaran dan dukungan (*Deliver and Support*)
d. Pengawasan dan evaluasi (*Monitor and Evaluate*)

2.3 Risk Assessment

Risk assessment merupakan suatu metodologi untuk menjabarkan kemungkinan terjadinya suatu event yang dapat menghalangi suatu organisasi dalam mencapai tujuan dari startegi bisnis, sehingga kemungkinan risiko dan dampaknya dapat diukur, dievaluasi dan diuji baik dari segi likelihood dan impact-nya (dampak).[1]

2.4 Risk Rating Methodology

Setiap risiko diukur dan dikelompokkan berdasarkan 2 kriteria yakni berdasarkan *likelihood* dan *impact*-nya. Berdasarkan *likelihood* risiko dapat dikelompokkan menjadi beberapa kategori seperti "*High*", "*medium*", "*Low*". *High* menunjukkan bahwa suatu risiko memiliki kemungkinan yang tinggi untuk terjadi, dan semakin mengarah ke *low* maka kemungkinan terjadi risiko sangat kecil yang juga berarti hampir mustahil terjadi. [3]

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

Gambar 1. Level Likelihood dan Impact

Dalam melakukan penilaian likelihood dan impact setiap risiko dibutuhkan beberapa kriteria yang dapat membantu. Setiap kriteria yang ada pun memiliki beberapa pilihan yang membantu mengidentifikasi nilai dari setiap risiko, setiap pilihan memiliki nilai antara 0 sampai dengan 9. Angka – angka ini yang nantinya akan digunakan untuk menghitung likelihood dan impact dari setiap risiko. Kriteria yang digunakan untuk menilai *likelihood* adalah kriteria yang merupakan kemungkinan penyebab munculnya risiko tersebut. Setelah dilakukan penghitungan nilai likelihood dan impact dari setiap risiko maka akan didapatkan nilai dari setiap risiko, dari nilai yang didapat maka akan bisa diketahui level dari likelihood. Gambar 2 dibawah ini memberikan contoh penilaian likelihood.

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 2. Penilaian Likelihood

Gambar 3 dibawah ini memberikan contoh tentang penilaian impact.

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	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Gambar 3. Penilaian Impact

Setelah mengetahui level dari likelihood maupun impact maka langkah selanjutnya yang dilakukan adalah menggabungkan likelihood dan impact agar menghasilkan urutan bahaya setiap risiko. Gambar 4 menjelaskan bagaimana menggabungkan likelihood dan impact dari setiap risiko yang ada.

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

2.5 Penilaian aspek impact berdasarkan prioritas

Penilaian aspek *impact* didasari oleh prioritas *impact* yang menurut perusahaan paling berbahaya. Menurut hasil kuesioner oleh beberapa narasumber di perusahaan.

3. KRITERIA PENILAIAN LIKELIHOOD DAN IMPACT

3.1 Likelihood

1. Skill Level

Bagaimana keahlian dari kelompok pengguna.
(9) *Staff* atau manajemen tidak memiliki pemahaman dan tidak memiliki kemampuan untuk melakukan
(7) *Staff* atau manajemen seharusnya memiliki kemampuan yang cukup tetapi tidak ada pemahaman
(5) *Staff* atau manajemen memiliki pemahaman tetapi tidak memiliki kemampuan untuk melakukan
(1) *Staff* atau manajemen memiliki pemahaman dan memiliki kemampuan untuk melakukan

1. Management and Stakeholder Support

Seberapa mudah hal tersebut dilakukan dan seberapa besar dukungan dari management maupun stakeholder

(9) Tidak ada dukungan dari manajemen maupun *stakeholder*

(6) Tidak ada kebijakan yang mengatur tetapi seharusnya jumlah *staff* dan biaya mencukupi

(4) Ada kebijakan yang mengatur tetapi jumlah *staff* tidak memadai dan tidak ada biaya yang disediakan

(1) Adanya dukungan penuh dari sebagian besar manajemen dan *stakeholder*

2. Awareness

Seberapa besar tingkat kesadaran yang dimiliki dari risiko yang terjadi
(9) Tidak ada kesadaran sama sekali terhadap risiko
(7) Sadar akan risiko tetapi diabaikan
(5) Sadar akan risiko yang ada dan dilakukan penanganan secara sederhana
(3) Sadar akan risiko yang ada dan dilakukan penanganan secara rinci

(1) Sadar akan risiko yang ada dan dilakukan penanganan secara rinci , konseptual dan berkala

3.2 Impact

Setelah selesai dengan penghitungan Likelihood maka langkah yang dilakukan selanjutnya adalah melakukan penghitungan impact. Sama seperti perhitungan likelihood, dalam perhitungan impact juga menggunakan beberapa kriteria dengan pilihan dan nilai di dalamnya.

1. Loss of Confidentialy

Seberapa banyak hal pribadi perusahaan jatuh ke tangan umum, dan seberapa sensitive hal tersebut.

(9) Semua hal jelek bisa dibocorkan

(7) Data tambahan yang sensitif dapat bocor

(5) Hal – hal yang penting tidak ada yang bocor

(1) Tidak ada hal sensitif yang bocor

2. Loss of Integrity

Seberapa banyak hal yang tidak sesuai dengan kenyataan, seberapa parah rusaknya

(9) Semua layanan IT tidak bisa diandalkan dan tidak sesuai dengan harapan

(6) Sebagian besar layanan IT tidak memenuhi harapan

(4) Sebagian kecil layanan IT tidak sesuai

(1) Hanya hal – hal tertentu saja yang tidak sesuai atau rusak

3. Loss of Availability

Seberapa banyak layanan IT yang hilang dan seberapa vital kah hal tersebut.

(9) Semua layanan hilang

(6) Sebagian besar layanan IT yang penting tidak berfungsi

(4) Hanya sebagian layanan kecil saja yang terganggu

(1) Hal – hal yang tidak penting saja yang mengganggu

4. Loss of Accountability

(9) Tidak ditemukan orang yang bertanggung jawab

(6) Ada kelompok yang ditunjuk untuk bertanggung jawab tetapi tidak ad individu yang bertanggung jawab

(4) Ada kelompok yang ditunjuk, ada individu yang bertanggung jawab tetapi tidak ada tanggung jawab yang jelas

(1) Jelas siapa yang bertanggung jawab dan tanggung jawab apa yang dilakukan

5. Service

Seberapa besar pengaruh risiko terhadap layanan di perusahaan

(9) Semua layanan tidak berfungsi

(6) Layanan yang vital yang terganggu

(4) Layanan yang tidak terlalu vital yang terganggu

(1) Hanya sedikit layanan yang terganggu

6. Privacy Violation

Seberapa banyak informasi pribadi dapat tersebar

(9) Hampir semua orang

(7) Ratusan sampai dengan ribuan

(5) Puluhan sampai dengan ratusan

(3) Hanya individu tertentu

4. MODEL DAN STRATEGI BISNIS PERUSAHAAN

4.1 Model Bisnis dan Tujuan Bisnis Perusahaan

Model bisnis perusahaan dapat dideskripsikan melalui sembilan pilar utama atau yang biasa disebut *Nine Building Block.* [4]

1. *Value Proposition*
2. *Target Customer*
3. *Distribution Channel*
4. *Relationship*
5. *Value Configuration*
6. *Core Competency*
7. *Partner Network*
8. *Cost Structure*
9. *Revenue Model*

4.2 Strategi Bisnis Perusahaan

4.2.1 Proses Bisnis

Proses bisnis yang terdapat di BAKA adalah proses administrasi realisasi kegiatan, proses realisasi anggaran kegiatan, satuan Kredit Kegiatan Kemahasiswaan (SKKK), administrasi kemahasiswaan, Pelatihan pendamping kemahasiwaan, beasiswa mahasiswa, angsuran / pinjaman mahasiswa, asuransi mahasiswa, santunan mahasiswa. BAKA merupakan salah satu biro pendukung di Universitas Kristen Petra yang dibentuk sebagai bagian dari wakil rektor bidang kemahasiswaan yang menangani bidang kemahasiswaan dan alumni. *Goal* yang ingin dicapai BAKA adalah menjadi suatu Biro Administrasi Kemahasiswaan dan Alumni dari kampus Kristen kelas dunia pada tahun 2017.

4.3 Kondisi *Information Technology* di BAKA

4.3.1 Teknologi

Teknologi yang digunakan BAKA saat ini ialah :
- Windows Server 2003
- SQL Server 2005
- PHP for Windows
- Visual Studio 6
- Crystal Report 8.5
- Microsoft Office 2003

4.3.2 Data

BAKA memiliki satu *database Server* dan satu *Web Server*. *Web Server* digunakan untuk menyimpan semua aplikasi yang digunakan BAKA, sedangkan *Database Server* digunakan untuk menyimpan data yang digunakan untuk di BAKA.

4.3.3 Software

Aplikasi yang digunakan di BAKA adalah sebuah aplikasi yang dibuat oleh *staff IT* yang diletakkan di BAKA yang berjumlah satu orang, aplikasi ini berbasis Visual Basic dan menggunakan *database* SQL Server 2005. Semua data di BAKA dari setiap bagian dicatat melalui aplikasi ini, sehingga lebih mempermudah dalam proses pencatatan, penyimpanan dan pengumpulan data.

BAKA juga memiliki sebuah *website* yang berfungsi sebagai media informasi untuk seluruh civitas akademika Universitas Kristen Petra dan alumni. *website* BAKA hanya mengunakan

PHP biasa, dan *website* BAKA terhubung di 1 server yang sama di BAKA.

Untuk proses *backup* data, BAKA setiap hari melakukan *backup* rutin ke server. BAKA memiliki 2 Server, yaitu *database Server* dan *web Server*. Untuk *backup* local ke *database Server* dilakukan jam 16.30 setiap harinya. Sedangkan untuk *backup* ke puskom dilakukan setiap jam 23.00 untuk *database Server* dan jam 4.30 untuk *Web Server*. Proses *backup* dilakukan secara otomatis

dengan menggunakan aplikasi *Test Schedule* yang terdapat di *Windows*.

4.3.4 Proses Permintaan Data

Beberapa permintaan data masih dilakukan secara manual, tetapi ada beberapa biro yang biasanya memberikan *login user* untuk mengambil data langsung dari SQL Server, biasanya beberapa biro sudah menyediakan *field* untuk *view*. BAKA sendiri sudah menyediakan proses permintaan data dari BAKA untuk jurusan – jurusan yang membutuhkan data, tetapi untuk saat ini hanya data – data yang sering diminta saja yang dibuat dalam bentuk *software*, seperti permintaan data beasiswa, kegiatan Lembaga Kemahasiswaan, prestasi ekstrakurikuler. Selebihnya permintaan data dilakukan secara pribadi melalui *email* dan *programmer* harus melakukan *query* satu persatu di SQL Server.

4.3.4 Permasalahan dan Kebutuhan *Information Technology* di BAKA

Server BAKA pernah mengalami virus yang berasal dari jaringan internet, penyebab Server terkena virus ialah karena pada saat itu *firewall* dimatikan, sedangkan *Windows* sendiri masih memiliki banyak *bug*, sehingga saat *firewall* dimatikan sistem langsung terkena virus dan efek yang diakibatkan dari virus tersebut adalah virus tersebut menanam sebuah *software* di dalam server yang menyebabkan server terus mengirim *email* ke server pusat di Jerman.

Dari segi Hardware : beberapa hardware di BAKA perlu dilakukan *upgrade*, karena aplikasi yang digunakan BAKA sekarang masih berbasis Visual basic, sedangkan BAKA ingin mengubah aplikasinya dengan berbasis .Net, tetapi dengan kondisi hardware saat ini yang masih menggunakan pentium 4 agak susah untuk merealisasikan hal tersebut.

Dari segi Software : masalah yang terjadi di *software* adalah masalah kompatibilitas, contohnya seperti, jika diluaran sudah menggunakan Microsoft office 2007 dan di BAKA sendiri masih menggunakan Microsoft office 2003 terkadang data jadi tidak bisa terbuka, tetapi hal tersebut hanya terjadi sekali saja setelah itu akan dilakukan update. Terkadang antivirus yang dimiliki juga telat di-*update.*Untuk masalah yang terjadi pada aplikasi internal BAKA adalah, aplikasi yang digunakan beberapa kali sering terjadi *error* seperti *'run time error',* biasanya setelah muncul tulisan seperti itu maka aplikasi akan menutup secara otomatis dan mengakibatkan pekerjaan harus diulang dari awal kembali.

5. PENENTUAN IT AUDIT DOMAIN DAN IT AUDIT UNIVERSE

5.1 IT Audit Universe

IT Audit Universe di BAKA meliputi semua sistem *IT* yang terdapat di BAKA. Dalam melakukan proses bisnisnya BAKA menggunakan aplikasi internal dan *website*, selain itu juga dalam sistem IT BAKA memiliki dua macam database yaitu *web server* dan *database server*. [5]

5.2 IT Audit Domain

Faktor *risk domain* didapat dari hasil wawancara dan observasi kepada pihak BAKA, sehingga menghasilkan *mapping* dari Cobit ke *IT Audit Domain.*

6. PENANGANAN RISIKO

6.1 Risiko Tertinggi

Dari hasil wawancara dan observasi maka ditemukan risiko tertinggi seperti yang terdapat pada tabel 1.

Tabel 1 : Risiko Tertinggi

No.	Faktor Risiko	Risk Severity	Level	Overall Level
14	Perusahaan tidak pernah memikirkan apa yang harus dilakukan jika suatu saat terjadi bencana dan bagaimana mengamankan security technologynya dari gangguan, tidak ada Disaster recovery plan dan juga tidak ada tindakan preventif untuk sesuatu yang berpotensial jadi masalah	49,27	HH	Critical
15	Keamanan belum dijadikan prioritas tertinggi perusahaan, sehingga perusahaan tidak tahu sistem mana saja yang belum memenuhi standar keamanan, oleh karena itu perusahaan juga tidak memiliki rencana perlindungan terhadap infrastruktur IT yang sensitif	32,11	HH	CRITICAL
4	Tidak pernah dilakukan proses audit maupun penilaian risiko dalam perusahaan secara umum dalam mekanisme kerja maupun dalam bidang IT	26,19	HM	HIGH
16	Ruang server yang dimiliki belum memenuhi standar,	24,99	MH	HIGH

	semua orang diperbolehkan untuk masuk ruang server, bahkan ruang server tergabung dengan gudang dan tempat meletakkan tas untuk para MPW			
7	Proses backup yang dilakukan perusahaan bersifat fisik dan *onsite*, karena perusahaan hanya melakukan backup dalam server dan tidak dibawa ke luar (*offsite*).	19,96	MM	MEDIUM
13	Tidak pernah dilakukan pengujian ataupun verifikasi terkait jalannya suatu sistem, langsung diimplementasikan ke pengguna, jika ada complain baru diperbaiki	16,04	HM	HIGH
10	Perusahaan sangat bergantung pada staff IT yang hanya berjumlah satu orang. Karena tidak ada standar tertentu yang digunakan dalam pembuatan program maka akan sulit bila terjadi pergantian staff IT, karena harus mempelajari lagi program yang telah ada.	15,8	HM	HIGH

6.2 Risk Response Planning

Risk Response Planning merupakan bagaimana perusahaan harus menangani risiko tersebut. Dari risiko tertinggi yang ada, maka [5]

1. Perusahaan tidak pernah memikirkan apa yang harus dilakukan jika suatu saat terjadi bencana dan bagaimana mengamankan security technologynya dari gangguan, tidak ada Disaster recovery plan dan juga tidak ada tindakan preventif untuk sesuatu yang berpotensial jadi masalah

Response: *Reduce* atau *Transfer*

Dampak dari risiko tidak adanya *disaster recovery plan* dan IT *security plan* dapat diperkecil dengan membuat *disaster recovery plan* dan IT *security plan*. Jika tidak memungkinkan disarankan untuk melakukan audit terhadap perusahaan oleh pihak di luar perusahaan. Dengan begitu hasil dari audit adalah auditor membuatkan *disaster recovery plan* dan IT *security plan.* Dampak dari tidak adanya *disaster recovery plan* juga dapat dialihkan dengan mengasuransikan perusahaan sehingga kerugian yang dialami akibat bencana akan ditanggung oleh pihak asuransi. *Disaster recovery plan* adalah sebuah perencanaan sistem informasi yang dirancang untuk mengembalikan operasional, aplikasi, dan infrastruktur setelah terjadinya keadaan darurat yang dampaknya berkepanjangan seperti yang tertulis dalam NIST SP 800-34 dan mengacu pada COBIT 4.1 *Control Objective Delivery and Support* 4. Perusahaan harus terlebih dahulu menentukan insiden-insiden apa yang tergolong ke dalam bencana. *Disaster recovery plan* dan IT *security plan* dapat dibuat berdasarkan standar keamanan ISO 27002:2005 seperti membuat *non-disclosure agreement* dengan pihak eksternal maupun internal perusahaan, kontrol untuk perlindungan dari *software* yang tidak terjamin otoritasnya, *backup* secara *off site* yaitu membuat media *backup* data di luar jangkauan perusahaan, perlindungan data *backup* dengan adanya enkripsi, pengecekan data *backup* secara berkala untuk menjamin konsistensi data, dan penghapusan data penting pada media yang sudah tidak terpakai.

2. Keamanan belum dijadikan prioritas tertinggi perusahaan, sehingga perusahaan tidak tahu sistem mana saja yang belum memenuhi standar keamanan, oleh karena itu perusahaan juga tidak memiliki rencana perlindungan terhadap infrastruktur IT yang sensitive

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

Reduce untuk masalah tidak adanya training terkait keamanan dan insiden dalam perusahaan.

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.

3. Tidak pernah dilakukan proses audit maupun penilaian risiko dalam perusahaan secara umum dalam mekanisme kerja maupun dalam bidang IT

Response: *Reduce*

Dampak dari tidak adanya *risk assessment* dalam bidang IT dapat diperkecil dengan melakukan *risk assessment* di perusahaan oleh pihak di luar perusahaan yang sudah berpengalaman dan dapat menggunakan metode-metode atau panduan seperti *Global Technology Audit Guidelines* atau ISO/IEC 31010:2009 dengan IT *Audit Domain* yang dapat ditentukan dengan panduan COBIT 4.1. *Global Technology Audit Guidelines* berisi tahap melakukan *risk assessment* mulai dari pemahaman bisnis, penentuan area-area IT yang akan diaudit, penentuan faktor-faktor risiko, dan penilaian risiko. ISO/IEC 31010:2009 berisi tentang konsep, proses, dan pemilihan teknik *Risk assessment* yang dapat digunakan di perusahaan.

4. Ruang *server* yang dimiliki belum memenuhi standar, semua orang diperbolehkan untuk masuk ruang server, bahkan ruang server tergabung dengan gudang dan tempat meletakkan tas untuk para MPW

5. Proses backup yang dilakukan perusahaan bersifat fisik dan *onsite*, karena perusahaan hanya melakukan backup dalam server dan tidak dibawa ke luar (*offsite*).

Response: *Reduce*

Dampak dari risiko ini dapat diperkecil dengan melakukan *backup* sesuai dengan standar NIST 800-34. *Backup* dapat dilakukan secara *off site*. Backup dilakukan dengan menyimpan data pada *hard disk* atau dapat juga secara *cloud backup* sehingga data disimpan mengunakan internet. Perusahaan bisa mengakses data backup kapan saja dan dimana saja apabila menggunakan *cloud backup.* Hasil dari *backup* juga sebaiknya di-*restore* secara berkala untuk mengecek apakah data *backup* sesuai dengan data yang ada dan proses *restore* sudah berjalan dengan baik.

6. Tidak pernah dilakukan pengujian ataupun verifikasi terkait jalannya suatu sistem, langsung diimplementasikan ke pengguna, jika ada komplain baru diperbaiki. Response: seharusnya sebuah layanan IT harus diuji terlebih dahulu sebelum digunakan, agar dapat bekerja secara efisien dan efektif serta menjamin tingkat kinerja dari IT tersebut.

7. Perusahaan sangat bergantung pada staff IT yang hanya berjumlah satu orang. Karena tidak ada standar tertentu yang digunakan dalam pembuatan program maka akan sulit bila terjadi pergantian staff IT, karena harus mempelajari lagi program yang telah ada.

Response: *Reduce*

Dampak ketergantungan terhadap *staff* IT dapat dikurangi dengan menambah *staff* IT untuk mengelola dan melakukan pengawasan secara berkala terhadap sistem IT di perusahaan. Hal tersebut dilakukan agar satu orang *staff* tidak memegang kunci penting terlalu banyak dan mengantisipasi apabila suatu saat *staff* IT tidak ada pada keadaan darurat.

8. Perusahaan tidak pernah ada prosedur tertentu dan pendokumentasian untuk setiap pengembangan dan perubahan software, hardware maupun jaringan di perusahaan ataupun masalah yang pernah terjadi di perusahaan khusunya di bidang IT.

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

Reduce untuk masalah tidak adanya training terkait keamanan dan insiden dalam perusahaan.

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.

7. DAFTAR PUSTAKA

[1] Reharge, Kirk.,Steve Hunt dan Fernando D.Nikitin. 2008. *Global Technology Audit Guide : Developing the Audit Plan*. USA : The Institute of Internal Auditors

[2] Gondodiyoto, Sanyoto. 2007. *Audit sistem informasi + pendekatan CobIT*. Jakarta : Mitra Wacana Media.

[3] OWASP Foundation (2008). *OWASP Testing Guide*.

[4] Osterwalder, Alexander. (2010). *Business Model Generation*. United States of America: John Willey and Sons, Inc.

[5] Project Management Institute. (2008). *A Guide to the Project Management of Body Knowledge 4th Edition.*