IT *RISK ASSESSMENT* DI PERPUSTAKAAN UNIVERSITAS KRISTEN PETRA

Inge Chrisdiyanto[1], Adi Wibowo[2], Ibnu Gunawan[3]
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jalan Siwalankerto 121-131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
Email: inge_rocketmail@yahoo.co.uk[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK: Universitas Kristen Petra memiliki unit organisasi yakni Perpustakaan yang menyediakan layanan koleksi. Sistem di Perpustakaan dikerjakan dengan memanfaatkan layanan IT (otomasi), dengan tujuan mempermudah proses pemberian layanan informasi pencarian koleksi dan peminjaman. Permasalahan yang terjadi pada layanan IT yang pernah dihadapi adalah seperti *downserver*, *Unit Power Supply* yang rusak dan terjadinya inkonsistensi data. Hal ini dapat menghambat kinerja layanan Perpustakaan seperti peminjaman dan pengembalian koleksi, pencarian koleksi di *website*, juga layanan pencarian informasi seperti referensi. Untuk itu dibutuhkan suatu analisa risiko, yang bertujuan menganalisa faktor-faktor risiko apa saja yang mengganggu proses bisnis perusahaan dan meberikan respon terhadap risiko yang paling kritikal.

Pada penelitian ini, dilakukan proses *risk assessment* terhadap layanan IT yang dimanfaatkan dalam layanan bisnis Perpustakaan dan dibuatlah analisa berdasarkan pemahaman terhadap model dan strategi bisnis, penjabaran IT Audit *Universe* dan IT *Domain, Contro Objectivel*, serta penilaian terhadap faktor-faktor risiko IT yang ditemukan. Proses analisa risiko dilakukan dengan memanfaatkan metode berdasarkan *Global Technology Audit Guidelines* (GTAG) *: Developing IT*, COBIT 4.1, *OWASP Risk Rating Methodology*.

Berdasarkan pengujian, ditemukan faktor-faktor risiko IT yang ada di Perpustakaan. Beberapa faktor-faktor risiko tersebut antara lain belum ada strategi dan perencanaan IT yang jelas untuk masa mendatang, media *backup* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *backup* secara khusus.

Kata Kunci: Analisa risiko IT, *IT Audit Universe*, GTAG, COBIT, Metode Kualitatif

ABSTRACT: *Library of Petra Christian University has the organizational unit that provides collection services. Library system is processed by utilizing IT services (automation), with the aim of facilitating the process of providing information services and search collections of borrowing. The problems that occur in IT services have ever experienced such as down server, faulty Power Supply Unit and inconsistencies in data. All of these problems can hinder the performance of library services such as circulation, acquisition, cataloging and receiving collection, searching collections by using the web-based media, as well as reference information services. Those requires a risk analysis, which in order to analyze the risk factors that disrupt any business process and give the company's response to the most critical risks.*

In this thesis, risk assessment is purposed to analyze the IT services that support Library services. This analysis is executed based on an understanding of the business models and strategies, the translation of IT Audit Universe and IT Domains, Control Objectives, so as the assessment of IT risk factors that are exposed. The process of risk analysis is done by using the method based Global Technology Audit Guidelines (GTAG): Developing IT, COBIT 4.1, OWASP Risk Rating Methodology.

Based on testing, IT risk factors that exist in the library services are found. Some of these risk factors included, no IT strategy and a clear plan for the future, media backups have never been tested, evaluated or refreshed, and also no backup procedures in particular.

Keywords: *IT risk analysis, IT Audit Universe, GTAG, COBIT, Qualitative Methods*

1. PENDAHULUAN

Perpustakaan UK Petra juga menjadi organisasi yang bergerak di bidang penyedia layanan (jasa). Dalam rangka mewujudkan visi dan misi tersebut, layanan-layanan yang disediakan Perpustakaan meliputi pengadaan, pegolahan, sirkulasi, online katalog dengan reverensi, koleksi digital, dan layanan koleksi serial majalah dan jurnal. Sebagian besar layanan yang diberikan perpustakaan, telah mengalami proses otomasi, kecuali untuk proses layanan koleksi majalah dan jurnal.

Adanya proses otomasi yang telah diterapkan di Perpustakaan hingga saat ini membuat kebergantungan Perpustakaan terhadap Teknologi Informasi (TI) sangat tinggi. Tidak menutup kemungkinan bahwa permasalahan seperti mati lampu, *server down*, atau sistem keamanan komputer yang dapat diretas, perangkat keras yang rusak, oleh pihak luar dan permasalahan lainnya dapat terjadi di Perpustakaan. Contoh-contoh tersebut merupakan bentuk-bentuk risiko yang bila terjadi dapat menyebabkan kurang maksimalnya kinerja Perpustakaan

Mengingat pentingnya peranan TI dalam mendukung proses bisnis perpustakaan, maka perlu dilakukan suatu *risk assessment* terhadap risiko TI yang dapat berdampak terhadap proses bisnis perpustakaan. Melalui *risk assessment* pihak perpustakaan dapat terbantu dalam mengetahui risiko-risiko apa saja yang dapat terjadi, mengukur seberapa mungkin risiko tersebut terjadi dan apa dampaknya, kemudian ditunjukkan hasil perhitungan risiko manakah yang menjadi prioritas yang dalam hal ini butuh penangan segera dan manakah risiko yang dapat menemukan penangan berikutnya.

Namun sejauh implementasi TI tersebut dijalankan, belum pernah dilakukan suatu bentuk *risk assessment*, maupun penelitian lain

terkait penanganan risiko di Perpustakaan Universitas Kristen Petra khususnya yang terkait dengan peranan TI dalam menunjang proses bisnisnya.

Tujuan dari penelitian ini adalah untuk melakukan analisis dan mengetahui faktor-faktor risiko yang paling berpengaruh dalam penggunaan teknologi informasi terhadap pencapaian tujuan dan strategi bisnis dari Perpustakaan Universitas Kristen Petra dan memberikan usulan mitigasi risiko yang diperlukan.

2. DASAR TEORI

2.1. Global Technology Audit Guideline

Langkah-langkah yang dibutuhkan untuk melakukan proses audit Menurut GTAG (2008) [1] adalah sebagai berikut:

a. Mengerti bisnis perusahaan (*Understanding the Business)* Proses ini dapat dilakukan dengan menjabarkan apakah tujuan bisnis yang ingin dicapai Perusahaan, dan memetakannya ke dalam suatu model dan strategi bisnis.
b. Menjabarkan *IT Universe (Define IT Universe)* Mengelompokkan tiap-tiap area bisnis, mengidentifikasi aplikasi apa saja yang mendukung tiap-tiap kegiatan bisnis tersebut, infrasrtuktur apa saja yang penting untuk mendukung aplikasi tersebut, dan memahami peran-peran dari teknologi informasi pendukung tersebut.
c. Melakukan *risk assessment (Perform Risk Assessment)* Menjabarkan faktor-faktor risiko apa yang mungkin terjadi, menilai faktor-faktor risiko berdasarkan faktor risiko IT dan faktor risiko bisnis.
d. Membuat perencanaan audit *(Formalize Audit Plan)*

2.2. COBIT 4.1.

Control Objectives for Information and related Technology [2] atau yang biasa disingkat dengan COBIT merupakan suatu bentuk kerangka kerja yang diciptakan oleh suatu lembaga para Auditor yakni Information System Audit and Control Association (ISACA) yang bertujuan untuk mengaudit sudah seberapa baik Teknologi Informasi (TI/IT) berperan dalam suatu organisasi sebagai pendukung proses bisnis organisasi tersebut. COBIT dimunculkan mengingat pesatnya perkembangan peranan IT di dalam suatu organisasi. Hal ini memunculkan adanya suatu tata laksana IT atau yang dikenal dengan istilah IT Governance, yakni tanggung jawab dari para eksekutif dan direksi, yang terdiri dari aspek kepemimpinan, struktur organisasi, dan proses yang memastikan bahwa enterprise IT tetap menjaga dan mengembangkan strategi dan tujuan organisasi.

ISACA (2005) mengembangkan COBIT versi 4.1. Dalam penelitian ini COBIT yang dipakai adalah COBIT versi 4.1. Ada 4 domain proses yang diukur dalam COBIT 4.1. Keempat domain tersebut meliputi:

- *Plan and Organise*
- *Acquire and Implementation*
- *Delivery and Support*
- *Monitor and Evaluate*

2.3. *Risk Rating Methodology*

Risk Rating Methodology apabila diterjemahkan berarti metode pembobotan (pemberian nilai) [3] risiko. Ada berbagai cara yang dilakukan dalam mengukur aspek *likelihood* dan *impact* dari suatu risiko. OWASP adalah singkatan dari *Open Web Application Security Project* merupakan suatu organisasi nirlaba yang memiliki misi yaitu meningkatan keamanan dari suatu software. Dalam OWASP Testing Guide versi 3.0 (2008), OWASP merumuskan suatu metode penilaian risiko dalam hal pembobotan terhadap aspek *likelihood* dan *impact*.

OWASP (2008) mengemukakan bahwa "menemukan risiko-risiko itu memang penting, sama pentingnya dengan kemampuan untuk dapat menghitung estimasi risiko yang terkait dalam bisnis". Ada banyak pendekatan untuk melakukan penilaian risiko, yang umum diketahui adalah *Likelihood * Impact* untuk dapat menemukan *Risk Severity* seperti yang dikemukan oleh Rehage et al. (2008). Agar dapat memberikan nilai yang dapat mewakili kondisi sesungguhnya dalam aspek *likelihood* dan *impact*, maka baik dari segi *likelihood* maupun *impact* harus ditentukan dulu faktor-faktor yang berpengaruh terhadap 2 aspek tersebut. Berikut adalah metode penilaian risiko yang dibuat OWASP (2008) :

- Mengidentifikasi risiko,
- Menentukan faktor-faktor yang berpengaruh terhadap *likelihood*,
- Menentukan faktor-faktor yang berpengaruh terhadap *impact*,
- Menghitung *risk severity*,
- Memutuskan risiko mana saja yang harus diprioritaskan berdasarkan *Risk Severity* nya.

Tabel 1 menggambarkan probabilitas tabel nilai yang ada dari hasil perkalian antara *likelihood* dengan *impact*. Sedangkan tabel 2 mencerminkan kategori *risk severity* berdasarkan perhitungan tersebut.

Tabel 1. Probabilitas hasil *likelihood*impact*

I\L	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	21	24	27
4	4	8	12	16	20	24	28	32	36
5	5	10	15	20	25	30	35	40	45
6	6	12	18	24	30	36	42	48	54
7	7	14	21	28	35	42	49	56	63
8	8	16	24	32	40	48	56	64	72
9	9	18	27	36	45	54	63	72	81

Tabel 2. Kategori *Risk Severity*

		Likelihood								
		1	2	3	4	5	6	7	8	9
Impact	1	Note			Low			Medium		
	2									
	3									
	4	Low			Medium			High		
	5									
	6									
	7	Medium			High			Critical		
	8									
	9									

3. MODEL DAN STRATEGI BISNIS

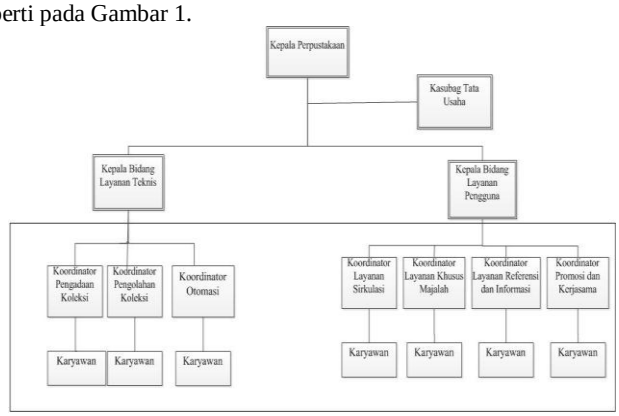
3.1 Model Bisnis

Dalam rangka mencapai tujuan bisnis tersebut, berikut diuraikan model bisnis Perpustakaan dalam 9 pilar model bisnis berdasarkan hasil wawancara (Osterwalder, 2010) [4]. Berikut dijabarkan secara singkat beberapa pilar model bisnis Perpustakaan.

Value Propositions berupa layanan utama yang diberikan oleh Perpustakaan Universitas Kristen Petra kepada pelanggan (pemustaka) adalah berupa jasa peminjaman koleksinya. *Target Customer* yang menjadi tujuan pemberian layanan merupakan pemustaka. Pemustaka Perpustakaan dapat merupakan mahasiswa Universitas, karyawan dan dosen tetap Universitas, serta mitra pustaka. *Value Configuration* merupakan proses yang dijalankan dijalankan oleh Perpustakaan untuk dapat memberikan value bagi pemustakan. Proses-proses tersebut meliputi pengajuan usulan, pembelian koleksi, pengadaan, pengolahan dan sirkulasi.

3.2 Strategi Bisnis

Strategis Bisnis dijabarkan dengan 2 cara yaitu menggambarkan struktur organisasi beserta deskripsi tugas yang harus dilakukan dan proses bisnis yang terjadi. Struktur Organisasi Perpustakaan secara sederhana dapat digambarkan dengan bagan seperti pada Gambar 1.



Gambar 1. Struktur Organisasi Perpustakaan

Proses bisnis Perpustakaan yang inti meliputi Pengadaan, Pengolahan dan Sirkulasi. Dalam penelitian ini penjabaran proses bisnis Perpustakaan dilakukan dengan memanfaatkan *Business Process Modelling Notation* (BPMN) [5].

Proses pengadaan merupakan proses bisnis yang bertujuan untuk menyediakan koleksi di Perpustakaan. Pengadaan meliputi proses pengumpulan usulan koleksi, pengadaan koleksi dengan melakukan pembelian ke *supplier* hingga penyusunan laporan terkait penambahan data koleksi terbaru. Setelah melewati proses pengadaan, koleksi yang baru diolah datanya di dalam proses pengolahan. Dalam proses pengolahan terjadi proses katalogisasi dan penginputan data koleksi yang disiapkan untuk proses sirkulasi, serta proses *packing*.

Proses bisnis selanjutnya adalah proses bisnis pengolahan, dimana pada proses ini terjadi transaksi peminjaman koleksi oleh pemustaka. Transaksi tidak hanya meliputi peminjaman saja tetapi juga proses pengembalian dan perhitungan denda bila pengembalian dilakukan tidak tepat waktu.

3.3 Kondisi Internal IT

Kondisi Internal IT dijabarkan dan disesuaikan dengan Proses Bisnis yang terjadi. Kondisi internal IT didapat melalui proses observasi juga wawancara. Hal ini dilakukan sebagai dasar untuk menentukan IT *Audit Universe*. Penjabaran kondisi IT meliputi struktur topologi jaringan, *software*, *hardware* dan kondisi sesungguhnya dari kinerja layanan IT yang dimanfaatkan. Berikut adalah penjabaran singkat terkait kondisi internal IT.

- *RAM : 2GB*
- *Processor: Core i3*
- *Harddisk Drive : 500GB*

Dari segi software, software yang secara umum terpasang (install) dalam semua unit komputer di Perpustakaan meliputi:

- *Operating System* yang digunakan secara umum dapat berupa *Windows 7, Windows XP*
- *Microsoft Office 2007* yang digunakan untuk pengolahan dokumen secara umum di Perpustakaan.
- *Google Chome, Internet Explorer, Mozilla Firefox* sebagai media *browser* untuk dapat mengakses program berbasis web, seperti *Online Catalog*
- Aplikasi bisnis yang dipakai oleh Perpustakaan adalah iSPEKTRA.

Beberapa kendala yang dialami terkait layanan IT adalah lambatnya koneksi internet, beberapa program yang masih belum terintegrasi dengan iSPEKTRA, dan inkonsistensi data.

4. IT AUDIT *UNIVERSE*

Beberapa penjabaran IT *Universe* di Perpustakaan meliputi infrastruktur teknologi, aplikasi yang dimanfaatkan, *brainware* yang terlibat dalam proses bisnis. Infrastruktur meliputi struktur topologi jaringan dan perangkat keras yang dipakai., aplikasi merupakan sistem informasi (*software*) yang sering dimanfaatkan, dan *brainware* meliputi orang-orang yang terlibat di dalamnya.

Area-area dalam IT Audit Universes inilah yang akan menjadi bagian dalam proses audit. Berikut dijabarkan IT Universe di Perpustakaan.

i. Proses penyusunan strategi
ii. Proses pengadaan dan pemeliharaan IT
   - Proses pembuatan, analisa, pemilihan dan perancangan aplikasi
   - Pengembangan aplikasi yang sudah ada
   - Sistem keamanan dan recovery plan terhadap aplikasi

- Pelatihan dan proses pembelajaran suatu sistem atau aplikasi
- Proses pengadaan dan pemeliharaan *hardware*, proses evaluasi dan dokumentasi laporan terkait *hardware* yang dimanfaatkan
- Perancangan struktur jaringan

iii. Proses pengadaan koleksi
- Pengajuan usulan
- Pengiriman informasi status usulan
- Penginputan data koleksi secara umum

iv. Proses pengolahan koleksi
- Proses katalogisasi (penentuan subject, penamaan dan lain-lain) berdasarkan standar LCSH
- Meng-update data yang telah diinputkan bagian pengadaan secara lebih rinci

v. Proses sirkulasi
- Penginputan informasi transaksi peminjaman koleksi
- Perhitungan denda

vi. Proses pelayanan referensi
- Proses penyediaan database jurnal

vii. Proses dalam sekretariat
- Penanganan administrasi karyawan

Setiap bagian dalam IT Universe di-*mapping* kan dengan IT Domain untuk memperoleh faktor-faktro risiko yang ada. Dalam menentukan IT *Domain* digunakan 34 *control objectives* yang ada dalam COBIT 4.1.

5. PENILAIAN RISIKO

Penilaian risiko dilakukan dengan mengacu pada metode *Risk Rating Methodology* yang dikeluarkan OWASP.

5.1 *Risk Likelihood*

Kriteria yang dijadikan acuan untuk mengukur *likelihood* meliputi *Skill Level* (SL), *Management* dan *Stakeholder Support* (MS), *Teamwork* (TW), *Project Management* (PM), *Awareness* (AW). Dalam Tabel 3. dijabarkan hasil penilaian kriteria *likelihood*. Hasil *likelihood* pada Tabel 3 merupakan hasil yang dimanfaatkan untuk menghitung *risk severity*.

Tabel 3. Penilaian *Likelihood*

No.	Resiko	SL	M	TW	PM	A	Likeli-hood
1	IT belum memiliki strategi dan perencanaan yang jelas untuk masa mendatang. Hal ini membuat tidak adanya taktik untuk pervujudan strategi dan analisa antara sistem yang sekarang ada dan dibutuhkan di masa depan.	3	8	7	8	7	6.60
4	Belum dilakukannya proses audit dan *risk assessment*, maupun pembuatan Standar Manajemen Kualitas (SMK) dan tidak ada tindakan preventif ataupun pengawasan secara berkala terkait hal-hal yang berpotensi menjadi resiko	5	3	9	0	7	4.80
6	*Back up* logika masih belum dilakukan, dan media *back up* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *back up* secara khusus	1	0	5	7	7	4.00

Sambungan Tabel 3. Penilaian *Likelihood*

12	Tidak ada IT Control Framework, SOP atau kebijakan tertentu untuk bidang IT	1	0	7	9	1	3.60
18	Tidak adanya penyusunan, evaluasi, *review* dan dokumentasi *Service Level Agreement* (SLA) terkait layanan yang harus diberikan kepada pengguna IT	5	0	0	7	7	3.80
19	Tidak adanya prosedur pencegahan insiden (khususnya untuk *hardware*), *IT Continuity Plan, Disaster Recovery Plan, IT Security Plan*, tidak ada pelatihan karyawan terkait kemungkinan adanya insiden	5	0	3	7	7	4.40
20	Tidak ada pembaharuan, perencanaan dan evaluasi terkait keamanan IT, seperti hak akses (baik untuk pengguna baru, yang sedang aktif, maupun sudah tidak aktif), ruang server yang bisa dimasuki siapa saja, *coding* dari sistem belum diproteksi, *malicious code* masih belum dapat dicegah, Sistem masih bisa diretas	5	0	0	7	7	3.80

5.2 *Risk Impact*

Kriteria yang dijadikan acuan dalam mengukur *impact* meliputi *Confidentiality* (C), Kehilangan Integritas (I), *Avalability* (AV), *Accountability* (AC), Layanan (S), Gangguan Privasi (P). Untuk setiap kriteria *impact* dibuat suatu komposisi nilai untuk tiap kriteria. Hal ini disebabkan tiap-tiap *impact* punya porsi berbeda terhadap dampak bisnis. Komposisi nilai tiap kriteria *impact* dijabarkan dalam Tabel 4.

Tabel 4. Komposisi Penilaian *Impact*

Impact	A	B	C	D	E	F	Jumlah	Persentase	Desimal	Pengali
Confidentiality	2	2	5	1	2	2	14	11%	0.11	0.99
Integrity	5	5	6	2	5	3	26	20%	0.20	1.84
Avalability	4	6	2	6	4	4	26	20%	0.20	1.84
Accountability	3	1	3	6	3	5	21	17%	0.17	1.49
Sevice	6	4	4	4	6	6	30	24%	0.24	2.13
Privasi	1	3	1	3	1	1	10	8%	0.08	0.71
Total							127	100%	1	9

Berdasarkan hasil komposisi tersebut maka dihasilkan nilai *impact* seperti yang dijabarkan dalam Tabel 5.

Tabel 5. Penilaian *Impact*

No.	Resiko	C	I	AV	AC	S	PV	Sum
1	IT belum memiliki strategi dan perencanaan yang jelas untuk masa mendatang. Hal ini membuat tidak adanya taktik untuk perwujudan strategi dan analisa antara sistem yang sekarang ada dan dibutuhkan di masa depan.	0.00	1.02	1.43	0.00	1.18	0.00	3.64
4	Belum dilakukannya proses audit dan *risk assessment*, maupun pembuatan Standar Manajemen Kualitas (SMK) dan tidak ada tindakan preventif ataupun pengawasan secara berkala terkait hal-hal yang berpotensi menjadi resiko	0.00	0.61	1.43	0.50	1.42	0.00	3.96
6	*Back up* logika masih belum dilakukan, dan media *back up* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *back up* secara khusus	0.00	1.43	1.84	0.00	2.13	0.00	5.40
12	Tidak ada IT Control Framework, SOP atau kebijakan tertentu untuk bidang IT	0.00	1.02	1.02	0.83	1.18	0.24	4.06
18	Tidak adanya penyusunan, evaluasi, *review* dan dokumentasi *Service Level Agreement* (SLA) terkait layanan yang harus diberikan kepada pengguna IT	0.11	1.02	1.43	0.83	1.65	0.08	5.05
19	Tidak adanya prosedur pencegahan insiden (khususnya untuk *hardware*), *IT Continuity Plan, Disaster Recovery Plan, IT Security Plan*, tidak ada pelatihan karyawan terkait kemungkinan adanya insiden	0.11	1.43	1.43	0.17	1.65	0.24	4.80
20	Tidak ada pembaharuan, perencanaan dan evaluasi terkait keamanan IT, seperti hak akses (baik untuk pengguna baru, yang sedang aktif, maupun sudah tidak aktif), ruang server yang bisa dimasuki siapa saja, *coding* dari sistem belum diproteksi, *malicious code* masih belum dapat dicegah, Sistem masih bisa diretas	0.55	1.43	1.43	0.50	0.71	0.00	4.62

5.3 *Risk Severity*

Risk Severity dapat dicari dengan cara mengalikan hasil *likelihood* terhadap *impact*. Tabel 6 menunjukkan *risk severity* dari masing-masing risiko.

Tabel 6. Penilaian *Risk Severity*

No	Resiko	Likeli-hood	Impact	Risk Severity
1	IT belum memiliki strategi dan perencanaan yang jelas untuk masa mendatang. Hal ini membuat tidak adanya taktik untuk perwujudan strategi dan analisa antara sistem yang sekarang ada dan dibutuhkan di masa depan.	6.60	3.64	24.01
6	*Back up* logika masih belum dilakukan, dan media *back up* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *back up* secara khusus	4.00	5.40	21.61
19	Tidak adanya prosedur pencegahan insiden (khususnya untuk *hardware*), *IT Continuity Plan, Disaster Recovery Plan, IT Security Plan*, tidak ada pelatihan karyawan terkait kemungkinan adanya insiden	4.40	4.80	21.10
18	Tidak adanya penyusunan, evaluasi, *review* dan dokumentasi *Service Level Agreement* (SLA) terkait layanan yang harus diberikan kepada pengguna IT	3.80	5.05	19.18
4	Belum dilakukannya proses audit dan *risk assessment*, maupun pembuatan Standar Manajemen Kualitas (SMK) dan tidak ada tindakan preventif ataupun pengawasan secara berkala terkait hal-hal yang berpotensi menjadi resiko	4.80	3.96	19.01
20	Tidak ada pembaharuan, perencanaan dan evaluasi terkait keamanan IT, seperti hak akses (baik untuk pengguna baru, yang sedang aktif, maupun sudah tidak aktif), ruang server yang bisa dimasuki siapa saja, *coding* dari sistem belum diproteksi, *malicious code* masih belum dapat dicegah, Sistem masih bisa diretas	3.80	4.62	17.56
12	Tidak ada IT Control Framework, SOP atau kebijakan tertentu untuk bidang IT	3.60	4.06	14.60

5.4 *Risk Response*

Untuk tiap-tiap risiko tersebut diberikan respon. Respon terhadap risiko dapat berupa *accept*, *avoid*, *reduce* (*lessen* atau *mitigate*), dan *transfer*. *Risk Response* dijabarkan dalam Tabel 7.

Tabel 7. *Risk Response*

Rank	No	Resiko	*Risk Severity*	*Risk Response*	Latar Belakang Pemelihan *Risk Response*
1	1	IT belum memiliki strategi dan perencanaan yang jelas untuk masa mendatang. Hal ini membuat tidak adanya taktik untuk perwujudan strategi dan analisa antara sistem yang sekarang ada dan dibutuhkan di masa depan.	*High*	*Lessen*	Respon terhadap resiko ini bertujuan untuk mengurangi *likelihood* resiko tidak adanya strategi IT dengan anjuran pembuatan strategi IT memanfaatkan suatu *framework*. Perpustakaan dianjurkan untuk membuat strategi dan perencanaan IT, hal ini dapat diwujudkan dengan penyusunan strategi memanfaatkan *Framework* seperti *The Open Group Architecture Framework* (TOGAF) , atau Zachman *Framework* untuk perencanaan sistem IT, COBIT untuk perencanaan *IT Governance*, ITIL dukungan layanan IT, NIST untuk security.
2	6	*Back up* logika masih belum dilakukan, dan media *back up* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *back up* secara khusus	*Medium*	*Lessen*	Respon terhadap resiko ini bertujuan untuk mengurangi *likelihood* resiko ini, sehingga *impact* seperti hilangnya data dalam media *backup* juga dapat diminimalkan. Anjurannya adalah dengan melakukan prosedur *backup* sesuai dengan standard NIST 800-34. Beberapa langkah yang dilakukan adalah menguji media *backup* dengan cara me-*restore* isi informasi ke dalam sistem untuk menguji integritas data, menyediakan media *backup*, setiap informasi harus digandakan (*copy*) tidak hanya ke dalam media *backup offsite* saja tetapi juga ke dalam *site* tertentu (seperti *dropbox*) yang menyediakan fasilitas *backup*.

Sambungan Tabel 7 *Risk Response*

Rank	No	Resiko	*Risk Severity*	*Risk Response*	Latar Belakang Pemelihan *Risk Response*
3	19	Tidak adanya prosedur pencegahan insiden (khususnya untuk *hardware*), *IT Continuity Plan, Disaster Recovery Plan, IT Security Plan*, tidak ada pelatihan karyawan terkait kemungkinan adanya insiden	*Medium*	*Lessen*	Respon untuk resiko ini adalah mengimplementasikan bentuk penanganan insiden, dan pembuatan *plan* terkait *continuity, security* dan *disaster recovery* dengan tujuan untuk mengurangi kemungkinan dan dampak terjadinya insiden, tidak adanya *plan* untuk IT. Perpustakaan dianjurkan membuat prosedur penanganan insiden, dengan memanfaatkan *Guidelines* dari NIST SP 800-61. Beberapa yang dapat dilakukan seperti membuat kebijakan, prosedur dan perencanaan respon terhadap insiden, membentuk dan melatih suatu tim penanganan insiden. *IT Security Plan* dapat diterapkan di Perpustakaan dengan mengacu pada NIST 800-53. Beberapa langkah yang dapat dilakukan antara lain menganalisa resiko-resiko terkait *security*, kemudian dikategorikan, dan dipilih kontrol yang cocok terhadap tiap-tiap resiko keamanan dan diimplementasikan, daserta diawasi secara berkala.
4	18	Tidak adanya penyusunan, evaluasi, *review* dan dokumentasi *Service Level Agreement* (SLA) terkait layanan yang harus diberikan kepada pengguna IT	*Medium*	*Lessen*	Bentuk respon terhadap resiko ini adalah dengan mengurangi bentuk kemungkinan terjadinya resiko dengan pembuatan suatu layanan berbasis SLA. Beberapa aspek yang harus ada di dalam SLA antara lain, penjabaran lingkup dan tujuan yang dicapai, pihak-pihak siapa saja yang terlibat, priode berlakunya persetujuan SLA, penjabaran dari tiap-tiap aktvitas yang harus disetujui, proses kerja dan pelaporan dari tiap aktivitas, manajemen permasalahan, dan kualitas dari suatu layanan yang diberikan.
5	4	Belum dilakukannya proses audit dan *risk assessment*, maupun pembuatan Standar Manajemen Kualitas (SMK) dan tidak ada tindakan preventif ataupun pengawasan secara berkala terkait hal-hal yang berpotensi	*Medium*	*Lessen*	Respon terhadap resiko ini adalah untuk mengurangi dampak resiko dengan melaksanakan proses audit dan manajemen resiko secara berkala dengan berdasarkan suatu standar. Perpustakaan dianjurkan melakukan risk assessment dan audit berdasarkan metode audit yang diajukan ISACA (dengan memanfaatkan COBIT) ataupun metode yang diajukan IIA (dengan menggunakan *Global Technology Audit Guidelines*)
6	20	Tidak ada pembaharuan, perencanaan dan evaluasi terkait keamanan IT, seperti hak akses (baik untuk pengguna baru, yang sedang aktif, maupun sudah tidak aktif), ruang *server* yang bisa dimasuki siapa saja, *coding* dari sistem belum diproteksi, *malicious code* masih belum dapat dicegah. Sistem masih bisa diretas	*Medium*	*Avoid*	Respon terhadap resiko ini bertujuan agar resiko terkait keamaan IT jangan sampai terjadi. Beberpa anjurannya antara lain untuk keamanan seperti *server room* Perpustakaan dapat menyesuaikan standar ruang *server* sesuai dengan ISO 27001, UCSD *Server Room Standard* dan NIST 800-123. Beberapa langkah yang dilakukan antara lain pembuatan ruang khusus untuk *server* agar ruang *server* tidak bisa diakses sembarangan, adanya (*fire surpression system*), dan media yang mengawasi (seperti CCTV),*alicious code* dapat dicegah dengan beberapa cara seperti larangan terhadap pengunduhan *file* atau program, tertentu dari sumber yang tidak terpercaya, melakukan proses review secara berkala terhadap *software* dan isi data dari suatu sistem untuk mencegah adanya *file* dan program yang tidak terotorisasi, serta memasang program *intrusion detection* yang bisa mendeteksi *malicious code* yang terjadi, dan juga dengan pemasangan *antivirus*.

6. KESIMPULAN DAN SARAN

Dari proses analisa risiko yang dilakukan dapat disimpulkan beberapa hal:

- Peran layanan IT terhadap bisnis di Perpustakaan cukup besar. Hal ini ditunjukkan dengan pemanfaatan IT untuk tiap proses bisnis inti di Perpustakaan yakni pada bagian Pengadaan, Pengolahan Sirkulasi dan Referensi (Bab 3, subbab 3.2)
- Proses Penilaian risiko dan pemberian respon terhadap risiko yang paling kritikal. Beberapa risiko tersebut antara lain:
  Risiko yang menjadi prioritas 1:
  IT belum memiliki strategi dan perencanaan yang jelas untuk masa mendatang. Hal ini membuat tidak adanya taktik untuk perwujudan strategi dan analisa antara sistem yang sekarang ada dan dibutuhkan di masa depan.
  Risiko yang menjadi prioritas 2:
  Backup logika masih belum dilakukan, dan media *backup* belum pernah diuji, dievaluasi ataupun di-*refresh*, tidak ada prosedur *backup* secara khusus.

Dalam penelitian ini, keterbukaan dari nara sumber sangatlah diperlukan untuk bisa mengungkap hal-hal apa saja yang secara fakta terjadi. Fakta-fakta ini sangat berguna dalam penelitian berbentuk analisa seperti penelitian ini, agar bisa didapat hasil yang maksimal, sehingga untuk penelitian-penelitian selanjutnya fakta-fakta yang berkaitan dengan penelitian juga harus bisa diperoleh dengan metode yang baik.

Selain hal tersebut, perlu diharapkan pada penelitian selanjutnya dapat dirumuskan suatu metode untuk menentukan kriteria penilaian faktor risiko yang lebih umum, sehingga bisa digunakan untuk mengukur berbagai jenis risiko baik dari aspek *likelihood* maupun *impact*.

7. REFERENSI

[1] Rehage, Steven Hunt dan Fernando N. (2008). *Developing IT Audit Plan*. USA: The Institute of Internal Auditors.

[2] Information Technology Governance Institute. (2005). *Control Objectives and related Information Technology 4.0*. IT Governance Intitute: USA

[3] The Open Web Application Security Project. *OWASP Testing Guide*. USA: OWASP Security Foundation.

[4] Osterwalder, A., dan Pigenur, Y.(2010) *Business Model Generation*. USA: John Wiley and Sons.

[5] Bridgeland, David dan Zahavi, Ron.(2009).Business Modelling: A Practical Guide to Realizing Business Value. US : Elsevier Inc.