Analisa Risiko pada bidang *Software Acquisition,Implementation,Maintenance* PT. Z

Albert Kurniawan[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: russetburbank07@gmail.com[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK

PT Z adalah sebuah perusahaan percetakan yang berpusat di sidoarjo dan menangani berbagai *customer* baik di dalam maupun di luar negeri. Teknologi informasi sudah dimanfaatkan untuk mendukung hampir di semua proses yang ada pada PT.Z, akan tetapi belum pernah dilakukan analisa risiko sehingga perusahaan tidak dapat mengetahui tentang risiko IT apa saja yang dapat terjadi. Untuk itu dibutuhkan sebuah analisa risiko sehingga perusahaan dapat mengetahui risiko apa saja yang dapat terjadi dan bagaimana menyikapi risiko tersebut.

Pada skripsi ini, dilakukan proses *risk assessment* terhadap proses *software acquisition, implementation*, dan *maintenance*. Langkah-langkah yang digunakan dalam melakukan *risk assasment* tersebut yaitu mengukur tingkat kedewasaan IT perusahaan menggunakan *Capability Maturity Model Integration* (CMMI), kemudian melakukan *mapping* CMMI kepada COBIT 4.1, dan menggunakan *OWASP Risk Rating Methodology* sebagai pedoman dalam melakukan perhitungan risiko. Dalam melakukan *risk assesment* Beberapa faktor risiko yang ditemukan antara lain belum adanya proses monitoring menggunakan matriks nilai yang jelas, tidak ada identifikasi proses IT yang berpengaruh besar pada proses bisnis perusahaan, serta tidak adanya verifikasi nilai hasil pengumpulan data monitoring.

Kata Kunci : Analisa risiko IT, CMMI, COBIT, Metode Kualitatif

ABSTRACT

PT.Z is a printing company based in Sidoarjo. PT.Z handle various customers both domestic and abroad. Information technology has been used to support nearly in all processes in PT.Z, but they has never done a risk analysis before so that the company do not know anything about IT risks that can occur. Therefore, it takes a risk analysis so that the company can determine what risks may occur and how to respond to those risks.

In this thesis, risk assessment performed in the process of software acquisition, implementation, and maintenance. The steps used in performing the risk assessment are measuring the level of maturity of the IT using the Capability Maturity Model Integration (CMMI), then perform mapping of CMMI to COBIT 4.1, and using the OWASP Risk Rating Methodology as a guide in the calculation of risk. Some of these risk factors include the lack of monitoring process based on clear value of metrics, no identification of IT processes that have great impact on the company's business process, there is no verification of value in the result of monitoring data collection.

Keywords: *IT risk analysis,* CMMI*,* COBIT*, Qualitative Methods*

1. PENDAHULUAN

Pada era globalisasi dewasa ini sistem informasi tidak dapat dipungkiri telah menjadi kebutuhan hampir di semua aspek kehidupan. Sektor bisnis pun tidak lepas dari peran sistem informasi sebagai aspek yang dipercaya dapat membantu menunjang proses bisnis dalam sebuah perusahaan. Oleh sebab itu, banyak perusahaan yang mulai mengalokasikan anggaran yang tidak sedikit untuk mengoptimalkan sistem informasi dari perusahaan tersebut. Hal ini harus diimbangi dengan sebuah sistem informasi yang benar-benar optimal, tidak hanya dalam segi *performance* saja akan tetapi proses *acquire and implementation software* juga perlu diperhatikan dengan baik, karena dapat ikut mempengaruhi keberhasilan proses bisnis sebuah perusahaan.

Berdasarkan hasil wawancara awal, PT.Z adalah sebuah perusahaan yang bergerak di bidang percetakan dengan skala internasional. PT.Z telah menyadari bahwa sistem informasi merupakan salah satu aspek yang dapat menunjang proses bisnis dalam sebuah perusahaan. Maka dari itu PT.Z telah mengalokasikan dana untuk menggunakan *software Enterprise Resource Planning* (*ERP*) JD Edward. *Software Enterprise Resource Planning* (*ERP*) ini sangat membantu dalam segi *exchange of information* antar divisi sehingga proses bisnis dalam perusahaan dapat menjadi lebih cepat dan efisien, Dari fakta ini dapat disimpulkan bahwa *Software* telah menjadi salah satu *core* dalam menunjang proses bisnis PT.Z.

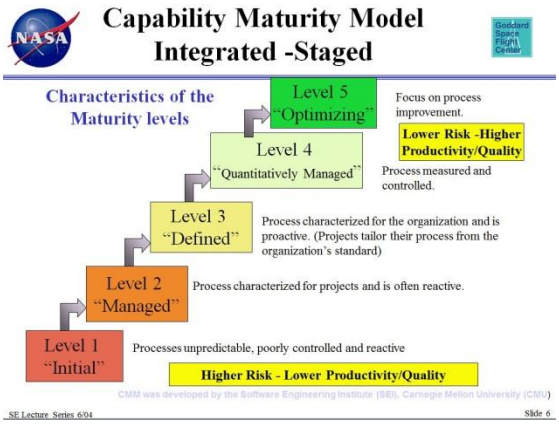
Mengingat bahwa peranan *Software* sangat besar dalam mendukung proses bisnis yang ada di PT.Z dalam hal ini *software* ERP, proses *Aquire, implementation and miantenance* menjadi sebuah aspek yang sangat penting dan harus ditangani secara serius. Melalui *Risk Assesement* perusahaan dapat mengetahui faktor risiko apa saja yang dapat terjadi, tingkat keseringan risiko itu terjadi, juga mengukur seberapa besar dampak risiko tersebut terhadap proses bisnis dalam perusahaan, kemudian dari hasil Risk Assesement tersebut dapat ditarik kesimpulan dan ditentukan risiko mana yang yang memiliki dampak paling besar dan dapat segera diberikan penanganan sesuai dengan standar yang ada. Diharapkan dari *Risk Assesment* yang dilakukan ini perusahaan dapat memanfaatkan hasil analisa ini untuk dapat mengatasi segala risiko yang berkaitan dengan proses pengadaan dan implementasi *softwre* sehingga mampu membantu meningkatkan proses bisnis dalam perusahaan.

2. DASAR TEORI

2.1.Capability Maturity Model (CMMI)

CMMI[1] adalah suatu model pendekatan dalam penilaian skala kematangan dan kedewasaan software sebuah organisasi. yang dikembangkan oleh Software Enginnering Institute di Pittsburgh.

Dalam penilaian CMMI terdapat 5 tingkat kedewasaan sebuah organisasi, dan dapat dilihat pada **Gambar 1** :



Gambar 1. CMMI Staged

2.2.COBIT 4.1.

Control Objective for Information and Related Technology (COBIT)[3] adalah sebuah standar pengelolaan *IT* yang berisi praktik-praktik yang baik (*best practices*) dalam dunia *IT* dikembangkan oleh *Information Technology Governance Institute* (ITGI) dari *Information System Audit and Control Association* (ISACA). Menurut Sarno[5] COBIT mendefinisikan tujuan bisnis terkait dengan aktivitas teknologi informasi yang umumnya ada di perusahaan. Pada kerangka kerja COBIT hanya menjelaskan tujuan-tujuan bisnis yang berkaitan dengan proses teknologi informasi. Demi memudahkan proses kontrol, COBIT mengelompokkan tujuan tersebut ke dalam perspektif kinerja Balanced Scorecard.

Definisi COBIT menurut gondodiyoto[2] adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. Perusahaan/organisasi mungkin tidak memiliki semua tujuan bisnis seperti yang dikelompokkan dalam tabel tersebut. Dalam penyusunan tujuan bisnis, perusahaan dapat memilih yang sesuai dengan karakteristik organisasinya masing-masing. Pemilihan tujuan bisnis dapat dilakukan dengan mendefinisikan proses bisnis utama maupun bisnis pendukung organisasi terlebih dahulu. Dalam CobiT 4.1 terdapat 4 *domain* dan terdapat 34 proses. 4 domain COBIT yaitu:

1. *Plan and Organise*
2. *Acquire and Implementation*
3. *Delivery and Support*
4. *Monitor and Evaluate*

2.3.*Mapping* CMMI *to* COBIT4.1

Mapping CMMI kepada COBIT 4.1[4] digunakan untuk memperjelas batasan domain dan area COBIT 4.1 mana yang akan digunakan untuk melakukan proses *risk assesment.* Berikut *mapping* CMMI pada COBIT 4.1 dapat dilihat pada

Gambar 2 Mapping CMMI to COBIT

Figure 13—Capability Maturity Level Mapping

CMMI Process Capability Levels Generic Practices	CMMI Generic Practice Mapping to CobiT Processes and Control Objectives	CobiT Maturity Attributes: Awareness and Communication	Policies, Standards and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
Capability Level 2: Managed Process							
GP2.1: Establish policy.	PO6, PO8.1		3				
GP2.2: Plan (to perform) the process.	N/A						
GP2.3: Provide resources: adequate funding, appropriate physical facilities, skilled people and appropriate tools.	PO4, PO8.1		3	3			
GP2.4: Assign responsibility.	PO4, PO8.1					3	
GP2.5: Train the people.	DS7				3		
GP2.6: Manage configuration.	AI6, DS9						
GP2.7: Identify and involve relevant stakeholders.	PO1, PO4, PO6, PO7, PO8, PO10, AI1, AI4, AI5, AI6, AI7, DS7, DS9, ME1, ME2, ME4						
GP2.8: Monitor and control the process.	PO8.6, ME1						
GP2.9: Objectively evaluate adherence.	PO8.6						
GP2.10: Review status with higher management	PO8.6, ME1, ME4.6						
Capability Level 3: Defined Process							
GP3.1: Establish and maintain a defined process.	PO4, PO8.2, PO8.3	4	4	4	4	4	4
GP3.2: Collect improvement information.	PO8.5, ME1						4
Capability Level 4: Quantitatively Managed Process							
GP4.1: Establish quantitative objectives for the process.	PO8.6, ME1						5
GP4.2: Stabilise subprocess performance.	N/A						
Capability Level 5: Optimising Process							
GP5.1: Ensure continuous process improvement.	PO8.5, ME1						5
GP5.2: Correct root causes of problems.	PO8.6, ME1						

2.4.OWASP *Risk Rating Methodology*

Menemukan *vulnurability* memang penting, tetapi mampu memperkirakan risiko yang terkait dengan bisnis sama pentingnya. Pada awal siklus hidup, seseorang dapat mengidentifikasi masalah keamanan dalam arsitektur atau desain dengan menggunakan *threat modeling*. Kemudian, orang dapat menemukan masalah keamanan menggunakan *code review* atau *penetration testing*. Atau masalah mungkin tidak ditemukan sampai aplikasi selesai di buat.

Dengan mengikuti pendekatan OWASP[7] *risk rating methodology*, dimungkinkan untuk memperkirakan tingkat keparahan risiko untuk segi bisnis dan membuat keputusan tentang apa yang harus dilakukan untuk risiko tersebut. Sistem peringkat risiko akan menghemat waktu dan menghilangkan perdebatan tentang prioritas risiko. Sistem ini akan membantu untuk memastikan bahwa bisnis tidak terganggu oleh risiko kecil dan mengabaikan risiko yang lebih serius yang kurang dipahami dengan baik.

Beberapa metode dari OWASP (2008) adalah:

a. Identifikasi risiko,
b. Menentukan *likelihood* dari faktor risiko
c. Menentukan *impact* dari faktor risiko
d. Menghitung *risk severity*,
e. Memutuskan *risk response* dan tingkat keparahan risiko.

Tabel 1 menunjukan contoh penilaian aspek *likelihood* sedangkan Tabel 2 menunjukan contoh penialaian *aspek business impact.*

Tabel 1. Contoh Penilaian Aspek *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)							

Tabel 2.Contoh Penilaian Aspek *Business Impact*

Business Impact			
Financial damage	Reputation damage	Non-compliance	Privacy violation
1	2	1	5
Overall business impact=2.25 (LOW)			

Setelah menghitung *likelihood* dan *impact* perkiraan, sekarang hasil tersebut dapat digabungkan menjadi peringkat keparahan akhir untuk risiko ini seperti terlihat pada **Tabel 3**

Tabel 3. Overall Risk Severity

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

3. MODEL DAN STRATEGI BISNIS

3.1 Model Bisnis dan Strategi Bisnis

Perusahaan Percetakan PT.Z berdiri pada tanggal 10 Juli 1991 di Sidoarjo, Jawa Timur, dengan nama PT.Z. Pada awalnya perusahaan hanya bergerak di bidang percetakan umum, terutama mencetak dokumen niaga saja. Kemudian pada tahun 1996 PT.Z menerima lisensi dari BOTASUPAL untuk mencetak dokumen sekuriti.

Pada tanggal 16 April 2002, PT.Z menjadi perusahaan publik, sehingga namanya menjadi PT.Z, Tbk. Sahamnya tercatat pada Bursa Efek Jakarta dengan kode JTPE. Pada tahun 2003, PT.Z, Tbk. meraih sertifikat ISO 9001 dari SGS International.

Saat ini PT.Z, Tbk. telah memiliki tiga pabrik utama, yaitu pabrik untuk mencetak dokumen sekuriti, pabrik untuk memproduksi kartu VISA & Master dan kartu sekuriti lainnya, serta pabrik untuk mencetak dokumen niaga. Ketiganya dibangun secara moderen, berada dalam lingkungan yang tertata asri serta dilengkapi dengan sistem dan peralatan terkini untuk menunjang kelancaran dan kinerja perusahaan.

Pada tahun 2004 PT. Z membeli software ERP yaitu JD Edwards yang digunakan untuk menunjang proses bisnis yang ada. Software ERP ini menjadi salah satu faktor penunjang dalam proses binis PT.Z.

Model bisnis perusahaan dapat dijabarkan dalam *nine building blocks* yang di ambil dari buku *Business Model Canvas* oleh Tim PPM Manajemen tahun 2012[6]. Ada 9 pilar utama dalam mendeskripsikan model bisnis, akan tetapi karena adanya unsur kerahasiaan maka tidak semua pilar dapat disebutkan. Beberapa pilar bisnis pada PT.Z adalah :

1. Value Proposition

   Memproduksi dokumen niaga dan dokumen dengan sekuriti.

2. Target Customer

   Semua kalangan yang membutuhkan dokumen niaga.

3. Distribution Channel

   Customer dapat datang langsung untuk mendapatkan solusi dokumen untuk kebutuhan nya atau bisa juga dengan media telepon maupun *e-mail.*

4. Relationship

   Tidak ada perlakuan khusus untuk *customer* semua customer diperlakukan secara sama dan profesional.

5. Value Configuration

   Proses pembelian bahan baku untuk keperluan produksi kepada *supplier* sesuai dengan kebutuhan produksi.

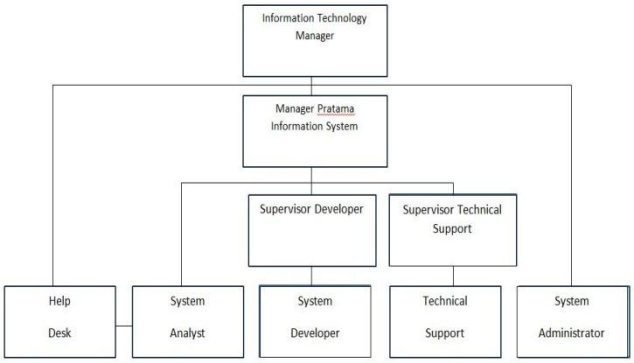
   Proses Produksi dokumen sesuai dengan permintaan dan tenggat waktu yang telah disepakati dengan *customer*

   Proses Pengiriman hasil produksi kepada *customer* dilakukan sesuai dengan perjanjian diawal.

6. Core competency

   Perusahaan percetakan dengan dokumen sekuriti yang terpercaya, baik untuk instansi swasta maupun negara.

Sedangkan untuk struktur organisasi perusahaan dapat dilihat pada **Gambar 3**.



Gambar 3.Struktur Organisasi Perusahaan

3.2 Kondisi Internal IT

Menrut hasil wawancara dengan pihak perusahaan, ada 3 software utama yang menunjang proses bisnis perusahaan yaitu :

1. JD. Edward ERP

ERP JD.Edward ini bisa dikatakan sebagai *main application* pada PT.Z karena hampir semua proses utama perusahaan menggunakan aplikasi ini. Proses-proses pemesanan/*order,* produksi, *accounting*, *finance* menggunakan modul-modul dari ERP JD.Edward.

Sejak pertama kali di terapkan pada PT.Z ERP JD.Edward masih sangat stabil dan mampu menunjang proses binis di PT.Z dengan baik, belum ada kendala yang berarti saat menggunakan aplikasi ini.

2. Track Studio

Track Studio digunakan untuk mencatat dan melakukan semua manajemen komplain, seperti kebutuhan *hardware,* tiket perjalanan, laporan *bug software* dan apapun yang di butuhkan satu departemen kepada departemen lain nya semua telah terpusat pada Track Studio.

Sampai sekarang Track Studio masih menjadi cara paling efektif dan stabil untuk melakukan komplain dan *request* kebutuhan antar divisi. Belum ada kendala yang berarti dalam penggunaan aplikasi ini.

3. ACTS HRM System

ACTS HRM system adalah aplikasi yang digunakan untuk melakukan proses absensi karyawan, penggajian karyawan dan segala seuatu yang berhubungan dengan *Human Resource Development* di PT.Z.

ACTS HRM system sampai saat ini masih mampu menjawab kebutuhan perusahan untuk sebuah sistem absensi dan penggajian yang efektif, ini dapat dilihat dari tidak ada kendala dan kesulitan dalam penggunaan ACTS HRM system hingga sekarang.

Sedangkan untuk kondisi dari *hardware,* PT.Z memiliki komputer yang berjumlah 200 unit dan sebagian besar menggunakan sistem operaasi windows 7, beberapa komputer menggunakan sistem operasi windows 8 karena menyesusaikan dengan aplikasi yang akan digunakan (*compabilty*). Lisensi windows dari PT.Z adalah lisensi OLP.

4. ANALISA CMMI

Berdasarkan wawancara mengenai CMMI dan survei tingkat kepentingan CMMI kepada beberapa responden dari divisi IT kemudian dilakukan pembobotan untuk mendapatkan *general pratices* yang dianggap penting akan tetapi belum terpenuhi secara maksimal. *General practices* itulah yang kemudian akan dipetakan (*mapping*) pada domain COBIT. Hasil pembobotan CMMI dapat dilihat pada **Tabel 4**.

Tabel 4.Pembobotan CMMI

Rank	General Practices	Nilai Survei	Persentase
1	GP2.3	25	10.46%
2	GP2.4	25	10.46%
3	GP2.5	25	10.46%
4	GP2.8	25	10.46%
5	GP2.10	25	10.46%
6	GP2.1	24	10.04%
7	GP2.6	24	10.04%
8	GP2.7	24	10.04%
9	GP2.2	21	8.78%
10	GP2.9	21	8.78%
TOTAL		239	100%

Setelah ditemukan *general practices* dengan persentase tertinggi, dilakukan peninjauan kepada 5 *general practices* tertinggi untuk mengetahui pada objektif *genral practices* mana perusahaan paling tidak dapat memenuhinya. Berdasarkan proses wawancara dan observasi dapat disimpulkan bahwa pada *general practices* 2.8 masih banyak objektif yang belum dapat dipenuhi oleh perusahaan.

5. PENILAIAN RISIKO

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

5.1 *Risk Likelihood*

Kriteria yang dijadikan pedoman untuk menilai aspek *likelihood* meliputi *Awareness* (AW), *Skill Level* (SL), *Teamwork* (TW), *Management* dan *Stakeholder Support* (MS) Dalam **Tabel 5** dijabarkan hasil penilaian kriteria *likelihood.* Hasil *likelihood* pada **Tabel 5**, Tabel 6, dan Tabel 7 merupakan hasil yang akan digunakan untuk menghitung overall *risk severity*.

Tabel 5.Penilaian Likelihood

No	Faktor Risiko	AW	SL	TW	MS	*Likelihood*	*Category*
1	Tidak adanya pendekatan monitoring peforma IT yang menggunakan metriks nilai menyebabkan tidak bisa dipastikan keberlangsungan proses IT yang di implementasikan sehingga dapat menggangu proses bisnis mulai dari produksi, HRD, penggajian dan segala proses bisnis yang didukung oleh IT pada perusahaan.	8	8	6	8	7.5	*High*

Tabel 6.Penilaian Likelihood

No	Faktor Risiko	AW	SL	TW	MS	*Likelihood*	*Category*
2	Tidak adanya identifikasi terhadap proses-proses yang berpengaruh besar pada proses bisnis perushaaan menyebabkan proses monitoring tidak berjalan secara efektif karena tidak dapat langsung fokus kepada proses yang mendukung proses bisnis perusahaan sehingga proses utama yang berpengaruh besar pada bisnis bisa saja terabaikan	8	3	8	8	6.75	*High*

Tabel 7.Penilaian Likelihood

No	Faktor Risiko	AW	SL	TW	MS	*Likelihood*	*Category*
3	Tidak ada aturan/prosedur untuk menangani penyimpangan juga tidak ada pemantauan lagi apakah penanganan penyimpangan itu sudah berjalan dengan baik atau belum mengakibatkan tidak ada kepastian tentang apa yang harus dilakukan jika terjadi penyimpangan proses IT.	8	2	8	0	4.5	*Medium*

5.2 *Risk Impact*

Kriteria yang dijadikan pedoman dalam menilai aspek *impact* meliputi Kehilangan Integritas (I), *Avalability* (AV),

Accountability (AC), Layanan (S). Untuk setiap kriteria *impact* dilakukan pembobotan seperti terlihat pada Tabel 8 agar sesuai dengan dampak bisnis pada perusahaan.

Tabel 8.Pembobotan Aspek *Impact*

Impact	Jumlah	Persentase	Desimal	Pengali
Kehilangan Integritas	53	26.5%	0.265	2.385
Avalability	45	22.5%	0.225	2.025
Accountability	47	23.5%	0.235	2.115
Layanan	55	27.5%	0.275	2.475
TOTAL	200	100%	1	9

Berdasarkan hasil dari pembobotan diatas dapat diberikan penilaian aspek *impact* seperti terlihat pada Tabel 9, Tabel 10, dan Tabel 11.

Tabel 9.Penilaian Aspek *Impact*

No	Faktor Risiko	I	AV	AC	S	*Sum*
1	Tidak adanya pendekatan monitoring peforma IT yang menggunakan metriks nilai menyebabkan tidak bisa dipastikan keberlangsungan proses IT yang di implementasikan sehingga dapat menggangu proses bisnis mulai dari produksi, HRD, penggajian dan segala proses bisnis yang didukung oleh IT pada perusahaan.	2.12	1.8	0.7	2.2	6.82

Tabel 10.Penilaian Aspek *Impact*

No	Faktor Risiko	I	AV	AC	S	*Sum*
2	Tidak adanya identifikasi terhadap proses-proses yang berpengaruh besar pada proses bisnis perushaaan menyebabkan proses monitoring tidak berjalan secara efektif karena tidak dapat langsung fokus kepada proses yang mendukung proses bisnis perusahaan sehingga proses utama yang berpengaruh besar pada bisnis bisa saja terabaikan	2.12	0.225	0.7	1.9	4.94

Tabel 11.Penilaian Aspek *Impact*

No	Faktor Risiko	I	AV	AC	S	*Sum*
3	Tidak ada aturan/prosedur untuk menangani penyimpangan juga tidak ada pemantauan lagi apakah penanganan penyimpangan itu sudah berjalan dengan baik atau belum mengakibatkan tidak ada kepastian tentang apa yang harus dilakukan jika terjadi penyimpangan proses IT.	2.12	1.575	0.7	1.9	6.29

5.3 *Risk Severity*

Risk Severity didapat dari hasil perkalian penilaianaspek *likelihood* dengan penilaian aspek *impact*. Hasil *risk severity* dapat dilihat pada Tabel 12.

Tabel 12.Risk Severity

No	Risiko	L	I	*Risk Severity*
1	Tidak adanya pendekatan monitoring peforma IT yang menggunakan metriks nilai menyebabkan tidak bisa dipastikan keberlangsungan proses IT yang di implementasikan sehingga dapat menggangu proses bisnis mulai dari produksi, HRD, penggajian dan segala proses bisnis yang didukung oleh IT pada perusahaan.	7.5	6.82	51.15
2	Tidak adanya identifikasi terhadap proses-proses yang berpengaruh besar pada proses bisnis perushaaan menyebabkan proses monitoring tidak berjalan secara efektif karena tidak dapat langsung fokus kepada proses yang mendukung proses bisnis perusahaan sehingga proses utama yang berpengaruh besar pada bisnis bisa saja terabaikan karena tidak ada kesepakatan dan integrasi antara monitoring IT dengan perfomance management dari perusahaan. Hal ini dapat menyebabkan manajamen tidak dapat mengetahui apakah proses bisnis yang didukung oleh IT berjalan baik atau tidak.kemudian dapat menggangu proses bisnis pada perusahaan.	6.75	4.94	33.345

Tabel 13.Risk Severity

No	Risiko	L	I	*Risk Severity*
3	Tidak ada aturan/prosedur untuk menangani penyimpangan juga tidak ada pemantauan lagi apakah penanganan penyimpangan itu sudah berjalan dengan baik atau belum mengakibatkan tidak ada kepastian tentang apa yang harus dilakukan jika terjadi penyimpangan proses IT, juga dibutuhkan waktu yang lama untuk melakukan analisa tentang tindakan yang akan diambil untuk menangani penyimpangan tersebut, terlebih lagi dengan tidak ada pemantauan tentang tindakan yang diambil tidak dapat diketahui apakah tindakan tersebut benar-benar dapat mengatasi penyimpangan tersebut atau tidak.	4.5	6.29	28.305

5.4 *Risk Response*

Untuk tiap-tiap risiko diberikan *response* yang sesuai. *Response* yang dapat diberikan antara lain adalah *accept, avoid, reduce/lessen* ataupun *transfer* seperti dapat dilihat pada Tabel 14, Tabel 15, dan Tabel 16.

Tabel 14.Risk Response

Rank	Risiko	*Severity*	*Response*	Latar Belakang
1	Tidak adanya pendekatan monitoring peforma IT yang menggunakan metriks nilai menyebabkan tidak bisa dipastikan keberlangsungan proses IT yang di implementasikan sehingga dapat menggangu proses bisnis mulai dari produksi, HRD, penggajian dan segala proses bisnis yang didukung oleh IT pada perusahaan.	*Critical*	*Lessen*	*Risk response* terhadap risiko ini adalah membuat metriks nilai yang jelas mengenai proses yang akan dimonitoring sehingga hasil dari monitoring dapat dipastikan secara detail dan lengkap. Pedoman dalam melakukan monitoring dapat mengacu pada. NIST 800-55 *Metrics for Assesing Information Technology Perfomance* atau pada NIST 800-26 mengenai *Security Self-assesment Guide.*

Tabel 15.Risk Response

Rank	Risiko	*Severity*	*Response*	Latar Belakang
2	Tidak adanya identifikasi terhadap proses-proses yang berpengaruh besar pada proses bisnis perushaaan menyebabkan proses monitoring tidak berjalan secara efektif karena tidak dapat langsung fokus kepada proses yang mendukung proses bisnis perusahaan sehingga proses utama yang berpengaruh besar pada bisnis bisa saja terabaikan	*High*	*Lessen*	*Risk* response ini bertujuan untuk membuat proses monitoring fokus terhadap proses-proses IT penting yang mendukung proses bisnis secara langsung seperti pada standar NIST 800-137

Tabel 16.Risk Response

Rank	Risiko	*Severity*	*Response*	Latar Belakang
3	Tidak ada aturan/prosedur untuk menangani penyimpangan juga tidak ada pemantauan lagi apakah penanganan penyimpangan itu sudah berjalan dengan baik atau belum mengakibatkan tidak ada kepastian tentang apa yang harus dilakukan jika terjadi penyimpangan proses IT.	*High*	*Lessen*	*Risk response* ini bertujuan untuk mengurangi *impact* dari risiko ini dengan membuat sebuah aturan/prosedur untuk menangani berbagai penyimpangan proses IT yang mengacu pada ISO 9001 mengenai pembuatan SOP.

6. KESIMPULAN DAN SARAN

Dari proses analisa risiko yang dilakukan dapat disimpulkan beberapa hal:

a. Berdasarkan analisa, survei, dan observasi CMMI ditemukan bahwa GP2.8 merupakan *general practices* yang paling penting sekaligus sebagai *general practices* dengan objektif yang paling tidak dapat dipenuhi oleh perusahaan.

b. PO8.6 dan ME1 menjadi domain COBIT yang digunakan dalam proses analisa risiko sesuai dengan *mapping* level CMMI kepada COBIT.

c. Ditemukan risiko yang paling kritikal dan dilakukan pemberian respon. Risiko tersebut adalah

   Risiko yang menjadi prioritas pertama:

   Tidak adanya pendekatan monitoring peforma IT yang menggunakan matriks nilai menyebabkan tidak bisa dipastikan keberlangsungan proses IT yang di implementasikan di PT.Z.

   Risiko yang menjadi prioritas kedua:

   Tidak adanya identifikasi terhadap proses-proses yang berpengaruh besar pada proses bisnis perushaaan menyebabkan proses monitoring tidak berjalan secara efektif karena tidak dapat langsung fokus kepada proses yang mendukung proses bisnis perusahaan.

Pada analisa risiko keterangan dari wawancara terhadap pihak terkait menjadi sesuatu yang sangat penting. Banyak hal yang tidak dapat diungkap risikonya apabila metode wawancara yang digunakan kurang maksimal. Oleh karena itu untuk pengembangan selanjutnya dapat menggunakan metode wawancara yang lebih baik.

Penelitian ini dapat menjadi saran bagi pengembangan analisa risiko ketahap audit sistem informasi, sehingga dapat menghasilkan analisa yang lebih lengkap dan bermanfaat bagi peusahaan.

7. REFERENSI

[1] Carnegie Mellon University. 2006. Capability Maturity Model Integration. USA: Carnegie Mellon University.

[2] Gondodiyoto, S. 2007. In *Audit Sistem Informasi + Pendekatan Cobit* . Jakarta: Mitra Wacana Media.

[3] Information Technology Governance Institute. 2007. *Control Objectives and related Information Technology 4.1*. IT Governance Institute: USA

[4] ISACA. 2007. COBIT Mapping: Mapping of CMMI for Development V1. 2 with COBIT 4.1. ISACA :USA

[5] Sarno, R. 2009. In *Strategi Sukses Bisnis dengan Teknologi Informasi*. Surabaya: ITS Press.

[6] Tim PPM Manajemen. 2012. *Business Model Canvas Penerapan di Indonesia.* Indonesia: Penerbit PPM.

[7] The Open Web Application Security Project. 2015.*OWASP Testing Guide*. USA: OWASP Security Foundation.