Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 2, No. 1, Januari 2018, hlm. 91-100 http://j-ptiik.ub.ac.id

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)

Nurfitri Zukhrufatul Firdaus[1], Suprapto[2]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]fitri.firdaus0@gmail.com, [2]spttif@ub.ac.id

Abstrak

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Petrokimia Gresik untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Petrokimia Gresik menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level*, analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik.

Kata kunci: *COBIT 5, capability level, manajemen risiko, analisis gap, risk assessment, mitigasi risiko*

Abstract

SAP (System Application and Product in Data Processing) is a type of ERP Software that used by PT. Petrokimia Gresik to support business process automation and support decision-making process to be more effective and efficient. To anticipate the potential problems that might obstruct business processes at the company, so PT. Petrokimia Gresik managed to use risk management based on the standards of ISO 31000:2009. An evaluation on the implementation of IT risk management was done to measure its capability level accomplishment. COBIT 5 Framework, especially in process domain APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation), was used as the basis of the evaluation. To collect accurate data, the data were obtained by filling evaluation worksheet, conducting a direct observation and an interview to the people in charge. The process of evaluating the implementation of IT risk management consists of several stages, including capability level analysis, gap analysis and risk assessment analysis to identify potential risks and assess the extent of the impacts of each risk. From the evaluation result, it turned out that capability level for process domain EDM03 was on level 2 and on level 3 for process domain APO12 and 16 mitigation strategy and 9 recommendation were made to support the improvement for the implementation of risk management information and technology at PT. Petrokimia Gresik.

Keywords: *COBIT 5, capability level, risk management, gap analysis, risk assessment, risk mitigation*

1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Petrokimia Gresik. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Petrokimia Gresik menerapkan sistem ERP – SAP yang terdiri dari sepuluh

modul. Disamping itu PT. Petrokimia Gresik juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Petrokimia Gresik telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003.

Padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh karena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Petrokimia Gresik. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi manajemen risiko Teknologi Informasi (TI) pada PT. Petrokimia Gresik adalah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

2. LANDASAN KEPUSTAKAAN

2.1. Kajian Pustaka

Adapun penelitian – penelitian terdahulu yang relevan dengan penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan oleh Astri Dyahaloka yang berjudul "Evaluasi Manajemen Risikio *E-Procurement* Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Pertamina (Persero))". Penelitian tersebut menggunakan kerangka kerja COBIT 5 dengan domain EDM03 dan APO12. Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *capability level*, analisis *gap* dan analisis SWOT, sehingga menghasilkan nilai *capability level* yang telah dicapai dan rekomendasi untuk perbaikan penerapan manajemen risiko.
2. Penelitian yang dilakukan oleh Sigit Samaptoaji yang berjudul "Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri". Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *risk assessment* dan penentuan strategi atau langkah mitigasi, sehingga menghasilkan dokumen profil risiko teknologi informasi yang dapat dijadikan sebagai masukan atau pertimbangan dalam proses pengambilan keputusan.

2.2 Manajemen Risiko

Djojosoedarso (2003) menjelaskan bahwa manajemen risiko merupakan proses menjalankan aktivitas manajemen untuk menanggulangi munculnya risiko, baik yang dihadapi perusahaan maupun yang dihadapi oleh masyarakat. Sehingga dapat disimpulkan bahwa fungsi – fungsi manajemen yang dijalankan untuk menanggulangi risiko mencakup proses pengelolaan, pengukuran dan penilaian risiko. Dalam hal ini manajemen risiko dimaksudkan untuk mengurangi dampak negatif dari suatu risiko, menghindari terjadinya risiko, menampung sebagian atau keseluruhan dari konsekuensi risiko atau mengalihkan risiko kepada pihak lain.

2.3. COBIT 5

Control Objective for Information and Related Technology (COBIT) merupakan seperangkat pedoman dan hasil dokumentasi yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT

dikembangkan untuk menerapkan *Governance of Enterprise IT*. Versi terbaru yang dikeluarkan oleh *IT Governance Institute* dikenal sebagai COBIT 5. COBIT 5 terbentuk dengan mengintegrasikan Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

Dalam melakukan evaluasi, ISACA (2012) menjelaskan bahwa terdapat tujuh buah tahapan yang harus diterapkan menurut siklus implementasi COBIT 5, antara lain:

1. *Initiate Programme*, yaitu proses identifikasi pemicu perubahan seperti kondisi trend, kinerja, implementasi perangkat lunak, isu penting dan tujuan organisasi yang mampu memberikan dorongan untuk berubah.
2. *Define Problems and Opportunities*, yaitu proses penyelarasan antara tujuan penerapan TI dengan risiko maupun strategi organisasi, serta mengutamakan tujuan penerapan TI, tujuan organisasi dan proses penerapan TI yang paling utama.
3. *Define Road Map*, yaitu proses penetapan target untuk meningkatkan upaya perbaikan dan diikuti dengan analisis *gap* untuk menentukan beberapa solusi potensial.
4. *Plan Programme*, yaitu proses perencanaan solusi yang dianggap layak untuk dijalankan.
5. *Execute Plan*, yaitu proses penerapan solusi yang telah disarankan ke dalam aktivitas keseharian serta melakukan pemantauan untuk memastikan bahwa keselarasan bisnis dapat dicapai dan kinerja dapat diukur.
6. *Realise Benefits*, yaitu proses transisi secara berkelanjutan dengan menerapkan praktik tata kelola atau manajemen yang telah ditingkatkan ke dalam proses bisnis dan memantau perkembangannya dengan memetakannya pada matriks berdasarkan kinerja dan manfaat yang ingin diperoleh.
7. *Review Effectiveness*, yaitu proses evaluasi keberhasilan yang telah dicapai secara umum, kemudian melakukan identifikasi segala kebutuhan perbaikan secara berkala untuk lebih meningkatkan praktik tata kelola atau manajemen.

Menurut ISACA (2012), COBIT 5 telah menyediakan dua proses yang berkaitan dengan penerapan manajemen risiko, antara lain:

1. EDM03 : *Ensure Risk Optimisation*
   Proses EDM03 bertujuan untuk memastikan apakah tingkat risiko dan besarnya toleransi yang dapat diterima oleh perusahaan telah dimengerti, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko – risiko yang terkait dengan Teknologi Informasi (TI) telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terbagi menjadi 3 atribut, yaitu *Evaluate Risk Management*, *Direct Risk Management* dan *Monitor Risk Management.*
2. APO12 : *Manage Risk*
   Proses APO12 bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan teknologi Informasi (TI) agar tidak melebihi batas toleransi yang telah ditentukan oleh manajemen eksekutif organisasi. Selain itu proses APO12 juga bertujuan untuk mengintegrasikan manajamen risiko Teknologi Informasi (TI) dengan manajemen risiko perusahaan (ERM). Proses APO12 terbagi menjadi enam subdomain, yaitu *Collect Data*, *Analyse Risk*, *Maintain A Risk Profile*, *Articulate Risk*, *Define a Risk Management Action Portofolio* dan *Respond to Risk*

Penilaian *Capability Level* untuk setiap proses tersebut digolongkan menjadi enam tingkatan, yaitu Level 0 (*Incomplete Process*), Level 1 (*Performed Process*), Level 2 (*Managed process*), Level 3 (*Established Process*), Level 4 (*Predictable process*) dan Level 5 (*Optimized process*).

2.4. *Risk Assessment*

ISACA (2012) menjelaskan bahwa Secara umum *Risk Assessment* berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari *internal* maupun *eksternal* organisasi, selain itu juga menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Besarnya dampak dapat diukur melalui penilaian *Inherent Risk* dan *Residual Risk*, serta dianalisis melalui dua perspektif antara lain *Probability/Likelihood* dan *Impact/Consequence*.

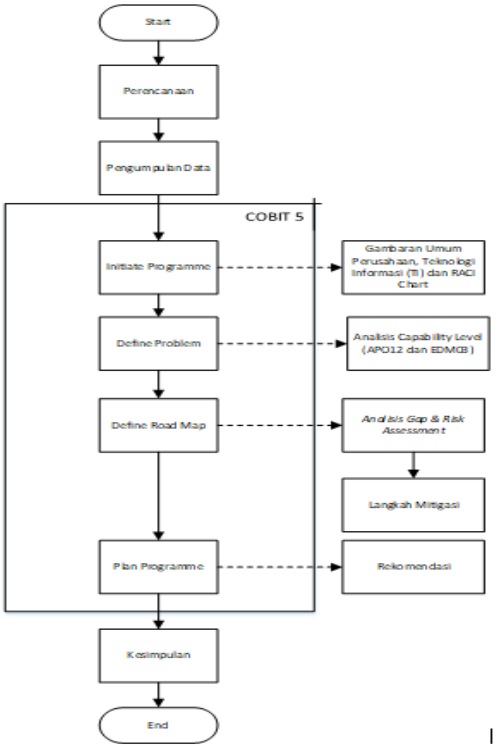
Untuk menyelaraskan antara risiko - risiko yang ditemukan dengan batas toleransi risiko yang telah ditentukan oleh organisasi, maka diperlukan adanya *Risk Response* atau Respon Risiko. Dalam penelitian ini, langkah yang diambil untuk merespon risiko adalah dengan melakukan *Risk Reduction* atau *Mitigation*, yaitu salah satu metode yang dilakukan dengan cara mengurangi besarnya *Probability* atau

Likelihood (Peluang atau kecenderungan) dan *Impact* atau *Consequence* (Dampak) yang ditimbulkan dari risiko tersebut.

2.5. Sistem ERP – SAP

System Application and Product in Data Processing (SAP) merupakan *software* jenis *Enterprise Resources Planning* (ERP) yang dikembangkan untuk menunjang jalannya kegiatan operasional suatu organisasi agar lebih efektif dan efisien. Adapun modul – modul SAP yang diimplementasikan di PT. Petrokimia Gresik antara lain *Material Management, Production Planning, Plant Maintenance, Sales Distribution, Financial Accounting Controlling, Human Capital Management, Quality Management, Fund Management, Business Planning and Consolidation* dan *Dashboard*.

3. METODOLOGI



Gambar 1. Diagram Alur Penelitian

1. Menentukan objek penelitian dan kerangka kerja yang tepat serta menggali informasi yang terkait**.**
2. Melakukan pengumpulan data, baik data primer maupun data sekunder dengan cara melakukan pengisian lembar kerja evaluasi, melakukan observasi langsung, melakukan wawancara dengan pihak – pihak yang berwenang dan studi kepustakaan.
3. Mendeskripsikan gambaran umum mengenai kondisi umum organisasi, visi dan misi sebagai tujuan organisasi, gambaran umum sistem informasi atau teknologi informasi yang diterapkan dan pihak – pihak yang bertanggung jawab dalam penerapan manajemen risiko berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *Gap Analysis*, *Risk Assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi perusahaan berdasarkan data yang diperoleh dari hasil lembar kerja evaluasi, observasi dan wawancara.
6. Membuat rekomendasi untuk menentukan solusi potensial berdasarkan hasil analisis *Capability Level*, *Gap Analysis* dan *Risk Assessment*.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah - langkah yang telah dilalui dalam melakukan penelitian.

4. HASIL

4.1. Hasil Lembar Kerja Evaluasi

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi lembar kerja evaluasi adalah sejumlah tiga orang, antara lain Manager Dept. TEKINFO, Kabag. Infrastruktur TEKINFO dan Manager Dept. TKP & MR.

Tabel 1. Rekapitulasi Hasil Lembar Kerja Evaluasi

Prosess Assesment Results							
Nama Proses	***Proces Capability Level***						**Total Responden**
	0	**1**	**2**	**3**	**4**	**5**	
Evaluate, Direct, and Monitoring							
EDM03	0	0	3	0	0	0	3
Align, Plan, and Organise (APO)							
APO12	0	0	0	3	0	0	3

Dari Tabel 1 diatas, dapat diketahui bahwa hasil pengisian lembar kerja evaluasi yang dilakukan oleh tiga orang responden menunjukkan nilai *Capability Level* terkait proses EDM03 berada pada Level 2 dan nilai *Capability Level* terkait proses APO12 berada pada Level 3.

4.2. Hasil Observasi dan Wawancara

Dalam mengelola proses bisnis perusahaan, PT. Petrokimia Gresik telah mendukung penerapan sistem yang bernama ERP-SAP. Sistem tersebut diharapkan mampu

mengintegrasikan seluruh proses bisnis yang ada pada perusahaan dan mensinergiskan proses bisnis dari masing – masing anggota Pupuk Indonesia *Holding Company* (PIHC). Dalam hal ini, pihak yang bertanggung jawab mendukung jalannya Sistem ERP-SAP, mengintegrasikan sistem atau aplikasi yang dibuat sendiri dengan Sistem ERP-SAP, serta meningkatkan kualitas SDM untuk mendukung penerapan Sistem ERP-SAP adalah Departemen TEKINFO.

Dalam penerapan Sistem ERP – SAP tersebut, tidak pernah lepas dari suatu risiko. Oleh karena itu untuk mengelola segala bentuk risiko perusahaan, Departemen TKP & MR telah menerapkan manajemen risiko berdasarkan standart dan kebijakan yang ditetapkan yaitu ISO 31000 : 2009. Standart dan kebijakan tersebut tertuang dalam dokumen Kebijakan Manajemen Risiko, Pedoman Penerapan Manajemen Risiko, Prosedeur Penerapan Manajeen Risiko, Panduan Penilaian Penerapan Manajemen Risiko dan Pedoman Manajemen Risiko PT. Pupuk Indonesia (Persero). Selama ini penerapan manajemen risiko pada PT. Petrokimia Gresik dimulai dengan melakukan identifikasi terhadap semua risiko yang muncul, menganalisis setiap risiko yang telah diidentifikasi, mengevaluasi setiap risiko, melakukan pengendalian dan penanganan risiko serta melakukan monitoring dan review terhadap pengendalian dan penanganan. Selanjutnya hasil dari aktivitas pengelolaan risiko tersebut disusun dalam sebuah dokumen yang bernama Profil Risiko PT. Petrokimia Gresik.

Dalam mengelola setiap risiko perusahaan, Departemen TKP & MR memiliki aplikasi yang bernama SIMAR (Sistem Informasi Manajemen Risiko) dan program kerja yang bernama Klinik Risiko. Dengan adanya aplikasi SIMAR dan program Klinik Risiko tersebut, dapat memudahkan Departemen TKP & MR dalam memantau penerapan manajemen risiko pada setiap unit kerja.

4.3. Hasil Temuan

Berdasarkan hasil lembar kerja evaluasi, observasi dan proses wawancara dengan pihak Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik, didapatkan beberapa temuan berikut:

1. Adanya layanan Tata Kelola Perusahaan dan Manajemen Risiko pada PT. Petrokimia Gresik, namun belum adanya manajemen atau team yang dibentuk secara khusus untuk mengelola segala macam risiko terkait dengan teknologi informasi.
2. Pengelolaan risiko yang dilakukan oleh Departemen TKP & MR pada PT. Petrokimia Gresik masih secara umum yaitu dilakukan pada seluruh unit kerja perusahaan dan belum berfokus secara spesifik pada penerapan teknologi informasi.
3. Tidak semua risiko teknologi informasi telah didokumentasikan dan dikelola dengan baik.
4. Belum secara penuh memantau kesesuaian seluruh risiko yang dikelola dengan risk appetite.
5. Dalam melakukan analisis risiko tersebut, belum disertai dengan analisis *cost benefit* yaitu perkiraan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan penanganan setiap skenario risiko.

5. PEMBAHASAN

5.1. Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada Level 3. Hal tersebut dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2. Rekapitulasi Hasil Gap Analysis

Nama Proses	Level Saat Ini	Level Target	*Gap*
EDM03	2	3	1
APO12	3	4	1

5.2. Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

5.3. *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

Risk Analysis bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*.

Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel 3 berikut ini.

Tabel 3. Rekapitulasi Berdasarkan Skenario Risiko

No	Skenario Risiko	Jumlah *Risk Issue*
1	*New Technology*	1
2	*Software Implementation*	2
3	*Destruction of Infrastructure*	1
4	*IT Staff*	1
5	*IT Expertise and Skills*	2
6	*Software Integrity*	2
7	*Infrastructure (Hardware)*	3
8	*System Capacity*	2
9	*Malware*	1
10	*Logical Attacks*	1
11	*Utilities Performance*	1
12	*Data(base) Integrity*	2
13	*Logical Trespassing*	1
14	*Operational IT Errors*	2
15	*Acts of Nature*	1
	Total	23

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel 4 berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

No	Kategori Aset	Jumlah *Risk Issue*	Persentase
1	Aplikasi	5	21,74 %
2	Fasilitas	1	4,35 %
3	Infrastruktur TI	3	13,04 %
4	Informasi / Data	7	30,43 %
5	Proses	4	17,39 %
6	SDM	3	13,04 %
	Total	23	100 %

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 5 berikut ini.

Tabel 5. Penilaian *Inherent Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	0	0	4	0	1
2	Fasilitas	0	0	1	0	0
3	Infrastruktur TI	0	1	2	0	0
4	Informasi / Data	0	0	5	2	0
5	Proses	0	0	4	0	0
6	SDM	0	0	2	1	0
	Total	0	1	18	3	1

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 6 berikut ini.

Tabel 6. Penilaian *Residual Risk* Berdasarkan Aset

No	Kategori Aset	Nilai Risiko Dasar				
		Rendah	Rendah Menengah	Menengah	Menengah Tinggi	Tinggi
1	Aplikasi	4	0	1	0	0
2	Fasilitas	1	0	0	0	0
3	Infrastruktur TI	3	0	0	0	0
4	Informasi / Data	5	0	2	0	0
5	Proses	3	1	0	0	0
6	SDM	1	0	2	0	0
	Total	17	1	5	0	0

2. *Risk Evaluation*

Risk Evaluation bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk

mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel 7 berikut ini.

Tabel 7. *Risk Map*

Impact							
	Sangat Besar (5)	0	0	0	0	0	0
	Besar (4)	0	0	0	0	0	0
	Sedang (3)	1	0	0	0	0	1
	Kecil (2)	11	5	0	0	0	16
	Sangat Kecil (1)	3	3	0	0	0	6
	Total	15	8	0	0	0	23
		Sangat Jarang (1)	**Jarang (2)**	**Kadang-kadang (3)**	**Sering (4)**	**Sangat Sering (5)**	**Total**
		Probability					

Berdasarkan Tabel 7 di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

5.4. Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology*, 1 *Risk Issue* yang termasuk dalam *System Capacity*, 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Petrokimia Gresik dalam menyikapi beberapa *Risk Issue* dapat dilihat pada Tabel 8 sampai Tabel 11 berikut ini.

Tabel 8. Langkah Mitigasi *New Technology*

Risiko	Langkah Mitigasi
1. Permintaan aplikasi diluar modul SAP tidak terpenuhi.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi. - Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini. - Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi. - Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu.

Tabel 9. Langkah Mitigasi *System Capacity*

Risiko	Langkah Mitigasi
1. Operasional SAP lambat dan kurang optimal	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP. - Mengadakan *User Licence* pada setiap unit kerja.

Tabel 10. Langkah Mitigasi *Data(base) Integrity*

Risiko	Langkah Mitigasi
1. Gangguan komunikasi data antara PG dengan PIHC. 2. Gangguan transmisi data antar departemen.	- Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data. - Menjalin kerja sama dengan Team IT dari PIHC. - Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera. - Menggunakan teknik *outomatic switch* jika terjadi *failure.*

Tabel 11. Langkah Mitigasi *IT Expertise and Skills*

Risiko	Langkah Mitigasi
1. Dukungan teknis dari Team IT kurang optimal. 2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT	- Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP. - Memperbaiki pola rekruitmen dan pelatihan SDM. - Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT. - Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT. - Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP. - Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan.

5.5.Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko teknologi informasi PT. Petrokimia Gresik dengan menggunakan analisis *capability level* dan *risk assessment* (Penilaian Risiko), disusunlah beberapa rekomendasi yang dapat digunakan untuk mengembangkan dan memperbaiki penerapan manajemen risiko teknologi informasi serta mengurangi terjadinya risiko teknologi informasi di PT. Petrokimia Gresik. Berikut ini adalah hasil rekomendasi yang telah dibuat berdasarkan domain proses EDM03 dan APO12. Berikut ini merupakan hasil rekomendasi yang diberikan kepada PT. Petrokimia Gresik:

1. Membentuk *team* atau manajemen khusus di bawah naungan Departemen TKP & MR yang bertugas untuk mengelola dan mengkoordinasikan penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
2. Melakukan evaluasi terhadap kinerja staff serta memberikan pelatihan terkait penerapan manajemen risiko teknologi informasi untuk meningkatkan kompetensi SDM.
3. Membuat dokumen tertulis yang fokus membahas mengenai pedoman dan prosedur penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
4. Menetapkan metode yang tepat untuk memonitoring penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik sehingga dapat memantau kesesuaian antara risiko yang ditemukan dengan *Risk Appetite.*
5. Membuat dokumen tertulis yang membahas mengenai mitigasi risiko, *Business continuity Plan*, *Disaster Recovery Plan*, dan *risk respond* dari seluruh risiko terkait dengan penerapan teknologi informasi.
6. Membuat dokumen tertulis yang membahas mengenai *Cost Benefit Analysis* untuk memperkirakan frekuensi besarnya kerugian dan keuntungan yang harus ditanggung ketika melakukan penanganan pada setiap skenario risiko teknologi informasi.
7. Meningkatkan intensitas kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi melalui program Klinik Risiko dan Kajian Ulang Manajemen Risiko.
8. Membuat dokumen tertulis yang berbentuk seperti Profil Risiko namun secara khusus menampung hasil identifikasi risiko, analisis risiko (baik berupa analisis sumber, penyebab dan akibat dari risiko), evaluasi penilaian risiko dan pengendalian atau penanganan risiko terkait dengan risiko teknologi informasi.
9. Mengoptimalkan penggunaan Sistem Informasi Manajemen Risiko (SIMAR) dalam melakukan pengelolaan risiko teknologi informasi

6. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik, maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process.*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Petrokimia Gresik adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko,

diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

7. DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. *Prinsip-Prinsip Manajemen Risiko dan Asuransi*, Edisi Pertama, Jakarta: Salemba Empat.

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)).* Malang : Universitas Brawijaya.

Febriyanti, Aulia., and Bekti C.H, S.Si., M.Kom., 2012. *Manajemen Risiko pada Pengelolaan Data di Bagian Pengolahan Data PT. Petrokimia Gresik. Jurnal Teknik POMITS,* 1(1), pp 1-6. Tersedia di: <http://digilib.its.ac.id> [Diakses 26 Januari 2017]

Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

ITGI., 2003. *Broad Briefing on IT Governance 2nd Edition*. [e-book]. Rolling Meadows : IT Governance Institute.

Petrokimia Gresik, 2012. *Profil.* [Online] Tersedia di : <http://www.petrokimia-gresik.com/> [Diakses 11 Juli 2016].

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung. Tersedia di : <http://www.academia.edu/> [Diakses 6 Oktober 2016].

Pressman, Roger S., 2005. *Software*

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta). SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL). Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2). Tersedia di: <http:// http://jutisi.maranatha.edu/index.php/jutisi> [Diakses 6 Oktober 2016]

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia. Tersedia di: <http://lib.ui.ac.id> [Diakses 29 Maret 2017]

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1. No. 1. Tersedia di: <http:// http://www.jurnal.uii.ac.id/index.php> [Diakses 24 September 2016]

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.