

ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI DAN PEMETAAN *MATURITY LEVEL* PADA PT. XYZ MENGGUNAKAN *FRAMEWORK* COBIT 4.1

Rani Puspita Dhaniawaty
Sistem Informasi UNIKOM
ranipuspita@email.unikom.ac.id

ABSTRAK

Pesatnya perkembangan teknologi informasi yang saat ini, menuntut setiap perusahaan untuk selalu berkembang, dengan mengaplikasikan teknologi informasi terbaru pada perusahaannya. Disisi lain penerapan teknologi informasi perlu biaya investasi yang cukup mahal dan menimbulkan resiko terjadinya kegagalan yang cukup besar. Kondisi perusahaan seperti ini membutuhkan konsistensi dalam melakukan pengelolaan penerapan teknologi informasi. Oleh karena itu manajemen resiko sangat dibutuhkan oleh perusahaan yang bertujuan untuk mengetahui resiko apa saja yang akan terjadi apabila melakukan penerapan teknologi informasi. *Framework* COBIT 4.1 merupakan *framework* yang paling cocok dengan kebutuhan perusahaan karena *framework* ini memastikan bahwa teknologi informasi telah diselaraskan dengan proses bisnis, sumber daya teknologi informasi, mengidentifikasi resiko, melakukan penilaian terhadap resiko, menangani resiko dengan tepat, melakukan pemetaan *maturity level* dan menghasilkan rekomendasi untuk dapat mencapai target yang sesuai dengan keinginan perusahaan.

Kata kunci : Manajemen Resiko, *Maturity Level*, COBIT 4.1 *Framework*.

I. PENDAHULUAN

Teknologi informasi merupakan elemen penting dalam sebuah perusahaan untuk dapat bertahan, bersaing dan meraih keunggulan kompetitif. Pemanfaatan teknologi informasi memberikan solusi dan keuntungan bagi perusahaan dalam hal operasional, bisnis dan keuntungan dalam segi finansial. Penggunaan teknologi informasi juga membantu perusahaan untuk dapat bersaing dengan perusahaan lain. Tetapi dalam penggunaan teknologi informasi selalu terdapat ancaman atau resiko yang selalu ada dan dapat mengganggu operasional kinerja perusahaan.

Beberapa resiko yang biasanya muncul pada saat penggunaan teknologi informasi yaitu adanya serangan virus yang dapat mengganggu kinerja dari teknologi informasi, serangan *cracker* yang dapat mengacaukan sistem bahkan sampai mencuri data rahasia suatu perusahaan, kesalahan dan kerusakan sistem pendukung seperti jaringan listrik putus, dan lain sebagainya. Resiko-resiko tersebut harus dikelola dan diantisipasi dengan baik, sehingga resiko tersebut tidak menyebabkan kerugian yang fatal.

Dalam menghadapi resiko atau ancaman yang terjadi, perusahaan berharap mendapatkan solusi dalam hal mengurangi tingkat kemunculan resiko

dan dapat mengatasi resiko yang sering terjadi sampai resiko yang jarang terjadi diperusahaan. Dilihat dari permasalahan tersebut, maka dibutuhkan adanya tatakelola teknologi informasi yang dapat mengatasi resiko yang terjadi atau yang dapat melakukan manajemen terhadap resiko yang sudah terjadi.

Salah satu tatakelola teknologi informasi yang dapat membantu dalam manajemen resiko yang terdapat pada perusahaan adalah *Framework COBIT 4.1*. *Framework COBIT 4.1* memungkinkan perusahaan dalam melakukan pengembangan kebijakan dan *best practices* untuk pengendalian teknologi informasi. Dalam mendukung tatakelola teknologi informasi, *Framework COBIT 4.1* menyediakan suatu kerangka kerja yang dapat memastikan bahwa teknologi informasi sudah diselaraskan dengan proses bisnis dan sumber daya teknologi informasi, dimana apabila terdapat resiko-resiko teknologi informasi yang terjadi didalam perusahaan akan ditangani dengan cepat dan tepat.

II. KAJIAN PUSTAKA

1. *Framework COBIT 4.1*.

Framework COBIT 4.1 (Control Objective for Information and related Technology) merupakan suatu *framework* yang dapat memberikan kebijakan untuk melakukan pengendalian teknologi informasi, membantu perusahaan dalam memahami dan mengelola resiko yang terkait dengan tata kelola teknologi informasi. Dengan menerapkan *framework COBIT 4.1*, maka perusahaan akan mendapatkan panduan tujuan pengendalian secara terperinci (*detailed control objective*).

Penerapan teknologi informasi pada perusahaan dikatakan berhasil, jika perusahaan dapat membuat sistem pengendalian internal dengan

menggunakan kerangka kerja. Dilihat dari kebutuhan perusahaan tersebut *Framework COBIT 4.1* dapat memberikan kontribusi pengendalian kebutuhan seperti (ITGI, 2007) :

- a. Menyusun atau mengatur kegiatan teknologi informasi kedalam suatu proses yang berlaku secara umum.
- b. Membuat acuan kebutuhan bisnis suatu perusahaan.
- c. Mengidentifikasi jumlah sumber daya teknologi utama yang sudah ada di perusahaan.
- d. Menentukan tujuan pengendalian kebutuhan teknologi informasi.

Framework ini dirilis dan disusun oleh *IT Governance Institute (ITGI)* yang merupakan bagian dari *ISACA (Information Systems Audit and Control Association)* pada tahun 1996. *COBIT* versi pertama diterbitkan pada tahun 1996, versi kedua tahun 1998, versi 3.0 tahun 2000, versi 4.0 tahun 2005 dan *COBIT 4.1* dirilis pada tahun 2007 serta versi terakhir yang baru saja dirilis tahun 2011 adalah *COBIT* versi 5.

2. Manajemen Resiko.

Manajemen resiko adalah suatu pendekatan terstruktur dalam mengelola ketidakpastian yang berkaitan dengan ancam. Didalam proses manajemen resiko terdapat penilaian resiko yang berguna untuk menilai dilevel dan prioritas manakah resiko atau ancaman tersebut berada. Dibutuhkan strategi dalam mengelola resiko dan ancaman tersebut salah satunya yaitu dengan memindahkan resiko kepada pihak lain, menghindari resiko, mengurangi efek negatif resiko dan menampung sebagian resiko tertentu.

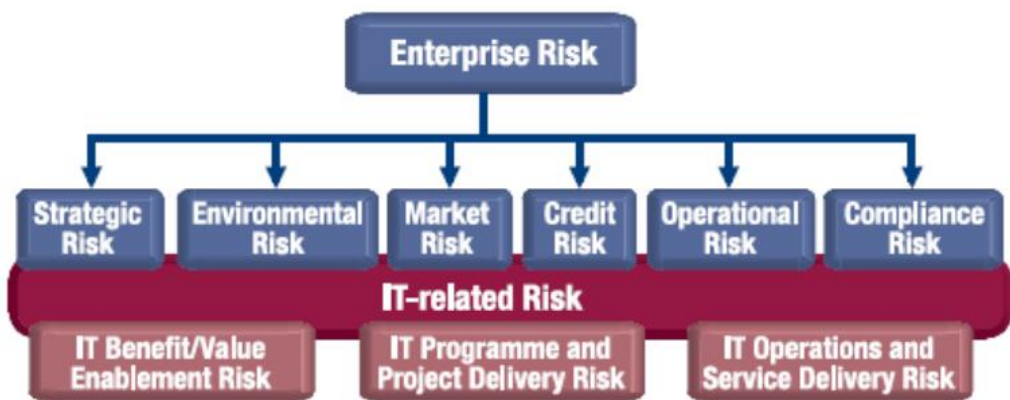
Manajemen resiko teknologi informasi merupakan hal penting yang harus dihadapi oleh perusahaan, karena memiliki dampak besar bagi operasional perusahaan. Terdapat beberapa resiko yang dihadapi perusahaan pada saat

penerapan teknologi informasi diantara adanya virus yang menyebar di komputer yang dapat mengganggu kinerja dari teknologi informasi perusahaan, adanya serangan dari *cracker* yang dapat mengacaukan sistem atau mencuri data, kesalahan dan kerusakan sistem pendukung kinerja contohnya seperti jaringan listrik terputus. Semua resiko tersebut harus dihadapi, dikelola dan diantisipasi dengan baik sehingga resiko

tersebut tidak sampai menyebabkan kerugian yang fatal bagi perusahaan.

3. Resiko Teknologi Informasi.

Resiko teknologi informasi adalah resiko yang dimiliki oleh suatu perusahaan yang diakibatkan oleh adanya penggunaan atau penerapan teknologi informasi, resiko teknologi informasi ini merupakan salah satu komponen dari keseluruhan resiko yang terdapat didalam perusahaan, seperti pada gambar 1 berikut ini :



Gambar 1. Resiko Teknologi Informasi

Resiko teknologi informasi dapat mempengaruhi operasional perusahaan dan dapat menciptakan tantangan dalam mencapai tujuan dan sasaran strategis. Resiko teknologi informasi dikategorikan menjadi tiga bagian, yaitu sebagai berikut (ISACA, 2009) :

- a. *IT Benefit/Value Enablement Risk* – Bagian ini terkait dengan hilangnya kesempatan perusahaan dalam penggunaan teknologi bagi peningkatan efisiensi dan efektifitas proses bisnis atau sebagai *enabler* untuk inisiatif bisnis baru.
- b. *IT Programme and Project Delivery Risk* – Bagian ini terkait dengan kontribusi teknologi informasi terhadap solusi bisnis baru dalam bentuk proyek dan program.

c. *IT Operation and Service Delivery Risk* – Bagian ini terkait dengan semua aspek kinerja sistem dan layanan teknologi informasi yang dapat merusak dan mengurangi nilai bagi perusahaan.

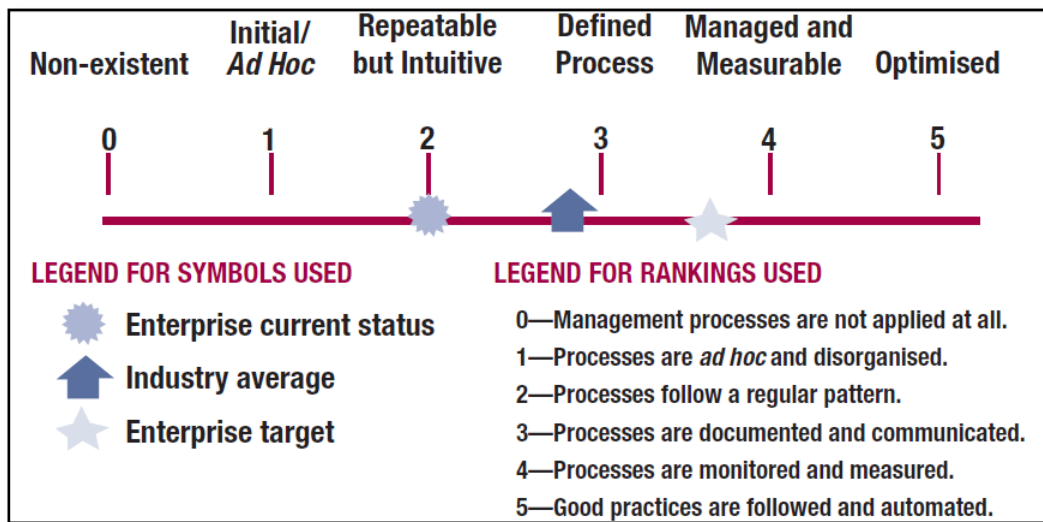
4. Tingkat Kematangan (*Maturity Level*).

Pemodelan tingkat kematangan untuk manajemen dan pengendalian proses teknologi informasi perusahaan yang didasarkan pada metode evaluasi, sehingga perusahaan dapat menilai tingkat kematangan dari yang statusnya tidak ada (0) sampai dengan status yang dioptimalkan (5). Pendekatan ini berasal dari model tingkat kematangan yang disebut *Software Engineering Institute*

(SEI) dimana dapat mendefinisikan kematangan atau kemampuan perusahaan dalam pengembangan *software*.

Tingkat kematangan (*maturity level*) dirancang untuk melihat profil proses teknologi informasi yang akan diterapkan di perusahaan sebagai deskripsi tentang kemungkinan yang akan terjadi di masa depan dan digunakan sebagai acuan dalam mencapai target sesuai dengan

yang diinginkan perusahaan. COBIT 4.1 *Framework* mempunyai model kematangan (*maturity model*) untuk mengontrol proses-proses teknologi informasi dengan menggunakan metode penilaian (*scoring*) sehingga suatu perusahaan dapat menilai proses-proses teknologi informasi yang dimilikinya, pemetaan model *maturity level* dapat dilihat pada gambar 2 berikut ini :



Gambar 2. Tingkat Kematangan (*Maturity Level*).

Skala pembulatan tingkat *maturity model* diperlukan jika nilai yang dihasilkan berada diantara 0-5, berikut ini

skala pembulatan dan penjelasan tingkat *maturity model*:

Tabel 1. Skala dan Tingkat *Maturity Model*.

Skala	Tingkat <i>Maturity Model</i>
4.51-5.00	5-Dioptimalkan (<i>Optimized</i>)
3.51-4.50	4-Diatur (<i>Managed</i>)
2.51-3.50	3-Ditetapkan (<i>Defined</i>)
1.51-2.50	2-Dapat Diulang (<i>Repeatable</i>)
0.51-1.50	1-Inisialisasi (<i>Initial</i>)
0.00-0.50	0-Tidak Ada (<i>Non Existend</i>)

Keterangan :

0-Tidak Ada (*Non Existend*). Kurang lengkapnya proses yang sudah diterapkan, bahkan perusahaan belum menyadari

bahwa terdapat masalah yang perlu diperbaiki dan ditangani.

1-Inisialisasi (*Initial*). Perusahaan sudah menyadari bahwa masalah yang ada perlu ditangani dan diperbaiki. Namun, tidak

ada standarisasi proses yang harus ditangani dan diperbaiki itu seperti apa.

2-Dapat Diulang (Repeatable). Proses yang berulang tetapi berkembang ditahap yang sama terus menerus. Hal ini terjadi karena tidak adanya pelatihan formal, komunikasi standar, dan tanggung jawab diserahkan kepada individu sesuai dengan bagiannya.

3-Diterapkan (Defined). Proses yang Ditetapkan telah distandarisasi, didokumentasikan, dan dikomunikasikan melalui pelatihan. Proses ini seharusnya dilakukan, tetapi masih saja terdapat penyimpangan yang terlihat seperti tidak melakukan dan mengerjakan instruksi yang diberikan.

4-Diatur (Managed). Proses ini memonitor dan mengukur kepatuhan terhadap prosedur dan mengambil

tindakan pada proses yang tidak berjalan secara efektif.

5-Dioptimalkan (Optimized). Proses yang Dioptimalkan telah disempurnakan ke tingkat praktik yang lebih baik, berdasarkan hasil pemodelan perbaikan dan pematangan berkelanjutan adanya perbandingan antara perusahaan dengan perusahaan kompetitor. Teknologi informasi digunakan secara terpadu untuk mengotomatisasi alur kerja, menyediakan alat untuk meningkatkan kualitas dan efektivitas, serta membuat perusahaan cepat beradaptasi.

III. METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini terdapat beberapa tahapan yang perlu dilakukan, yaitu sebagai berikut :



Gambar 3. Metodologi Penelitian.

1. Studi Literatur.
Studi literatur dilakukan dengan melakukan pencarian data di internet, buku dan beberapa jurnal mengenai manajemen resiko yang akan digunakan sebagai referensi dan

- landasan teori dalam menganalisis manajemen resiko perusahaan.
2. Pengumpulan Informasi.
Dalam proses pengumpulan informasi terdapat beberapa tahapan

yang dilakukan, yaitu sebagai berikut :

- a. Observasi.
Pada tahap ini dilakukan pengamatan langsung ke lokasi penelitian untuk melihat secara langsung data-data yang berkaitan dengan materi yang dibutuhkan dalam penyusunan penelitian.
 - b. Wawancara.
Pada tahap ini dilakukan proses tanya jawab dengan pihak yang berhubungan dengan penerapan teknologi informasi dan manajemen resiko teknologi informasi.
 - c. Kuisioner.
Pada tahap ini dilakukan proses pengumpulan data secara acak yang dibagikan kepada beberapa responden. Data yang sudah terkumpul akan digunakan dalam melakukan analisis terhadap resiko yang terdapat di perusahaan.
3. Penetapan Objektif.
Prinsip pada *framework* COBIT 4.1 ini yaitu melakukan investasi dibidang teknologi informasi serta mengatur dan mengontrol sumber daya teknologi informasi sesuai dengan yang dibutuhkan oleh perusahaan. Untuk mencapai tujuan tersebut dibutuhkan tujuh kriteria informasi yang sesuai :
- a. *Effectiveness*.

- b. *Efficiency*.
- c. *Confidentiality*.
- d. *Integrity*.
- e. *Availability*.
- f. *Compliance*.
- g. *Reliability of information*.

4. Identifikasi Resiko.
Tahap ini berfungsi untuk mengidentifikasi resiko-resiko yang mungkin terjadi selama pelaksanaan penerapan teknologi informasi. Beberapa sumber resiko biasanya berasal dari manusia, bagian internal perusahaan, bagian eksternal perusahaan, bencana, virus komputer, kegagalan sistem, kesalahan dalam melakukan pemilihan teknologi informasi, masalah dalam pengembangan dan implementasi sistem di perusahaan.
5. Penilaian Resiko.
Tahapan ini berfungsi untuk menilai seberapa sering resiko terjadi dan seberapa besar dampaknya terhadap perusahaan. Dampak resiko dapat dilihat dari segi finansial, reputasi perusahaan menurun, terhentinya operasi yang sedang berjalan dan bahkan sampai penundaan proses pengambilan keputusan. Kecenderungan terjadinya resiko dapat dilihat dari dampak resiko yang ada di perusahaan. Berikut ini tabel tingkatan dampak resiko dan kecenderungan terjadinya resiko didalam penerapan teknologi informasi perusahaan :

Tabel 2. Dampak Resiko dan Kecenderungan yang Terjadi.

Level	Dampak Resiko (<i>Business Impact</i>)	Kecenderungan (<i>Likelihood</i>)
0	Kerusakan yang hampir tidak signifikan	Hampir mustahil terjadi
1	Kerusakan kecil	Jarang terjadi

2	Kerusakan yang signifikan tapi masih bisa ditolerir	Mungkin terjadi
3	Kerusakan besar	Sering terjadi
4	Kerusakan yang dapat mengancam kelangsungan bisnis	Sangat sering terjadi

6. Respon dan Monitor Resiko.
 Respon resiko, pada tahapan ini yaitu melakukan penetapan terhadap domain proses yang berhubungan dengan resiko management. Proses domain COBIT 4.1 yang berkaitan dengan manajemen resiko adalah :
- PO1 (*Define a Strategic IT Plan*).
 - PO9 (*Assess and Manage Risk*).
 - AI6 (*Manages Change*).
 - DS5 (*Ensure System and Security*).
 - DS11 (*Manage Data*).
 - ME1 (*Monitor and Evaluate IT Performance*).
- Sedangkan pada tahapan monitor resiko berfungsi untuk menjamin bahwa resiko dan respon akan berjalan sepanjang waktu dan sesuai dengan target yang diinginkan oleh perusahaan.
7. Pemetaan *Maturity Level*.
 Pada tahapan ini diperlukan untuk mengetahui tingkat kematangan perusahaan dalam penerapan teknologi informasi itu berada di level mana, mengetahui target level yang diinginkan oleh perusahaan, dan mengetahui *gap level* antara *maturity level* saat ini dengan *maturity level* yang diinginkan.
8. Membuat Rekomendasi.
 Pada tahapan ini perusahaan akan diberikan beberapa rekomendasi, tahapan dan proses dalam melakukan penerapan teknologi informasi, supaya perusahaan dapat mencapai

target sesuai dengan yang diinginkan.

IV. HASIL DAN PEMBAHASAN

Tahapan yang dilakukan dalam penelitian ini sesuai dengan metodologi penelitian yang sudah dipaparkan, hasil yang sudah didapat dari penelitian ini, yaitu sebagai berikut :

1. Penetapan Objektif, Identifikasi Resiko dan Penilaian Resiko.
 Setelah mendapatkan data dari perusahaan berkaitan dengan resiko, maka didapatkan penetapan objektif resiko sebagai berikut :
 - a. Intergritas.
 Berkaitan dengan keakuratan dan kelengkapan informasi serta keabsahan yang sesuai dengan harapan dan nilai bisnis perusahaan XYZ.
 - b. Kerahasiaan.
 Berkaitan dengan perlindungan informasi yang sensitif dari akses yang tidak sah dan dilakukan daripihak intern atau ekstern perusahaan XYZ.
 - c. Ketersediaan.
 Berkaitan dengan informasi yang tersedia yang diperlukan oleh proses bisnis saat ini dan yang akan datang serta berkaitan dengan penjagaan sumberdaya yang perlu dan kemampuan yang terkait.

Berikut ini hasil penetapan objektif, identifikasi resiko dan penilaian resiko pada perusahaan XYZ :

Tabel 3. Daftar Resiko yang Terjadi

Objektif	Deskripsi Resiko	Kerentanan	Dampak	Level
Integritas	Kehilangan data akibat komputer mati	Medium	High	3
	Data rusak akibat virus	Medium	Medium	2
	Virus lokal tidak terdeteksi antivirus	Medium	Medium	2
	Penyebaran virus melalui flashdisk	Medium	Medium	2
	<i>Cracker</i> mencuri data	Medium	High	3
	Tidak ada pemberitahuan kehilangan data	Medium	Medium	2
	Data yang sudah lama dan tidak terpakai tidak dihapus	Medium	Low	1
Kerahasiaan	<i>Hacker</i> dapat membobol website	Medium	High	3
	Pengubahan database diluar wewenang	Medium	Medium	2
	Informasi didalam laptop tidak dilindungi	Medium	Medium	2
	Pencurian data yang dilakukan karyawan yang tidak berwenang	High	High	4
	Password login mudah diketahui	High	High	4
	Secara sadar atau tidak sadar memberikan informasi ke pihak lain mengenai informasi keuangan perusahaan	Medium	High	3
	Memberitahu <i>password</i> kepada orang lain	Medium	Medium	2
Ketersediaan	Permintaan perubahan aplikasi yang tidak ditanggapi tepat waktu	Medium	Medium	2
	Aplikasi laporan keuangan yang diperbaharui tidak sesuai dengan keinginan departemen	Medium	Medium	2
	Pencurian <i>hardware</i>	High	High	4
	Listrik padam	High	High	4
	Virus mengakibatkan	Medium	Medium	2

	aplikasi tidak tersedia			
	Kesalahan <i>entry</i> data	Medium	Medium	2
	Hubungan arus pendek listrik yang menyebabkan kerusakan pada komputer	Medium	High	3

2. Respon dan Monitor Resiko.

Hasil respon resiko yang didapat sudah menyesuaikan antara proses-proses *Framework* COBIT 4.1 dengan manajemen resiko yang sebagai berikut :

a. Proses PO (*Planning and Organisation*).

Hasil pengujian yang dilakukan pada proses PO (*Planning and Organisation*) memiliki rata-rata nilai **2.9** dan *maturity level* berada diposisi **Defined**.

Tabel 4. Hasil Pengujian Pada Proses PO (*Planning and Organisation*).

No	Kode	Proses	Hasil Pengujian	Tingkat Maturity
1	PO1	Define IT Strategic Plan	2.99	Defined
2	PO9	Assess and Manage Risk	2.85	Defined
Rata-rata proses PO			2.9	Defined

b. Proses AI (*Acquisition and Implementation*).

Hasil pengujian yang dilakukan pada proses AI (*Acquisition and*

Implementation) memiliki rata-rata nilai **3** dan *maturity level* berada diposisi **Defined**.

Tabel 5. Hasil Pengujian Pada Proses AI (*Acquisition and Implementation*).

No	Kode	Proses	Hasil Pengujian	Tingkat Maturity
1	AI6	Manage Change	3	Defined
Rata-rata proses AI			3	Defined

c. Proses DS (*Delivery and Support*).

Hasil pengujian yang dilakukan pada proses DS (*Delivery and*

Support) memiliki rata-rata nilai **2.5** dan *maturity level* berada diposisi **Repeatable**.

Tabel 6. Hasil Pengujian Pada Proses DS (*Delivery and Support*).

No	Kode	Proses	Hasil Pengujian	Tingkat Maturity
1	DS5	Ensure System and Security	2.44	Repeatable
2	DS11	Manage Data	2.67	Defined
Rata-rata proses DS			2.5	Repeatable

d. Proses ME (*Monitoring and Evaluation*).

Hasil pengujian yang dilakukan pada proses ME (*Monitoring and Evaluation*) memiliki rata-rata

nilai 3 dan maturity level berada diposisi *Defined*.

Tabel 7. Hasil Pengujian Pada Proses ME (*Monitoring and Evaluation*).

No	Kode	Proses	Hasil Pengujian	Tingkat Maturity
1	ME1	Monitor and Evaluate IT Performance	3	Defined
Rata-rata proses ME			3	Defined

3. Pemetaan *Maturity Level*.

Berdasarkan target yang ingin dicapai oleh perusahaan XYZ, maka diperoleh sejumlah penilaian dengan mempertimbangkan kapasitas sumber daya yang dimiliki. Tabel 8

ini akan menjelaskan mengenai perbandingan perolehan *maturity level* yang diperoleh perusahaan saat ini dengan target yang ingin dicapai oleh perusahaan XYZ.

Tabel 8. Pemetaan *Maturity Level*.

Domain	Maturity Level		
	Sekarang	Target	GAP
PO (<i>Planning and Organisation</i>)	2.9	3.5	0.6
AI (<i>Acquisition and Implementation</i>)	3	3.5	0.5
DS (<i>Delivery and Support</i>)	2.5	3.5	1
ME (<i>Monitoring and Evaluation</i>)	3	3.5	0.5
Rata-Rata	2.85	3.5	0.65

Berikut ini kondisi *maturity level* pada perusahaan XYZ dilihat dari hasil pemetaan *maturity level* :



Gambar 4. Kondisi *Maturity Level*

Keterangan :

◆ : Merupakan posisi perusahaan saat ini

● : Merupakan target perusahaan

Berdasarkan hasil perhitungan *maturity level* pada Tabel 8, perusahaan XYZ berada pada posisi

level 2,85 yaitu *Defined*. Dilihat dari hasil *maturity level* yang didapat masih ada beberapa hal yang belum sepenuhnya mencapai target sesuai dengan keinginan perusahaan. Target yang sesuai dengan keinginan perusahaan yaitu 3,5 untuk setiap domain proses.

Hal ini menyebabkan munculnya *gap* sebesar 0,65 dari keseluruhan domain proses, dikarenakan masih terdapat prosedur yang sama dan diikuti oleh individu yang berbeda dalam proses pengerjaan tugas yang sama.

4. Rekomendasi.

Setelah diketahui bahwa perusahaan berada pada level 3 (*Defined*), selanjutnya bisa diajukan beberapa rekomendasi berdasarkan proses yang terdapat pada COBIT untuk membawa perusahaan menuju level yang lebih tinggi sesuai yang ditargetkan oleh perusahaan. Dari hasil penilaian *maturity level*, pada dasarnya sudah baik hanya perlu peningkatan, sebagai berikut :

a. Rekomendasi untuk proses PO1.

Memiliki alur proses yang baik dalam menentukan penggunaan sumber daya internal maupun eksternal untuk pengembangan dan pengoperasian suatu sistem.

b. Rekomendasi untuk proses PO9.

Dapat menganalisis resiko khusus pada suatu kerangka kerja proyek yang terkait dengan teknologi informasi.

Mengadakan training kepada semua staff perusahaan XYZ.

c. Rekomendasi untuk AI6.

Setiap proses atau aktivitas yang terjadi diperusahaan, harus memiliki dokumentasi yang lengkap dan akurat.

Meningkatkan koordinasi antara manajemen perubahan teknologi informasi dan proses desain ulang bisnis.

d. Rekomendasi untuk DS5.

Manager teknologi informasi beserta divisi teknologi informasi

mengelola dan menangani keamanan teknologi informasi dengan cepat.

Menganalisis kebutuhan bisnis, resiko dan keamanan teknologi informasi secara menyeluruh.

e. Rekomendasi untuk DS11.

Melakukan backup dan restore data, sesuai dengan kebutuhan bisnis.

Melakukan pengujian terhadap media backup dan proses restorasi data.

f. Rekomendasi untuk ME1.

Membuat kerangka kerja untuk menentukan scope perusahaan, mengukur solusi dan pelayanan teknologi informasi.

Memantau kontribusi teknologi informasi untuk bisnis perusahaan.

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan pada perusahaan XYZ dapat ditarik kesimpulan, sebagai berikut :

1. Pada hasil perhitungan *maturity level* perusahaan XYZ berada pada level 3 (*Define*), sedangkan target yang diinginkan oleh perusahaan XYZ yaitu dilevel 4 (*Managed*). Dilihat dari perbedaan tersebut terdapat *gap* antara level yang didapat dengan level yang diinginkan.
2. Pada dasarnya kinerja perusahaan sudah baik, hanya perlu ditingkatkan saja kewaspadaan terhadap resiko yang terjadi didalam perusahaan.
3. Menjalankan fungsi pengawasan, pelaporan dan evaluasi terhadap resiko yang terjadi diperusahaan, agar resiko tinggi yang akan terjadi diperusahaan dapat diminimalisir secepat mungkin.
4. Memfasilitasi setiap karyawan yang bertanggung jawab pada setiap proses penerapan teknologi informasi

mendapatkan knowledge sharing supaya memiliki tingkat penguasaan sistem yang sama.

DAFTAR PUSTAKA

- [1] Heru Nugroho, “Analisis Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1”, Konferensi Nasional ICT-M Politeknik Telkom (KNIP), Politeknik Telkom, 2012.
- [2] Arif Dwi Laksito, Kusri, Emha Taufiq Luthfi., “Pengukuran Tingkat Model Kematangan Proses COBIT Menggunakan Aplikasi Berbasis Web”, Seminar Nasional Teknologi Informasi dan Multimedia, STMIK AMIKOM Yogyakarta, 2013.
- [3] Trivina Ayu Megawati, Hnim Maria Astuti, Anisah Herdiyanti., “Pengelolaan Risiko Aset Teknologi Informasi Pada Perusahaan Properti PT XYZ, Tangerang Berdasarkan Kerangka Kerja COBIT 4.1”, Seminar Nasional Sistem Informasi Indonesia, Institut Teknologi Sepuluh Nopember, Surabaya, 2014.
- [4] IT Governance Institute ,”COBIT 4.1”, ISACA, USA, 2007.