PENILAIAN KAPABILITAS PENERAPAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5

(Studi Pada PDAM Kota Malang Jawa Timur)

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Yani Iriana Putri
NIM: 145150401111029

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2018

PENGESAHAN

PENILAIAN KAPABILITAS PENERAPAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5
(STUDI PADA PDAM KOTA MALANG JAWA TIMUR)

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Yani Iriana Putri
NIM: 145150401111029

Skripsi ini telah diuji dan dinyatakan lulus pada
04 Juni 2018
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Suprapto, S.T, M.T	Admaja Dwi Herlambang, S.Pd., M. Pd.
NIP: 19710727 199603 1 001	NIK: 2016098908021001

Mengetahui
Ketua Jurusan Sistem Informasi

Dr. Eng. Herman Tolle, S.T, M.T
NIP: 19740823 200012 1 001

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata di dalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 04 Juni 2018

Yani Iriana Putri

NIM: 145150401111029

DAFTAR RIWAYAT HIDUP

PENDIDIKAN

2003-2009	SDN. PB Kelapa Dua Tangerang
2000-2011	SMP Negeri 1 Kelapa Dua Kab. Tangerang
2011-2014	SMA Negeri 6 Kota Tangerang
2014-2018	Universitas Brawijaya, Fakultas Ilmu Komputer

PENGALAMAN

Periode 2015-2016	Eksekutif Mahasiswa Sistem Informasi (EMSI)
	Staff Departemen Pengembangan dan Penelitian Studi

KEPANITIAAN

2014	Ketua Divisi Konsumsi Inaugurasi Mahasiswa FILKOM 2014
2015	Anggota Divisi Acara Database Study Club for Exam
2015	Bendahara Road to PKM
2016	Ketua Pelaksana CRYSTAL 2K15 (Basic Programming with Accompanied Learn for 2015)
2016	Lean Organizer (LO) ICACSIS 2016 (2016 International Conference on Advanced Computer Science and Information Systems)
2016	Anggota Divisi Dana dan Usaha i-FEST 3.0 (National Innovation Festival 3.0)

PENGHARGAAN

2015	Juara 1 Lomba Badminton Ganda Campuran Olimpiade PTIIK 2015
2015	Juara 1 Lomba Badminton Tunggal Putri Olimpiade PTIIK 2015
2015	Juara 1 Lomba Grand Desain ISINDO 2015
2015	Juara 3 Lomba Bulutangkis Ganda Putri Olimpiade Brawijaya 2015
2015	Juara 3 Lomba Bulutangkis Ganda Campuran Olimpiade Brawijaya 2015

KATA PENGANTAR

Puji syukur penulis penjatkan kepada Tuhan Yang Maha Esa, karena berkat rahmat dan ridho-Nya penulis mampu menyelesaikan tugas akhir atau skripsi yang berjudul "Penilaian Kapabilitas Penerapan Manajemen Risiko Menggunakan Kerangka Kerja COBIT 5 (Studi Pada PDAM Kota Malang Jawa Timur)" dengan baik dan tepat waktu.

Dalam penyusunannya tentunya tidak terlepas dari dukungan, bimbingan serta doa dari berbagai pihak. Oleh karena itu, penulis menyampaikan banyak terimakasih kepada:

1. Wayan Firdaus Mahmudy, S.Si, M.T., Ph.D. selaku Dekan Fakultas Ilmu Komputer Universitas Brawijaya.
2. Dr. Eng. Herman Tolle, S.T., M.T. selaku Ketua Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
3. Suprapto, S.T., M.T. selaku Ketua Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
4. Suprapto, S.T., M.T. selaku Dosen Pembimbing I.
5. Admaja Dwi Herlambang, S.Pd., M. Pd. selaku Dosen Pembimbing II.
6. Bapak Rusdiyanto dan Ibu Harmini selaku orang tua dari penulis.
7. Pihak lain yang tidak dapat disebutkan satu-persatu.

Semoga semua saran, dukungan, ilmu, serta bantuan baik dari semua mendapatkan balasan yang setimpal dari Tuhan Yang Maha Esa. Dengan segala kerendahan hati, penulis menyadari bahwa dalam skripsi ini masih terdapat kekurangan dan jauh dari kata sempurna. Oleh karena itu, penulis mengharapkan kritik serta saran yang membangun demi penyempurnaan skripsi ini. Semoga skripsi ini dapat bermanfaat dan berguna di masa depan.

Malang, 04 Juni 2018

Penulis

irianapuput@gmail.com

ABSTRAK

Yani Iriana Putri, Penilaian Kapabilitas Penerapan Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Pada PDAM Kota Malang Jawa Timur)

Dosen pembimbing: Suprapto, S.T, M.T dan Admaja Dwi Herlambang, S.Pd., M. Pd.

Sasaran PDAM Kota Malang yaitu memanfaatan teknologi informasi yang efektif. Sehingga perusahaan memiliki prioritas tentang peningkatan kehandalan sistem informasi manajemen, perbaikan sistem layanan, pengelolaan data pelanggan dan pengembangan serta implementasi aplikasi. Untuk mengukur penerapan manajemen risiko, dilakukan penilaian terhadap tingkat kapabilitas dari proses EDM03 (optimasi risiko), APO12 (pengelolaan risiko) dan APO13 (pengelolaan keamanan) dengan menggunakan kerangka kerja COBIT 5. Dalam penelitian ini melakukan tahapan *self assessment.* Mulai dari pemilihan proses yang akan dinilai, penilaian untuk level 1, penilaian untuk level 2-5, merekam semua hasil penilaian, analisis *gap* dan pembuatan rekomendasi. Hasil tingkat kapabilitas didapatkan melalui beberapa metode, yaitu wawancara, observasi dan lembar penilaian. Rekomendasi disusun setelah mengetahui kesenjagan antara *targeted level* dengan *capability level* saat ini. Rekomendasi diharapkan mampu membantu perusahaan dalam mencapai *targeted level* yaitu pada proses EDM03, APO12 dan APO13 di mana ketiga proses ini berada pada *capability level* 1 dan untuk *targeted level* yaitu pada *level* 2. Sehingga, kesenjangan dari ketiga *subdomain* yaitu sebesar 1. Rekomendasi bagi perusahaan yaitu terkait dokumen masing-masing proses yang harus diperbaiki, melakukan analisis lebih lanjut untuk mengetahui kemungkinan yang terjadi di masa depan, pembentukan tim khusus manajemen risiko dan keamanan, pemisahan tugas dan tanggung jawab, hingga penentuan metode untuk kontrol masing-masing proses.

Kata Kunci: Tingkat kapabilitas, manajemen risiko, manajemen keamanan, COBIT 5

ABSTRACT

Yani Iriana Putri, ***Capability Assessment of Application Information Technology Risk Management Using COBIT 5 Framework (A Case Study on PDAM Kota Malang Jawa Timur)***

***Supervisors*: Suprapto, S.T, M.T and Admaja Dwi Herlambang, S.Pd., M. Pd.**

PDAM Kota Malang's target is utilizing an effective information technology. Therefore, the company has priority on improving the reliability of information system management, service system, customer data management, development, and implementation of the applications. In order to measure the implementation of risk management, an assessment has been done to capability level of the EDM03 subdomain (ensure risk optimization), APO12 (manage risk), and APO13 (manage security) using COBIT 5 Framework. In this research, self-assessment is implemented. This methodology started with choosing the processes to be assessed, assessing for level 1 to 5, recording all of the assessment results, analyzing gap, and making recommendations. The result of capability level is obtained through several methods, there are viz. interviews, observation, and self-assessment worksheet. Recommendations were expected to assist the company in achieving the targeted level in EDM03, APO12, and APO13 processes. These three processes were in capability level 1. Meanwhile, the targeted level is in level 2. Thus, the gap between the three subdomains is 1. Recommendations for the company are related to documents of each process which need to be improved. Further analysis is done to know the possibility that will occur in the future, establishing a special team for risk and security management, separation of duties and responsibilities, and determining methods to control each process.

Keyword: capability level, risk management, security management, COBIT 5

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1 PENDAHULUAN

1.1 Latar belakang

PDAM Kota Malang merupakan salah satu dari Badan Usaha Milik Daerah (BUMD) yang telah menerapkan teknologi informasi dalam menjalankan segala bentuk kegiatan perusahaan. PDAM Kota Malang telah berkomitmen bahwa dalam menjalankan seluruh proses bisnis, akan didukung dengan teknologi informasi dan komunikasi yang memadai. Pemanfaatan ini merupakan upaya dari perusahaan untuk mewujudkan optimalisasi performa kinerja operasional perusahaan. Sehingga diharapkan dengan menerapkan teknologi informasi, perusahaan akan mampu memanfaatkan sumber daya yang ada secara maksimal. Penerapan teknologi informasi ini juga mampu mendukung gerakan hemat kertas *(paperless)* pada perusahaan. Salah satu sasaran perusahaan yaitu pemanfaatan teknologi informasi yang efektif. Artinya, mampu memberikan dampak yang berguna dan memberikan keuntungan serta kemudahan dalam proses bisnis yang diterapkan diseluruh bagian organisasi. Dalam salah satu strategi umum perusahaan, yaitu meningkatkan kehandalan *hardware* sistem informasi manajemen dan pengembangan serta implementasi aplikasi. Tentunya dengan strategi umum TI yang ditentukan harus didukung dengan bagaimana *software* dan *hardware* mampu berkontribusi dalam penanganan masalah yang diakibatkan dari penggunaan teknologi informasi. Sehingga, pemanfaatan teknologi informasi mampu memberikan pertahanan lebih kepada perusahaan dalam menjalani segala proses bisnisnya.

Strategi umum lainnya, yaitu terkait *improvement* atau perbaikan yang dilakukan oleh perusahaan. Salah satunya, perbaikan sistem layanan, perbaikan sistem pengelolaan data pelanggan, perbaikan sistem penanganan pengaduan dan perbaikan dan penyediaan fasilitas. Perbaikan sistem layanan, perbaikan sistem pengelolaan data pelanggan dan perbaikan sistem penanganan pengaduan diwujudkan dengan adanya Sistem Informasi *Work Order* (SIWO). Berkembangnya jumlah penduduk di Kota Malang mengakibatkan tingginya kebutuhan akan air bersih, sehingga dalam memenuhi kebutuhan pelanggan perusahaan harus mampu memanfaatkan sumber daya secara maksimal. SIWO digunakan sebagai wadah perusahaan dalam mengelola data pelanggan, menerima keluhan dan pengaduan dari pelanggan dan pesanan dari pelanggan. Ini yang mampu menjadi ketakutan bagi perusahaan terkait data yang dimiliki, sehingga adanya proses perbaikan dari sistem layanan, pengelolaan data dan penanganan pengaduan diharapkan mampu memperbaiki sistem dari kegagalan yang pernah terjadi. Dan untuk perbaikan dan penyediaan fasilitas salah satunya diwujudkan dengan aplikasi Pengelolaan Aset Sistem Pengamanan Air Minum (PASPAM). Aplikasi ini dibangun guna melakukan *maintenance* terjadwal terkait seluruh aset yang dimiliki perusahaan. Karena perusahaan berpendapat bahwa aset-aset yang dimiliki, merupakan milik negara yang harus dirawat dan dijaga.

Risiko TI, merupakan salah satu faktor eksternal maupun internal organisasi yang berdampak kepada pencapaian tujuan. Dalam pengertian ini, risiko sebenarnya mengacu kepada sumber dari risiko itu sendiri. Sehingga dapat dikatakan bahwa risiko bersifat tidak pasti, artinya memiliki kemungkinan terjadi ataupun tidak. Menurut Elky (2006), risiko ini merupakan potensi bahaya yang mungkin timbul dari beberapa proses yang saat ini diterapkan atau dari beberapa kejadian di masa depan. Sehingga diperlukan manajemen risiko sebagai alat bantu organisasi dalam mengetahui bahaya yang mungkin terjadi. Manajemen risiko merupakan proses yang dapat memungkinkan manajer TI untuk menyeimbangkan antara biaya operasional dan ekonomi dari tindakan perlindungan dan memperoleh keuntungan dengan melindungi sistem dan data TI yang mendukung tujuan serta misi dari organisasi (Stoneburner, Goguen dan Feringa, 2002). Proses ini dibutuhkan organisasi untuk memahami apa risikonya, siapa yang berisiko atau terkena dampaknya, apa kendali saat ini dan keputusan apa yang perlu dibuat ketika risiko TI terjadi.

Perusahaan telah mempertimbangkan risiko terkait penggunaan teknologi informasi, ini dibuktikan dengan adanya penggunaan *software* Zabbix. Zabbix digunakan dalam pengelolaan risiko teknis TI, seperti permasalahan SQL *database*, *server*, *processor load to high*, dan lain sebagainya. Dengan *software* ini akan memudahkan dalam penanganan risiko teknis TI, karena yang bertugas menyelesaikan masalah akan diberikan notifikasi terkait status dari risiko yang terjadi. Belum adanya evaluasi lebih lanjut mengenai ancaman TI yang dapat terjadi di masa depan, mengakibatkan kekhawatiran terhadap pencapaian tujuan dari perusahaan. Selain itu, tugas dan tanggung jawab dalam pengelolaan risiko yang masih tumpang tindih mengakibatkan banyak staf yang memiliki pekerjaan ganda karena masih banyak staf yang tidak memiliki latar belakang TI. Selain itu, perusahaan pernah mengalami masalah keamanan informasi, yaitu ketika dokumen lengkap dari *business plan* dapat diakses oleh publik. Tentunya ini menjadikan bahan evaluasi terkait keamanan informasi dari perusahaan agar mampu melindungi aset informasi dan data.

Risiko penggunaan TI pada organisasi harus mampu dikelola dengan baik sehingga manfaat dari TI mampu dirasakan dan risiko TI dapat diminimalisasi. Arief (2018) telah melakukan penelitian terkait evaluasi manajemen risiko TI dengan menggunakan kerangka kerja COBIT 5. Dari penelitian ini dilakukan penilaian *capability level* untuk proses EDM03 dan APO12. Proses EDM03 mengenai bagaimana optimasi risiko TI dan APO12 mengenai bagaimana pengelolaan dari risiko TI tersebut. Diperoleh *capability level* 2 pada kedua proses. Selanjutnya, dilakukan *gap* analisis terkait *targeted level* atau *level* yang diharapkan oleh perusahaan dan hasil penilaian yang dilakukan peneliti. Setelah diketahui kesenjangannya, dilakukan identifikasi risiko TI untuk mengetahui apakah kontrol yang dilakukan telah sesuai sehingga mampu meminimalisir dampak dan tingkat probabilitas timbulnya risiko itu sendiri. Sehingga disusun strategi untuk mitigasi risiko TI.

Pada penelitian ini menggunakan kerangka kerja COBIT 5 sehingga mampu mendukung perusahaan yang telah menerapkan ISO 9001:2015 tentang sistem manajamen mutu. Fokus proses yaitu EDM03 *(Ensure Risk Optimisation)*, APO12 *(Manage Risk)* dan APO13 *(Manage Security)*. Proses EDM03 untuk memastikan pengoptimalan risiko, APO12 untuk mengelola risiko dan APO13 untuk keamanan sistem informasi perusahaan. Untuk mengukur pencapaian PDAM Kota Malang dalam penerapan manajemen risiko TI maka dilakukan penilaian kapabilitas. Menurut ISACA (2012b), proses penilaian tingkat kapabilitas merupakan pengukuran pencapaian tujuan dan penerapan praktik yang baik. Dari penilaian ini nantinya akan dihasilkan rekomendasi sehingga mampu meningkatkan tingkat kapabilitas dari perusahaan. Pada penelitian ini tidak dilakukan *risk assessment* atau pengkategorian risiko TI, hanya fokus kepada keluaran rekomendasi guna memperbaiki manajemen dari risiko TI.

1.2 Rumusan masalah

Sesuai dengan latar belakang yang telah dijabarkan, rumusan masalah yang dapat ditarik adalah:

1. Bagaimana kondisi BP *(Base practice)*, GP *(Generic Practice)*, WP *(Work product)* dan GWP *(Generic Work product)* pada domain EDM03 *(Ensure Risk Optimisation)*, APO12 *(Manage Risk)*, dan APO13 *(Manage Security)* pada PDAM Kota Malang?
2. Bagaimana kondisi *gap* (kesenjangan) antara *capability level* dengan target *level* pada domain EDM03 *(Ensure Risk Optimisation)*, APO12 *(Manage Risk)*, dan APO13 *(Manage Security)* di PDAM Kota Malang?
3. Bagaimana rekomendasi untuk domain EDM03 *(Ensure Risk Optimisation)*, APO12 *(Manage Risk)*, dan APO13 *(Manage Security)* untuk mencapai *targeted level* yang diharapkan?

1.3 Tujuan

Sesuai dengan rumusan masalah yang sudah ditentukan, maka tujuan dari penelitian ini adalah:

1. Mendeskripsikan analisis tentang kondisi BP *(Base practice)*, GP *(Generic Practice)*, WP *(Work product)* dan GWP *(Generic Work product)* yang ada pada PDAM Kota Malang.
2. Mendeskripsikan penilaian *capability* penerapan manajemen risiko teknologi informasi menggunakan *framework* COBIT 5. Dan kesenjangan *(gap)* antara *targeted level* dengan hasil dari penilaian *level capability* pada penerapan manajemen risiko di PDAM Kota Malang.
3. Mendeskripsikan rekomendasi bagi PDAM Kota Malang terkait penerapan manajemen risiko teknologi informasi.

1.4 Manfaat

Manfaat yang dapat diperolah dari penelitian yang dilakukan adalah:

1. Mampu memberikan rekomendasi yang dapat digunakan PDAM Kota Malang di masa depan dalam melakukan pengembangan serta perbaikan guna mencapai tujuan yang diharapkan organisasi.
2. Memperkaya kajian keilmuan tentang risiko, mengelola risiko dan mengelola keamanan.
3. Mampu menjadi acuan untuk penelitian selanjutnya yang lebih baik di masa depan.

1.5 Batasan masalah

Batasan masalah dari penelitian yang dilakukan adalah:

1. Penelitian ini fokus kepada posisi dari manajemen risiko teknologi informasi perusahaan yang bersifat teknis.
2. Penelitian ini menggunakan *framework* COBIT 5 karena untuk mendukung PDAM Kota Malang yang telah menerapkan ISO 9001:2015 tentang sistem manajemen mutu.
3. Penelitian ini menggunakan domain EDM03 *(Ensure Risk Optimisation)*, APO12 *(Manage Risk)*, dan *APO13 (Manage Security)* pada *framework* COBIT 5 karena fokus pada penerapan manajemen risiko TI PDAM Kota Malang.
4. Barang bukti yang ditemukan merupakan dokumen dan aset yang diperbolehkan untuk diketahui publik.

1.6 Sistematika pembahasan

BAB I. PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian dan batasan masalah.

BAB II. LANDASAN KEPUSTAKAAN

Pada bab ini berisi tentang kajian pustaka yang mendukung penelitian serta teori yang menjadi dasar penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan tentang langkah yang dilakukan dalam melakukan penelitian, dan metode pengumpulan data.

BAB IV. HASIL DAN ANALISIS

Pada bab ini berisi hasil dari data yang dibutuhkan dalam melakukan penelitian dan analisisnya.

BAB V. REKOMENDASI

Pada bab ini berisi tentang rekomendasi yang diperoleh dari hasil analisis.

BAB VI. KESIMPULAN DAN SARAN

Bab ini memuat tentang kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian di masa depan.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Dalam penulisannya, peneliti menggunakan beberapa penelitian yang telah dilakukan dengan topik dan bahasan yang sama sebagai rujukan. Salah satunya penelitian yang dilakukan oleh Suminar, Fitroh dan Ratnawati (2015). Penelitian ini bertujuan untuk mengevaluasi tata kelola dari teknologi informasi menggunakan COBIT 5 dengan fokus proses pada APO13 *(Manage Security)* dan DSS05 *(Manage Security Service)* pada Pusat Pendayagunaan Informatika dan Kawasan Strategis Nuklir (PPIKSN) BATAN. Terdapat permasalahan yaitu web besar yang ada pada unit PPIKSN BATAN diretas, ini dikerenakan tidak adanya SOP dan unit keamanan khusus serta minimnya informasi untuk mengevaluasi keamanan informasi. Dalam penelitian ini menggunakan metode kualitatif dengan menggunakan observasi, wawancara dan tinjauan literatur. Setelah data diterima, dilakukan inisiasi, lalu merencanakan penilaian, pengumpulan data, validasi data, menentukan tingkat dari masing-masing atribut proses dan melaporkan hasil yang diperoleh. Dilakukan perbandingan antara *capability level as is* dengan *to be.* Pada APO13 dan DSS05 berada pada *capabiliy level as is* 2 dan untuk *capability level to be* untuk keduanya yaitu 3, sehingga *gap* yang dihasilkan sebasar 1. Selanjutnya disusun rekomendasi agar mencapai *capavility level to be¸* yaitu memiliki dokumentasi bagan RACI dalam hal menetapkan manajemen keamanan sistem informasi dan menjaga keamanan dari operasional. Dan memiliki kebijakan dan standar organisasi yang selaras, serta menerapkan prosedur standar dalam mengelola manajemen keamanan sistem informasi dan keamanan operasional.

Penelitian selanjutnya oleh Arief (2018) dengan melakukan evaluasi terkait manajemen risiko TI yang fokus pada proses EDM03 *(Ensure Risk Optimisation)* dan APO12 *(Manage Risk)*. Penelitian dimulai dengan perencanan, kedua dilakukan pengumpulan data melalui metode kuisioner, wawancara dan observasi, ketiga mengetahui gambaran umum perusahaan, teknologi informasi serta RACI *Chart*, keempat melakukan analisis *capability level* sehingga didapatkan *capability level* pada *subdomain* EDM03 berada pada *level* 2 dan APO12 juga berada pada *level* 2. Kelima, dilakukan perbandingan atau analisis *gap*, yaitu kesenjangan yang diperoleh dari *level* yang didapatkan dari hasil penilaian dan keinginan atau *targeted level* yang diharapkan oleh perusahaan. *Targeted level* yang diharapkan yaitu berada pada level 3, sehingga *gap* yang dihasilkan sebesar 1. Lalu, merumuskan langkah mitigasi dan diakhiri dengan rekomendasi. Terdapat 12 rekomendasi yang dibuat agar mencapai *targeted level.* Dan dibuat langkah mitigasi terhadap skenario risiko *New Technology, IT Expertise and Skills, IT Staff,* dan *System Capacity.*

Penelitian selanjutnya yaitu mengenai evaluasi sistem keamanan teknologi informasi. Mufti (2017), melakukan evaluasi pada *subdomain* APO13 *(Manage Security)* dan DSS05 *(Manage Security Service).* Data diperoleh melalui metode wawancara, kuisioner dan observasi. Hasilnya pada *subdomain* APO13 dan DSS05 mencapai *level* 1. Dan untuk *targeted level* yaitu berada pada level 2, sehingga

gap yang dihasilkan sebesar 1. Selanjutnya peneliti melakukan analisis SWOT yaitu membandingkan faktor eksternal peluang dan ancaman dengan faktor kekuatan internal dan kelemahannya. Dilanjutkan dengan pembuatan rekomendasi, contoh rekomendasinya salah satunya yaitu pembentukkan unit khusus mengenai keamanan informasi, dan penanganan risiko keamanan informasi sehingga tidak terjadi risiko terkait keamanan teknologi informasi.

Terakhir yaitu hasil prosiding oleh Astuti, et al. (2017), pada konferensi 4th *Information Systems International Conference* 2017, ISICO di Bali, Indonesia. Penelitian ini membahas mengenai *risk assessment* TI berdasarkan *framework* COBIT 5 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Insitut Teknologi Sepuluh Nopember (ITS). Penelitian ini berfokus pada atribut proses APO12-BP2 mengenai analisis risiko. Dibagi menjadi tiga fase, fase pertama untuk pengumpulan data melalui wawancara, tinjauan dokumen dan observasi. Hasilnya diperoleh daftar risiko yang akan digunakan sebagai proses penilaian risiko. Fase kedua, analisis data. Dari data sebelumnya, disusun jenis risiko, kategori risiko, dan faktor internal dan eksternal dari setiap risiko. Dan fase ketiga, yaitu analisis risiko. Ini dilakukan dengan menganalisis dampak dan menilai probabilitas risiko yang telah diidentifikasi. Hasilnya berupa penilaian risiko dan rencana mitigasinya.

Dari beberapa penelitian yang dijadikan rujukan, diperoleh hasil mengenai analisis dari manajemen risiko sebuah perusahaan yang telah menerapkan TI dalam proses bisnisnya. Ini dianggap penting, karena kemungkinan risiko yang terjadi dari penerapan TI tidak dapat diprediksi. Sehingga perlu adanya manajemen risiko TI, di mana mampu menganalisis ancaman yang mungkin terjadi, dampaknya, serta probabilitas terjadinya risiko. Manajemen risiko juga mampu memberikan rekomendasi sehingga risiko yang terjadi tidak memberikan dampak yang besar bagi keberlangsungan proses bisnis perusahaan. Dan perusahaan tetap mampu bertahan ketika risiko terjadi.

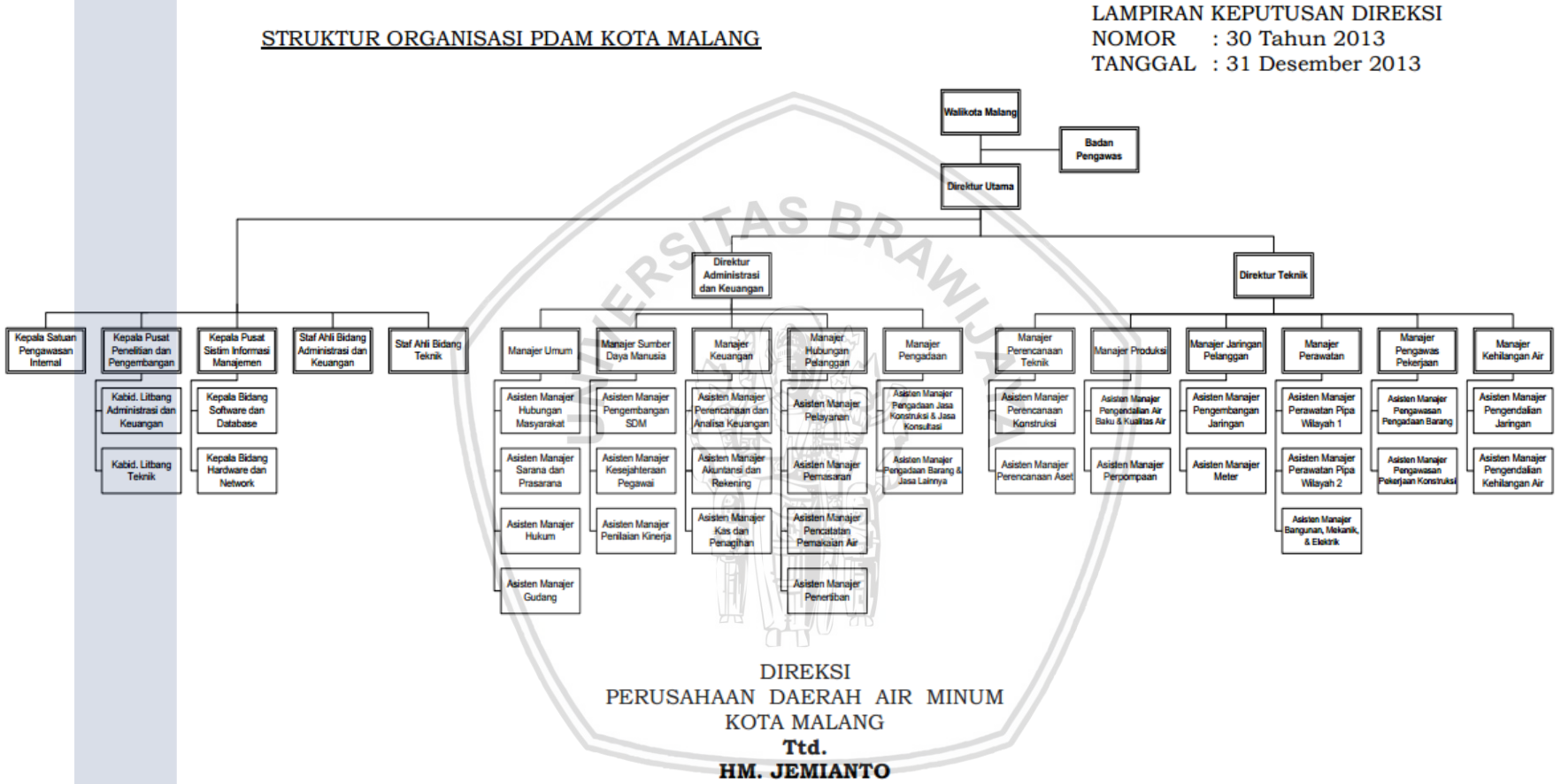
2.2 Profil PDAM Kota Malang

Perusahaan Air Minum Daerah (PDAM) Kota Malang merupakan Badan Usaha Milik Daerah (BUMD), di mana perusahaan ini didirikan dan dimiliki oleh pemerintah daerah. BUMD menjadi salah satu sumber pendapatan daerah sehingga mampu memiliki peran penting dalam pembangunan daerah. Perusahaan Air Minum Daerah (PDAM) Kota Malang sudah berjalan sejak Pemerintahan Belanda pada tanggal 31 Maret 1915. Awalnya perusahaan ini dikenal dengan nama WATERLEIDING VERORDENING Kota Besar Malang, namun sejak pada tanggal 18 Desember 1974 dengan diterbitkannya Peraturan Daerah Nomor: 11 Tahun 1974, Unit Air Minum berubah status menjadi Perusahaan Air Minum. Sejak saat Itu Perusahaan Daerah Air Minum Kota Malang memiliki Badan Hukum dan memiliki hak otonomi dalam mengelola air minum di Kota Malang.

PDAM Kota Malang sendiri telah memiliki sertifikat ISO 9001:2015 yaitu standar internasional mengenai manajemen mutu *(The International Organization for Standarization*). ISO 9001:2015 menetapkan persyaratan untuk sistem manajemen mutu di mana perusahaan menunjukkan kemampuannya secara konsisten untuk menyediakan produk atau jasa yang memenuhi persyaratan atau peraturan yang berlaku. Bukan hanya mampu menyediakan produk atau jasa, perusahaan harus mampu meningkatkan kepuasan pelanggan melalui penerapan sistem yang efektif, termasuk proses perbaikan sistem secara berkelanjutan dan jaminan kesesuaian terhadap pelanggan dan peraturan yang berlaku.

Sebagai salah satu perusahaan pelayanan publik, PDAM Kota Malang dituntut untuk selalu mengikuti perkembangan teknologi untuk meningkatkan pelayanan kepada masyarakat. Salah satunya dengan situs resmi dalam bentuk website sehingga masyarakat mampu mengakses informasi secara cepat dan mudah. Bukan hanya meningkatkan pelayanan yang berorientasi kepada pelanggan saja, PDAM Kota Malang juga fokus kepada menggunakan teknologi informasi guna meningkatkan proses bisnis mereka. Salah satunya dengan memiliki portal sendiri untuk menjalankan proses bisnis dengan baik. Karena PDAM Kota Malang berkomitmen dalam menjalankan seluruh proses bisnisnya akan memanfaatkan teknologi informasi dan komunikasi yang baik guna mewujudkan optimalisasi performa kinerja operasional perusahaan. Demi memahami profil PDAM Kota Malang lebih jauh visi dari PDAM Kota Malang yaitu mampu menjadi perusahaan air minum terkemuka dan tersehat di Indonesia. Untuk misinya, yang pertama meningkatkan dan mengutamakan pelayanan, meningkatkan professionalisme SDM, meningkatkan kinerja manajemen, menjaga kelestarian sumber air baku dengan, kerjasama antar daerah.

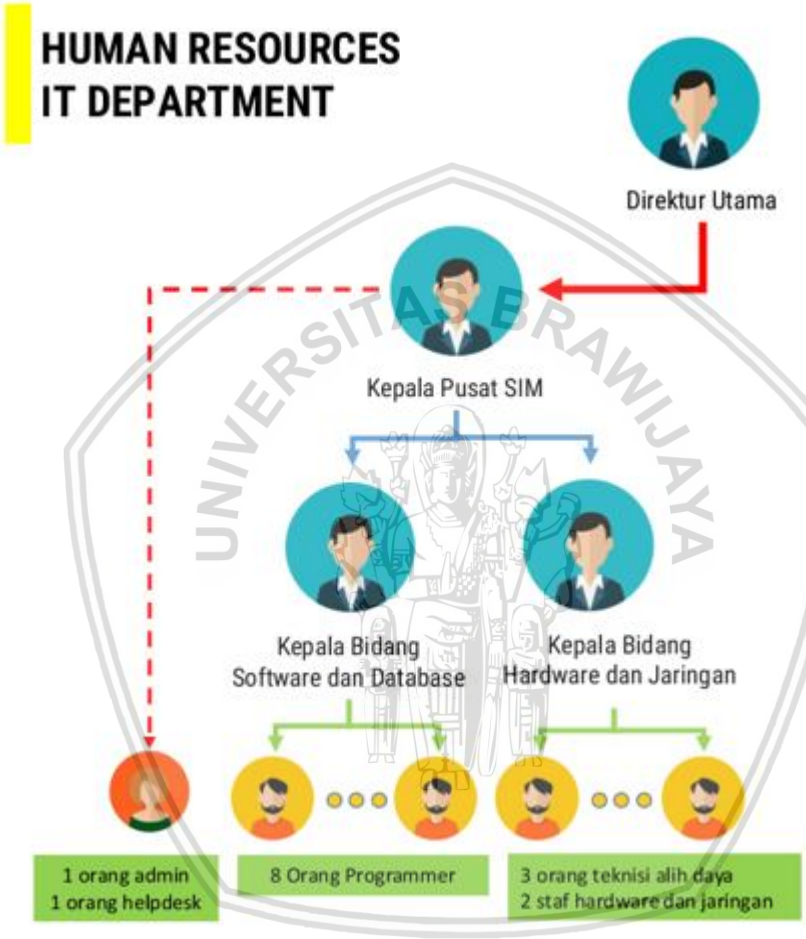
Berikut merupakan struktur organisasi secara keseluruhan dari PDAM Kota Malang:



Gambar 2.1 Struktur Organisasi PDAM Kota Malang

(Sumber: SK PDAM Kota Malang, 2013)

Pada Gambar 2.1 menggambarkan struktur organisasi dari PDAM Kota Malang. Direktur Utama dari PDAM Kota Malang bertanggung jawab langsung kepada Badan Pengawas dan Walikota Malang. Direktur Utama membawahi langsung Kepala Satuan Pengawasan Internal, Kepala Pusat Penelitian dan Pengembangan, Kepala Pusat Sistem Informasi Manajemen, Staf Ahli Bidang Administrasi dan Keuangan, Staf Ahli Bidang Teknik, Direktur Administrasi dan Keuangan, dan Direktur Teknik. Selanjutnya yaitu struktur organisasi dari Pusat Sistem Informasi Manajemen (SIM) PDAM Kota Malang.



Gambar 2.2 Struktur Organisasi Pusat SIM PDAM Kota Malang

(Sumber: SK PDAM Kota Malang, 2013)

Pada Gambar 2.2 menggambarkan struktur organisasi dari Pusat Sistem Informasi Manajemen di PDAM Kota Malang. Kepala Pusat SIM bertanggung jawab kepada Direktur Utama. Kepala Pusat SIM bertugas dalam merencanakan dan mengawasi kegiatan pemeliharaan dan pengembangan dari Sistem Informasi Manajemen. Kepala Pusat SIM membawahi Kepala Bidang *Software* dan *Database* yang bertugas untuk mengatur dan mengendalikan kegiatan pemeliharaan dan pengembangan akan *software* dan *database* dan Kepala Bidang *Hardware* dan Jaringan yang bertugas untuk mengatur dan mengendalikan kegiatan pemeliharaan *hardware* dan jaringan. Terdapat 8 orang *Programmer* yang

membantu Kepala Bidang *Software* dan *Database* dalam mencapai tujuannya dan terdapat 3 orang teknisi alih daya serta 2 staf *hardware* dan jaringan yang membantu Kepala Bidang *Hardware* dan Jaringan dalam mencapai tujuannya. Selain itu terdapat 1 orang admin dan 1 orang *help desk* yang bertanggung jawab langsung kepada Kepala Pusat SIM.

2.3 Manajemen Risiko

Dalam menerapkan teknologi informasi diperlukan pertimbangan risiko yang mungkin terjadi selama penerapannya. Pengelolaan risiko dari teknologi ini dapat dikatakan sebagai sebuah kewajiban yang harus dimiliki oleh mereka yang menerapkannya sehingga mampu mengetahui apa yang harus dilakukan ketika risiko muncul. Menurut IACOP (2014), definisi kunci mengenai risiko adalah sebuah *event* – insiden atau kejadian dari internal atau eksternal organisasi yang dapat mempengaruhi pencapaian tujuan organisasi atau perusahaan. *Event* ini bisa berdampak negatif, positif maupun keduanya. Peristiwa dengan dampak negatif merupakan risiko. Sedangkan peristiwa dengan berdampak positif merupakan peluang. Selain itu risiko dapat dikatakan sebagai kemungkinan bahwa sebuah peristiwa dapat terjadi dan berdampak buruk dalam mencapai tujuan. Risiko dapat diukur dalam hal dampak dan kemungkinan terjadinya.

Menurut ISACA (2013a), risiko TI dikategorikan menjadi 3 kategori. Kategori pertama yaitu *IT Benefit/Value Enablement Risk.* Pada kategori ini risiko dikategorikan berdasarkan hilangnya kesempatan untuk menggunakan teknologi demi meningkatkan efisiensi atau efektivitas dari proses bisnis. Contohnya, teknologi *enabler* untuk inisiatif bisnis baru dan teknologi *enabler* untuk operasi yang efisien. *Enabler* adalah faktor yang secara individu dan kolektif mempengaruhi apakah sesuatu akan bekerja atau berhasil, dalam hal ini, tata kelola dan manajemen TI perusahaan. *Enabler* ini merupakan segala sesuatu yang mampu membatu perusahaan untuk pencapaian tujuan. Framework COBIT 5 mendeskripsikan 7 kategori dari *enablers*, yaitu pertama *principles, policies and framework.* Ini merupakan *enabler* yang harus dipertimbangkan, karena nantinya secara teknis akan diterjemahkan ke dalam peraturan operasional untuk mengatur keseharian dari manajemen. Enabler kedua, *process.* Fungsinya untuk mengatur aktivitas organisasi dalam mencapai tujuannya. Proses ini menguraikan seperangkat praktik dan kegiatan yang terorganisir untuk mencapai tujuan tertentu dan menghasilkan keluaran untuk mendukung pencapaian sasaran TI. *Enabler* ketiga, *organizational structures.* Struktur organisasi merupakan entitas pengambil keputusan utama dalam perusahaan. Dibutuhkan agar mengetahui siapa yang memiliki peran penting, agak penting dan tidak penting dalam proses.

Enabler keempat, *culture, ethics and behavior.* Merupakan kebiasaan dari individu dan sering dianggap sebagai faktor penghambat kesuksesan di dalam aktivitas tata kelola dan manajemen. *Enabler* ini sering sekali lolos dari perhatian perusahaan. *Enabler* kelima, *information.* Informasi ini menyebar di seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. Informasi sangat dibutuhkan oleh organisasi agar tetap berjalan dan

mampu diatur dengan baik, tetapi pada tingkat operasional informasi seringkali merupakan produk kunci dari perusahaan itu sendiri. Informasi perlu dikelola sebagai sumber daya. Seperti, laporan manajemen dan informasi intelijen bisnis yang merupakan faktor penting dalam tata kelola dan manajemen perusahaan. *Enabler* keenam, *services, infrastucture, and applications.* Ini mencakup infrastruktur, teknologi, dan aplikasi yang menyediakan proses dan layanan teknologi informasi untuk perusahaan. *Enabler* ini juga merupakan sumber daya perusahaan yang perlu dikelola dan diatur. Dan *enabler* ketujuh, *people, skills and competencies.* Ini berkaitan dengan orang-orang dan dibutuhkan oleh perusahaan untuk menyelesaikan seluruh kegiatan dengan baik dan sukses. Selain itu, mampu membuat keputusan yang benar dan mengambil tindakan korektif. Sehingga, perlu diatur dan dikelola karena dianggap sebagai sumber daya perusahaan.

Ketegori risiko TI yang kedua, yaitu *IT Programmer and Project Delivery Risk.* Mengkategorikan risiko terkait kontribusi TI untuk solusi bisnis baru atau yang akan ditingkatkan, biasanya dalam bentuk proyek dan program sebagai bagian dari portofolio investasi. Contohnya, *project quality, project relevance* dan *project overrun.* Kategori risiko TI yang terakhir, yaitu *IT Operations and Service Delivery.* Pada kategori ini risiko dikategorikan berdasarkan semua aspek dari bisnis. Berkaitan dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan teknologi informasi dari seluruh aspek yang mampu menimbulkan kehancuran atau pengurangan nilai perusahaan.

Bukan hanya hal negatif saja yang ada pada risiko, hal positif pun ada dan biasanya disebut sebagai peluang. Peluang adalah kemungkinan bahwa suatu peristiwa akan terjadi secara positif dapat mempengaruhi pencapaian tujuan. Dalam risiko, terdapat risiko utama yang menjadi fokus perusahaan atau organisasi. Risiko utama ini merupakan risiko yang jika dikelola dengan baik akan membuat perusahaan atau organisasi berhasil dalam mencapai tujuannya, jika tidak dikelola dengan baik, organisasi tersebut tidak akan mencapai tujuannya. Untuk mengetahui risiko utama, ada hal yang paling melekat dari risiko yaitu tingkat risiko. Tingkat risiko dilakukan sebelum tindakan mitigasi risiko direalisasikan seperti kegiatan pengendalian yang telah diperhitungkan (misalnya risiko banjir yang melekat sebelum memperhitungkan tindakan pencegahan banjir).

Menurut Pithcard (2015), tujuan perencanaan manajemen risiko yaitu untuk memaksa manajer proyek untuk membuat yang berkaitan dengan risiko TI terorganisir, pemikiran yang bertujuan untuk manajemen risiko dan untuk menyediakan infastruktur organisasi untuk membantu resulasi risiko. Manajemen risiko mampu memberikan dampak yang baik dalam mengatur segala hal dalam membantu terwujudnya tujuan dari perusahaan atau organisasi. Prinsip manajemen risiko IT menurut ISACA (2013a), yaitu *Connect to enterprise objectives, Align with ERM, Balance cost/benefit of IT risk, Promote fair and open communication, Establish tone at the top and accountability, Function as part of daily activities* dan *Consistent approach.* Prinsip yang pertama yaitu, menghubungkan ke tujuan dari perusahaan. Pada prinsip ini risiko TI diperlakukan

sebagai risiko bisnis, pendekatannya komprehensif dan lintas fungsional dan fokusnya adalah pada hasil bisnis. Teknologi informasi harus mampu mendukung tercapainya tujuan bisnis, dan risiko TI dinyatakan sebagai dampak yang bisa saja didapatkan ketika mencapai tujuan atau strategi bisnis. Prinsip kedua yaitu, sejajar dengan ERM. Artinya besarnya risiko dan sasaran bisnis harus disiapkan perusahaan dengan jelas. Contohnya dalam proses pengambilan keputusan perusahaan harus mempertimbangkan berbagai konsekuensi potensial dan peluang dari risiko TI. Prinsip ketiga yaitu, menyeimbangkan biaya dan manfaat risiko teknologi informasi. Maksudnya risiko diprioritaskan dan ditangani sesuai dengan *risk appetite* dan *tolerance*. Kontrol diterapkan untuk mengatasi risiko berdasarkan analisis dari biaya-manfaat. Prinsip keempat yaitu, komunikasi yang adil dan terbuka. Informasi yang terbuka, akurat, tepat waktu dan transparan tentang risiko TI menjadi dasar untuk semua keputusan terkait risiko. Masalah risiko, prinsip dan metode pengelolaannya harus terintegrasi di seluruh perusahaan.

Prinsip kelima, menetapkan *tone* pada pihak atas dan akuntabilitas. Pihak atas yaitu orang yang penting seperti *influencer*, pemilik bisnis dan dewan direksi terlibat dalam manajemen risiko TI ini. Selanjutnya tedapat penugasan dan penerimaan kepemilikan risiko yang jelas, termasuk mengasumsikan akuntabilitas, melakukan pengukuran kinerja dan mengintegrasikan manajemen risiko ke dalam sistem penghargaan. Budaya sadar akan risiko harus dikenalkan secara aktif, dimulai dari *tone* atas. Ini akan membantu memastikan bahwa mereka yang terlibat dengan manajemen risiko operasional beroperasi berdasarkan asumsi risiko yang konsisten. Prinsip keenam yaitu, berfungsi sebagai bagian dari aktivitas sehari-hari. Karena risiko bersifat dinamis, manajemen risiko TI merupakan proses yang berulang-ulang, terus-menerus dan berkelanjutan. Setiap perubahan dilakukan pasti akan membawa risiko dan atau peluang, sehingga perusahaan mempersiapkan hal ini dengan melakukan pertimbangkan terhadap perubahan dalam organisasi atau perusahaan sehingga merupakan aktivitas sehari-hari yang terjadi. Dan yang terakhir pendekatan yang konsisten. Yaitu ketika telah ditetapkan pendekatan untuk mengatasi risiko TI, perusahaan harus tetap konsisten dalam menjalankan operasinya. Sehingga mampu meminimalkan risiko dan kemungkinan terjadinya, bahkan dampak yang ditimbulkan mampu dikurangi.

2.4 Optimasi Risiko

Optimasi risiko dapat dikatakan bagaimana mengoptimalkan risiko sehingga mampu dikelola dengan baik. Dengan melakukan optimasi risiko, maka mampu memastikan seberapa besar risiko dan toleransinya yang dapat diterima oleh perusahaan. Sehingga pihak terkait mampu mengerti, dan melakukan aktivitas dari identifikasi dan pengelolaan risiko yang berkaitan dengan TI pada perusahaan dengan baik sehingga perusahaan mampu bertahan. Salah satu domain dari *framework* COBIT 5 yang membahas tentang optimasi risiko yaitu EDM03 *(Ensure Risk Optimisation).*

Menurut ISACA (2013c), proses EDM03 *(Ensure Risk Optimisation)* ialah memastikan agar perusahaan memiliki *risk appetite* dan toleransinya dimengerti. *Risk appetite* adalah sejauh mana individu, sebuah tim proyek maupun organisasi mentoleransi jenis atau tingkat dari risiko tertentu (Pitchard, 2015). *Risk appetite* ini mencerminkan bagaimana lingkungan mampu menghadapi risiko tertentu atau bagaimana jika tidak sama sekali menghadapinya. Dalam COBIT 5, tujuan optimasi risiko agar risiko terkait TI pada perusahaan tidak melebihi *risk appetite dan risk tolerance*, sehingga dampak dari risiko TI kepada perusahaan dapat diidentifikasi dan dikelola, dan potensi kegagalannya dapat diminimalkan.

Subdomain EDM03 memiliki 3 *base pratices* di dalamya, EDM03-BP1 *(Evaluate Risk Management),* EDM03-BP2 *(Direct Risk Management)* dan EDM03-BP3 *(Monitor Risk Management). Base pratices* (BP) merupakan indikator untuk masing-masing kinerja proses yang digunakan untuk mengetahui tingkat kapabilitas dari proses. BPs pada setiap proses ini memberikan definisi tugas dan aktivitas yang diperlukan untuk mencapai tujuan proses dan memenuhi hasil proses. Setiap BP secara eksplisit terkait dengan hasil dari proses. Sehingga sifatnya mengatur kriteria yang nantinya akan dihasilkan atau dalam arti lain merupakan aturan untuk hasil. Ketika BPs dilakukan secara konsisten, maka akan berkontribusi untuk mencapai tujuan dari proses tertentu. *Base pratices* yang pertama pada *subdomain* EDM03 yaitu EDM03-BP1 *(Evaluate Risk Management)* yang bertujuan untuk secara terus menerus memeriksa serta membuat penilaian mengenai pengaruh risiko terhadap penggunaan teknologi informasi pada perusahaan saat ini dan masa depan. Selain itu, melakukan pertimbangan apakah *risk appetite* sesuai dengan kemampuan perusahaan dan risiko yang terkait dengan nilai penggunaan teknologi informasi di perusahaan mampu diidentifikasi dan dikelola. *Base pratices* yang kedua yaitu EDM03-BP2 *(Direct Risk Management)* yaitu bertujuan untuk mengarahkan praktik manajemen risiko agar memastikan bahwa praktik dari manajemen risiko teknologi informasi sesuai dan risiko dari teknologi informasi tidak melebihi pertumbuhan risiko perusahaan. Dan *base pratices* yang ketiga yaitu EDM03-BP3 *(Monitor Risk Management)* yang bertujuan untuk memantau tujuan utama dan metrik dari proses manajemen risiko dan menetapkan bagaimana masalah akan diidentifikasi, dilacak, dan dilaporan.

Selanjutnya yaitu ada *work products* (WPs). Sama seperti BPs, WPs merupakan seperangkat indikator kinerja proses. WPs akan memberikan panduan objektif untuk mencari masukan dan keluaran potensial, dan bukti objektif untuk mendukung penilaian berdasarkan dokumentasi. Masukan dan keluaran ini merupakan proses WP atau artefak yang dianggap perlu untuk mendukung pengoperasian proses. Masukan dan keluaran akan memberikan rekaman dan jejak audit dari aktivitas proses, dan memungkinkan tindak lanjut jika terjadi insiden. Proses *input dan ouput* digunakan untuk membantu memastikan proses operasi yang tepat, dan *output* WPs dapat dian*gap* sebagai aspek yang paling penting. Berikut adalah *input dan output* dari *work products* (WPs) pada setiap

proses dan terkait dengan satu atau lebih hasil keluarannya pada *subdomain* EDM03.

Tabel 2.1 *Inputs* dan *Outputs* WPs *subdomain* EDM03

***Work products* (WPs)**	
Inputs	***Outputs***
Prinsip manajemen risiko perusahaan	Panduan risiko yang dapat diterima
Isu dan faktor risiko	Tingkat toleransi terhadap risiko yang telah disetujui
Profil manajemen risiko dan rencana mitigasi	Aktivitas evaluasi manajemen risiko
Analisis risiko dan pelaporan profil risiko untuk *stakeholders*	Kebijakan manajemen risiko
Hasil analisis risiko	Tujuan utama yang diawasi oleh manajemen risiko
Analisis risiko dan laporan profil risiko untuk *stakeholders*	Proses yang telah disetujui untuk mengukur manajemen risiko
Review hasil dari penilaian pihak ketiga	Tindakan remedial untuk mengatasi penyimpangan manajemen risiko
Peluang untuk menerima risiko yang lebih besar	Isu manajemen risiko untuk dewan komisaris

(Sumber: ISACA, 2013c)

Tabel 2.1 menunjukkan *input* dan *output* WPs pada *subdomain* EDM03. Terdapat 8 *input* dan 8 *output*. Prinsip manajemen risiko, isu risiko dan faktor yang timbul, profil dari manajemen risiko perusahaan dan rencana mitigasi risiko, analisis risiko dan laporan profil risiko kepada pemangku kepentingan, hasil analisis risiko, laporan analisis risiko dan profil risiko untuk pemangku kepentingan, review hasil dari penilaian risiko pihak ketiga, dan peluang untuk menerima risiko yang lebih besar merupakan *input* WPs dari subdomian EDM03. Sedangkan panduan risiko yang dapat diterima perusahaan, tingkat toleransi perusahaan, aktivitas evaluasi manajemen risiko, kebijakan manajemen risiko, tujuan utama yang harus diawasi manajemen risiko, tindakan remedial untuk mengatasi penyimpangan manajemen risiko dan isu manajemen risiko merupakan *output* WPs dari *subdomain* EDM03.

2.5 Mengelola Risiko

Setelah memahami bagaimana *risk appetite* dan toleransinya terhadap risiko oleh perusahaan selanjutnya yaitu bagaimana mengelola risiko. Yaitu organisasi akan mengambil langkah yang akan digunakan dalam menyelesaikan risiko yang sudah diidentifikasi. Menurut Elky (2006), penting untuk mengelola risiko karena

mampu melindungi misi dan aset organisasi. Oleh karena itu, manajemen risiko harus menjadi fungsi manajemen daripada fungsi teknis. Sangat penting untuk mengelola risiko terhadap sistem. Memahami risiko, dan khususnya, memahami risiko spesifik pada suatu sistem memungkinkan pemilik sistem untuk melindungi sistem informasi yang sepadan dengan nilainya bagi organisasi. Risiko dapat dikelola dengan *mitigation, transference, acceptance, avoidance, communicating risks and risk management strategies,* dan *implementing risk management strategies.*

Mitigation adalah strategi manajemen risiko yang paling umum dipertimbangkan. Mitigasi mampu memperbaiki cacat atau menyediakan beberapa jenis kontrol kompensasi untuk mengurangi kemungkinan atau dampak terkait risiko. Salah satu contohnya mitigasi umum untuk kesalahan keamanan teknis adalah menginstal patch yang disediakan vendor. Proses penentuan strategi mitigasi ini disebut dengan analisis kontrol. *Transference,* yaitu dengan mengirimkan dampak dari risiko kepada pihak ketiga, bersamaan dengan kepemilikan respon. Mentransfer risiko hanya memberikan tanggung jawab kepada pihak lain untuk mengelolanya. Alat transferensi bisa pada penggunaan asuransi, rasio kinerja, jaminan dan sebagainya. Kontrak atau kesepakatan pun dapat digunakan untuk mengalihkan tanggung jawab atas risiko tertentu kepada pihak ketiga. Ini tidak mengurangi kemungkinan atau memperbaiki kekurangan apa pun, tetapi mengurangi dampak keseluruhan (terutama keuangan) pada organisasi. *Acceptance* adalah praktik yang memungkinkan sistem beroperasi dengan risiko yang diketahui sebelumnya. Contohnya banyak risiko rendah diterima begitu saja. Risiko yang memiliki biaya yang sangat tinggi untuk mitigasi juga sering begitu saja diterima. Pastikan bahwa strategi yang ditulis mengenai risiko TI dan risiko yang dapat diterima perusahaan dibuat oleh manajer yang membuat keputusan. Biasanya, manajer bisnis bukan personil keamanan TI, adalah orang yang berwenang untuk menerima risiko atas nama organisasi.

Avoidance yaitu ketika risiko dapat dihindari dengan menghapus penyebab risiko atau melaksanakan proses dengan cara yang berbeda namun tetap mencapai tujuan yang sama. Contohnya, memperluas jadwal, mengubah strategi atau mengurangi ruang lingkup. Misalnya, selama penilaian risiko, situs web memungkinkan vendor melihat fakturnya menggunakan ID vendor yang disematkan dalam nama file HTML sebagai identifikasi dan tidak ada autentikasi atau otorisasi per vendor. Ketika diberitahu tentang halaman web dan risiko untuk organisasi, manajemen memutuskan untuk menghapus halaman web dan menyediakan faktur vendor melalui mekanisme lain. Dalam hal ini, risiko dihindari dengan menghapus halaman web yang rentan. Selanjutnya *Communicating Risks and Risk Management Strategies.* Risiko juga harus dikomunikasikan, setelah risiko dipahami, risiko dan strategi manajemen risiko harus dikomunikasikan dengan jelas sehingga mudah dipahami oleh manajemen organisasi. Dalam mengkomunikasikan risiko gunakan hal kemungkinan dan dampak, ini akan mempermudah dalam melakukan komunikasi risiko TI. Gunakan istilah yang konkret, sehingga manajemen organisasi akan memahami dan menerima temuan dan rekomendasi. Terakhir *Implementing Risk Management Strategies.* Salah satu

tools yaitu A Plan Of Action & Milestones (POAM), ini dibuat agar disetujui oleh manajemen. POAM ini mengandung risiko, strategi manajemen, Point Of Contact (POC) yang bertanggung jawab untuk mengimplementasikan strategi, sumber daya yang dibutuhkan dan berbagai tonggak yang terdiri dari implementasi. Untuk setiap pencapaian, tanggal penyelesaian target, dan tanggal penyelesaian aktual dicantumkan. POAM ini digunakan sebagai alat untuk berkomunikasi dengan manajemen.

Salah satu *subdomain* dari COBIT 5 yang membahas tentang mengelola risiko yaitu APO12 *(Manage Risk).* Menurut ISACA (2013c), APO12 (*Manage Risk)* yaitu secara terus menerus mengidentifikasi, menilai dan mengurangi risiko yang berhubungan dengan teknologi informasi dalam tingkat toleransi yang ditentukan oleh manajemen perusahaan. Tujuannya untuk mengintegrasikan pengelolaan risiko teknologi informasi perusahaan dengan keseluruhan ERM, dan mempertimbangkan biaya serta manfaat dari pengelolaan risiko teknologi informasi perusahaan. *Subdomain* APO12 memiliki 6 *base pratices*, yaitu APO12-BP1 *(Collect Data),* APO12-BP2 *(Analyse Risk),* APO12-BP3 *(Maintain a Risk Profile),* APO12-BP4 *(Articulate Risk),* APO12-BP5 *(Define a Risk Management Action Portofolio)* dan APO12-BP6 *(Respond to Risk).*

Base pratices (BP) merupakan indikator untuk masing-masing kinerja proses yang digunakan untuk mengetahui tingkat kapabilitas *subdomain*. BPs pada setiap proses ini memberikan definisi tugas dan aktivitas yang diperlukan untuk mencapai tujuan proses dan memenuhi hasil proses. Setiap BP secara eksplisit terkait dengan hasil dari proses. Sehingga sifatnya mengatur kriteria yang nantinya akan dihasilkan atau dalam arti lain merupakan aturan untuk hasil. Ketika BPs dilakukan secara konsisten, maka akan berkontribusi untuk mencapai tujuan dari proses tertentu. *Base practies* yang pertama yaitu, APO12-BP1 *(Collect Data).* Yaitu identifikasi dan mengumpulkan data yang relevan untuk identifikasi, analisis, dan pelaporan risiko teknologi informasi yang efektif. Sehingga hasilnya nanti dapat digunakan untuk *base practices* selanjutnya. Pada *base practices* ini, pihak terkait diharapkan mampu memiliki kemampuan dalam mengidentifikasi dan mengumpulkan data yang berpengaruh untuk selanjutnya akan dianalisis dan dilaporkan mengenai risiko teknologi informasi.

Base pratices kedua yaitu, APO12-BP2 *(Analyse Risk).* Pada BP ini dikembangkan informasi yang berguna dari BP sebelumnya untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis dan faktor risiko. Keputusan yang dihasilkan harus sesuai dengan tujuan dari bisnis, sehingga ketika melakukan sebuah aktivitas terkait risiko tidak mengurangi peluang untuk mencapai tujuan perusahaan. *Base practices* yang ketiga yaitu APO12-BP3 *(Maintain a Risk Profile)*, BP ini bertujuan untuk mempertahankan inventaris dari risiko yang diketahui dan atribut risiko (termasuk frekuensi yang diharapkan, dampak potensial dan respon) dan sumber daya terkait, kapabilitas (kemampuan) dan aktivitas pengendalian. *Base practices* yang keempat APO12-BP4 *(Articulate Risk).* Tujuan dari BP ini yaitu memberikan informasi tentang keadaan objek yang rentan terhadap risiko terkait teknologi informasi dan berdampak kepada kinerja perusahaan dan peluang TI saat ini kepada semua pemangku kepentingan untuk

selanjutnya mendapatkan tang*gap*an yang tepat. Tang*gap*an ini dapat digunakan oleh perusahaan dalam melakukan perbaikan dalam manajemen risiko teknologi informasi. *Base pratices* kelima yaitu APO12-BP5 *(Define a Risk Management Action Portofolio).* Pada proses ini yaitu mengelola peluang untuk mengurangi risiko ketingkat yang dapat diterima sebagai portofolio. Portofolio ini nantinya akan berisi tentang pengelolaan peluang guna menurunkan tingkat risiko pada perusahaan. *Base practices* keenam yaitu APO12-BP6 *(Respond to Risk*). Tujuannya yaitu menang*gap*i secara tepat waktu dengan langkah-langkah yang efektif untuk membatasi besarnya kerugian dari kejadian yang berhubungan dengan teknologi informasi.

Selanjutnya yaitu ada *work products* (WPs). Sama seperti BPs, WPs merupakan seperangkat indikator kinerja proses. WPs akan memberikan panduan objektif untuk mencari masukan dan keluaran potensial, dan bukti objektif untuk mendukung penilaian berdasarkan dokumentasi. Masukan dan keluaran ini merupakan proses WP atau artefak yang dianggap perlu untuk mendukung pengoperasian proses. Masukan dan keluaran ini memberikan rekaman dan jejak audit dari aktivitas proses, dan memungkinkan tindak lanjut jika terjadi insiden. Proses *input dan ouput* digunakan untuk membantu memastikan proses operasi yang tepat, *output* WPs dapat dian*gap* sebagai aspek yang paling penting. Berikut adalah *input dan output* dari *work products* (WPs) pada setiap proses dan terkait dengan satu atau lebih hasil keluarannya pada *subdomain* APO12.

Tabel 2.2 *Inputs* dan *Outputs* WPs *subdomain* APO12

***Work products* (WPs)**	
Inputs	***Outputs***
Evaluasi aktivitas manajemen risiko	Data lingkungan operasi yang berkaitan dengan risiko
Kebijakan manajemen risiko	Data kejadian risiko dan faktor pendukungnya
Tujuan utama yang diawasi	Isu dan faktor risiko yang muncul
Proses yang disetujui untuk mengukur manajemen risiko	Lingkup upaya analisis risiko
Status insiden dan laporan tentang tren	Skenario risiko TI
Saran untuk ancaman	Hasil analisis risiko
Analisis dampak bisnis	Skenario risiko berdasarkan bidang usaha dan fungsi
Evaluasi ancaman yang potensial	Profil risiko dan laporan profil risiko bagi *stakeholder*

Tabel 2.2 *Inputs* dan *Outputs* WPs *subdomain* APO12 (Lanjutan)

***Work products* (WPs)**	
Inputs	***Outputs***
Panduan risiko yang dapat diterima	Peninjauan kembali hasil penilaian risiko pihak ketiga
Tingkat toleransi risiko yang disetujui	Peluang untuk menerima risiko yang lebih besar
Identifikasi risiko pengiriman dari pemasok	Proposal proyek untuk mengurangi risiko
Evaluasi ancaman potensial	Dampak risiko untuk dikomunikasikan kepada pihak terkait
Tindakan remedial untuk mengatasi penyimpangan manajemen risiko	Penyebab utama risiko

(Sumber: ISACA, 2013c)

Tabel 2.2 menunjukkan *inputs* dan *outputs* WPs pada *subdomain* APO12. Terdapat 13 *inputs* WPs. Evaluasi aktivitas manajemen risiko, kebijakan manajemen risiko, tujuan utama yang diawasi manajemen risiko, proses yang disetujui untuk mengukur manajemen risiko, status insiden dan laporan mengenai tren, saran dan ancaman, analisis dampak bisnis, evaluasi ancaman yang bersifat potensial, panduan risiko yang dapat diterima oleh perusahaan, tingkat toleransi risiko yang disepakati, identifikasi risiko pengiriman dari pemasok, evaluasi ancaman yang bersifat potensial dan tindakan remedial untuk mengatasi penyimpangan manajemen risiko merupakan *input* WPs dari *subdomain* APO12. *Output* WPs *subdomain* APO12, terdapat 13 *outputs.* Data lingkungan operasi yang berkaitan dengan risiko, data kejadian risiko dan faktor pendukungnya, isu dan faktor risiko yang timbul, lingkup upaya analisis risiko, skenario risiko TI, hasil analisis risiko, skenario risiko berdasarkan bidang usaha dan fungsinya, profil risiko dan laporan profil risiko bagi pemangku kepantingan, peninjauan kembali hasil penilaian risiko pihak ketiga, peluang untuk menerima risiko yang lebih besar, proposal proyek untuk mengurangi risiko, dampak risiko untuk dikomunikasikan kepada pihak terkait, dan penyebab utama dari risiko merupakan *outputs* WPs dari *subdomain* APO12.

2.6 Mengelola Keamanan

Menggunakan teknologi informasi sebagai kebutuhan dalam menjalan proses bisnis secara maksimal mendorong perusahaan harus mampu mengelola keamanan informasi. Karena data dan informasi merupakan aset terpenting dalam perusahaan. Dengan mengelola keamanan informasi mampu mempertahankan kerahasiaan, ketersediaan dan integritas informasi yang dimiliki. Ini akan melibatkan penerapan dan pengelolaan pengendalian yang tepat dengan melakukan pertimbangan mengenai ancaman, dengan tujuan memastikan keberhasilan dan kelangsungan bisnis yang berkelanjutan, dan meminimalkan

konsekuensi insiden keamanan sistem informasi. Keamanan informasi dicapai melalui penerapan seperangkat kontrol yang sesuai. Kontrol ini perlu ditentukan, diimplementasikan, dipantau, ditinjau dan diperbaiki di mana diperlukan, untuk memastikan bahwa keamanan informasi spesifik dan tujuan bisnis perusahaan terpenuhi.

Menurut ISO/IEC 27000 (2016), keberhasilan dari penerapan *Information Security Management Systems* (ISMS) penting untuk melindungi aset informasi yang memungkinkan perusahaan untuk mencapai jaminan yang lebih besar bahwa aset informasinya dilindungi secara baik terhadap ancaman yang terus menerus timbul. Selain itu mampu memelihara kerangka kerja terstruktur dan komprehensif untuk mengidentifikasi dan menilai risiko keamanan informasi, memilih dan menerapkan pengendalian dan mengukur serta meningkatkan keefektifannya. Sehingga mampu terus menerus memperbaiki lingkungan pengendalian. Dan secara efektif mencapai kepatuhan hukum dan peraturan yang sudah ditetapkan perusahaan.

Pada COBIT 5 mengelola keamanan terdapat pada *subdomain* APO13. Menurut ISACA (2013c), APO13 *(Manage Security)* yaitu menjelaskan, menjalankan dan mengawasi sistem manajemen keamanan informasi. Mampu mempertahankan dampak dan insiden keamanan informasi dalam *risk appetite* perusahaan. *Subdomain* APO13 memiliki 3 *base practices* yaitu APO13-BP1 *(Establish and Maintain an ISMS)*, APO13-BP2 *(Define and Manage an ISMS)* dan APO13-BP3 *(Monitor and Review the ISMS). Base pratices* (BP) merupakan indikator untuk masing-masing kinerja proses yang digunakan untuk mengetahui tingkat kapabilitas *subdomain*. BPs pada setiap proses ini memberikan definisi tugas dan aktivitas yang diperlukan untuk mencapai tujuan proses dan memenuhi hasil proses. Setiap BP secara eksplisit terkait dengan hasil dari proses. Sehingga sifatnya mengatur kriteria yang nantinya akan dihasilkan atau dalam arti lain merupakan aturan untuk hasil. Ketika BPs dilakukan secara konsisten, maka akan berkontribusi untuk mencapai tujuan dari proses tertentu.

Base practices yang pertama APO13-BP1 *(Establish and Maintain an ISMS).* Pada BP yang pertama ini perusahaan menetapkan dan memelihara ISMS yang memberikan pendekatan standar, formal dan berkesinambungan terhadap manajemen keamanan untuk mendapatkan informasi, memungkinkan proses teknologi dan bisnis yang aman yang sesuai dengan persyaratan bisnis dan manajemen keamanan perusahaan. BP yang kedua, yaitu APO13-BP2 *(Define and Manage an ISMS).* BP ini menjaga rencana dari keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan disesuaikan dengan strategi perusahan dan arsitektur perusahaan. Memastikan bahwa rekomendasi untuk menerapkan perbaikan keamanan didasarkan pada kasus yang disetujui, kemudian dioperasikan sebagai bagian dari operasi bisnis. BP ketiga yaitu APO13-BP3 *(Monitor and Review the ISMS)*. Pada proses ini dilakukan penjagaan dan secara teratur mengkomunikasikan kebutuhan akan manfaat, perbaikan keamanan informasi terus-menerus. Dengan mengumpulkan dan analisis data tentang ISMS, dan meningkatkan keefektifan ISMS.

Selanjutnya yaitu ada *work products* (WPs). Sama seperti BPs, WPs merupakan seperangkat indikator kinerja proses. WPs akan memberikan panduan objektif untuk mencari masukan dan keluaran potensial, dan bukti objektif untuk mendukung penilaian berdasarkan dokumentasi. Masukan dan keluaran ini merupakan proses WP atau artefak yang dianggap perlu untuk mendukung pengoperasian proses. Masukan dan keluaran ini memberikan rekaman dan jejak audit dari aktivitas proses, dan memungkinkan tindak lanjut jika terjadi insiden. Proses *input dan ouput* digunakan untuk membantu memastikan proses operasi yang tepat, *output* WPs dapat dian*gap* sebagai aspek yang paling penting. Berikut adalah *input dan output* dari *work products* (WPs) pada setiap proses dan terkait dengan satu atau lebih hasil keluarannya pada *subdomain* APO13. Berikut merupakan *inputs* dan *outputs* WPs *subdomain* APO13.

Tabel 2.3 *Inputs* dan *Outputs* WPs *subdomain* APO13

***Work products* (WPs)**	
Inputs	***Outputs***
Pendekatan keamanan	Kebijakan ISMS
Kesenjangan dan perubahan yang dibutuhkan untuk mewujudkan target kapabilitas	Pernyataan tentang *scoper* ISMS
Domain dasar dan definisi arsitektur	Rencana penanganan risiko keamanan
Proposal proyek untuk mengurangi risiko keamanan informasi	Kasus bisnis keamanan informasi
Klasifikasi dan prioritas insiden dan permintaan layanan	Hasil audit ISMS
	Rekomendasi untuk meningkatkan ISMS

(Sumber: ISACA, 2013c)

Tabel 2.3 menunjukkan *inputs* dan *outputs* WPs pada *subdomain* APO13. Terdapat 5 *inputs* dan 6 *outputs.* Pendekatan mengenati keamanan perusahaan, kesenjangan dan perubahan yang dibutuhkan untuk mewujudkan target kapabilitas, domain dasar dan definisi arsitektur, proposal proyek untuk mengurangi risiko keamanan informasi dan klasifikasi dan prioritas insiden serta permintaan layanan merupakan *inputs* WPs pada *subdomain* APO13. Sedangkan kebijakan manajemen keamanan sistem informasi, rencana penanganan risiko keamanan sistem informasi, audit manajemen keamanan sistem informasi dan rekomendasi untuk perbaikan manajemen keamanan sistem informasi merupakan *outputs* WPs dari *subdomain* APO13.

2.7 COBIT 5 *Framework*

Menurut ISACA (2012a), COBIT 5 merupakan generasi terbaru dari panduan ISACA yang membahas mengenai tatakeloka dan manajemen IT. COBIT 5 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan dalam mencapai tujuan mereka untuk tata kelola dan manajemen teknologi informasi perusahaan (TI). Secara sederhana, COBIT 5 membantu perusahaan untuk menciptakan nilai yang optimal dari IT dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan tingkat risiko dan penggunaan sumber daya. COBIT 5 memungkinkan TI untuk diatur dan dikelola secara holistik untuk seluruh perusahaan, dengan mempertimbangkan penuh *end-to-end* bisnis dan bidang fungsional IT dari tanggung jawab dan mempertimbangkan kepentingan terkait IT pemangku kepentingan internal dan eksternal. COBIT 5 terdiri dari 5 prinsip dan 7 faktor pendukung. Faktor pendukung ini dalam COBIT 5 disebut sebagai *enablers.*

Prinsip pertama COBIT 5 yaitu *meeting stakeholder needs*, membantu *stakeholder* dalam menentukan dan pendefinisain prioritas. Pada tahap ini *stakeholder* menentukan apa yang diharapkan dari SI/TI yang diterapkan memiliki keuntungan seperti apa, penentuan tingkat risiko, dan bagaimana prioritas mereka dalam menjamin bahwa nilai tambah yang diharapkan telah dengan benar tersampaikan, dan berapa sumber daya yang dibutuhkan. Kebutuhan *stakeholder* diantaranya tujuan perusahaan (*Enterprise Goal*), tujuan yang terkait dengan IT (*IT-Related Goal*), dan tujuan yang akan dicapai *enabler* (*Enabler Goal*). Prinsip kedua yaitu *covering enterprise end-to-end,* bermanfaat untuk mengintegrasi tatakelola TI perusahaan ke dalam tata kelola perusahaan. Prinsip ini meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola TI perusahaan.

Prinsip ketiga, *applying a single integrated framework*, sebagai penyelarasan diri dengan standard dan *framework* relevan lain, sehingga perusahaan mampu menggunakan COBIT 5 sebagai *framework* tata kelola. Prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACA seperti COBIT, Val IT, dan *Risk IT*. Dan menyesuaikan dengan standar *framework* lainnya seperti ITIL, TOGAF, PMBOK, PRINCE2, COSO, dan ISO. Prinsip keempat, *enabling a holistic approach*, memandang bahwa setiap *enabler* saling mempengaruhi satu sama lain. COBIT 5 mendukung perpaduan bisnis dan IT secara menyeluruh dan mendukung semua aspek seperti struktur organisasi, kebijakan, dan budaya. Prinsip kelima, *separating governance from management*, COBIT adalah perbedaan yang dibuat antara tata kelola dan manajemen. Sejalan dengan prinsip ini, setiap perusahaan akan diharapkan untuk melaksanakan sejumlah proses tata kelola dan sejumlah proses manajemen untuk memberikan tata kelola dan manajemen perusahaan IT yang komprehensif.

COBIT 5 membedakan proses *governance* dengan proses *management*. *Governance process*, proses tata kelola yang menangani tata kelola pemangku kepentingan dengan tujuan-nilai, optimasi risiko dan optimasi sumber daya. Termasuk praktek dan kegiatan yang bertujuan untuk mengevaluasi pilihan

strategis, memberikan arahan untuk IT dan pemantauan hasil (*evaluation*, *direct* dan *monitoring* [EDM] garis -dalam dengan ISO / IEC 38500 konsep standar). Sedangkan *management process*, praktek dan kegiatan dalam proses manajemen mencakup tanggung jawab PBRM *enterprise IT*, dan harus menyediakan cakupan TI yang *end-to-end*. Pada *management process,* yaitu cakupannya berupa *Plan*, *Build*, *Run* dan *Monitor* (PBRM).

Dalam pemilihan subdomain penelitian, EDM03, APO12 dan APO13 memiliki keterkaitan antara satu sama lain. Pada EDM03, merupakan subdomain dari area *governance* (tata kelola). Pada *work product* yang dimiiki oleh EDM03, input WPs berasal dari hasil kerja dari APO12. Sehingga kedua subdomain ini saling berkaitan. Yaitu, WPs *input* hasil dari analisis risiko, analisis risiko dan laporan profil risiko untuk pemangku kepentingan, tinjauan hasil *risk assessment* pihak ketiga dan peluang untuk menerima risiko lebih besar yang berasal dari proses APO12 akan mendukung *base practices* EDM03-BP3 yaitu *monitor risk management.* Lalu, untuk isu risiko yang muncul dan faktornya mendukung *base pratices* EDM03-BP1 yaitu *evaluate risk management*. Dan analisis risiko dan laporan profil risiko untuk pemangku kepentingan mendukung *base practices* EDM03-BP2 yaitu *direct risk management*. Pada subdomain APO12, WPs *input* dari EDM03 yaitu evaluasi aktivitas manajemen risiko, kebijakan manajemen risiko, tujuan utama yang dipantau oleh manajemen risiko dan proses yang disetujui untuk melakukan penilaian manajemen risiko akan mendukung base practices APO12-BP1 yaitu *collect data.* Panduan risk appetite dan tingkatan yang diseutujui untuk toleransi risiko dari EDM03 akan mendukung *base practices* APO12-BP2 yaitu *analyse risk.* Tindakan remedial untuk mengatasi penyimpangan dari manajemen risiko pada EDM03 akan mendukun base practices dari APO12-BP6 yaitu *respond to risk.* Dan untuk APO13, WPs input dari APO12 mengenai proposal proyek untuk mengurangi risiko mendukung base practices dari APO13-BP3 yaitu *monitor and review the ISMS.*

2.8 RACI *Chart*

Pada COBIT 5 terdapat RACI *Chart* yaitu sebuah matrik dari sebuah tugas yang disarankan mengenai tingkat tanggung jawab untuk praktik proses terhadap berbagai peran dan struktur. RACI terdiri dari 4 komponen yaitu, R (*Responsible*), siapa yang menyelesaikan tugas? Mengacu kepada orang yang berperan pada bagian operasional utama dalam memenuhi aktivitas yang tercantum dan menciptakan hasil yang diharapkan. A (*Accountable*, siapa yang bertanggung jawab keberhasilan tugas? Yaitu di mana orang yang akhirnya bertanggungjawab dan memiliki otoritas untuk memutuskan suatu perkara. C *(Consulted),* siapa yang memberikan masukkan? Ini adalah kunci dari peran yang memberikan sebuah masukan. Dan I *(Informed),* siapa yang menerima informasi? Peran pada *Informed* yaitu mereka yang mendapat informasi tentang prestasi dan atau kiriman tugas. Perannya harus mampu selalu menerima informasi yang tepat untuk diawasi dengan baik (ISACA, 2012b). EDM03 memiliki 3 *key governance practices.* Pertama, EDM03.01 yaitu *Evaluate Risk Management* dengan tujuan secara terus menerus memeriksa serta membuat penilaian mengenai pengaruh risiko terhadap

penggunaan teknologi informasi pada perusahaan saat ini dan masa depan, EDM03.02 *Direct Risk Management,* bertujuan untuk mengarahkan praktik manajemen risiko agar sesuai dan teknologi informasi tidak melebihi pertumbuhan risiko perusahaan dan EDM03.03 *Monitor Risk Management,* untuk memantau tujuan utama dan menetapkan bagaimana masalah diidentifikasi, dilacak, dan dilaporkan. Berdasarkan RACI *Chart*, pihak yang terlibat dalam setiap 4 komponen RACI pada *subdomain* EDM03 adalah:

Tabel 2.4 Pihak Terlibat Pada *Subdomain* EDM03

Komponen	Pihak Terlibat
Responsible	1. *Chief Execution Officer* 2. *Business Executive* 3. *Strategy Executive Comittee* 4. *Chief Risk Officer* 5. *Chief Information Officer* 6. *Chief Information Security Officer* (EDM03.03)
Accountable	1. *Board*
Consulted	1. *Chief Financial Officer* 2. *Chief Operating Officer* 3. *Business Process Owner* 4. *Head Human Resource* 5. *Compliance* 6. *Audit* 7. *Head Architect* 8. *Chief Information Security Officer* (EDM03.01) 9. *Policy Officer* (EDM03.01 dan EDM03.03)
Informed	1. *Steering (Programmes/Project)Comittee* 2. *Project Management Officer* 3. *Value Management Officer* 4. *Architecture Board* 5. *Enterprise Risk Comittee* 6. *Head Development* 7. *Head IT Operations* 8. *Head IT Administration* 9. *Service Manager* 10. *Information Security Manager* 11. *Information Continuity Manager* 12. *Chief Information Security Officer* (EDM03.02) 13. *Policy Officer* (EDM03.02)

(Sumber: ISACA, 2012b)

Selanjutnya, APO12 memiliki 6 *key management practices.* Pertama, APO12.01 *(Collect Data).* Yaitu identifikasi dan mengumpulkan data yang relevan untuk efektifitas dari identifikasi, analisis, dan pelaporan risiko teknologi

informasi5. Kedua yaitu, APO12.02 *(Analyse Risk).* Mengembangkan informasi yang berguna dari *practices* sebelumnya untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis dan faktor risiko. Ketiga yaitu APO12.03 *(Maintain a Risk Profile)*, bertujuan untuk mempertahankan inventaris dari risiko yang diketahui dan atribut risiko (termasuk frekuensi yang diharapkan, dampak potensial dan respon) dan sumber daya terkait, kapabilitas (kemampuan) dan aktivitas pengendalian. Keempat APO12.04 *(Articulate Risk),* memberikan informasi tentang keadaan objek yang rentan terhadap risiko terkait teknologi informasi dan berdampak kepada kinerja perusahaan dan peluang TI saat ini kepada semua pemangku kepentingan untuk selanjutnya mendapatkan tang*gap*an yang tepat. Kelima yaitu APO12.05 *(Define a Risk Management Action Portofolio),* mengelola peluang untuk mengurangi risiko ketingkat yang dapat diterima sebagai portofolio. Dan keenam yaitu APO12.06 *(Respond to Risk*). Tujuannya yaitu menang*gap*i secara tepat waktu dengan langkah-langkah yang efektif untuk membatasi besarnya kerugian dari kejadian yang berhubungan dengan teknologi informasi. Berikut adalah RACI *Chart* untuk *subdomain* APO12 yang terlibat dalam setiap 4 komponen RACI pada *subdomain* EDM03 adalah:

Tabel 2.5 Pihak Terlibat Pada *Subdomain* APO12

Komponen	Pihak Terlibat
Responsible	1. *Business Process Owner* 2. *Project Management Officer* (APO12.01 dan APO12.06) 3. *Chief Risk Officer* (APO12.01, APO12.02, APO12.04, dan APO12.06) 4. *Chief Information Officer* (APO12.03 dan APO12.05) 5. *Chief Information Security Officer* (APO12.01 dan APO12.06) 6. *Compliance* (APO12.02 dan APO12.03) 7. *Audit* (APO12.02 dan APO12.03) 8. *Head Architect* (APO12.01 dan APO12.06) 9. *Head Development* (APO12.01 dan APO12.06) 10. *Head IT Operation* (APO12.01 dan APO12.06) 11. *Head IT Administration* (APO12.01 dan APO12.06) 12. *Service Manager* (APO12.01 dan APO12.06) 13. *Information Security Manager* (APO12.01 dan APO12.06) 14. *Business Continuity Manager* (APO12.01 dan APO12.06) 15. *Privacy Officer* (APO12.01 dan APO12.06)
Accountable	1. *Chief Risk Officer* (APO12.03 dan APO12.05) 2. *Chief Information Officer* (APO12.01, APO12.02, APO12.04, dan APO12.06)

Tabel 2.5 Pihak Terlibat Pada *Subdomain* APO12 (Lanjutan)

Komponen	Pihak Terlibat
Consulted	1. *Project Management Officer* (APO12.02, APO12.03, APO12.04, dan APO12.05) 2. *Chief Information Security Officer* (APO12.02, APO12.03, APO12.04, dan APO12.05) 3. *Compliance* (APO12.01, APO12.04, APO12.05, dan APO12.06) 4. *Audit* (APO12.01, APO12.04, APO12.05, dan APO12.06) 5. *Head Architect* (APO12.02, APO12.03, APO12.04, dan APO12.05) 6. *Head Development* (APO12.02, APO12.03, APO12.04, dan APO12.05) 7. *Head IT Operations* (APO12.02, APO12.03, APO12.04, dan APO12.05) 8. *Head IT Administration* (APO12.02, APO12.03, APO12.04, dan APO12.05) 9. *Service Management* (APO12.02, APO12.03, APO12.04, dan APO12.05) 10. *Information Security Management* (APO12.02, APO12.03, APO12.04, dan APO12.05) 11. *Business Continuity Management* (APO12.02, APO12.03, APO12.04, dan APO12.05) 12. *Privacy Officer* (APO12.02, APO12.03, APO12.04, dan APO12.05)
Informed	1. *Chief Execution Officer* 2. *Enterprise Risk Comittee*

(Sumber: ISACA, 2012b)

Selanjutnya untuk subdomain APO13 memiliki 3 *key management practices.* Pertama, APO13.01 *(Establish and Maintain an ISMS).* Perusahaan menetapkan dan memelihara ISMS yang memberikan pendekatan standar, formal dan berkesinambungan terhadap manajemen keamanan untuk mendapatkan informasi, memungkinkan proses teknologi dan bisnis yang aman yang sesuai dengan persyaratan bisnis dan manajemen keamanan perusahaan. Kedua, APO13.02 *(Define and Manage an ISMS).* Yaitu, menjaga rencana dari keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan disesuaikan dengan strategi perusahan dan arsitektur perusahaan. Dan ketiga, APO13.03 *(Monitor and Review the ISMS)*. Dilakukan penjagaan dan secara teratur mengkomunikasikan kebutuhan akan manfaat, perbaikan keamanan informasi terus-menerus. Dengan mengumpulkan dan analisis data tentang ISMS, dan meningkatkan keefektifan ISMS. Berdasarkan RACI *Chart* pihak yang terlibat dalam setiap 4 komponen RACI pada *subdomain* APO13 adalah

Tabel 2.6 Pihak Terlibat Pada *Subdomain* APO13

Komponen	Pihak Terlibat
Responsible	1. *Business Process Owners* (APO13.02) 2. *Project Management Office* (APO13.02) 3. *Chief Information Officer* 4. *Head Architect* (APO13.03) 5. *Head Development* (APO13.03) 6. *Head IT Operations* (APO13.03) 7. *Head IT Administration* 8. *Information Security Manager* 9. *Business Continuity Manager* (APO13.03) 10. *Privacy Officer* (APO13.03)
Accountable	1. *Chief Information Security Officer*
Consulted	1. *Chief Executive officer* (APO13.01 dan APO13.02) 2. *Chief Operation Officer* (APO13.01 dan APO13.02) 3. *Business Executives* 4. *Business Process Owners* (APO13.01 dan APO13.02) 5. *Strategy Executive Committee* 6. *Chief Risk Officer* (APO13.01 dan APO13.02) 7. *Architecture Board* (APO13.01 dan APO13.02) 8. *Enterprise Risk Committee* (APO13.01 dan APO13.02) 9. *Compliance* 10. *Audit* 11. *Head Architect* (APO13.02) 12. *Head Development* (APO13.02) 13. *Head IT Operations* (APO13.02) 14. *Services Manager* (APO13.02) 15. *Business Continuity Manager* (APO13.01 dan APO13.02) 16. *Privacy Officer* (APO13.01 dan APO13.02)
Informed	1. *Business Process Owners* (APO13.01) 2. *Steering (Programmers/Projects) Committee* (APO13.01 dan APO13.02) 3. *Project Management Office* (APO13.01 dan APO13.02) 4. *Head Architect* (APO13.01) 5. *Head Development* (APO13.01) 6. *Head IT Operations* (APO13.01) 7. *Services Manager* (APO13.01)

(Sumber: ISACA, 2012b)

Setelah mengetahui pihak mana saja yang terlibat dan memiliki peran R *(Responsible),* A *(Accountable),* C *(Consulted)* dan I *(Informed),* akan lebih baik apabila mengetahui deskripsi dari masing-masing peran. Menurut ISACA (2012a), peran *Board* merupakan pihak eksekutif yang paling senior dan / atau direktur non-eksekutif yang bertanggung jawab atas tata kelola dari perusahaan serta memiliki wewenang atas kontrol keseluruhan sumber dayanya. *Chief Executive Officer* atau yang lebih dikenal dengan CEO merupakan pihak yang paling bertanggung jawab atas seluruh manajemen perusahaan. *Chief Financial Officer* (CFO) bertanggung jawab atas seluruh aspek manajemen keuangan, termasuk risiko. *Chief Operating Officer* (COO) bertanggung jawab dalam segala operasi perusahaan. *Chief Risk Officer* (CRO) bertanggung jawab dalam semua aspek manajemen risiko perusahaan. Sebagai CRO dapat membentuk tim khusus untuk mengawasi risiko TI. *Chief Information Officer* (CIO) bertanggung jawab untuk menyelaraskan strategi TI dengan bisnis, serta bertanggung jawab atas perencanaan, sumber daya dan manajemen penyampaian layanan dan solusi TI untuk mendukung tujuan perusahaan. *Chief Information Security Officer* (CISO) merupakan pihak yang bertanggung jawab untuk menyelaraskan strategi TI dengan bisnis, serta bertanggung jawab atas perencanaan, sumber daya dan manajemen penyampaian layanan dan solusi TI untuk mendukung tujuan perusahaan. *Business Excecutive* bertanggung jawab atas pengoperasian unit usaha atau anak perusahaan tertentu.

Business Process Owner bertanggung jawab atas kinerja sebuah proses dalam mencapai tujuannya, mendorong perbaikan proses dan menyetujui perubahan proses. *Strategy (IT Excecutive) Committee* merupakan sekelompok eksekutif senior yang dipilih oleh dewan untuk memastikan dewan mengetahui, dan terus mendapatkan informasi, masalah dan keputusan utama terkait IT. Tanggung jawab dari komite untuk mengelola portofolio akan investasi TI, layanan TI dan aset TI, selanjutnya memastikan bahwa nilai dan risiko sudah dilakukan manajemen atau dikelola. Komite ini biasanya diketuai oleh anggota dewan bukan CIO. *(Project and Programme) Steering Committees* merupakan sekelompok pemangku kepentingan dan ahli yang bertanggung jawab atas pembinaan program dan proyek, termasuk manajemen dan pengawasan rencana, alokasi sumber daya, penyampaian manfaat dan nilai, serta pengelolaan program dan risiko proyek. *Architecture Board* merupakan sekelompok pemangku kepentingan dan ahli yang bertanggung jawab atas panduan mengenai masalah dan keputusan mengenai arsitektur perusahaan, dan untuk menentapkan kebijakan dan standar arsitekturalnya. *Enterprise Risk Committee* merupakan sekelompok eksekutif dari perusahaan yang bertanggung jawab atas kolaborasi dan tingkat konsensus perusahaan yang dibutuhkan untuk mendukung aktivitas dan keputusan manajemen risiko perusahaan (ERM). Sebuah dewan risiko TI dapat terbentuk demi mempertimbangkan risiko TI secara lebih detail nantinya dan memberikan saran kepada komite risiko perusahaan.

Head of HR ini bertanggung jawab akan perancanaan dan kebijakan yang terkait dengan sumber daya manusia di perusahaan. *Compliance* bertanggung jawab atas panduan akan kepatuhan terhadap hukum, peraturan serta kontrak

yang telah disepakati. *Audit* bertanggung jawab dalam penyediaan audit internal. *Head of Architecture* bertanggung jawab atas proses arsitektur enterprise. *Head of Development* memiliki tanggung jawab atas proses pengembangan solusi TI. *Head of IT Operations* memiliki tanggung jawab atas lingkungan serta infrastruktur operasional TI. *Head of IT Administration* bertanggung jawab atas dokumen TI dan mendukung masalah administrasi TI. *Programme and Project Management Office* (PMO) bertanggung jawab mendukung manajer program dan proyek, dan mengumpulkan, menilai serta melaporkan informasi pelaksanaan program dan proyek. *Value Management Office* (VMO) merupakan pihak yang mengelola portofolio investasi dan layanan, menilai dan memberi saran tentang peluang dari investasi dan merekomendasikan metode serta bagaimana kontrol tata kelola atau manajemen, melaporkan kemajuan dalam mempertahankan dan menciptakan nilai dari investasi dan layanan. *Services Manager* merupakan pihak yang mengelola pengembangan, pelaksanaan, evaluasi dan pengelolaan produk dan layanan baru. *Information Security Manager* pihak yang mengelola, merancang, dan mengawasi dan / atau menilai keamanan informasi perusahaan. *Business Continuity Manager* bertugas mengelola, merancang, mengawasi dan / atau menilai kemampuan kelangsungan bisnis perusahaan, memastikan bahwa fungsi kritis perusahaan terus berjalan setelah adanya gangguan. Dan *Privacy Officer* pihak yang mengelola, merancang, dan mengawasi dan / atau menilai keamanan informasi perusahaan.

2.9 *Self assessment*

Menurut ISACA (2013b), *Self assessment* merupakan sebuah pendekatan yang sederhana untuk melakukan penilaian yang tidak didasarkan pada bukti, tidak memerlukan penilai independen atau bersertifikat dan dapat dilakukan oleh manajemen perusahaan sebagai pendahuluan sehingga kedepannya dapat dilakukan penilaian formal. *Self asessment* ini dapat mengidentifikasi kesenjangan proses yang memerlukan perbaikan sebelum penilaian formal, dapat dilakukan untuk investasi yang bisa dibilang kecil tetapi mampu membantu manajemen perusahaan dalam menetapkan tingkat kapabilitas. Menurut ISACA (2013b) tahapan *self assessment* memiliki 5 tahapan. Tahapan pertama yaitu *decide on processes to assess.* Dalam tahap ini dilakukan penentuan proses apa saja yang akan dinilai. Penilai mencatat proses yang dipilih untuk dilakukan penilaian, contohnya seperti pada Tabel 2.7.

Tabel 2.7 Contoh Tabel Hasil Penilaian Proses

Process Capability level							
Prosess Name	***Targeted Level***	**0**	**1**	**2**	**3**	**4**	**5**
EDM03 *(Ensure Risk Optimisation)*							
APO12 *(Manage Risk)*							
APO13 *(Manage Security)*							

(Sumber: ISACA, 2013b)

Pada tahap ini, target dari proses *capability level* dapat dicatat. Tabel 2.7 memberikan contoh format yang dapat digunakan untuk mencatat target dari proses *capability level.* Yaitu dengan menuliskan proses apa saja yang ingin dilakukan penilaian, lalu tentukan target yang ingin dicapai oleh perusahaan. Selanjutnya dilakukan perekapan dari hasil penilaian kapabilitas *level* yang telah dilakukan dalam bentuk skala (N,P,L,F). Dalam menetapkan target *capability level*, harus dilakukan pertimbangan pada dampak yang dapat terjadi kepada tujuan bisnis perusahaan jika *level capability* tertentu tidak tercapai. Pertimbangan pertama yaitu dampaknya pada perusahaan jika prosesnya tidak ada atau tidak mampu bekerja secara efektif atau efisien. Pertimbangan kedua menyangkut konsekuensi tambahan dari proses bisnis yang efektif dan efisien dalam berbagai *capability level* seperti yang ditunjukkan pada Tabel 2.8 dari ISO/IEC 15504-4.

Tabel 2.8 Pertimbangan dalam Penentuan *Targeted Level*

Capability level	***Process Attribute Where Gap Occurs***	***Potential Consequence***
1	PA 1.1 *Process Performance*	Produk kerja tidak ada dan hasil dari proses tidak tercapai.
2	PA 2.1 *Performance Management*	Biaya atau waktu terjadi kelebihan, penggunaan sumber daya yang tidak efisien, tanggung jawab yang tidak jelas.
	PA 2.2 *Work product Management*	Kualitas dan integritas produk tidak dapat diprediksi, peningkatan biaya pendukung, masalah integrasi dan biaya terkait pengerjaan ulang meningkat.

Tabel 2.8 Pertimbangan dalam Penentuan *Targeted Level* (Lanjutan)

Capability level	***Process Attribute Where Gap Occurs***	***Potential Consequence***
3	PA 3.1 *Process Definition*	Perusahaan ingin mengidentifikasikan praktik terbaik dan mampu mempelajari hasil dari proyek-proyek sebelumnya, mendefinisikan segala proyek yang terdapat dalam organisasi dan ketika perusahaan belum ada fondasi terkait meningkatkan proses
	PA 3.2 *Process Deployment*	Proses yang diimplementasikan tidak terdapat praktik terbaik yang sudah diidentifikasi dari proyek sebelumnya, kinerja proses tidak konsisten antar organisasi dan kehilangan peluang untuk memahami proses dan identifikasi perbaikannya.
4	PA 4.1 *Process Management*	Perusahaan tidak memiliki pemahaman kuantitatif tentang seberapa baik proses, tujuan kinerja dan tujuan bisnis tercapai. Lalu, tidak adanya kemampuan kuantitatif untuk mendeteksi masalah kinerja sejak dini
	PA 4.2 *Process Control*	Proses tidak dapat diprediksi dalam batas yang ditentukan dan tujuan kinerja kuantitatif dan tujuan bisnis yang telah ditetapkan tidak terpenuhi.
5	PA 5.1 *Process Inovation*	Tujuan perbaikan proses tidak didefinisikan dangan jelas dan peluang untuk perbaikan tidak teridentifikasi.
	PA 5.2 *Process Optimization*	Perusahaan tidak mampu untuk mengubah proses secara efektif mencapai tujuan dari perbaikan proses dan ketidakmampuan mengevaluasi keefektifan perubahan proses.

(Sumber: ISACA, 2013b)

Tabel 2.8 menjelaskan apa saja konsekuensi yang dapat dipertimbangkan oleh perusahaan dalam operasi yang efektif dan efisien sehingga mampu menentukan *targeted level* yang diinginkan perusahaan. Pada *level* 1, memiliki atribut proses yaitu PA.1.1 *(Process Performance)* konsekuensi potensialnya yaitu ketika produk kerja tidak ada dan hasil dari proses tidak tercapai. Pada *level* 2 atribut PA 2.1 *(Performance Management)* yaitu yang pertama ketika biaya atau waktu terjadi kelebihan, penggunaan sumber daya yang tidak efisien, tanggung jawab yang tidak jelas. Kedua, keputusan tidak terkendali, ketidakpastian apakah tujuan, waktu dan biaya terpenuhi. Pada atribut PA 2.2 *(Work product Management),* ketika kualitas

dan integritas produk tidak dapat diprediksi, peningkatan biaya pendukung, masalah integrasi dan biaya terkait pengerjaan ulang meningkat. Selanjutnya pada *level* 3 atribut PA 3.1 *(Process Definition)*, ketika pada perusahaan ingin mengidentifikasikan praktik terbaik dan mampu mempelajari hasil dari proyek-proyek sebelumnya, mendefinisikan segala proyek yang terdapat dalam organisasi dan ketika perusahaan belum ada fondasi terkait meningkatkan proses. Pada atribut 3.2 *(Process Deployment),* konsekuensinya ketika proses yang diimplementasikan tidak terdapat praktik terbaik yang sudah diidentifikasi dari proyek sebelumnya, kinerja proses tidak konsisten antar organisasi dan kehilangan peluang untuk memahami proses dan identifikasi perbaikannya. Selanjutnya yaitu *level* 4, pada atribut 4.1 *(Process Management)* keadaan di mana perusahaan tidak memiliki pemahaman kuantitatif tentang seberapa baik proses, tujuan kinerja dan tujuan bisnis tercapai. Lalu, tidak adanya kemampuan kuantitatif untuk mendeteksi masalah kinerja sejak dini. Pada atribut 4.2 *(Process Control),* keadaan di mana proses tidak dapat diprediksi dalam batas yang ditentukan dan tujuan kinerja kuantitatif dan tujuan bisnis yang telah ditetapkan tidak terpenuhi. Terakhir yaitu *level* 5, pada atribut 5.1 *(Process Inovation)*, yaitu pertimbangannya ketika tujuan perbaikan proses tidak didefinisikan dangan jelas dan peluang untuk perbaikan tidak teridentifikasi. Pada atribut 5.2 *(Process Optimization),* ketika perusahaan tidak mampu untuk mengubah proses secara efektif mencapai tujuan dari perbaikan proses dan ketidakmampuan mengevaluasi keefektifan perubahan proses.

Tahap kedua yaitu, *Determine Whether the Selected Process is a Level 1 Capability.* Pada tahapan ini ditentukan apakah sebuah proses benar-benar dilakukan dan sedang mencapai hasil. Dalam *worksheet self-asessment* ada tabel untuk setiap proses. Indikator pada kapabilitas *level* 1 spesifik untuk setiap proses dan mampu menilai apakah atribut tersebut telah tercapai. Artinya proses yang diimplementasikan mencapai tujuannya. Pada tahap ini dilakukan penyusunan lembar penilaian dengan kriteria yang sudah ditentukan pada *Process Assessment Model* (PAM) dari COBIT 5. Tabel 2.9 merupakan contoh dari lembar penilaian.

Tabel 2.9 Lembar Penilaian

EDM03	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	*Not Achieved* (0%-15%)	*Partially Achieved* (>15%-50%)	*Largely Achieved* (>50%-85%)	*Fully Achieved* (>85%-100%)	Keterangan	
								Base practices (BPs) / *Generic Practices* (GPs)	*Work product* (WPs) / *Generic Work products* (GWPs)

(Sumber: ISACA, 2013b)

Pada Tabel 2.9 pada kolom proses EDM03 diisi dengan *level* 0-5 dari *capability level*. Nantinya isi dari kolom atribut proses sesuai dengan atribut yang dimiliki oleh masing-masing *level*. Kolom kriteria akan diisi dengan kriteria yang dapat

dicapai apabila berada pada suatu atribut proses pada *level* tertentu. Kriteria ini sudah ditentukan oleh COBIT 5. Pada tahap kedua ini dilakukan penilaian terlebih dahulu untuk *level* 1, menurut ISACA (2013b) pada *level* 0 *(incomplete)* tidak memiliki kriteria. *Level* 1 pada PA.1.1 *(Process Performance)* kriterianya yaitu memiliki *base practices* dan *work product.*

Tahap ketiga yaitu, *Determine Whether Capability levels 2 to 5 for the Selected Processes are being Achieved*. Selanjutnya dimulai untuk *level* 2 sampai dengan *level* 5. *Level* 2 *(Managed)* pada atribut proses PA 2.1 *(Performance Management)* memiliki kriteria apabila tujuan dari pelaksanaan proses telah diidentifikasi, kinerja proses direncanakan dan telah diawasi, kinerja proses disesuaikan untuk memenuhi rencana yang telah ditetapkan, tanggung jawab beserta wewenang dalam pelaksanaan proses telah didefisinikan, ditugaskan dan dikomunikasikan, sumber dan informasi yang diperlukan dalam melakukan proses telah dilakukan identifikasi, tersedia, dialokasikan dan digunakan, antarmuka antara pihak-pihak terlibat berhasil mewujudkan komunikasi yang efektif dan penugasan tanggung jawab jelas. Sedangkan untuk PA 2.2 *(Work product Management)* memiliki kriteria jika persyaratan untuk hasil kerja proses ada, melakukan persyaratan untuk dokumentasi dan pengendalian hasil kerja, hasil kerja mampu diidentifikasi, didokumentasikan dan dikontrol dengan tepat, dan hasil kerja ditinjau sesuai dengan peraturan yang telah direncanakan dan disesuaikan seperlunya untuk memenuhi persyaratan.

Untuk *level* 3 *(established)* pada atribut proses PA 3.1 *(Process Definition)* kriterianya yaitu standar proses, termasuk panduan yang tepat, menggambarkan unsur fundamental yang dimasukkan ke dalam proses yang telah ditentukan, urutan dan interaksi standar untuk suatu proses dengan proses lainnya ditentukan, kompetensi dan peran yang diperlukan unruk melakukan suatu proses telah diidentifikasi, infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan suatu proses telah diidentifikasi sebagai bagaian dari standar proses, dan metode sesuai telah ditentukan untuk memantau keefektifan dan kesesuaian proses. Atribut proses PA 3.2 *(Process Deployment)* memiliki kriteria ketika proses yang telah didefisinikan dikerahkan berdasarkan standar proses, peran, tanggung jawab dan wewenang yang diperlukan proses telah didefinisikan dan dikomunikasikan, personil yang melakukan proses berkompeten berdasarkan pendidikan, pelatihan dan pengalaman yang sesuai, sumber daya dan informasi yang diperlukan proses tersedia, teralokasi dan digunakan dengan baik, infrastruktur dan lingkungan kerja yang dibutuhan tersedia dikelola dan dipelihara dan data yang tepat dikumpukkan serta dianalisis sebagai dasar untuk memahami perilaku proses, menunjukkan efektivitasnya dan untuk mengevaluasi perbaikan. Untuk *level* 4 *(predictable)* pada atribut proses PA 4.1 *(Process Measurement)* kriterianya yaitu kebutuhan dari proses informasi mendukung tujuan bisnis, tujuan dari penilaian berasal dari kebutuhan proses informasi, tujuan kuantitatif untuk kinerja proses dalam mendukung tujuan bisnis, penilaian dan frekuensi penilaian diidentifikasi dan didefinisikan sesuai dengan tujuan penilaian, hasil penilaian dikumpulkan, dianalisis dan dilaporkan untuk mengawasi sejauh mana tujuan

kuantitatif kinerja proses terpenuhi dan hasil penilaiannya digunakan untuk melakukan karakteristik kinerja proses.

Pada atribut proses PA 4.2 *(Process Control)* kriterianya yaitu ketika terdapat teknik analisis dan pengendalian yang telah ditentukan dan diterapkan bila memungkinkan, variasi akan batas kontrol ditetapkan untuk kinerja proses normal, data penilaian dianalisis untuk mengetahui variasi penyebab khusus, terdapat tindakan korektif yang diambil untuk mengatasi variasi penyebab khusus tersebut, dan batas kontrol ditetapkan. Dan terakhir untuk *level* 5 *(optimizing)* pada atribut proses PA 5.1 *(Process Inovation)* memiliki kriteria apabila tujuan perbaikan proses didefinisikan untuk mendukung tujuan bisnis yang relevan, data yang tepat dianalisis untuk mengidentifikasi variasi penyebab umum dalam kinerja proses dan mengidentifikasi praktik peulang dan inovasi terbaik, peluang perbaikan yang berasal dari teknologi baru dan konsep proses diidentifikasi, serta strategi implementasi ditetapkan untuk mencapai tujuan perbaikan proses. Dan untuk PA 5.2 *(Process Optimisation)* kriterianya yaitu dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan proses dan standar yang ditetapkan, pelaksanaan semua perubahan berhasil dan segala gangguan dipahami serta ditindaklanjuti dan berdasarkan kinerja aktual, keefektifan perubahan proses dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk menentukan apakah hasil tersebut disebabkan oleh sebab umum atau khusus. Setiap proses harus dibuat apakah kriteria telah dipenuhi, dan keputusan itu harus diterjemahkan ke dalam penilaian dan dicatat. Ini harus diulang untuk setiap *capability* hingga *level capability* dinilai sebagai *'largely'* atau *'fully achieved'*. Isi kriteria juga nantinya pada *level* 2-5 akan sesuai dengan *Process Assessment Model* COBIT 5. Tahap keempat, *Record and Summarise the Capability levels.* Ringkasan hasil penilaian harus dicatat, contohnya pada Tabel 2.10. *Capability level* ditentukan pada *level* di mana kedua indikator *capability* tersebut *'largely'* atau *'fully achieved'*.

Tabel 2.10 Detail Penilaian Atribut Proses dengan Skala

Process Name	***Level* 0**	***Level* 1**	***Level* 2**		***Level* 3**		***Level* 4**		***Level* 5**	
EDM03		**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
Rating by Criteria										
Capability level Achieved										
N *(Not Achieved, 0%-15%),* P *(Partially Achieved, >15%-50%),* L *(Largely Achieved, >50%-85%),* F *(Fully Achieved, >85%-100%)*										

(Sumber: ISACA, 2013b)

Pada Tabel 2.10 merupakan contoh format tabel yang dapat digunakan dalam melakukan ringkasan dari hasil penilaian *level capability.* Diisi skala yang menunjukkan pada setiap atribut yang dicapai sehingga nantinya memudahkan dalam penentuan pembacaan pola, pada proses tertentu mencapai *level* berapa. Selanjutnya dilakukan ringkasan lebih singkat, yang hanya berisi nama proses dengan *capability level* yang dicapai dengan target *level* yang diinginkan perusahaan sehingga dapat dilihat kesenjangan antara *level* yang dicapai saat ini dengan target yang diharapkan perusahaan. Selanjutnya isi sesuai dengan *level* yang dicapai pada setiap proses. Contoh ringkasan tabel dari hasil penilaian sama seperti pada Tabel 2.7. Proses yang telah diketahui *capability level*nya akan disandingkan dengan target *level* yang diharapkan oleh perusahaan.

Tahap kelima, *Develop an Improvement Plan of Action*. Berdasarkan *self assessment*, pertimbangan harus diberikan pada pengembangan rencana tindakan untuk perbaikan proses. Salah satu pilihannya adalah memulai rencana perbaikan. Hal ini mampu mengatasi area yang paling penting bagi sasaran bisnis perusahaan dan berfokus pada area yang memiliki kesenjangan antara proses *capability level* 'saat ini' dengan '*targeted*'. Pilihan kedua adalah melakukan penilaian independen yang lebih formal, berdasarkan COBIT PAM dan panduan asesor. Ini akan memberikan penilaian yang lebih andal dan lebih banyak panduan untuk bidang perbaikan yang dibutuhkan. Pada tahap ini akan dihasil rekomendasi bagaimana perusahaan mampu mencapai *targeted level* yang diharapkan.

2.10 Proses Penilaian Kapabilitas Model COBIT 5

Kumpulan produk dari COBIT 5 mencakup model kemampuan proses, berdasarkan ISO-IEC 15504 *Software Engineering-Process Assessment* yang diakui secara internasional. Model ini akan mencapai keseluruhan tujuan dari penilaian proses dan dukungan dari perbaikan proses, yaitu akan menyediakan sarana untuk mengukur kinerja proses atau pengelolaan berbasis prinsip (berbasis EDM) atau proses pengelolaan (PBRM) dan akan memungkinkan daerah untuk perbaikan yang akan diidentifikasi. Proses perhitungan melibatkan beberapa *capability rating* untuk setiap prosesnya yaitu melibatkan pendefinisian *capability level*, atribut proses yang digunakan untuk menilai setiap proses, indikator yang menjadi dasar pencapaian penilaian setiap atribut proses dan skala penilaian standar.

Menurut ISACA (2013c), tingkatan dari kapabilitas yaitu, *Level 0 Incomplete Process*, pada *level* ini proses tidak diimplementasikan atau gagal dalam meraih tujuan dari proses sehingga tidak memiliki atribut pada *level* ini. *Level* 1 *Performed Process* (1 atribut), proses yang diimplementasikan mencapai tujuan prosesnya. *Level* 2 *Managed Process* (2 atribut), proses yang telah dijelaskan sebelumnya saat ini diterapkan dengan cara yang dikelola (direncanakan, diawasi, dan disesuaikan) dan produk kerjanya telah ditetapkan dengan benar. *Level* 3 *Establish Process* (2 atribut), proses pengelolaan yang telah dijelaskan sebelumnya saat ini diterapkan dengan menggunakan proses yang didefinisikan yang mampu mencapai hasil prosesnya. *Level* 4 *Predictable Process* (2 atribut), proses yang telah dijelaskan sebelumnya saat ini beroperasi dalam batasan yang ditetapkan untuk mencapai

hasil prosesnya. Dan *level* 5 *Optimising Process* (2 atribut), proses yang dapat diprediksi sebelumnya terus ditingkatkan untuk memenuhi tujuan bisnis saat ini dan diproyeksikan. Perlu diingat bahwa pada *level* 1 dijadikan indikator khusus bagi perusahaan pada setiap proses sehingga menilai apakah atribut terkait telah tercapai atau dalam artian dapat dijadikan acuan awal akan proses yang diimplementasikan mencapai tujuan dari proses itu sendiri. Untuk *level* 2-5 penilaian kapabilitas ini didasarkan pada indikator kinerja dari proses generik. Disebut generik karena berlaku di semua proses, namun tetap berbeda dari satu *level* ke *level* lainnya. Secara umum dapat dipahami bahwa ketika semakin tinggi *level* dari kapabilitas proses yang dicapai, maka semakin rendah risiko proses gagal memenuhi tujuannya. Dan juga ketika *level* kapabilitas semakin tinggi, maka semakin mahal proses operasinya.

Atribut proses yang terlibat dalam setiap *level* dengan diberikan label atau kode berupa PA *(Process Atribute).* Pada *level* 0 *(Incomplete)* tidak memiliki atribut. Pada *level* 1, memiliki 1 atribut yaitu PA.1.1 (*Process Performance)*, atribut ini adalah pengukuran mengenai seberapa jauh proses mampu mencapai tujuan yang telah didefinisikan atau direncakan. Berarti harus ada dokumen yang dapat ditunjukkan. Selanjutnya terdapat 2 atribut pada *level* 2, yaitu yang pertama PA 2.1 (*Performance Management*), yaitu pengukuran mengenai performa proses dikelola dan yang kedua PA 2.2 (*Work product Management*), pengukuran hasil kerja yang telah dihasilkan oleh proses yang dikelola. Pada *level* 3 memiliki dua atribut, yang pertama PA 3.1 (*Process Defintion*), pengukuran sejauh mana proses standar dikelola untuk mendukung proses yang telah didefinisikan. Kedua, PA 3.2 (*Process Deployement*), pengukuran proses standar secara efektif sudah sejauh mana dijalankan seperti proses yang telah didefinisikan untuk mencapai hasil dari proses. *Level* 4 memiliki dua atribut juga, yang pertama PA 4.1 (*Process Measurement*) proses pengukuran mengenai seberapa jauh hasil pengukuran digunakan untuk memastikan bahwa performa proses mendukung pecapaian tujuan proses dan tujuan organisasi. Kedua, PA 4.2 (*Process Control*), pengukuran tentang seberapa jauh suatu proses secara kuantitatif bisa menghasilkan proses yang stabil, mampu dan bisa diprediksi dalam batasan telah ditentukan. Dan yang terakhir untuk *level* 5 memiliki dua atribut yang pertama PA 5.1 (*Process Innovation)*, mengukur sebuah perubahan proses yang telah diidentifikasi dari analisis penyebab umum dari adanya variasi di dalam performa, dan dari investigasi pendekatan inovatif untuk mendefinisikan dan melaksanakan proses. Kedua, PA 5.2 (*Process Optimisation)*, mengukur perubahan untuk definisi, manajemen, performa proses agar memiliki hasil yang efektif untuk mencapai tujuan dari proses peningkatan.

Dalam melakukan pengukuran terhadap *level* yang dicapai pada setiap atribut proses diberikan penilaian menggunakan skala. Skala pertama yaitu, N (*Not Achieved* atau tidak tercapai), dalam kategori ini tidak ada atau hanya sedikit bukti atas pencapaian atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar antara 0-15%. Skala kedua, P (*Partially Achieved* atau tercapai sebagian), dalam kategori ini terdapat beberapa bukti mengenai pendekatan, dan beberapa pencapaian atribut atas proses tersebut. *Range* nilai yang diraih pada kategori ini

berkisar antara 15-50%. Skala ketiga, L (*Largely Achieved* atau secara garis besar tercapai), dalam kategori ini terdapat bukti atas pendekatan sistematis, dan pencapaian signifikan atas proses tersebut, meski mungkin masih ada kelemahan yang tidak signifikan. *Range* nilai yang diraih pada kategori ini berkisar antara 50-85%. Skala keempat, F *(Fully Achieved* atau tercapai penuh), jika terdapat bukti atas pendekatan sistematis dan lengkap, dan pencapaian penuh atas atribut diklarifikasikan dalam kategori ini. Tidak ada kelemahan terkait atribut proses tersebut. *Range* nilai yang diraih pada kategori ini berkisar antara 85-100%.

Dalam proses pencapaian *level*, terdapat pola yang digunakan. Maksudnya, ada skala yang harus dicapai ketika akan melanjutkan penilaian kapabilitas untuk *level* selanjutnya. Pola yang harus dipenuhi ketika melakukan penilaian *capability level.* Suatu proses dapat dinilai pada satu tingkat dengan atribut *'largely'* atau *'fully'* tercapai. Namun, atribut itu perlu dicapai hingga *'fully'* untuk dinilai pada tingkat berikutnya. Misal, *level* 1 pada atribut *process performance* dapat dicapai dengan Largely atau Fully. Namun, ketika melakukan penilaian untuk *level* 2 *process performance* harus dicapai Fully atau sekitar >85%-100%. Dan untuk atribut *performance management* dan *work product management* dapat dicapai dengan Largely atau Fully. Selanjutnya apabila ingin melakukan penilaian pada *level* selanjutnya, sama seperti apa yang telah dijelaskan pada *level* 1 dan 2. Berikut merupakan tabel yang berisi pola dalam pemberian penilaian atribut proses dengan skala.

Tabel 2.11 Pola Penilaian Skala Atribut Proses

Level	Atribut Proses	Skala
1	*Process Performance*	*Largely or Fully*
2	*Process Performance*	*Fully*
	Performance Management	*Largely or Fully*
	Work product Management	*Largely or Fully*
3	*Process Performance*	*Fully*
	Performance Management	*Fully*
	Work product Management	*Fully*
	Process Definition	*Largely or Fully*
	Process Deployment	*Largely or Fully*
4	*Process Performance*	*Fully*
	Performance Management	*Fully*
	Work product Management	*Fully*
	Process Definition	*Fully*
	Process Deployment	*Fully*

Tabel 2.11 Pola Penilaian Skala Atribut Proses (Lanjutan)

Level	Atribut Proses	Skala
	Process Measurement	*Largely or Fully*
	Process Control	*Largely or Fully*
5	*Process Performance*	*Fully*
	Performance Management	*Fully*
	Work product Management	*Fully*
	Process Definition	*Fully*
	Process Deployment	*Fully*
	Process Measurement	*Fully*
	Process Control	*Fully*
	Process Innovation	*Largely or Fully*
	Process Optimization	*Largely or Fully*

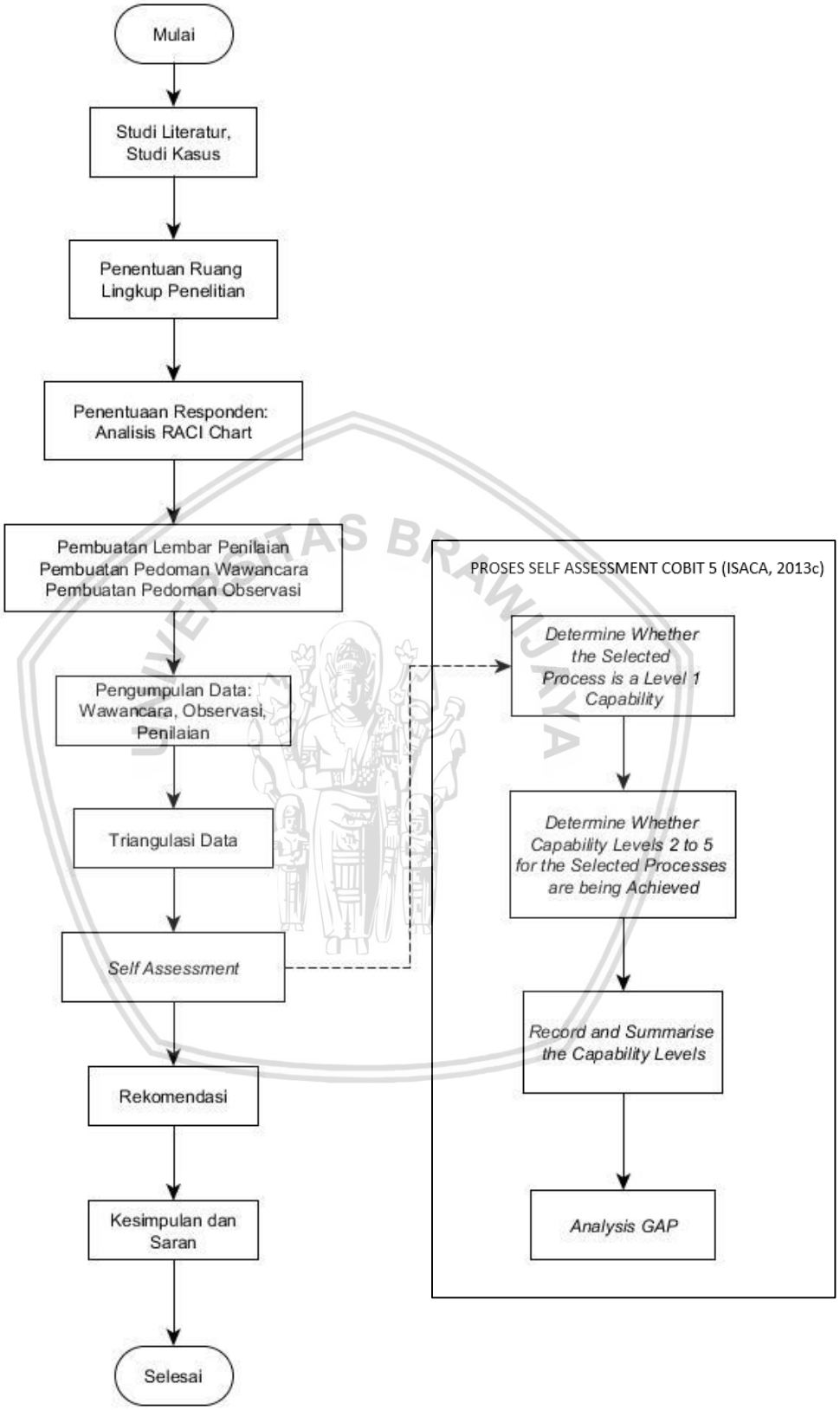
(Sumber: ISACA, 2013b)

BAB 3 METODOLOGI

3.1 Metodologi Penelitian

Dalam penelitian ini, metode yang digunakan yaitu metode kualitatif. Metode ini dirancang untuk membantu peneliti memahami fenomena dalam konteks. Menurut Recker (2013), metode kualitatif merupakan strategi investigasi yang menyelidiki fenomena dalam konteks kehidupan nyata. Metode ini cocok untuk penelitian eksplorasi, di mana fenomena belum sepenuhnya dipahami. Dengan menggunakan metode ini, fokus kepada interpretasi data. Data yang didapatkan nantinya berasal dari wawancara, observasi dan hasil dari lembar penilaian. Dari data yang didapatkan, dilakukan analisis guna mendapatkan *level capability* sehingga menghasilkan rekomendasi.

Dalam teknik mengumpulkan data, metode kualitatif ini memiliki berbagai cara. Pada penelitian ini menggunakan wawancara deskriptif, yaitu wawancara yang digunakan untuk memberikan gambaran yang jelas tentang fenomena yang dirasakan oleh individu. Dengan cara ini, pemahaman subjektif dapat dihasilkan. Wawancara memberikan keuntungan karena fokus langsung pada topik yang dipilih dan dapat memberikan kesimpulan kausal seperti yang dirasakan oleh mereka yang diwawancarai. Teknik kedua yang digunakan yaitu *direct observation*. Pengamatan langsung yang melibatkan peneliti sebagai pengamat pasif dan netral. Terakhir, yaitu dengan melakukan penilaian menggunakan lembar *checklist* yang telah diisi responden sesuai dengan hasil pemetaan RACI *Chart* dari masing-masing proses. Dari beberapa metode pengambilan data yang dilakukan, akan dilakukan triangulasi data untuk memastikan bahwa data yang telah didapatkan memiliki kredibilitas. Selanjutnya akan dilakukan *Self assessment* sesuai dengan COBIT 5 hingga dihasilkan rekomendasi bagi perusahaan. Pada Gambar 3.1 merupakan alur kerja yang dilakukan dalam penelitian:



Gambar 3.1 Diagram Alur Penelitian

Gambar 3.1 merupakan diagram alur dari penelitian yang dilakukan dalam penelitian beserta laporan yang akan dilakukan oleh peneliti dan mengacu pada *framework* COBIT 5, risiko, manajemen risiko dan keamanan. Ada sembilan tahap yang akan dilakukan, pertama yaitu melakukan studi literatur mengenai *framework* COBIT 5 dan jurnal maupun artikel yang berkaitan dengan *framework* COBIT 5. Kedua, penentuan untuk ruang lingkup, pada penelitian ini dilakukan penilaian terkait proses EDM03 *(Ensure Risk Optimisation),* APO12 *(Manage Risk)* dan APO13 *(Manage Keamanan).* Ketiga, melakukan analisis RACI *Chart* dan gambaran dari objek yang diteliti sehingga mampu mengetahui pihak yang terlibat dalam proses yang ditentukan. Keempat, melakukan pembuatan pedoman dalam mengumpulkan data untuk beberapa metode yang digunakan yaitu, wawancara, observasi dan lembar penilaian. Kelima, melalukan pengumpulan data dari pedoman yang telah disusun. Setelah data berhasil dikumpulan, keenam yaitu menganalisis data yang telah didapatkan dengan melakukan triangulasi data untuk memvaliditasi hasil temuan. Ketujuh, dilakukan *self assessment* untuk memastikan ketercapaian dari masing-masing proses pada *capability level.* Pada tahapan *self assessment* diberikan tambahan untuk melakukan analisis kesenjangan antara *level* yang didapatkan saat ini *(capability level)* dengan *targeted level* yang ingin dicapai oleh perusahaan. Sehingga terakhir akan dilakukan perumusan rekomendasi bagi perusahaan untuk mencapai *targeted level* yang diharapkan.

3.2 Studi Literatur

Pada tahap ini, dilakukan dengan mencari dan mempelajari literatur baik dari buku, jurnal, laporan penelitian maupun artikel yang berhubungan dengan penilaian *capability level* dengan menggunakan *framework* COBIT 5. Subjek penelitian ini yaitu evaluasi dari penilaian *capability* pada penerapan manajemen risiko. Dan objek penelitian ini yaitu penerapan manajemen risiko pada PDAM Kota Malang.

3.3 Penentuan Ruang Lingkup Penelitian

Sebelum melakukan penelitian, dilakukan penentuan untuk mengetahui proses apa saja yang akan diteliti. Pada tahapan ini mengadopsi dari tahap pertama dalam *self assessment* yaitu penentuan proses. Sehingga untuk proses yang akan diteliti yaitu proses EDM03 mengenai optimasi risiko, APO12 mengenai pengelolaan risiko dan APO13 mengenai pengelolaan keamanan.

3.4 RACI *Chart*

Dalam melakukan penilaian, peneliti terlebih dahulu melakukan analisis RACI *Chart* guna mengetahui sumber daya manusia yang terlibat dalam *subdomain* EDM03, APO12 dan APO13. Analisis dilakukan terhadap pihak yang berperan sebagai *responsible*, *accountable*, *consulted* dan *informed*. Sehingga hasilnya dapat digunakan untuk mengetahui responden yang tepat untuk mendapatkan data yang mendukung penelitian.

3.5 Pembuatan Pedoman Pengumpulan Data

Pembuatan pedoman pengumpulan data dilakukan sebagai acuan dalam melakukan wawancara, observasi dan penilaian. Pada lembar penilaian akan digunakan referensi COBIT 5 *Self assessment* dan PAM. Untuk wawancara akan disusun pertanyaan-pertanyaan sesuai dengan responden yang telah dipetakan menggunakan RACI *Chart*. Dan untuk observasi akan mengetahui apa saja yang harus diamati dalam mendukung penelitian dengan bantuan *checklist.* Kesesuaian antara jenis dokumen dalam hal ini *yaitu base practices, work products, generic products dan generic work products* perlu diterjemahkan kedalam tempat atau objek dari penelitian. Artinya, perlu adanya proses konsultasi antara responden dengan expert atau ahli. Sehingga terdapat kesesuaian antara dokumen yang tersedia di tempat penelitian dengan yang dituntut dalam COBIT 5.

3.6 Pengumpulan Data

Pada penelitian ini dilakukan tiga siklus dalam pengambilan datanya. Siklus yang pertama yaitu melakukan wawancara yang hasilnya akan digunakan sebagai studi pendahuluan. Sehingga ditemukan fakta ataupun masalah terkait dengan tema yang sudah ditentukan. Selain itu pada siklus pertama dilakukan pemetaan untuk menentukan RACI *Chart* dari perusahaan dan menggunakan *checklist* terkait *targeted level* yang diharapkan oleh perusahaan terkait proses atau *subdomain* EDM03, APO12 dan APO13. Siklus yang kedua yaitu menggunakan *checklist* guna menemukan *evidence* atau barang bukti terkait masing-masing proses atau *subdomain* EDM03, APO12 dan APO13. Pada *checklist* ini berisi *base practices* dan *work products subdomain* EDM03, APO12 dan APO13. Siklus ketiga yaitu melakukan kegiatan triangulasi. Dalam kegiatan triangulasi ini dilakukan konfirmasi terkait hasil yang didapatkan dari siklus kedua dan konfirmasi kembali terkait *targeted level* yang perusahaan harapkan.

3.7 Triangulasi Data

Triangulasi ini berarti mencari konvergensi (keadaan menuju satu titik pusat) dan menguatkan hasil dari berbagai metode yang sudah dilakukan untuk mengumpulkan data. Pada sub bab sebelumnya dijelaskan bahwa 3 metode dilakukan dalam pengumpulan data yaitu, wawancara, observasi dan lembar penilaian. Melalui triangulasi data, peneliti bisa mendapatkan gambaran situasi yang lebih bernuansa, dan meningkatkan kehandalan dan validitas temuan mereka. Maka akan mencapai kredibilitas, menjaga rantai bukti, dan menyimpan catatan yang jelas mengenai keputusan yang dibuat selama proses penelitian (Recker, 2013).

Menurut Bachri (2010), triangulasi merupakan metode sintesa data terhadap kebenarannya dengan menggunakan metode pengumpulan data yang lain atau berbagai paradigma triangulasi. Data yang dinyatakan valid oleh triangulasi mampu memberikan keyakinan terhadap peneliti akan keabsahan data, sehingga mampu mengambil kesimpulan dengan baik. Triangulasi menyediakan satu perangkat kuat ketika diperlukan satu respon yang cepat, atau ketika data harus

menjawab pertanyaan yang spesifik. Dengan demikian, triangulasi mampu meningkatkan pemahaman peneliti akan fakta yang dimilikinya bukan untuk mencapai kebenaran.

Pada tahap triangulasi data ini, yang pertama dilakukan kegiatan konfirmasi hasil dari siklus kedua pengambilan data dengan melakukannya pada siklus ketiga dengan cara melakukan wawancara dan observasi. Nantinya setelah didapatkan hasil wawancara dan observasi, penelitian akan melakukan *self assessment* untuk mendapatkan *capability level*. Setelah diperoleh hasil, akan dilakukan kegiatan konfirmasi kembali terkait hasil dan *targeted level*. Kegiatan konfirmasi ini yang termasuk dalam kegiatan triangulasi data.

3.8 *Self assessment*

Terdapat 5 tahapan yang akan dilakukan dalam *self assessment*. Pertama menentukan proses apa saja yang akan dinilai (EDM03, APO12, APO13). Namun untuk tahap pertama dilakukan pada awal penelitian. Kedua, menentukan setiap proses mampu mencapai *level* 1. Ketiga, melakukan penilaian pada setiap proses untuk mencapai *level* 2 sampai 5. Keempat, melakukan pencatatan akan hasil yang telah didapatkan dari penentuan *level* 1-5. Terdapat penambahan tahap yaitu analisis *gap*, yang digunakan untuk mengetahui kesenjangan antara *capability level* dan *targeted level* yang diinginkan sehingga akan mampu terorganisir dalam melakukan perumusan rekomendasi. Kelima, melakukan pertimbangan untuk dilakukan rencana perbaikan proses sehingga mampu memenuhi target *level* yang diharapkan. Pada tahap kelima ini dilakukan pemecahan tahap juga, sehingga dalam penelitian ini digunakan istilah rekomendasi.

3.9 Rekomendasi

Rekomendasi disusun berdasarkan analisis-analisis yang sudah dihasilkan. Nantinya rekomendasi ini diharapkan mampu membantu perusahaan dalam mencapai tujuannya dan mencapai tingkat kapabilitas yang diharapkan. Rekomendasi ini merupakan adaptasi dari tahap *self assessment* yang kelima, karena pada dasarnya tahap kelima dari *self assessment* adalah menentukan rencana untuk aksi yang akan dilakukan perusahaan demi mencapai *targeted level* yang diharapkan.

3.10 Kesimpulan dan Saran

Kesimpulan diperoleh berdasarkan jawaban dari rumusan masalah yang sudah ditetapkan dan hasil yang diperoleh, yaitu tentang penilaian dari *level capability* dalam bentuk deskriptif yang nantinya diberikan analisis terkait penerapan manajemen risiko TI berdasarkan *subdomain* EDM03, APO12 dan APO13.

BAB 4 HASIL DAN ANALISIS

4.1 Pemetaan RACI *Chart*

RACI *Chart* digunakan sebelum melakukan pengambilan data, sehingga mampu mengetahui siapa yang dapat menjadi responden bagi ruang lingkup atau proses yang telah ditentukan. Berikut adalah hasil dari pemetaan RACI *Chart* untuk proses EDM03 yaitu optimasi risiko.

Tabel 4.1 Hasil Pemetaan RACI *Chart* EDM03

Komponen	Tugas	Jabatan
Responsible	*a. Business Executive* *b. Strategy Executive Comittee*	Kepala Pusat SIM
Accountable	*Board*	Direktur Utama
Consulted	*a. Chief Operating Officer* *b. Business Process Owner*	Direktur Utama
Informed	*a. Head Development* *b. Information Security Manager*	Kepala Pusat SIM

Tabel 4.1 menunjukkan *roles* berdasarkan *framework* COBIT 5 siapa saja yang bertindak sebagai *responsible, accountable, consulted* dan *informed*. Pemilihan *roles* dilakukan dengan melakukan perhitungan sesuai dengan COBIT 5. Contohnya untuk komponen *responsible*, dipilih *roles* yang di mana memiliki komponen *resposible* terhadap ketiga *base practices* yang dimiliki dari *subdomain* EDM03. Yaitu EDM03-BP1 *(Evaluate Risk Management),* EDM03-BP2 (Direct *Risk* Management) dan EDM03-BP3 *(Monitor Risk Management).* Ini dilakukan karena penting untuk mengetahui bagaimana kondisi perusahaan terkait dengan ketiga *base practices* yang dimiliki sehingga hasil dari pengumpulan data melalui responden dapat lebih akurat. Namun, ISACA menentukan bahwa untuk menjadi responden hanya dapat dipilih jabatan yang memiliki komponen R atau A. Ini dikarenakan R terlibat langsung dalam proses atau memiliki peran yang penting dalam memenuhi aktivitas. Dan untuk A dikarenakan mereka bertanggung jawab atas keberhasilan dari aktivitas atau tugas yang dijalankan oleh R. Dan menurut hasil wawancara seperti yang terlampir pada Lampiran A.3, bahwa kepala pusat SIM memiliki beberapa tugas yang sama sesuai dengan yang telah dideskripsikan oleh ISACA yaitu *Business Excecutive* dan *Strategy Executive Comittee* pada komponen R. *Business Executive* memiliki wewenang untuk mengelola operasi unit bisnis tertentu dan *Strategy Executive Comittee* bertanggung jawab terhadap semua aspek risiko mulai dari risiko operasional, risiko bencana, risiko keuangan, dan risiko strategi.

Selanjutnya untuk komponen A pada proses ini yaitu *Board* di mana memiliki tanggung jawab yang sama dengan Direktur Utama. ISACA mendeskripsikan *board* bertanggung jawab dalam proses tata kelola organisasi dan memiliki kontrol penuh pada sumber daya organisasi. Komponen C pada proses ini yaitu *Chief Operating Officer* dan *Business Process Owner.* Deskripsi *Chief Operating Officer* yaitu bertanggung jawab dalam segala operasi perusahaan. Sedangkan untuk *Business Process Owner* bertanggung jawab atas kinerja sebuah proses dalam mencapai tujuannya, mendorong perbaikan proses, dan menyetujui perubahan proses. Ini sesuai dengan hasil wawancara pada Lampiran A.3 bahwa kedua tugas ini dipegang oleh Direktur Utama. Kompenen I pada proses ini yaitu *Head Development* dan *Information Security Manager.* Deskripsi *Head Development* yaitu bertanggung jawab atas pengembangan solusi TI dan *Information Security Manager* bertugas untuk mengelola, merancang dan mengawasi dan / atau menilai keamanan informasi perusahaan. Peneliti hanya melakukan pemaparan hasil dari RACI *Chart* yang memungkinkan untuk dijadikan responden namun karena keterbatasan akses maka peneliti memilih Kepala Pusat SIM sebagai responden terkait proses dari *subdomain* EDM03. Selanjutnya merupakan hasil pemetaan RACI *Chart* dari *subdomain* APO12.

Tabel 4.2 Hasil Pemetaan RACI *Chart* APO12

Komponen	Tugas	Jabatan
Responsible	*Chief Information Security Officer*	*Programmer* IT
	Business Process Owner	Direktur Utama
	Chief Risk Officer	a. Kepala Bidang *Software* dan *Database* b. Kepala Bidang *Hardware* dan Jaringan
Accountable	*Chief Information Officer*	a. *Programmer* dan b. *Help desk* TI
Consulted	*a. Head Development* *b. Information Security Manager*	Kepala Pusat SIM
Informed	*a. Chief Executive Officer* *b. Enterprise Risk Committee*	Direktur Utama

Tabel 4.2 menunjukkan *roles* berdasarkan *framework* COBIT 5 siapa saja yang bertindak sebagai *responsible, accountable, consulted* dan *informed*. Pemilihan *roles* dilakukan dengan melakukan perhitungan sesuai dengan COBIT 5. Contohnya untuk komponen *responsible*, dipilih *roles* yang di mana memiliki komponen *resposible* terhadap keenam *base practices* yang dimiliki dari *subdomain* APO12. Yaitu APO12-BP1 *(Collect Data),* APO12-BP2 *(Analyse Risk),* APO12-BP3 *(Maintain a Risk Profile)*, APO12-BP4 *(Articulate Risk),* APO12-BP5 *(Define a Risk*

Management Action Portofolio) dan APO12-BP6 *(Respond to Risk)*. Ini dilakukan karena penting untuk mengetahui bagaimana kondisi perusahaan terkait dengan keenam *base practices* yang dimiliki sehingga hasil dari pengumpulan data melalui responden dapat lebih akurat. Namun, ISACA menentukan bahwa untuk menjadi responden hanya dapat dipilih jabatan yang memiliki komponen R atau A. Ini dikarenakan R terlibat langsung dalam proses atau memiliki peran yang penting dalam memenuhi aktivitas. Dan untuk A dikarenakan mereka bertanggung jawab atas keberhasilan dari aktivitas atau tugas yang dijalankan oleh R. Menurut hasil wawancara seperti yang terlampir pada Lampiran A.3, bahwa *Programmer* IT memiliki tugas yang sama sesuai dengan telah dideskripsikan oleh ISACA yaitu *Chief Information Security Officer* pada komponen R. *Chief Information Security Officer* bertanggung jawab untuk menyelaraskan strategi TI dengan bisnis, serta bertanggung jawab atas perencanaan, sumber daya dan manajemen penyampaian layanan dan solusi TI untuk mendukung tujuan perusahaan. Direktur Utama juga berada pada komponen R di mana tugas dan tanggung jawab sama seperti *Business Process Owner* yaitu memberikan rencana pengelolaan risiko TI. Dan *Chief Risk Officer* yang bertanggung jawab terhadap semua aspek risiko mulai dari risiko operasional, risiko bencana, risiko keuangan dan strategi risiko. CRO ini bertugas dalam pengelolaan risiko TI perusahaan di mana pada perusahaan dipegang oleh Kepala Bidang *Software* dan *Database* serta Kepala Bidang *Hardware* dan Jaringan.

Selanjutnya untuk komponen A pada proses ini yaitu *Chief Information Officer* yaitu bertanggung jawab untuk menyelaraskan strategi TI dengan bisnis, serta bertanggung jawab atas perencanaan, sumber daya dan manajemen penyampaian layanan dan solusi TI untuk mendukung tujuan perusahaan. Tanggung jawab ini dipengang oleh *Programmer* dan *Help Desk* TI. Komponen C pada proses ini yaitu *Head Development* dan *Information Security Manager* di mana deskripsinya sama seperti tugas dan tanggung jawab dari Kepala Pusat SIM. *Head Development* yaitu bertanggung jawab atas proses pengembangan solusi TI dan *Information Security Manager* mengelola, merancang, dan mengawasi dan / atau menilai keamanan informasi perusahaan. Dan komponen I yaitu *Chief Executive Officer* dan *Enterprise Risk Committee* yang menurut hasil wawancara sama dengan tugas dan tanggung jawab Direktur Utama. *Chief Executive Officer* bertanggung jawab untuk mendapatkan informasi mengenai aktivitas pendefinisian dan pengelolaan rencana TI serta bertanggung jawab mengatur keseluruhan organisasi. *Enterprise Risk Committee* bertanggung jawab atas kolaborasi dan tingkat kosensus perusahaan yang dibutuhkan untuk mendukung aktivitas dan keputusan manajemen risiko perusahaan. Peneliti hanya melakukan pemaparan hasil dari RACI *Chart* yang memungkinkan untuk dijadikan responden namun karena keterbatasan akses, peneliti hanya memilih *Progammer* sebagai responden terkait proses dari *subdomain* APO12. Selanjutnya merupakan hasil pemetaan RACI *Chart* dari *subdomain* APO13.

Tabel 4.3 Hasil Pemetaan RACI *Chart* APO13

Komponen	Tugas	Jabatan
Responsible	*Chief Information Officer*	*a. Programmer* dan *b. Help desk* IT
	Information Security Manager	Kepala Pusat SIM
Accountable	*Chief Information Security Officer*	*a. Programmer* IT dan *b. Help desk* IT
Consulted	*a. Business Executive* *b. Strategy Executive Committee*	Kepala Pusat SIM
Informed	*Steering (Programmer/project) Commitee*	Direktur Utama

Tabel 4.3 menunjukkan *roles* berdasarkan *framework* COBIT 5 siapa saja yang bertindak sebagai *responsible, accountable, consulted* dan *informed*. Pemilihan *roles* dilakukan dengan melakukan perhitungan sesuai dengan COBIT 5. Contohnya untuk komponen *responsible*, dipilih *roles* yang di mana memiliki komponen *resposible* terhadap ketiga *base practices* yang dimiliki dari *subdomain* APO13. Yaitu APO13-BP1 *(Establish and Maintain an Information Security Management* (ISMS)*),* APO13-BP2 *(Define and Manage an Information Security Risk Treatment Plan),* dan APO13-BP3 *(Monitor and Review the* ISMS*).* Ini dilakukan karena penting untuk mengetahui bagaimana kondisi perusahaan terkait dengan ketiga *base practices* yang dimiliki sehingga hasil dari pengumpulan data melalui responden dapat lebih akurat. Namun, ISACA menentukan bahwa untuk menjadi responden hanya dapat dipilih jabatan yang memiliki komponen R atau A. Ini dikarenakan R terlibat langsung dalam proses atau memiliki peran yang penting dalam memenuhi aktivitas. Dan untuk A dikarenakan mereka bertanggung jawab atas keberhasilan dari aktivitas atau tugas yang dijalankan oleh R. Dan menurut hasil wawancara seperti yang terlampir pada Lampiran A.3, bahwa pada komponen R *Chief Information Officer* sama seperti *Programmer* dan *Help Desk* IT pada perusahaan. Di mana deskripsi dari *Chief Information Officer* yaitu bertanggung jawab untuk menangani masalah teknologi informasi pada perusahaan. Selanjutnya pada Komponen R terdapat *Information Security Manager* di mana sama seperti Kepala Pusat SIM pada perusahaan. *Information Security Manager* merupakan pihak yang bertanggung jawab dalam penerapan pengembangan keamanan TI perusahaan.

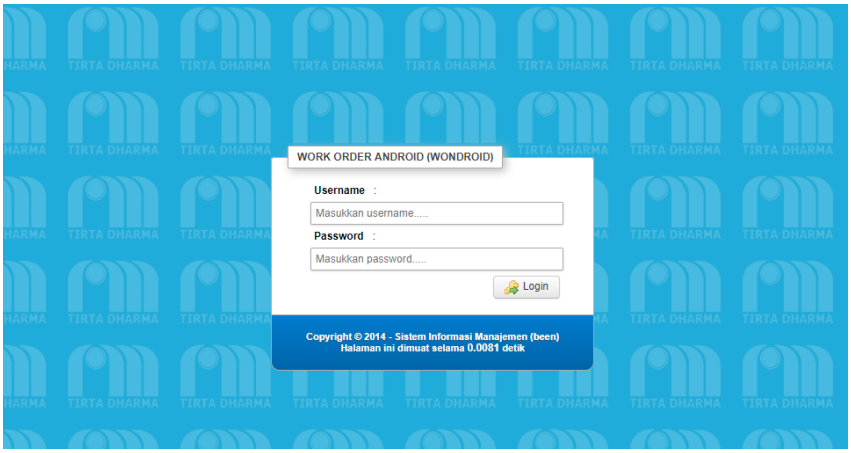
Selanjutnya untuk komponen A pada proses ini yaitu *Chief Information Security Officer* di mana deskripsinya sama seperti *Programmer* IT dan *Help Desk* IT pada perusahaan. *Information Security Manager* bertugas untuk mengelola, merancang dan mengawasi dan / atau menilai keamanan informasi perusahaan. Pada komponen C terdapat *Business Executive* dan *Strategy Executive Committee* di mana sama seperti Kepala Pusat SIM pada perusahaan. *Business Executive* memiliki wewenang untuk mengelola operasi unit bisnis tertentu sedangkan *Strategy Executive Committee* bertanggung jawab untuk mengelola portofolio akan investasi TI, layanan TI dan aset TI, selanjutnya memastikan bahwa nilai dan

risiko sudah dilakukan manajemen atau dikelola. Dan untuk komponen I pada proses ini yaitu *Steering (Progammer/Project) Committee* di mana deskripsinya sama seperti Direktur Utama pada perusahaan. *Steering (Progammer/Project) Committee* merupakan sekelompok pemangku kepentingan dan ahli yang bertanggung jawab atas pembinaan program dan proyek, termasuk manajemen dan pengawasan rencana, alokasi sumber daya, penyampaian manfaat dan nilai, serta pengelolaan program dan risiko proyek. Peneliti hanya melakukan pemaparan hasil dari RACI *Chart* yang memungkinkan untuk dijadikan responden namun karena keterbatasan akses, peneliti hanya memilih Kepala Pusat SIM sebagai responden terkait proses dari *subdomain* APO13.

4.2 Optimasi Risiko

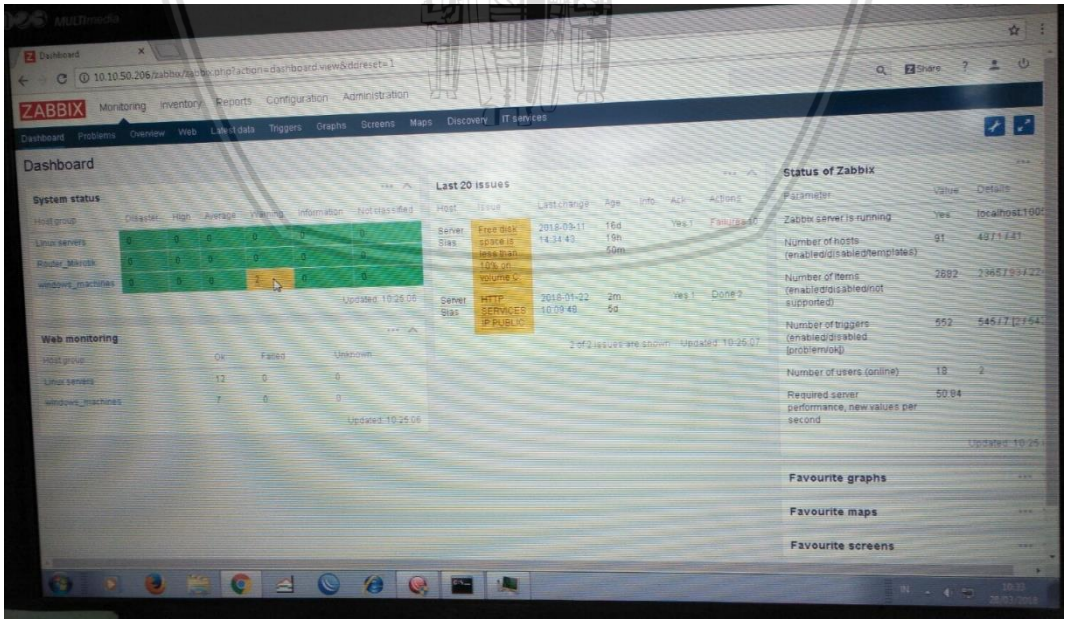
EDM03 merupakan proses mengenai optimasi risiko sehingga nantinya dapat dikelola dengan baik. Dalam melakukan penelitian terkait proses atau *subdomain* ini, peneliti melakukan observasi terkait *base practices* dan *work products* yang ada pada EDM03 sesuai dengan COBIT 5. Observasi dilakukan dengan bantuan dari *checklist* yang terlampir pada Lampiran B.1, pada *checklist* terdiri dari *base practices* dan *work products* yang ada pada EDM03. Observasi ini dilakukan guna menemukan *base practices* apa saja yang telah dilakukan oleh perusahaan dan *work products* atau hasil atau dokumen yang dimiliki oleh perusahaan. Sesuai dengan pemetaan dari RACI *Chart* yang telah dilakukan, responden yang pada proses ini yaitu Kepala Pusat SIM PDAM Kota Malang.

Dari hasil observasi yang telah dilakukan, diperoleh bahwa PDAM Kota Malang telah melakukan ketiga *base practices* yang ada pada COBIT 5. PDAM Kota Malang telah secara rutin memeriksa dan melakukan penilaian mengenai pengaruh dari penggunaan TI serta mempertimbangkan risiko yang dapat diterima oleh perusahaan. Ini terbukti karena setiap 6 bulan sekali dilakukan audit mutu internal dan setiap 1 tahun sekali melakukan audit mutu eksternal. Perusahaan juga telah menetapkan secara langsung praktik dari manajemen risiko sehingga risiko yang ada tidak melebihi kemampuan dari perusahaan. Menurut hasil wawancara yang telah dilakukan dengan Kepala Pusat SIM sebagai narasumber bahwa PDAM Kota Malang memiliki aplikasi bernama SIWO (Sistem Informasi *Work order*) di mana mampu mengubungkan antara pelanggan dengan petugas terkait. Aplikasi ini mampu menerima keluhan pelanggan terkait dengan layanan yang mereka terima. Nantinya komplain akan diteruskan kepada petugas terkait sehingga mampu dengan cepat melakukan tindakan. Sehingga, telah memiliki dokumen terkait identifikasi masalah dan proses *tracking* dalam aplikasi *work order* ini.



Gambar 4.1 Sistem Informasi *Work order* (SIWO)

Selain itu, menurut hasil wawancara untuk kategori risiko memang belum sepenuhnya ideal. Tapi perusahaan telah menggunakan *software* Zabbix di mana pada *software* tersebut merekam segala risiko TI yang terjadi dalam bentuk teknis dan ada beberapa kategorinya. Yaitu *Disaster, High, Averange, Warning, Information* dan *Not Classified.* Pada *software* tersebut juga diberikan penjelasan mengenai risiko apa yang terjadi, siapa yang bertanggung jawab, dan bagaimana statusnya apakah sudah ditangani atau masih dalam proses penanganan. Zabbix yang digunakan sebagai *monitoring* ini mampu mengetahui risiko TI apa saja yang sering terjadi pada periode tertentu pada kategori tertentu. Kategori ini ada *Windows machines, Linux services* dan *router Microtik*. Dari sistem ini ketika mengetahui data terkait risiko yang terjadi maka dapat menjadi bahan bagi perusahaan apakah perlu dilakukan penambahan spesifikasi dan lain sebagainya.



Gambar 4.2 *Software* Zabbix PDAM Kota Malang

Dari observasi selanjutnya perusahaan telah memiliki beberapa dokumen terkait proses dari optimasi risiko. Terdapat dokumen Proses ISO 9001:2015 Bagian SIM yang membahas tentang prinsip dari manajemen risiko perusahaan, kebijakan, tujuan utama, proses yang disetujui, tindakan remedial dan isu tentang manajemen risiko. PDAM Kota Malang telah bersertifikasi ISO 9001:2015 namun menurut hasil wawancara telah terdapat di dalamnya mengenai aspek risiko namun tidak secara detail membahas tentang risiko yang terkait dengan TI. Dalam hasil observasi juga didapatkan dokumen tentang laporan bulanan bagian dari SIM. Laporan bulanan ini menunjukkan bahwa PDAM Kota Malang terus melakukan evaluasi terkait risiko. Dan yang terakhir dokumen sasaran mutu bagian SIM. Dokumen ini beriisi panduan risiko yang mampu diterima oleh perusahaan dan tingkat risiko yang telah disetujui. Berikut adalah dokumen yang didapati pada EDM03.

Tabel 4.4 Hasil Dokumen EDM03

Jenis Dokumen	Nama Dokumen
BP	Sasaran Mutu Bagian
	Audit Mutu Internal
	Audit Mutu Eksternal
	Aplikasi *Work Order*
WP	Dokumen Proses ISO 9001:2015
	Manajemen Risiko ISO 9001:2015
	Laporan Bulanan Bagian SIM
	Sasaran Mutu Bagian
GP	Instruksi Kerja Bagian SIM
	SK PDAM Kota Malang 2013
	Sasaran Mutu Bagian
	Prosedur Penerapan *Software*
	Prosedur Penerapan *Hardware*
	Prosedur Penerapan Jaringan
	Software Zabbix
GWP	Laporan Bulanan Bagian SIM
	ISO 9001:2015
	Software Zabbix
	Aplikasi *Work Order*

Selanjutnya yaitu hasil dari lembar penilaian pada Tabel 4.5 yang telah dilakukan oleh responden terpilih, yaitu Kepala Pusat SIM. Pengisian lembar penilaian ini dilakukan dengan cara pendampingan. Peneliti melakukan pendampingan terhadap pengisian lembar penilaian agar mudah dilakukan pengisian oleh responden terkait.

Tabel 4.5 Hasil Lembar Penilaian Responden EDM03

Process Name	*Level* 0	*Level* 1	*Level* 2		*Level* 3		*Level* 4		*Level* 5	
EDM03		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria		F	L	P	L	P	P	N	N	N
Capability level Achieved		1								
N *(Not Achieved, 0%-15%)*, P *(Partially Achieved, >15%-50%)*, L *(Largely Achieved, >50%-85%)*, F *(Fully Achieved, >85%-100%)*										

Tabel 4.5 menunjukkan hasil dari lembar penilaian yang dilakukan oleh responden EDM03 dalam hal ini yaitu Kepala Pusat SIM. Untuk *capability level* proses EDM03 berada pada *level* 1 dengan skala F pada PA 1.1 yaitu >85%-100%. Atribut proses PA 2.1 berada pada skala L yaitu >50%-85%., PA 2.2 berada pada skala P yaitu >15%-50%, PA 3.1 dan PA 3.2 berada pada skala L yaitu >50%-85%. Sedangkan untuk atribut proses PA 4.1, PA 4.2 , PA 5.1 dan PA 5.2 berada pada skala N 0%-15%.

Setelah mengumpulkan data, dilakukan proses penilaian oleh peneliti untuk menentukan *capability level* yang diperoleh perusahaan terkait proses EDM03. Ini juga mampu memastikan bahwa hasil lembar penilaian yang telah diisi oleh responden telah sesuai dengan kenyataan sebenarnya di lapangan. Peneliti akan melakukan penilaian dengan melakukan triangulasi data dari metode observasi dan wawancara yang telah dilakukan. Terdapat 5 tahapan dalam melakukan *self assessment*. Tahap pertama yaitu menentukan proses yang akan dinilai. Dalam hal ini proses yang akan dinilai yaitu *subdomain* EDM03 mengenai optimasi risiko. Tahap kedua yaitu melakukan penilaian terhadap proses untuk *level* 1 dengan menggunakan lembar penilaian yang telah disusun yang terlampir pada Lampiran C.1. Pada *level* 1 ini memiliki atribut proses PA 1.1 dengan kriteria yang harus dipenuhi, kriterianya yaitu *base practices* yang dilakukan dan *work products* yang dimiliki perusahaan. Untuk mengetahuinya dapat dilakukan dengan mengolah data kualitatif dan hasil *checklist* yang sebelumnya telah dilakukan dalam pengambilan data.

Pada proses EDM03 memiliki 3 *base practices* sesuai dengan COBIT 5 dan perusahaan telah menerapkan ketiganya. Menurut hasil observasi dengan bantuan ceklis sesuai dengan Lampiran B.1 perusahaan melakukan ketiga BPs yaitu yang pertama tentang mengevaluasi manajemen risiko Ini dibuktikan dengan telah dilakukan audit terjadwal setiap 6 bulan sekali untuk internal dan eksternal setiap 1 tahun sekali. Dan disimpan dalam dokumen Audit Mutu Internal dan Audit Mutu Eksternal. Kedua mengarahkan manajemen risiko, perusahaan telah menetapkan praktik manajemen risiko dan memastikan bahwa risiko TI tidak melebihi kemampuan perusahaan ini dibuktikan dengan dimilikinya dokumen Sasaran Mutu Bagian yang berisi panduan mengenai risiko TI yang mampu diterima perusahaan dan toleransinya. Dan terakhir mengawasi atau melakukan kontrol terhadap manajemen risiko, perusahaan telah melakukan identifikasi masalah dan proses tracking yang semuanya tersimpan dalam aplikasi *work order*. Selain itu terdapat juga laporan bulanan bagian SIM dan identifikasi masalah dan proses tracking yang terdokumentasi dalam aplikasi *work order*.

Dalam melakukan penilaian *base practices* harus didukung dengan *work products* yang dimiliki oleh perusahaan. Pada proses EDM03 *work product* yang harus dimiliki berjumlah 16 dokumen. Sebelumnya telah dijelaskan pada subbab 2.4 tentang optimasi risiko. Hasil *checklist* yang didapatkan melalui metode observasi dengan bantuan *checklist* seperti yang terlampir pada lampiran B.1 menunjukkan bahwa perusahaan telah memiliki *work products* sebanyak 15. Perusahaan tidak memiliki WP mengenai review hasil penilaian risiko dari pihak ketiga. Sehingga atribut proses PA 1.1 *(Process Performance)* telah mencapai 94% dan termasuk skala *Fully Achieved (*>85%-100%). Sehingga sesuai dengan hasil yang telah didapatkan dari lembar penilaian oleh responden. Dari tabel 4.5 dapat diketahui bahwa proses EDM03 berhasil mencapai *capability level* 1 dengan pencapaian F pada atribut proses PA 1.1

Sama seperti *level* 1, pada *level* 2 sampai 5 memiliki atribut proses dengan kriteria tertentu. Selanjutnya dilakukan penilaian terhadap proses EDM03 untuk *level* 2 pada atribut proses PA 2.1 *(Performance Management)*. Pada atribut proses ini memiliki 6 kriteria yang harus dipenuhi dan memenuhi 5 kriteria. Perusahaan belum memenuhi kriteria mengenai sumber dan informasi yang diperlukan untuk melakukan proses telah diidentifikasi, tersedia, dialokasikan dan digunakan. Sebenarnya, perusahaan telah merekam segala bentuk informasi dalam melakukan optimasi risiko namun hanya dilakukan ketika dibutuhkan saja. Sehingga, belum sempurnanya pencapaian dari kriteria tersebut. Dalam pencapaian kriteria ISACA telah mendeskripsikan GPs dan GWPs yang ada ketika mencapai suatu kriteria. Pada atribut proses ini perusahaan telah memenuhi kriteria yang telah ditentukan. Perusahaan telah mengkomunikasikan dengan baik melalui Zabbix dan SIWO. Selanjutnya perusahaan juga telah merekam segala penanganan risiko teknis, sumber daya yang dibutuhkan tersedia dengan baik, informasi yang dibutuhkan semuanya telah terekam dalam sistem. Sehingga untuk atribut proses PA 2.1 mencapai angka 85% termasuk dalam skala Largely Achieved yaitu >50%-85%. Pencapaian hingga 80% karena perusahaan telah melakukan kategori risiko yang dilakukan oleh *software* Zabbix yang diterapkan. Selain itu

perusahaan menggunakan SIWO (Sistem Informasi *Work order*) sebagai antarmuka yang digunakan oleh antar petugas maupun petugas dengan pelanggan sehingga tugas dan tanggung jawab telah dikomunikasikan dengan baik. Namun untuk dokumentasi proses hanya dilakukan secara insidental. Pencapaian akan atribut proses ini sesuai dengan lembar penilaian yang telah diisi oleh responden.

Selanjutnya melakukan penilaian untuk atribut proses PA 2.2 *(Work product Management).* Dalam atribut proses ini terdapat 4 kriteria yang harus dipenuhi. Perusahaan telah mendokumentasikan hasil audit yang telah dilakukan terbukti dengan adanya ISO 9001:2015 dan untuk pelaporan risiko teknis yang terekam dalam Zabbix perusahaan melakukannya ketika dibutuhkan saja atau bersifat insidental salah satu contohnya yaitu Laporan Bulanan Bagian SIM. Pada atribut proses ini perusahaan hanya memenuhi 50% sehingga masuk pada skala P (>15%-50%) karena belum ada persyaratan mengenai hasil dokumen atau hasil kerja. Penilaian dilanjutkan untuk atribut proses PA 3.1. Pada atribut proses ini menurut hasil wawancara oleh Kepala Pusat SIM yang terlampir pada Lampiran A.2, perusahaan telah melakukan pengesahan terkait bagaimana prosedur untuk penerapan *software*, *hardware*, dan jaringan dan terdokumentasi dengan baik. Langkah-langkah untuk petugas dalam melakukan proses juga telah ditentukan pada dokumen Instruksi Kerja Bagian SIM. Hasil observasi yang dilakukan oleh peneliti dari segi infrastruktur yang mendukung proses semua telah dilakukan *maintenance* dengan baik dan menyimpan segala jadwal dan datanya terkait dalam PASPAM. Sehingga untuk atribut proses ini mencapai 80%, termasuk dalam skala L yaitu (>50%-85%) sesuai dengan hasil lembar penilaian yang telah didapatkan dari responden. Dari 5 kriteria, perusahaan mampu memenuhi 4 kriteria. Kriteria yang belum terpenuhi yaitu terkait, belum adanya metode yang ditentukan untuk memantau keefektifan dan kesesuaian proses.

Pada atribut proses PA 3.2, menurut hasil wawancara yang terlampir pada Lampiran A.2 mengatakan bahwa perusahaan melakukan dokumentasi untuk infrastruktur dalam sebuah sistem PASPAM sehingga lebih mudah dilakukan *maintenance*. Peran dan tanggung jawab dikomunikasikan melalui sistem dan merekam segala penanganan risiko pada Zabbix. Jadi, pada atribut proses ini perusahaan hanya mampu mencapai 48% dikarenakan personil yang terlibat dalam proses banyak dari mereka yang masih belum berasal dari latar belakang TI, bahkan data yang dikumpulkan masih bersifat insidental sehingga berada pada skala P (>15%-50%) dan sesuai dengan hasil dari lembar penilaian yang didapatkan. Dari 6 kriteria, perusahaan hanya memenuhi 3 kriteria. Yaitu, personil terkait proses belum didefinisikan berdasarkan kompetensi, pendidikan, pelatihan dan pengalaman yang sesuai. Namun, perusahaan telah berupaya dalam memenuhi kriteria ini. Lalu, belum tersedianya informasi dan sumber daya mengenai proses karena hanya ketika dibutuhkan saja dan belum mengumpulkan data yang tepat untuk perbaikan proses yang dilakukan secara terus menerus.

Atribut proses PA 4.1 mencapai 34% yaitu pada skala P (>15%-50%), ini dikarenakan perusahaan telah melakukan audit mutu internal yang telah terjadwal yaitu setiap 6 bulan sekali dan terdokumentasi dengan baik. Namun belum secara kuantitatif dilakukan. Hanya pada risiko TI yang sifatnya teknis. Ini dibuktikan dengan hanya memenuhi 2 kriteria dari 6 kriteria yang telah dideskripsikan. Yaitu, kebutuhan dari proses informasi mendukung tujuan bisnis dan tujuan dari penilaian berasal dari kebutuhan proses informasi. Sedangkan atribut proses PA 4.2 mencapai skala N dikarenakan perusahaan belum melakukan pengukuran proses secara kuantitatif yang ideal atau secara keseluruhan. Sehingga sesuai dengan hasil lembar penilaian yang telah didapatkan. Selanjutnya atribut proses PA 5.1 dan PA 5.2 yang mencapai skala N dikarenakan menurut hasil observasi dan wawancara perusahaan belum melakukan inovasi dari proses yang telah ditetapkan. Sejauh ini perusahaan masih mengikuti proses serta prosedur yang telah ditetapkan. Sehingga secara keseluruhan dari atribut proses telah sesuai dengan hasil lembar penilaian yang telah didapatkan. Berikut ringkasan mengenai triangulasi data dari metode observasi dan wawancara yang telah dilakukan.

Tabel 4.6 Hasil Triangulasi Data EDM03

Nama Proses	Hasil Lembar Penilaian	Observasi	Wawancara	Validasi
EDM03	*Level* 1	Sesuai	Sesuai	√

Jadi, hasil dari penilaian *capability level* untuk proses EDM03 *(Ensure Risk Optimisation)* adalah sebagai berikut.

Tabel 4.7 Hasil *Capability level* EDM03

		Process *Capability level*					
Prosess Name	*Targeted Level*	0	1	2	3	4	5
EDM03 *(Ensure Risk Optimisation)*	2		★				

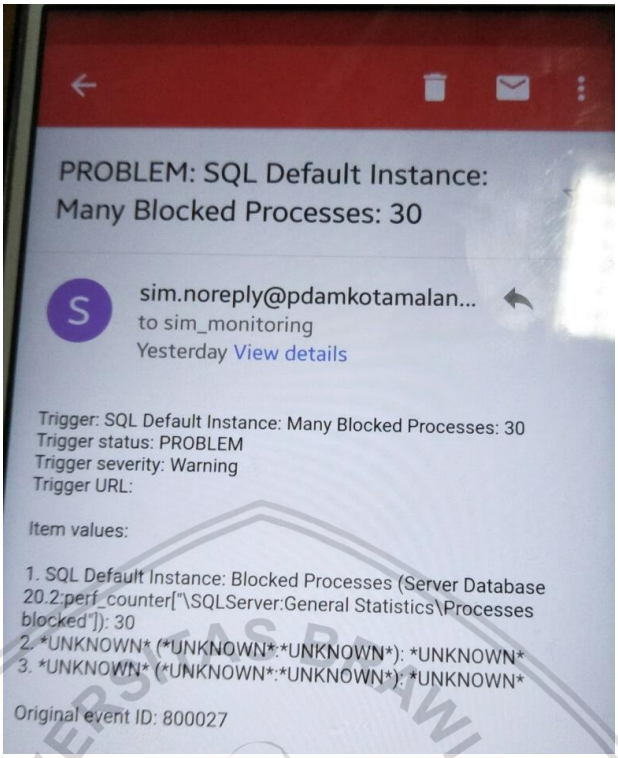
Pada tahapan *self assessment* hanya terdapat 5 tahapan di mana tahap keempat hanya melakukan pembuatan tabel guna mengetahui hasil *capability level* dengan *targeted level* seperti pada Tabel 4.7. Namun pada penelitian ini setelah tahap keempat dilakukan analisis mengenai kesenjangan antara *targeted level* dengan hasil penilaian *capability level*. Seperti yang pada Tabel 4.7 terdapat kesenjangan berupa satu *level* agar perusahaan mampu mencapai *level* yang diharapkan. Sehingga dari hasil kesenjangan mampu dirumuskan langkah-langkah atau upaya perbaikan untuk mencapai *capability level* yang diharapkan. Tahapan kelima yaitu membuat rencana untuk perbaikan proses, pada tahapan kelima ini keluarannya berupa rekomendasi yang mampu menjadi gambaran serta saran bagi perusahaan di masa depan. Untuk tahap kelima ini akan dibahas pada bab 5.

4.3 Mengelola Risiko

Selanjutnya dilakukan penilaian terhadap proses APO12 yaitu mengenai pengelolaan risiko. Yaitu penelitian tentang sejauh mana perusahaan mampu mengambil langkah yang akan digunakan dalam menyelesaikan atau mengatasi risiko yang sudah diidentifikasi pada proses EDM03. Dalam melakukan penilaian dilakukan observasi terkait *base practices* dan *work products* yang ada pada *subdomain* APO12 pada perusahaan sesuai dengan yang sudah ditentukan oleh COBIT 5. Untuk mempermudah observasi disusun *checklist* yang terlampir dalam Lampiran B.1 guna membantu peneliti dalam melakukan dokumentasi. Sesuai dengan hasil pemetaan RACI *Chart*, responden yang dipilih dalam proses ini yaitu *Programmer* IT dari PDAM Kota Malang.

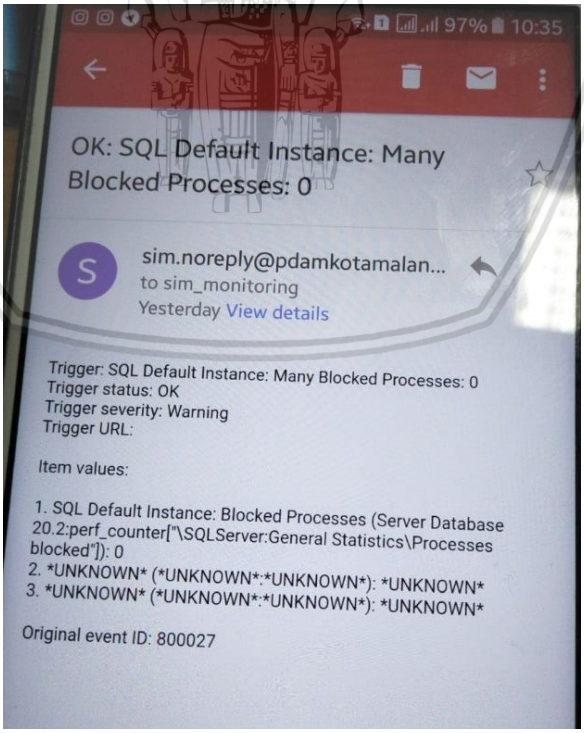
Dari hasil observasi yang telah dilakukan, diperoleh bahwa PDAM Kota Malang telah melakukan keenam *base practices* yang telah dideskripsikan sebelumnya pada sub bab 2.5. Terbukti dari dimilikinya dokumen Instruksi Kerja Bagian SIM. Di dalamnya memiliki langkah-langkah efektif untuk mengurangi kerugian yang berhubungan dengan penggunaan TI. Menurut hasil wawancara dengan Kepala Pusat SIM pada Lampiran A.2, telah dilakukan *maintenance* yang terjadwal sehingga mampu terus melakukan pemantauan terkait penggunaan TI dan dapat secara cepat mengetahui risiko yang terjadi. Aset yang ada pada PDAM Kota Malang bukan hanya aset TI saja, umumnya seperti pipa, pompa dll. Dalam melindungi aset-aset ini, PDAM Kota Malang memiliki aplikasi yang disebut dengan PASPAM (Pengelolaan Aset Sistem Pengamanan Air Minum). Pada dasarnya aplikasi ini untuk aset-aset terkait pengelolaan air minum, namun dapat juga digunakan untuk aset-aset TI sehingga mampu dilakukan maintenance secara terus-menerus dan mengetahui secara cepat apabila terjadi masalah.

Menurut hasil wawancara pada Lampiran A.2, penggunaan Zabbix dilakukan sebagai langkah mitigasi risiko yang telah perusahaan terapkan. Ini karena dua tahun lalu perusahaan mengetahui masalah dari *user* atau pelanggan, sehingga perusahaan berupaya untuk mengetahui risiko sedini mungkin atau dalam arti melakukan tindakan preventif. Ketika ada risiko yang terjadi, perusahaan langsung mengirimkan *e-mail* kepada petugas terkait. Apabila risiko tersebut selesai diatasi, akan ada *e-mail* kembali yang menunjukkan status dari masalah tersebut saat ini. Dari sistem ini ketika mengetahui data terkait risiko yang terjadi maka dapat menjadi bahan bagi perusahaan apakah perlu dilakukan penambahan spesifikasi dan lain sebagainya. Karena perusahaan menggunakan virtual jadi tidak harus mengganti bentuk fiisiknya sehingga mampu menghemat biaya. Tetapi tetap semua harus sesuai dengan SOP. Berikut merupakan contoh *e-mail* yang diterima petugas yang bertanggung jawab.



Gambar 4.3 Notifikasi *E-mail Problem*

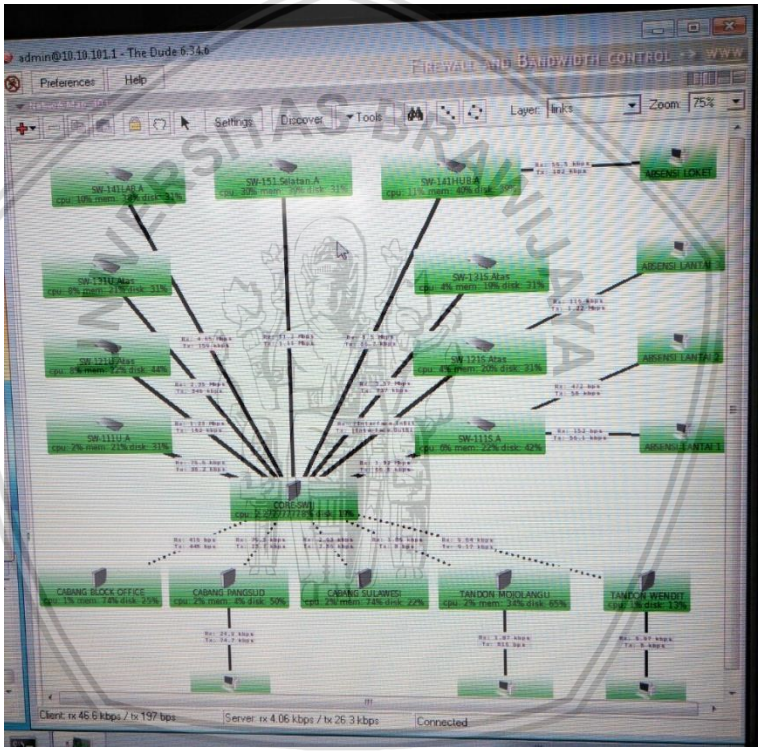
Selanjutnya apabila masalah telah selesai ditangani, maka tetap akan mengirimkan notifikasi melalui *e-mail* namun statusnya akan berubah menjadi OK.



Gambar 4.4 Notifikasi *Problem* Selesai

Selain itu, perusahaan telah memiliki *backup* secara periodik. Ini dibuktikan dari hasil wawancara yang terlampir pada Lampiran A.2 bahwa ketakutan terbesar

perusahaan adalah ketika data yang dimiliki dan pelanggan semakin banyak. Perusahaan telah menggunakan beberapa *software* yang digunakan untuk mengetahui kondisi terkait koneksi dan kondisi dari *database*. Yaitu dengan menggunakan *software* The Dude. The Dude juga digunakan untuk memantau transfer data dan ketersediaan jaringan ruangan dimasing-masing lantai. Dengan *software* ini divisi IT yang bertugas langsung mengetahui masalah yang terjadi apabila mendapatkan laporan bahwa jaringan bermasalah. Semisal lantai 2 ruangan A terjadi masalah kita mampu langsung pantau lewat sistem ini sehingga tidak perlu harus menuju keruangannya dan langsung ke *switch*. Jadi untuk cara kerjanya petugas akan memonitoring *switch*, karena tidak mungkin untuk memantau lebih dari 300 *user* yang dimiliki perusahaan. Karena *user* langsung terhubung dengan *switch* maka *switch* yang akan dilakukan pemantauan tidak perlu langsung ke *user*.



Gambar 4.5 *Software* The Dude PDAM Kota Malang

Untuk *work products*, perusahaan telah memiliki laporan bulanan bagian di mana berisi tentang status dari insiden dan laporan mengenai apa yang terjadi dalam satu bulan terakhir. PDAM Kota Malang telah menerapkan ISO 9001:2015 mengenai manajemen mutu, di dalamnya terdapat aspek risiko namun belum secara detail membahas tentang risiko TI. Pada dokumen ini terdapat beberapa risiko yang mampu diterima perusahaan namun belum secara detail membahas tentang TI. Berikut adalah dokumen yang didapati pada APO12.

Tabel 4.8 Hasil Dokumen APO12

Jenis Dokumen	Nama Dokumen
BP	Instruksi Kerja Bagian SIM
WP	Manajemen Risiko ISO 9001:2015
	Laporan Bulanan Bagian SIM
GP	Instruksi Kerja Bagian SIM
	SK PDAM Kota Malang 2013
	Prosedur Penerapan *Software*
	Prosedur Penerapan *Hardware*
	Prosedur Penerapan Jaringan
	Software Zabbix
	Software PASPAM
GWP	Laporan Bulanan Bagian SIM
	Manajemen Risiko ISO 9001:2015
	Software Zabbix
	Software PASPAM

Selanjutnya yaitu hasil dari lembar penilaian pada Tabel 4.9 yang telah dilakukan oleh responden terpilih, yaitu *Programmer* IT. Pengisian lembar penilaian ini dilakukan dengan cara pendampingan. Peneliti melakukan pendampingan terhadap pengisian lembar penilaian agar mudah dilakukan pengisian oleh responden terkait.

Tabel 4.9 Hasil Lembar Penilaian Responden APO12

Process Name	*Level* 0	*Level* 1	*Level* 2		*Level* 3		*Level* 4		*Level* 5	
APO12		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria		L	L	P	L	L	N	P	N	N
Capability level Achieved		1								
N *(Not Achieved, 0%-15%),* P *(Partially Achieved, >15%-50%),* L *(Largely Achieved, >50%-85%),* F *(Fully Achieved, >85%-100%)*										

Tabel 4.9 menunjukkan hasil dari lembar penilaian yang dilakukan oleh responden dari APO12 yaitu *Programmer IT* PDAM Kota Malang. Untuk *capability level* proses APO12 berada pada *level* 1 dengan skala L yaitu >50%-85%. Atribut proses PA 2.1 berada pada skala L, PA 2.2 dan PA 3.1 pada skala P yaitu >15%-50%, dan PA 3.2 berada pada skala L yaitu >50%-85%. Untuk atribut proses PA 4.1 berada pada skala N yaitu 0%-15%, PA 4.2 berada pada skala P yaitu >15%-50%. Dan PA 5.1 dan 5.2 pada skala N yaitu 0%-15%.

Setelah mengumpulkan data, dilakukan proses penilaian untuk menentukan *capability level* yang diperoleh perusahaan terkait proses APO12. Terdapat 5 tahapan dalam melakukan *self assessment*. Tahap pertama yaitu menentukan proses yang akan dinilai. Dalam hal ini proses yang akan dinilai yaitu *subdomain* APO12 mengenai pengelolaan risiko. Tahap kedua yaitu melakukan penilaian terhadap proses untuk *level* 1 dengan menggunakan lembar penilaian yang telah disusun yang terlampir pada Lampiran C.2. Pada *level* 1 ini memiliki atribut proses PA 1.1 dengan kriteria yang harus dipenuhi, kriterianya yaitu *base practices* yang dilakukan dan *work products* yang dimiliki perusahaan. Untuk mengetahuinya dapat dilakukan dengan mengolah data kualitatif dan hasil *checklist* yang sebelumnya telah dilakukan dalam pengambilan data yaitu pada Lampiran B.1. Pada proses APO12 memiliki 6 *base practices* sesuai dengan COBIT 5 dan perusahaan telah menerapkan keenamnya. Yaitu tentang mengumpulkan data terkait risiko TI yaitu sesuai dengan hasil wawancara pada Lampiran A.2 mengenai pengumpulan data risiko TI dilakukan insidental, ini dilakukan ketika ingin melakukan analisis risiko, selanjutnya memelihara profil risiko, memberikan informasi mengenai objek yang rentan terhadap risiko, mengelola peluang untuk mengurangi risiko dan melakukan respon terhadap risiko. Terbukti dari dimilikinya laporan bulanan bagian, sehingga data yang dibutuhkan mampu didapatkan dengan efektif.

Dalam melakukan penilaian *base practices* harus didukung dengan *work products* yang dimiliki oleh perusahaan. Pada proses APO12 *work product* yang harus dimiliki berjumlah 26 *work products*. Sebelumnya telah dijelaskan pada subbab 2.5 tentang mengelola risiko. Hasil *checklist* menunjukkan bahwa perusahaan telah memiliki *work products* sebanyak 21. Perusahaan belum memiliki WP mengenai saran akan ancaman, identifikasi risiko dari pemasok, peninjauan kembali hasil penilaian risiko pihak ketiga, peluang untuk menerima risiko yang lebih besar dan dampak risiko untuk dikomunikasikan kepada pihak terkait. Sehingga atribut proses PA 1.1 *(Process Performance)* telah mencapai 81% masuk dalam skala *Largely Achieved* >50%-85%. Ini sesuai dengan hasil yang ada pada lembar penilaian. Menurut hasil wawancara pada Lampiran A.2, perusahaan telah melakukan penanganan yang tepat sesuai risiko teknis yang terjadi pada *software* Zabbix.

Tahap ketiga yaitu melakukan penilaian untuk *level* 2-5. Hasil lembar penilaian pada Tabel 4.9 menyatakan bahwa pada atribut proses PA 2.1 mencapai skala L yaitu >50%-85%. Pada atribut proses ini perusahaan telah memenuhi kriteria yang telah ditentukan ISACA. Perusahaan mencapai skala ini dikarenakan ada beberapa

dokumen yang belum terdokumentasi dengan baik. GP yang telah dilakukan pada atribut proses ini menurut hasil lembar penilaian yaitu menyatakan bahwa untuk tugas dan tanggung jawab telah ditetapkan, bahkan dibantu dengan *software* Zabbix. Ini tentunya sesuai dengan hasil wawancara pada Lampiran A.2 yang menyatakan bahwa pada *software* tersebut, ketika ada risiko yang terjadi telah dilakukan pengiriman notifikasi melalui *e-mail* kepada petugas terkait dan terekam dalam *software* untuk status dari penanganannya. Dari hasil observasi dan wawancara yang telah dilakukan maka sesuai dengan hasil lembar penilaian yang telah dilakukan untuk pencapaiannya 68% yaitu berada pada skala L >50%-85% karena dari 6 kriteria hanya mampu memenuhi 4 kriteria saja. Belum dilakukannya identifikasi tujuan proses dan sumber informasi hanya bersifat insidental.

Atribut proses PA 2.2 mencapai skala P di mana sesuai dengan hasil wawancara pada Lampiran A.2 yang mengatakan bahwa untuk dokumentasi belum sepenuhnya sesuai atau detail. Dan belum ada persyaratan terkait konten dari dokumen hasil. Sehingga pencapaiannya hanya sebesar 25% karena hanya memenuhi 1 kriteria dalam 4 kriteria, yaitu hanya meninjau hasil pengelolaan atau penanganan risiko dalam *software* sehingga masuk pada skala P (>15%-50%). Pada atribut proses PA 3.1 mencapai skala L ini sesuai dengan hasil wawancara pada Lampiran A.2 yang mengatakan bahwa untuk GP sudah banyak yang dilakukan namun untuk dokumentasi masih belum detail atau sempurna. Dari 5 kriteria, perusahaan hanya mampu memenuhi 3 kriteria. Selain itu banyak pertugas yang masih belum berkompetensi, karena banyak yang tidak memiliki latar belakang TI. Dan belum adanya metode yang dilakukan dalam memantau keefektifan suatu proses yang memungkinkan atribut proses ini pencapaiannya 60% yaitu mencapai skala L (>50%-85%).

Atribut proses selanjutnya yaitu atribut proses PA 3.2 telah mencapai skala L (>50%-85%), ini dikarenakan perusahaan telah memenuhi beberapa kriteria. Menurut hasil wawancara pada Lampiran A.2, perusahaan mengenai sumber daya dan informasi semua telah terdapat pada *software* yang digunakan. Perusahaan juga telah membuat laporan bulanan demi mengumpulkan data yang tepat dalam analisis pengelolaan risiko TI. Dan semua tanggung jawab serta tugas dikomunikasikan dengan baik sehingga dari 6 kriteria perusahaan mampu memenuhi 5 dan mencapai 85% pada skala L (>50%-85%). Sedangkan untuk PA 4.1 pencapaiannya hanya pada N (0%-15%) karena belum dilakukannya penilaian kuantitatif terkait pengeloaan risiko. Atribut proses PA 4.2 mencapai 40% pada skala P (>15%-50%) kerena perusahaan telah menerapkan langkah mitigasi sesuai dengan hasil wawancara pada Lampiran A.2 yang mengatakan bahwa penggunakan Zabbix menjadi salah satu tindakan mitigasi yang dilakukan perusahaan. Dan menyusun laporan bulanan yang nantinya akan dilakukan analisis guna melakukan langkah mitigasi risiko TI tersebut. Pada atribut proses PA 5.1 dan 5.2 perusahaan mencapai 0% pada skala N (0%-15%) karena perusahaan masih mengikuti proses serta prosedur yang telah ditetapkan. Sehingga secara keseluruhan dari atribut proses telah sesuai dengan hasil lembar penilaian yang

telah didapatkan. Berikut ringkasan mengenai triangulasi data dari metode observasi dan wawancara yang telah dilakukan.

Tabel 4.10 Hasil Triangulasi Data APO12

Nama Proses	Hasil Lembar Penilaian	Observasi	Wawancara	Validasi
APO12	*Level* 1	Sesuai	Sesuai	√

Jadi, hasil dari penilaian *capability level* untuk proses EDM03 *(Ensure Risk Optimisation)* adalah sebagai berikut.

Tabel 4.11 Hasil Tahap Keempat *Self assessment* APO12

	Process Capability level						
Prosess Name	*Targeted Level*	0	1	2	3	4	5
APO13 (*Manage Security)*	2		★				

Pada tahapan *self assessment* hanya terdapat 5 tahapan di mana tahap keempat hanya melakukan pembuatan tabel guna mengetahui hasil *capability level* dengan *targeted level* seperti pada Tabel 4.10. Namun pada penelitian ini setelah tahap keempat dilakukan analisis mengenai kesenjangan antara *targeted level* dengan hasil penilaian *capability level*. Seperti yang pada Tabel 4 terdapat kesenjangan berupa satu *level* agar perusahaan mampu mencapai *level* yang diharapkan. Sehingga dari hasil kesenjangan mampu dirumuskan langkah-langkah atau upaya perbaikan untuk mencapai *capability level* yang diharapkan. Tahapan kelima yaitu membuat rencana untuk perbaikan proses, pada tahapan kelima ini keluarannya berupa rekomendasi yang mampu menjadi gambaran serta saran bagi perusahaan di masa depan. Untuk tahap kelima ini akan dibahas pada bab 5.

4.4 Mengelola Keamanan

Terakhir dilakukan penilaian terhadap proses APO13 yaitu mengenai pengelolaan keamanan. Karena menurut observasi ditemukan masalah terkait keamanan dari data perusahaan. Di mana peneliti sempat menemukan data yang seharusnya bersifat rahasia namun mampu diunduh secara bebas tanpa hak akses. Sehingga ini mampu menjadikan saran yang baik bagi perusahaan dalam mengelola keamanan informasi yang ada. Dengan mengelola keamanan informasi mampu mempertahankan kerahasiaan, ketersediaan dan integritas informasi yang dimiliki. Dalam melakukan penilaian dilakukan observasi terkait *base practices* dan *work products* yang ada pada *subdomain* APO13 pada perusahaan sesuai dengan yang sudah ditentukan oleh COBIT 5. Untuk mempermudah observasi disusun *checklist* yang terlampir dalam Lampiran B.1 guna membantu peneliti dalam melakukan dokumentasi. Sesuai dengan hasil pemetaan RACI

Chart, responden yang dipilih dalam proses ini yaitu Kepala Pusat SIM dari PDAM Kota Malang.

Dari hasil wawancara pada Lampiran A.2 didapatkan dua *software* yang digunakan PDAM Kota Malang dalam keamanannya. Yaitu Forninet, ini untuk firewall dan untuk antivirusnya menggunakan Eset. Selain itu hasil observasi yang telah dilakukan, diperoleh bahwa PDAM Kota Malang telah melakukan ketiga *base practices* yang telah dideskripsikan sebelumnya pada sub bab 2.6. Terbukti karena telah dilakukan audit yang terjadwal pada perusahaan. Menurut hasil wawancara, ketakutan terbesar terkait besarnya data yang dimiliki karena semakin bertambahnya pelanggan. Perusahaan juga telah menggunakan *software* yang dapat digunakan untuk maintenance kondisi *database* mereka. Terkait hasil *work products* dari 11 *work products* yang dideskripsikan oleh COBIT 5 perusahaan telah memiliki 9 *work products* yang termuat dalam dokumen hasil audit internal bagian SIM. Berikut adalah dokumen yang didapati pada APO13.

Tabel 4.12 Hasil Dokumen APO12

Jenis Dokumen	Nama Dokumen
BP	Instruksi Kerja Bagian SIM
	SK PDAM Kota Malang
WP	Dokumen Audit Mutu Internal Bagian SIM
GP	Instruksi Kerja Bagian SIM
	SK PDAM Kota Malang 2013
	Software Zabbix
	Prosedur Penerapan *Hardware*
	Prosedur Penerapan *Software*
	Prosedur Penerapan Jaringan
	Software Zabbix
GWP	Laporan Bulanan Bagian SIM
	SK PDAM Kota Malang 2013
	Software Zabbix
	Software PASPAM
	Audit Mutu Internal

Selanjutnya yaitu hasil dari lembar penilaian pada Tabel 4.12 yang telah dilakukan oleh responden terpilih, yaitu Kepala Pusat SIM. Pengisian lembar penilaian ini dilakukan dengan cara pendampingan. Peneliti melakukan pendampingan terhadap pengisian lembar penilaian agar mudah dilakukan pengisian oleh responden terkait.

Tabel 4.13 Hasil Lembar Penilaian Responden APO13

Process Name	*Level* 0	*Level* 1	*Level* 2		*Level* 3		*Level* 4		*Level* 5	
APO12		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria		L	L	L	P	P	P	N	N	N
Capability level Achieved		1								
N *(Not Achieved, 0%-15%)*, P *(Partially Achieved, >15%-50%)*, L *(Largely Achieved, >50%-85%)*, F *(Fully Achieved, >85%-100%)*										

Tabel 4.12 menunjukkan hasil dari lembar penilaian yang dilakukan oleh responden APO13 dalam hal ini yaitu Kepala Pusat SIM. Untuk *capability level* proses APO13 berada pada *level* 1 dengan skala L yaitu >50%-85%. Atribut proses PA 2.1 dan PA 2.2berada pada skala L >50%-85%. Atribut proses PA 3.1 , PA 3.2 dan PA 4.1 berada pada skala P yaitu >15%-50%. Sedangkan untuk atribut proses PA 4.2, PA 4.2 , PA 5.1 dan PA 5.2 berada pada skala N 0%-15%.

Setelah mengumpulkan data, dilakukan proses penilaian untuk menentukan *capability level* yang diperoleh perusahaan terkait proses APO13. Terdapat 5 tahapan dalam melakukan *self assessment*. Tahap pertama yaitu menentukan proses yang akan dinilai. Dalam hal ini proses yang akan dinilai yaitu *subdomain* APO13 mengenai pengelolaan keamanan. Tahap kedua yaitu melakukan penilaian terhadap proses untuk *level* 1 dengan menggunakan lembar penilaian yang telah disusun yang terlampir pada Lampiran C. Pada *level* 1 ini memiliki atribut proses PA 1.1 dengan kriteria yang harus dipenuhi, kriterianya yaitu *base practices* yang dilakukan dan *work products* yang dimiliki perusahaan. Untuk mengetahuinya dapat dilakukan dengan mengolah data kualitatif dan hasil *checklist* yang sebelumnya telah dilakukan dalam pengambilan data. Pada proses APO13 memiliki 3 *base practices* sesuai dengan COBIT 5 dan perusahaan telah menerapkan ketiganya. Yaitu tentang menetapkan dan memelihara ISMS, menentukan dan mengelola rencana penanganan risiko keamanan informasi dan mengawasinya. Terbukti dari dimilikinya laporan bulanan bagian, sehingga data yang dibutuhkan mampu berbeda setiap bulannya dan menjadi bahan bagi perusahaan dalam menentukan serta mengelola rencana penanganan risiko keamanan informasi.

Dalam melakukan penilaian *base practices* harus didukung dengan *work products* yang dimiliki oleh perusahaan. Pada proses APO13 *work product* yang harus dimiliki berjumlah 11 *work products*. Sebelumnya telah dijelaskan pada subbab 2.6 tentang mengelola keamanan. Hasil *checklist* menunjukkan bahwa perusahaan telah memiliki *work products* sebanyak 9. Perusahaan belum memiliki

WP terkait pernyataan ruang lingkup manajemen keamanan sistem informasi dan mengenai kasus bisnis dari keamanan informasi. Sehingga atribut proses PA 1.1 *(Process Performance)* telah mencapai skala *Largely Achieved*. Selanjutnya dilakukan penilaian untuk *level* 2-5. Pada PA 2.1, APO13 berada pada skala L (>50%-85%) ini dibuktikan dari hasil wawancara pada Lampiran A.2 yang menjelaskan bahwa untuk tugas dan tanggung jawab semua telah terdokumentasi dengan baik. Dan untuk penerapan *software* terkait telah memiliki prosedur yang telah ditetapkan dan dilakukan pemantauan. Antarmuka dibuat agar mampu menciptakan komunikasi yang efektif semisal muncul masalah dan penanganannya. Sehingga dari 6 kriteria, perusahaan mampu memenuhi 4 kriteria dan bernilai 68%. Perusahaan belum memenuhi kriteria terkait sumber informasi yang hanya bersifat insidental dan belum mememiliki dokumen yang membahas langsung mengenai tujuan dari APO13. Selanjutnya untuk atribut proses PA 2.2 mencapai skala L (>50%-85%) dikarenakan perusahaan menurut hasil observasi dengan *checklist* pada Lampiran B.1 menyatakan perusahaan terkait keamanan telah melakukan Audit Mutu Internal dan telah didokumentasikan dengan baik. Tentunya sesuai dengan hasil dari lembar penilaian yang telah didapatkan. Sehingga dari 4 kriteria, perusahaan memenuhi 3 kriteria dan pencapaiannya sebesar 74%. Kriteria yang belum dipenuhi mengenai persyaratan untuk dokumentasi dan penentuan pengendalian hasil kerja.

Atribut proses pada PA 3.1 mencapai skala P (>15%-50%) ini dikarenakan telah memiliki prosedur pengenai penerapan *software*, *hardware* dan jaringan yang telampir pada Lampiran C.3. Dari 5 kriteria yang ditentukan perusahaan memenuhi 2 kriteria. Tentunya sesuai dengan hasil dari lembar penilaian yang didapatkan, dengan pencapaian 40%. Pada PA 3.2 mencapai skala P karena hanya 3 dari 6 kriteria yang terpenuhi. Maka mencapai 50%. Ini sesuai dengan hasil dari lembar penilaian yang didapatkan. Pada 4.1 mencapai skala P (>15%-50%) menurut hasil dari lembar penilaian. Ini sesuai dengan hasil dari wawancara pada Lampiran A.1 yang mengatakan bahwa dilakukan audit internal selama 6 bulan sekali. Namun karena belum sepenuhnya mengenai keamanan IT maka hanya mencapai P. Dan dari 6 kriteria, perusahaan hanya memenuhi 2 kriteria sehingga mendapatkan skala 34%. Pada 4.2, skalanya hanya N (0%-15%) ini dikarenakan belum adanya teknik analisis dan penilaian serta tindakan korektif yang berarti masalah keamanan. atribut proses PA 5.1 dan PA 5.2 yang mencapai skala N (0%-15%) dikarenakan menurut hasil observasi dan wawancara perusahaan belum melakukan inovasi dari proses yang telah ditetapkan. Sejauh ini perusahaan masih mengikuti proses serta prosedur yang telah ditetapkan. Sehingga secara keseluruhan dari atribut proses telah sesuai dengan hasil lembar penilaian yang telah didapatkan. Berikut ringkasan mengenai triangulasi data dari metode observasi dan wawancara yang telah dilakukan.

Tabel 4.14 Hasil Triangulasi Data APO13

Nama Proses	Hasil Lembar Penilaian	Observasi	Wawancara	Validasi
APO13	*Level* 1	Sesuai	Sesuai	√

Jadi, hasil dari penilaian *capability level* untuk proses EDM03 *(Ensure Risk Optimisation)* adalah sebagai berikut.

Tabel 4.15 Hasil Tahap Keempat *Self assessment* APO13

		Process *Capability level*					
Prosess Name	*Targeted Level*	0	1	2	3	4	5
APO13 *(Manage Security)*	2		★				

Pada tahapan *self assessment* hanya terdapat 5 tahapan di mana tahap keempat hanya melakukan pembuatan tabel guna mengetahui hasil *capability level* dengan *targeted level* sesuai dengan Tabel 4.13. Namun pada penelitian ini setelah tahap keempat dilakukan analisis mengenai kesenjangan antara *targeted level* dengan hasil penilaian *capability level*. Seperti yang pada Tabel 4 terdapat kesenjangan berupa satu *level* agar perusahaan mampu mencapai *level* yang diharapkan. Sehingga dari hasil kesenjangan mampu dirumuskan langkah-langkah atau upaya perbaikan untuk mencapai *capability level* yang diharapkan. Tahapan kelima yaitu membuat rencana untuk perbaikan proses, pada tahapan kelima ini keluarannya berupa rekomendasi yang mampu menjadi gambaran serta saran bagi perusahaan di masa depan. Untuk tahap kelima ini akan dibahas pada bab 5.

4.5 Analisis Kesenjangan *(gap)*

Analisis *Gap* atau kesenjangan sangat diperlukan guna membantu dalam melakukan perumusan terkait rekomendasi. Sehingga nantinya rekomendasi mampu menjadi acuan bagi perusahaan dalam mencapai targetnya. Berikut adalah hasil *gap* dari masing-masing *subdomain* yang diteliti.

Tabel 4.16 Hasil *Gap*

Proses	*Targeted level*	*Capability level*	*Gap*
EDM03 *(Ensure Risk Optimisation)*	2	1	1
APO12 *(Manage Risk)*	2	1	1
APO13 *(Manage Security)*	2	1	1

Dari hasil Tabel 4.14 menunjukkan bahwa dari masing-masing proses yang telah dilakukan penilaian terdapat kesenjangan 1 *level* untuk mencapai *level* yang

diharapkan. Untuk proses EDM03 hasil penilaian *capability level* saat ini yaitu berada pada *level* 1, sedangkan *targeted level* yang ingin dicapai perusahaan yaitu *level* 2. Ini berarti untuk mencapai target *level* nantinya akan diberikan rekomendasi terkait bagaimana proses yang telah mencapai *level* 1 untuk mencapai *level* 2. Seperti yang telah diketahui pada Tabel 4.3 bahwa pada atribut proses PA 2.1 telah mencapai skala L. Sehingga untuk penyusunan rekomendasi dapat diawali dengan bagaimana agar perusahaan mampu mencapai PA 2.1 pada skala F. Dilanjutkan dengan PA 2.2. Dan setelahnya diberikan rekomendasi agar mampu mencapai *level* 2.

Proses APO12 hasil penilaian *capability level* saat ini yaitu berada pada *level* 1, sedangkan *targeted level* yang ingin dicapai perusahaan yaitu *level* 2. Ini berarti untuk mencapai target *level* nantinya akan diberikan rekomendasi terkait bagaimana proses yang telah mencapai *level* 1 untuk mencapai *level* 2. Seperti yang telah diketahui pada Tabel 4.6 bahwa pada atribut proses PA 1.1 telah mencapai skala L. Sehingga untuk penyusunan rekomendasi dapat diawali dengan bagaimana agar perusahaan mampu mencapai atribut proses PA 1.1 pada skala F. Dan selanjutnya diberikan rekomendasi agar mampu mencapai *level* 2. Terakhir untuk proses APO13 hasil penilaian *capability level* saat ini yaitu berada pada *level* 1, sedangkan *targeted level* yang ingin dicapai perusahaan yaitu *level* 2. Ini berarti untuk mencapai target *level* nantinya akan diberikan rekomendasi terkait bagaimana proses yang telah mencapai *level* 1 untuk mencapai *level* 2. Seperti yang telah diketahui pada Tabel 4.9 bahwa pada atribut proses PA 1.1 telah mencapai skala L. Sehingga untuk penyusunan rekomendasi dapat diawali dengan bagaimana agar perusahaan mampu mencapai atribut proses PA 1.1 pada skala F. Dan selanjutnya diberikan rekomendasi agar mampu mencapai *level* 2.

BAB 5 PEMBAHASAN

5.1 Temuan Hasil

Berdasarkan hasil analisis yang sudah dilakukan pada bab sebelumnya, yaitu mengenai analisis *capability level* yang diperoleh melalui observasi, wawancara dan lembar penilaian didapati beberapa temuan. Yaitu pertama, tugas dan tanggung jawab yang dimiliki tumpang tindih sesuai dengan hasil pemetaan dari RACI *Chart*. Karena ketika satu orang dipilih untuk bertanggung jawab dalam suatu proses, maka orang tersebut yang bertanggung jawab sekaligus menyelesaikan permasalahan yang terjadi. Kedua, dokumen yang dimiliki oleh perusahaan masih belum sempurna. Ini dikarenakan ketika ingin melakukan analisis terhadap suatu risiko, dokumentasi baru dilakukan. Sehingga hanya bersifat insidental saja. Temuan ketiga, dalam melakukan kategori risiko TI hanya dalam risiko teknis yang lebih banyak dari internal. Belum dilakukan analisis risiko yang mungkin terjadi dari pihak ketiga atau eksternal, ini menjadikan kekhawatiran di masa depan bagi perusahaan. Karena seperti yang diketahui risiko terkadang bersifat tidak dapat diprediksi. Temuan keempat, keamanan informasi masih ada beberapa kendala. Ini terbukti dari bocornya *business plan* perusahaan, yang seharusnya tidak perbolehkan untuk diakses oleh publik. Temuan kelima, masih banyak petugas atau karyawan yang belum memiliki latar belakang dari TI. Sehingga banyak karyawan yang memiliki tugas dan tanggung jawab berlebih sesuai dengan hasil dari pemetaan RACI *Chart* yang telah dilakukan. Temuan keenam, masih banyak dokumen yang belum memiliki standar. Beberapa yang seharusnya harus memiliki dokumentasi, tetapi hanya dilakukan ketika bersifat insidental. Yaitu ketika dibutuhkan analisis saja. Temuan ketujuh, banyak staff yang tidak berlatang belakang TI. Temuan kedelapan, belum adanya metode kontrol yang ditentukan oleh perusahaan dalam pelaksanaannya. Dan temuan kesembilan, belum adanya penilaian atau pengukuran untuk mengetahui bagaimana keberhasilan dari suatu proses sehingga di masa depan mampu merumuskan perbaikan.

5.2 Optimasi Risiko

Menurut IACOP (2014), risiko merupakan sebuah insiden atau kejadian yang berasal dari internal atau eksternal perusahaan sehingga mampu mempengaruhi pencapaian tujuan dari perusahaan. Risiko telah memiliki label negatif dalam kehidupan sehari-hari, namun ternyata risiko ada yang positif dan ada yang negatif. Hanya istilahnya saja yang berbeda, risiko yang mampu berdampak positif dikatakan sebagai peluang. Risiko harus dikelola oleh tim khusus sehingga mampu memberikan gambaran mengenai kemampuan dari perusahaan beserta kelemahannya dan bagaimana cara mempertahankan perusahaan. Manajemen risiko dalam hal ini dibutuhkan. Menurut Pithcard (2015), manajemen risiko memiliki tujuan untuk memaksa manajer proyek untuk membuat terorganisir, memiliki pemikiran untuk manajemen risiko proyek dan menyediakan infrastruktur perusahaan dalam segala bentuk manajemen risiko. Ketika perusahaan memiliki manajemen risiko, ini mampu memberikan dampak yang

baik dalam mengatur segala hal dalam mewujudkan tujuan dari perusahaan. Pada sub bab ini, akan membahas hasil dari optimasi risiko. Atau dapat dikatakan bagaimana perusahaan mampu memastikan kemampuan dari dirinya sendiri. Menurut ISACA (2013c), *subdomain* EDM03 ialah memastikan agar perusahaan memiliki *risk appetite* dan toleransi dari risiko mampu dimengerti oleh seluruh pihak dalam perusahaan. Perusahaan harus mampu mengidentifikasi dampak risiko TI dan mengelolanya sehingga mampu mengurangi dan meminimalkan kegagalan.

Pada subdomain EDM03 perusahaan telah mencapai *capability level* 1 yaitu dengan pencapaian skala L (>50%-85%) untuk atribut proses PA 2.1 *(Performance Management)* dan pada atribut proses PA 2.2 *(Work product Management)* skala P (>15%-50%). Seperti yang sudah dijelaskan sebelumnya pada *level* 1 yaitu *Performed Process* bahwa proses yang diimplementasikan telah mencapai tujuan dari proses itu sendiri. Berdasarkan keinginan dari perusahaan bahwa untuk *targeted level* yang ingin yaitu pada *capability level* 2. Sehingga besarnya *gap* yang dimiliki yaitu sebesar 1. Sehingga disusun beberapa rekomendasi yang dapat diadopsi oleh perusahaan guna mencapai *targeted level* yang diharapkan.

Untuk penilaian pada *capability level* 1 pada hasil *checklist* yang terlampir pada Lampiran B.1 perusahaan belum memiliki hasil kerja terkait laporan analisis risiko dari pihak ketiga terkait penilaian risiko. Sehingga mampu dikatakan bahwa selama ini perusahaan fokus hanya pada bagaimana pelayanan mereka di dalam perusahaan, tanpa mempertimbangkan risiko yang mampu saja terjadi dari luar perusahaan. Berdasarkan hasil penelitian, perusahaan hanya melakukan kategori risiko berdasarkan risiko teknis saja pada Zabbix. Maka, rekomendasi pertama untuk subdomain EDM03 yaitu dengan melakukan kategori risiko secara lebih luas. Menurut ISACA (2013a), risiko TI dikategorikan menjadi 3 kategori. Kategori pertama yaitu *IT Benefit/Value Enablement Risk.* Pada kategori ini risiko dikategorikan berdasarkan hilangnya kesempatan untuk menggunakan teknologi demi meningkatkan efisiensi atau efektivitas proses bisnis. Contohnya, teknologi *enabler* untuk inisiatif bisnis baru dan teknologi *enabler* untuk operasi yang efisien. *Enabler* adalah faktor yang, secara individu dan kolektif mempengaruhi apakah sesuatu akan bekerja atau berhasil, dalam hal ini, tata kelola dan manajemen TI perusahaan. *Enabler* ini segala sesutu yang mampu membatu perusahaan untuk pencapaian tujuan. Dalam COBIT 5 terdapat 7 enabler, pertama *principles, policies and framework.*

Kedua, *process. Enabler* ketiga, *organizational structures. Enabler* keempat, *culture, ethics and behavior. Enabler* kelima, *information. Enabler* keenam, *services, infrastucture, and applications.* Dan *enabler* ketujuh, *people, skills and competencies.* Ketegori risiko TI yang kedua, yaitu *IT Programmer and Project Delivery Risk.* Mengkategorikan risiko terkait kontribusi TI untuk solusi bisnis baru atau yang akan ditingkatkan, biasaya dalam bentuk proyek dan program sebagai bagian dari portofolio imvestasi. Contohnya, *project quality, project relevance* dan *project overrun.* Kategori risiko TI yang terakhir, yaitu *IT Operations and Service Delivery.* Pada kategori ini risiko dikategorikan berdasarkan semua aspek dari

bisnis. Berkaitan dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan teknologi informasi dari seluruh aspek yang mampu menimbulkan kehancuran atau pengurangan nilai perusahaan.

Rekomendasi kedua, perusahaan mampu membentuk tim sendiri untuk manajemen risiko dan pembagian tugas dan tanggung jawab sesuai dengan deskripsi ISACA. Menurut ISACA (2012b), yang terlibat dalam EDM03 dalam hasil pemetaan RACI *Chart* yaitu untuk R *(Respobsible)* pihak yang menjalankan tugas. Karena menurut hasil wawancara yang terlampir pada Lampiran A.3, banyak pihak yang memiliki tugas dan tanggung jawab yang tumpang tindih menurut deskripsi dari COBIT 5. Orang yang berperan pada bagian operasional utama (R) dalam memenuhi aktivitas yang tercantum dan menciptakan hasil yang diharapkan adalah *Business Executive* dan *Strategy Executive Committee*. *Business Executive* merupakan pihak yang memiliki wewenang untuk mengelola operasi unit bisnis tertentu atau anak organisasi dan *Strategy Executive Committee* merupakan pihak yang memiliki wewenang untuk mengelola portofolio investasi, layanan dan aset TI. Untuk komponen A *(Accountable)* pihak yang bertanggung jawab atas keberhasilan tugas, di mana pihak ini memiliki otoritas untuk memutuskan suatu perkara adalah *Board*. *Board* merupakan pihak yang bertanggung jawab dalam proses tata kelola organisasi dan memiliki kontrol penuh pada sumber daya organisasi. *Board* biasanya terdiri dari sekelompok eksekutif senior atau direktur non eksekutif. Untuk komponen C *(Consulted)* yaitu peran yang memberikan sebuah masukan terhadap sebuah proses adalah *Chief Operating Officer* dan *Business Process Owner. Chief Operating Officer* merupakan Pihak yang bertanggung jawab dalam segala operasi perusahaan dan *Business Process Owner* merupakan pihak yang bertanggung jawab atas kinerja sebuah proses dalam mencapai tujuannya, mendorong perbaikan proses dan menyetujui perubahan proses. Dan untuk komponen I *(Informed)* yaitu pihak yang selalu menerima informasi yang tepat untuk diawasi dan dipantau dengan baik adalah *Head Development* dan *Information Security Manager. Head Development* merupakan pihak yang bertanggung jawab atas proses pengembangan solusi TI dan *Information Security Manager* merupakan pihak yang mengelola, merancang, dan mengawasi dan / atau menilai keamanan informasi perusahaan. Perusahaan harus mampu memisahkan tugas dan tanggung jawab dari yang telah dijelaskan diatas sehingga tidak ada pihak yang memiliki dua atau lebih tanggung jawab sehingga jelas dan mampu terorganisir dengan baik.

Rekomendasi ketiga, sumber informasi yang dibutuhkan telah tersedia dengan baik namun belum diidentifikasi terkait dengan proses optimasi risiko. Karena perusahaan belum memiliki daftar ancaman yang mungkin saja terjadi di masa depan. Menurut Elky (2006), manajemen risiko TI yang profesional harus memiliki pandangan yang berbagai macam mengenai dampak potensial dari ancaman risiko TI yang mengganggu atau menghambat pencapaian misi perusahaan. Contoh sebagian ancaman dengan sumber ancaman yang perlu dipertimbangkan oleh perusahaan, pertama *Accidental Disclosure* atau pengungkapan yang tidak disengaja. Yaitu pelepasan informasi rahasia, pribadi, atau rahasia yang tidak sah atau tidak disengaja. Kedua, *Acts of Nature.* Yaitu

semua jenis kejadian alam, misalnya gempa bumi, banjir, dan lain sebagainya yang dapat merusak atau mempengaruhi sistem atau aplikasi. Salah satu ancaman potensial ini dapat menyebabkan pemadaman sebagian atau seluruhnya, sehingga mempengaruhi ketersediaan.

Ketiga, *Alteration of Software* atau perubahan perangkat lunak. Yaitu, modifikasi yang disengaja, penyisipan, penghapusan sistem operasi atau program sistem aplikasi, baik oleh pengguna yang berwenang atau tidak, yang membahayakan kerahasiaan, ketersediaan, atau integritas data, program, sistem, atau sumber daya yang dikendalikan oleh sistem. Ini termasuk kode jahat, seperti *boms, trojan horses, trapdoors* dan virus. Keempat, penggunaan *bandwidth*. Yaitu penggunaan *bandwidth* komunikasi yang tidak disengaja atau disengaja untuk tujuan lain yang dimaksudkan. Kelima, gangguan listrik. Ini dapat saja terjadi sebagai akibat dari kegagalan daya komersial. Sehingga menyebabkan penolakan layanan kepada pengguna yang berwenang atau modifikasi data (fluktasi). Keenam, perubahan data yang disengaja. Modifikasi yang disengaja, penyisipan, atau penghapusan data, baik oleh pengguna yang berwenang atau tidak, yang mengorbankan kerahasiaan, ketersediaan, atau integritas data yang dihasilkan, diproses, dikendalikan, atau disimpan oleh sistem pemrosesan data. Ketujuh, *System Configuration* Error *(Accidental).* Yaitu kesalahan konfigurasi tidak disengaja selama instalasi awal atau peningkatan perangkat keras, perangkat lunak, peralatan komunikasi atau lingkungan operasional. Dan kedelapan, kerusakan atau gangguan telekomunikasi. Yaitu setiap sambungan komunikasi, kegagalan unit atau komponen cukup menyebabkan interupsi dalam transfer data melalui telekomunikasi antara terminal komputer, prosesor jarak jauh atau didistribusikan, dan fasilitas komputasi host.

Rekomendasi keempat, perusahaan harus menetapkan persyaratan dalam hal dokumentasi khususnya untuk proses optimasi risiko. Perusahaan harus memiliki syarat bagaimana dokumentasi yang baik terkait ini kontennya, rincian, dll mengenai seberapa besar risiko dan toleransinya yang mampu diterima oleh perusahaan. Sehingga semua pihak yang terlibat mampu memahami dan melakukan semua aktivitas terkait risiko TI khususnya dengan baik. Menurut Stoneburner, Goguen dan Feringa (2002), perusahaan harus melakukan *risk assessment.* Karena itu merupakan tahap pertama dari metodologi manajemen risiko. Ini dibutuhkan untuk menentukan sejauh mana potensi ancaman dan risiko yang terkait dengan TI. Output dari proses ini membantuk untuk mengidentifikasi kontrol yang tepat untuk mengurangi atau bahkan memghilangkan risiko selama proses dari mitigasi risiko. Dalam dokumen, penting bagi perusahaan untuk menentukan kemungkinan kejadian buruk di masa depan, ancaman terhadap sistem TI yang digunakan harus dianalisis bersamaan dengan potensi kerentanan dan kontrol yang ada. Harus juga membahas mengenai dampak yang mengacu kepada besarnya bahaya yang disebabkan oleh ancaman. Sehingga mampu memberikan gambaran mengenai kekritisan dan sensitivitas komponen maupun data dari sistem TI. Dokumen berupa hasil *risk assessment* yang menjelaskan ancaman dan kerentanan, pengukuran risiko dan memberikan rekomendasi untuk implementasi kontrol.

Dari hasil wawancara yang terlampir pada Lampiran A.2 masih banyak karyawan yang tidak berasal dari latar belakang pendidikan TI. Sehingga rekomendasi selanjutnya, yaitu perusahaan mampu menetapkan kompetensi yang dibutukan terkait staffnya. Kompetensi ini dapat berupa sumber daya manusia yang memiliki kemampuan atau pengalaman dalam melakukan identifikasi, penilaian dan analisis risiko TI. Selain itu sumber daya manusia ini harus memiliki inisiatif dalam menentukan berbagai jenis risiko TI sehingga tidak hanya risiko teknis saja, dapat risiko yang berasal dari luar, pemangku kepentingan, maupun hal yang tidak dapat terduga seperti bencana dan lain sebagainya. Selain itu juga dapat dlilakukan dengan memberikan pelatihan terhadap staff atau sumber daya manusia yang dimiliki. Penelitian yang telah dilakukan oleh Djajalaksana dan Gantini (2013), mengelompokan jabatan dan karakteristiknya. Misal untuk optimasi risiko dibutuhkan seorang *IT Manager*, atau nama jabatan sejenis dan variasinya yaitu *IT Head Departement*, Manajer Proyek, atau *IT Development*. Asal jurusan atau program studinya yaitu Teknik Informatika, Manajemen Informatika, atau Sistem Informasi. Kelompok ini membutuhkan keterampilan sistem operasi, *database*, pemrograman, dan infrastruktur Teknologi Informasi. Selain itu membutuhan kelompok *System Analyst*. Kelompok ini membutuhkan keterampilan perancangan *database*, pemrograman dan manajemen proyek. Nama jabatan sejenis dan variasinya yaitu *Programmer,* dan *Management Information System.* Di mana asal jurusan atau program studinya yaitu sistem informasi, manajemen sistem informasi dan teknik informatika. Tabel 5.1 merupakan ringkasan mengenai rekomendasi yang disusun untuk proses EDM03.

Tabel 5.1 Rekomendasi Proses EDM03

PROSES	REKOMENDASI	ALASAN
EDM03	Melakukan kategori risiko secara lebih luas dengan mempertimbangkan faktor internal dan eksternal perusahaan.	Karena perusahaan hanya melakukan kategori risiko yang bersifat teknis.
	Membentuk tim sendiri untuk manajemen risiko TI. Pembagian tugas dan tanggung jawab sesuai dengan deskripsi ISACA untuk tim manajemen risiko TI.	Karena perusahaan belum memiliki tim khusus untuk manajemen risiko TI. Sehingga dengan adanya tim khusus mampu memaksimalkan kinerja dari proses.
	Menentukan persyaratan untuk dokumen terkait konten, rincian, ruang lingkup, siapa	Karena perusahaan hanya melakukan dokumentasi yang sifatnya insidental. Sehingga perlu dilakukan penentuan terkait dokumentasi agar

Tabel 5.2 Rekomendasi Proses EDM03 (Lanjutan)

PROSES	REKOMENDASI	ALASAN
	yang bertanggung jawab dan lain sebagainya.	mampu memaksimalkan kinerja dan meningkatkan kapabilitas proses.
	Membuat daftar ancaman terkait dengan teknologi informasi yang mungkin saja terjadi di masa depan.	Karena perusahaan belum memiliki dokumen khusus mengenai ancaman yang mungkin terjadi di masa depan dan rekomendasi ini mampu meningkatkan kapabilitas dari proses.
	Menetapkan kompetensi yang dibutuhkan terkait dengan sumber daya manusia.	Karena menurut hasil temuan, banyak staf yang belum memiliki latar belakang TI.

5.3 Mengelola Risiko

Dalam pengelolaan risiko, akan dilakukan pengambilan langkah yang akan digunakan dalam menyelesaikan risiko yang telah diidentifikasi. Risiko dengan dampak yang merugikan disebut dengan risiko negatif atau yang biasa disebut dengan risiko. Sedangkan risiko yang berdampak menguntungkan bagi individu maupun organisasi disebut dengan peluang. Menurut Elky (2006), risiko dapat dikelola dengan *mitigation, transference, acceptance, avoidance, communicating risks and risk management strategies,* dan *implementing risk management strategies. Mitigation* adalah strategi manajemen risiko yang paling umum dipertimbangkan. Mitigasi mampu memperbaiki cacat atau menyediakan beberapa jenis kontrol kompensasi untuk mengurangi kemungkinan atau dampak terkait risiko. Salah satu contohnya mitigasi umum untuk kesalahan keamanan teknis adalah menginstal patch yang disediakan vendor. Proses penentuan strategi mitigasi ini disebut dengan analisis kontrol.

Transference yaitu dengan mengirimkan dampak dari risiko kepada pihak ketiga, bersamaan dengan kepemilikan respon. Mentransfer risiko hanya memberikan tanggung jawab kepada pihak lain untuk mengelolanya. Alat transferensi bisa pada penggunaan asuransi, rasio kinerja, jaminan dan sebagainya. Kontrak atau kesepakatan pun dapat digunakan untuk mengalihkan tanggung jawab atas risiko tertentu kepada pihak ketiga. Ini tidak mengurangi kemungkinan atau memperbaiki kekurangan apa pun, tetapi mengurangi dampak keseluruhan (terutama keuangan) pada organisasi. *Acceptance* adalah praktik yang memungkinkan sistem beroperasi dengan risiko yang diketahui sebelumnya. Contohnya banyak risiko rendah diterima begitu saja. Risiko yang memiliki biaya yang sangat tinggi untuk mitigasi juga sering begitu saja diterima. Pastikan bahwa strategi yang ditulis mengenai risiko TI dan risiko yang dapat diterima perusahaan dibuat oleh manajer yang membuat keputusan. Biasanya, manajer bisnis, bukan

personil keamanan TI, adalah orang yang berwenang untuk menerima risiko atas nama organisasi. *Avoidance* yaitu ketika risiko dapat dihindari dengan menghapus penyebab risiko atau melaksanakan proses dengan cara yang berbeda namun tetap mencapai tujuan yang sama. Contohnya, memperluas jadwal, mengubah strategi atau mengurangi ruang lingkup. Misalnya, selama penilaian risiko, situs web memungkinkan vendor melihat fakturnya menggunakan ID vendor yang disematkan dalam nama file HTML sebagai identifikasi dan tidak ada autentikasi atau otorisasi per vendor. Ketika diberitahu tentang halaman web dan risiko untuk organisasi, manajemen memutuskan untuk menghapus halaman web dan menyediakan faktur vendor melalui mekanisme lain. Dalam hal ini, risiko dihindari dengan menghapus halaman web yang rentan.

Selanjutnya *Communicating Risks and Risk Management Strategies.* Risiko juga harus dikomunikasikan, setelah risiko dipahami, risiko dan strategi manajemen risiko harus dikomunikasikan dengan jelas sehingga mudah dipahami oleh manajemen organisasi. Dalam mengkomunikasikan risiko gunakan hal kemungkinan dan dampak, ini akan mempermudah dalam melakukan komunikasi risiko TI. Gunakan istilah yang konkret, sehingga manajemen organisasi akan memahami dan menerima temuan dan rekomendasi. Terakhir *Implementing Risk Management Strategies.* Salah satu tools yaitu A Plan Of Action & Milestones (POAM), ini dibuat agar disetujui oleh manajemen. POAM ini mengandung risiko, strategi manajemen, Point Of Contact (POC) yang bertanggung jawab untuk mengimplementasikan strategi, sumber daya yang dibutuhkan dan berbagai tonggak yang terdiri dari implementasi. Untuk setiap pencapaian, tanggal penyelesaian target, dan tanggal penyelesaian aktual dicantumkan. POAM ini digunakan sebagai alat untuk berkomunikasi dengan manajemen.

Pada subdomain APO12 perusahaan telah mencapai *capability level* 1 yaitu dengan pencapaian skala L (>50%-85%) untuk atribut proses PA 1.1 *(Process Performance)*. Pada *capability level* 1 ini yaitu kondisi di mana proses pengelolaan risiko berhasil meraih tujuan dengan mempertimbangkan BPs dan WPs. Berdasarkan keinginan atau harapan dari perusahaan untuk *targeted level* pada APO12 yaitu pada *capability level* 2. Sehingga besarnya *gap* yang dimiliki yaitu sebesar 1. Berdasarkan hasil observasi dengan bantuan *checklist* seperti yang terlampir pada lampiran B.1 yang sesuai dengan ISACA (2013c) bahwa perusahaan belum memiliki dokumen mengenai saran akan ancaman yang mungkin terjadi pada pemanfaatan teknologi informasi. Sehingga, rekomendasi dari peneliti yang pertama yaitu mampu memiliki dokumen khusus mengenai saran akan ancaman yang mungkin terjadi di masa depan demi mengantisipasi dampak dari risiko yang dihasilkan dari ancaman tersebut. Selanjutnya, perusahaan belum memiliki dokumen mengenai peluang untuk menerima risiko yang lebih besar. Dokumen ini berisi bagaimana analisis dan penilaian terhadap kemampuan dari perusahaan, sehingga memiliki kekuatan dalam menghadapi risiko TI yang lebih besar. Dokumen mengenai dampak dari risiko harus dimiliki perusahaan sehingga pihak terkait mengetahui dampak tersebut, saran penanganan dan mempersiapkan diri untuk menghadapinya. Dokumen lain yaitu mengenai penilaian risiko sehingga

mampu merumuskan cara untuk mengurangi risiko TI. Di mana membahas juga mengenai biaya serta manfaatnya.

Rekomendasi selanjutnya yaitu pemisahan antara tanggung jawab dan tugas seperti yang telah ditentukan oleh ISACA pada RACI *Chart*. Sehingga penggunaan sumber daya khususnya manusia mampu dimanfaatkan dengan baik dan teratur. Selain itu, perusahaan harus memiliki standar khusus yang ditetapkan mengenai dokumen dari pengelolaan risiko sehingga seluruh pihak yang membutuhkan informasi mengenai hasil dari dokumen tersebut mampu memanfaatkannya dengan maksimal. Selain itu perusahaan mampu menentukan kompetensi seperti apa yang dibutuhkan dalam pengelolaan risiko, sehingga hasilnya mampu lebih detail. Menurut ISACA (2012b), hasil dari pemetaan RACI *Chart* untuk komponen *responsible* yaitu pihak yang menjalankan tugas pada subdomain APO12 adalah *Chief Information Security Officer*, *Business Process Owner* dan *Chief Risk Officer*. *Chief Information Security Officer* bertanggung jawab dalam menyelaraskan strategi TI dengan bisnis serta bertanggung jawab atas perencanaan, sumber daya dan manajemen dalam penyampaian layanan dan solusi TI untuk mendukung tujuan dari perusahaan. *Business Process Owner* yaitu pihak yang memberikan rencana mengenai pengelolaan risiko TI. Dan *Chief Risk Officer* yang bertanggung jawab atas segala aspek risiko tertutama dalam mengelola risiko TI pada perusahaan.

Selanjutnya, untuk komponen *accountable* yaitu pihak yang bertanggung jawab atas keberhasilan tugas, di mana pihak ini memiliki otoritas untuk memutuskan suatu perkara. Dalam hasil pemetaan pada subdomain APO12 adalah *Chief Information Officer* yaitu pihak yang bertanggung jawab dalam menangani masalah teknologi informasi pada perusahaan. Komponen selanjutnya yaitu untuk *consulted* yaitu peran yang memberikan masukan terhadap sebuah proses. Pada subdomain ini salah satunya yaitu *Head Development* dan *Information Security Officer. Head Development* yaitu merupakan pihak yang bertanggung jawab atas proses pengembangan solusi TI sehingga mampu memberikan saran mengenai sebuah proses. *Information Security Manager* bertanggung jawab dalam mengelola, merancang, dan mengawasi dan / atau menilai keamanan informasi perusahaan. Terakhir untuk komponen *informed* yaitu pihak yang selalu menerima informasi yang tepat untuk diawasi dan dipantau dengan baik adalah *Chief Executive Officer* dan *Enterprise Risk Committee. Chief Executive Officer* paling bertanggung jawab atas seluruh manajemen perusahaan. *Enterprise Risk Committee* ini merupakan sekelompok eksekutif dari perusahaan yang bertanggung jawab atas kolabirasi dan tingkat konsensus perusahaan yang dibutuhkan untuk mendukung segala aktivitas dan keputusan dari manajemen risiko perusahaan. Sebuah dewan risiko TI dapat terbentuk demi mempertimbangkan risiko TI secara lebih detail dan mampu memberikan saran kepada komite risiko perusahaan.

Rekomendasi yang lainnya, perusahaan harus mampu menentukan metode yang tepat dan sesuai untuk memantau hasil dari pengelolaan risiko sehingga risiko TI tersebut tetap berada dalam risiko yang mampu diterima oleh

perusahaan. Menurut Stoneburner, Goguen dan Feringa (2002), dokumen kontrol di dalamnya dapat berupa pertimbangan prioritas dari pengelolaan risiko. Ini dilakukan guna melakukan mitigasi risiko. Pertama, menjelaskan opsi dari mitigasi risiko. Selanjutnya strategi dari mitigasi risiko. Ini berisi mengenai kapan dan dalam keadaan apa harus bertindak? Atau kapan menerapkan kontrol ini untuk mengurangi risiko dan melindungi organisasi?. Selanjutnya ketika tindakan kontrol diambil, aturan yang berlaku yaitu dalam mengatasi risiko terbesar, dan berusaha untuk melakukan mitigasi risiko yang cukup dengan biaya terendah, dengan dampak minimal pada kemapuan.

Dalam dokumen kontrol berisi mengenai urutan atau peringkat tindakan dari tinggi ke rendah, daftar yang berisi kontrol yang layak, analisis biaya-manfaat yang menggambarkan biaya dan manfaat dari penerapan atau tidak dari pengimplementasian kontrol. Selanjutnya dari analisis biaya dan manfaat, manajemen menentukan kendali yang paling hemat biaya untuk mengurangi risiko. Didapati juga personil yang terlibat sehingga memudahkan dalam melakukan kontrol. Terdapat juga rencana proteksi dari implementasi dan terakhir melakukan implementasi dari kontrol yang dpilih. Selain itu membahas mengenai mekanisme dari pemantauan dan tinjau ulang. Di mana keduanya memiliki elemen proses beserta persyaratan dan bukti yang memperkuat elemen proses yang telah berjalan dengan baik. Dokumen juga harus membahas isu-isu yang muncul. Pada kontrol ini perusahaan juga harus mengukur kinerja dari manajemen risiko, agar mampu memantau secara efektif dan meninjau kemajuan dari kinerja aktivitas manajemen risiko yang diterapkan dalam organisasi. Contoh, memantau perubahan dampak atau kemungkinanan risiko, misal jika organisasi memerlukan sejumlah staff dengan keterampilan khusus untuk direktut dalam jangka waktu tertentu untuk menyelesaikan suatu proyek, maka tingkat keberhasilan rekrutmen yang sebenarnya dapat dijadikan indikator kemungkinan, dan karena itu dampak secara keseluruhan proyek tidak terselesaikan. Selanjutnya, pemantauan akan perubahan efektivitas kontrol dan proses serta kegiatan yang sesuai diterapkan. Jika *firewall* organisasi adalah kontrol utama untuk risiko *hacked,* maka jumlah pelanggaran mengenai *firewall* dapat menjadi indikator efektivitas *firewall.* Dan pemantauan akan proses dan kegiatan yang dilakukan sesuai dengan yang ditetapkan. Perusahaan dapat memantau kepemilikan risiko dan kontrol untuk memastikan bahwa risiko dikelola dengan tepat. Tabel 5.2 merupakan ringkasan mengenai rekomendasi yang disusun untuk proses APO12.

Tabel 5.3 Rekomendasi Proses APO12

PROSES	REKOMENDASI	ALASAN
APO12	Membuat dokumen khusus mengenai saran akan ancaman yang mungkin terjadi di masa depan demi mengantisipasi dampak dari risiko yang	Disusun untuk meningkatkan kapabilitas proses.

Tabel 5.4 Rekomendasi Proses APO12 (Lanjutan)

PROSES	REKOMENDASI	ALASAN
	dihasilkan dari ancaman tersebut.	
	Melakukan identifikasi dan penilaian terkait risiko TI untuk mengurangi risiko dengan mempertimbangkan biaya dan manfaat.	Disusun untuk meningkatkan kapabilitas proses.
	Pemisahan antara tanggung jawab dan tugas seperti yang telah ditentukan oleh ISACA untuk proses mengelola risiko TI.	Karena pada proses banyak tugas dan tanggung jawab yang dipegang oleh satu orang.
	Menentukan kompetensi sumber daya manusia dalam proses mengelola risiko. Sehingga pihak yang bertanggung jawab merupakan orang yang ahli dibidangnya.	Karena menurut hasil temuan, banyak staf yang belum memiliki latar belakang TI.
	Menentukan metode yang tepat dan sesuai untuk memantau hasil dari pengelolaan risiko sehingga risiko TI tetap berada dalam risiko yang mampu diterima oleh perusahaan.	Disusun untuk mencapai *targeted level* yang diharapkan untuk proses APO12.

5.4 Mengelola Keamanan

Data dan informasi perusahaan merupakan salah satu aset terpenting. Dengan melakukan pengelolaan terhadap keamanan informasi mampu mempertahankan kerahasiaan yaitu mampu melindungi data serta informasi dari pengguna yang tidak memiliki otoritas, ketersediaan yaitu data dan informasi tersedia bagi pihak-pihak yang membutuhkan dan memiliki otoritas dalam menggunakannya dan integritas informasi yang dimiliki oleh perusahaan yaitu seluruh sistem informasi harus memberikan gambaran yang akurat mengenai sistem fisik yang mereka wakili. Menurut ISO/IEC 27000 (2016), keberhasilan dari penerapan *Information Security Management Systems* (ISMS) penting untuk melindungi aset informasi yang memungkinkan perusahaan untuk mencapai jaminan yang lebih besar bahwa aset informasinya dilindungi secara baik terhadap ancaman maupun risiko yang terus menerus timbul. Selain itu perushaaan harus mampu memelihara kerangka kerja terstruktur dan komprehensif untuk

mengidentifikasi dan menilai risiko keamanan informasi, memilih dan menerapkan pengendalian dan mengukur serta meningkatkan keefektifannya. Sehingga mampu terus menerus memperbaiki lingkungan pengendalian. Dan secara efektif mencapai kepatuhan hukum dan peraturan yang sudah ditetapkan perusahaan.

Pada subdomain APO13 perusahaan telah mencapai *capability level* 1 yaitu dengan pencapaian pada skala L (>50%-85%) unruk atribut proses PA 1.1 *(Process Performance).* Pada *capability level* 1 ini kondisinya proses dari pengelolaan keamanan informasi berhasil meraih tujuan yaitu di mana mempertahankan integritas informasi, kerahasiaan dan ketersediaan informasi yang dimiliki dengan mempertimbangan BPs dan WPs. Berdasarkan keinginan atau harapan dari perusahaan untuk *targeted level* pada APO13 yaitu *capability level* 2. Sehingga *gap* yang dimiliki sebesar 1. Rekomendasi pertama, yaitu perlu dibentuk tim khusus mengenai manajemen keamanan informasi bagi PDAM Kota Malang. Seperti yang telah didapatkan dari hasil pemetaan RACI *Chart*, banyak pihak yang memiliki tugas dan tanggung jawab ganda sesuai dengan deskripsi dari ISACA. Sehingga rekomendasinya mampu membentuk tim khusus untuk keamanan informasi dan pemisahan tugas dan tanggung jawab. Menurut ISACA (2012b), yang terlibat pada APO13 sesuai dengan hasil pemetaan RACI *Chart*, untuk komponen *responsible* yaitu pihak yang menjalankan tugas. Orang yang berperan pada bagian operasional utama dalam memenuhi aktivitas yang tercantum dan menciptakan hasil yang diharapkan adalah *Chief Information Officer* dan *Information Security Manager. Chief Information Officer* yaitu pihak yang bertanggung jawab dalam menangani masalah teknologi informasi pada perusahaan dan *Information Security Manager* merupakan pihak yang bertanggung jawab dalam penerapan dan pengembangan keamanan teknologi informasi perusahaan.

Selanjutnya komponen *accountable* yaitu pihak yang bertanggung jawab atas keberhasilan tugas, di mana pihak ini memiliki otoritas untuk memutuskan suatu perkara pada subdomain APO13 yaitu *Chief Information Security Manager.* Bertangung jawab atas keamanan informasi perusahaan. Untuk komponen *consulted* yaitu pihak yang memberikan sebuah masukan terhadap sebuah proses yaitu pada subdomain APO13 *Business Executive* dan *Strategy Executive Committee. Business Executive* bertanggung jawab atas pengoperasian unit usaha atau anak perusahaan tertentu dan *Strategy Executive Committee* merupakan sekelompok eksekutif senior yang dipilih oleh dewan untuk memastikan dewan mengetahui, dan terus mendapatkan informasi, masalah dan keputusan utama mengenai TI. Tanggung jawabnya adalah untuk mengelola portofolio akan investasi TI, layanan TI dan aset TI, selanjutnya memastikan bahwa nilai dan risiko sudah dilakukan manajemen dan dikelola. Komite ini biasanya diketuai oleh anggota dewan bukan CIO. Dan untuk komponen *informed* yaitu pihak yang selalu menerima informasi yang tepat untuk diawasi dan dipantau dengan baik pada subdomain APO13 adalah *Steering (Programmer/Project) Committee.* Merupakan sekelompok pemangku kepentingan dan ahli yang bertanggung jawab atas pembinaan program dan proyek, termasuk manajemen dan pengawasan rencana,

alokasi sumber daya, penyampaian manfaat dan nilai serta pengelolaan program dan risiko proyek.

Pada hasil *checklist* yang terlampir pada Lampiran B.1, maka dapat diberikan rekomendasi bagi perusahaan untuk mendokumentasikan seluruh kasus mengenai keamanan informasi dan bagaimana lingkup dari manajemen keamanan sistem informasi tersebut. Sehingga manajemen atau tim yang dibentuk mengetahui lingkup mereka dalam mengelola keamanan. Ini sesuai dengan kriteria yang belum dipenuhi menurut ISACA. Selanjutnya yaitu melakukan identifikasi dan analisis dari risiko yang mampu terjadi dari keamanan informasi dan disesuaikan dengan strategi perusahaan dan arsitektur perusahaan yang disimpan kedalam sebuah dokumen dengan menentapkan persyaratan akan konten dari dokumen tersebut sehingga pihak yang membutuhkan informasi terkait mampu memanfaatkannya dengan baik. Menurut Rezwinda (2015), dokumen mengenai kebijakan keamanan merupakan infrastruktur terkait keamanan yang harus dimiliki organisasi atau perusahaan dalam melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi mengenai berbagai kendali yang dilakukan dalam mengontrol manajemennya, mekanismenya, prosedurnya serta tata cara dalam mengamanankan informasi. Dengan adanya kebijakan ini, selain membantu organisasi dalam mengamanan aset pentingnya, juga mengihindari insiden atau tuntutan hukum ketika organisasi atau perusahaan lalai dalam pengelolaan aset internal.

Standar keamanan organisasi harus menetapkan serangkaian kontrol dan pedoman untuk memastikan bahwa prosedur keamanan yang mengatur penggunaan aset dan sumber daya TI organisasi ditegakkan dengan benar dan diterapkan sesuai dengan tujuan dan misi organisasi. Manajemen memainkan peran penting dalam mengawasi implementasi kebijakan dan memastikan pembentukan kontrol operasional yang tepat. Sehingga rekomendasi selanjutnya menurut Stoneburner, Goguen dan Feringa (2002), menetapkan tanggung jawab keamanan untuk memastikan bahwa keamanan yang memadai disediakan untuk sistem TI. Tanggung jawab ini seperti yang telah disampaikan sebelumnya pada rekomendasi pertama. Lalu, mengembangkan dan mengelola rencana keamanan sistem untuk nantinya didokumentasikan hasil kontrol saat ini dan mengarahkan kontrol yang direncanakan untuk sistem TI demi mendukung tujuan organisasi. Laksanakan kontrol keamanan personil, termasuk pemisahan tugas, paling tidak hak yang istimewa mengenai akses dan penghentian akses komputer pengguna. Rekomendasi lainnya menurut Stoneburner, Goguen dan Feringa (2002), lakukan kesadaran akan keamanan dan pelatihan teknik untuk memastikan bahwa pengguna akhir dan pengguna sistem sadar akan aturan perilaku dan tanggung jawab mereka dalam melindungi tujuan dari organisasi.

Agar lebih baik dalam manjemen kemanan informasi, perusahaan harus mampu membuat karakteristik sistem. Menurut Datta (2010), mengkarakterisasi suatu sistem informasi, menetapkan ruang lingkup upaya penilaian risiko, menggambarkan batas otorisasi operasional (atau akreditasi), dan memberikan informasi (misalnya, perangkat keras, perangkat lunak, konektivitas sistem, dan

divisi atau personel pendukung yang bertanggung jawab). Langkah ini dimulai dengan identifikasi batas-batas sistem informasi, sumber daya, dan informasi. Minimal, karakterisasi sistem menggambarkan masing-masing komponen sistem berikut, yaitu *hardware* (*hardware* dan OS untuk setiap *individual server*, workstation, terminal, dll), *software* (RDBMS, Server Web, Internet, Server, dll), antarmuka atau *interface* (eksternal) ke sistem lain, data dan *people*. Karakterisasi sistem juga menggambarkan faktor-faktor lain yang berpotensi mempengaruhi keamanan sistem, seperti persyaratan fungsional sistem, kebijakan dan arsitektur keamanan organisasi, topologi jaringan sistem, arus informasi di seluruh sistem, manajemen, operasional dan kontrol keamanan teknis yang dilaksanakan atau direncanakan, dan fisik dan lingkungkan dari mekanisme keamanan. Selain itu Elky (2006) memberikan saran untuk melakukan analisis terkait dampak. Berikut dijelaskan pada Tabel 5.3., karena seperti yang telah dijelaskan sebelumnya dengan mengelola keamanan informasi mampu mempertahankan kerahasiaan, integritas dan ketersediaan informasi.

Tabel 5.5 Contoh Definisi Dampak

	Kerahasiaan	**Integritas**	**Ketersediaan**
Low	Kehilangan kerahasiaan menyebabkan efek yang terbatas pada organisasi.	Hilangnya integritas menyebabkan efek yang terbatas pada organisasi.	Hilangnya ketersediaan menyebabkan efek yang terbatas pada organisasi.
Moderate	Hilangnya kerahasiaan menyebabkan efek yang serius pada organisasi.	Hilangnya integritas menyebabkan efek yang serius pada organisasi.	Hilangnya ketersediaan menyebabkan efek yang serius pada organisasi.
High	Kehilangan kerahasiaan menyebabkan efek yang parah pada organisasi.	Hilangnya integritas menyebabkan efek yang parah pada organisasi.	Hilangnya ketersediaan menyebabkan efek yang parah pada organisasi.

Tabel 5.4 merupakan ringkasan mengenai rekomendasi yang disusun untuk proses APO13.

Tabel 5.6 Rekomendasi Proses APO13

PROSES	**REKOMENDASI**	**ALASAN**
APO13	Membentuk tim khusus manajemen keamanan informasi dengan tugas dan tanggung jawab sesuai ISACA pada RACI *Chart* APO13.	Karena perusahaan belum memiliki tim khusus untuk manajemen risiko TI. Sehingga dengan adanya tim khusus mampu memaksimalkan kinerja dari proses.

PROSES	REKOMENDASI	ALASAN
	Melakukan dokumentasi terhadap seluruh kasus beserta ruang lingkupnya.	Karena informasi mengenai kasus dapat digunakan oleh pihak lain untuk menjalankan prosesnya.
	Melakukan identifikasi dan analisis mengenai risiko terkait keamanan infromasi dan disimpan pada dokumen khusus dengan persyaratan yang telah ditetapkan.	Karena perusahaan belum melakukan identifikasi khusus mengenai risiko keamanan informasi sehingga mampu meningkatkan tingkat kapabilitas dari proses mengelola keamanan.
	Membuat dokumen kebijakan mengenai keamanan informasi termasuk kendali, mekanisme, prosedur dan tata cara mengamanankan informasi.	Karena kebijakan merupakan dasar dalam melakukan proses. Rekomendasi ini disusun untuk meningkatkan tingkat kapabilitas dari proses mengelola keamanan.
	Menetapkan serangkaian kontrol dan pedoman untuk memastikan bahwa prosedur keamanan yang ditegakkan dan diterapkan sesuai tujuan.	Rekomendasi ini disusun untuk meningkatkan tingkat kapabilitas dari proses mengelola keamanan.
	Melakukan kesadaran akan keamanan informasi kepada seluruh pihak.	Rekomendasi ini disusun untuk meningkatkan tingkat kapabilitas dari proses mengelola keamanan.
	Melakukan karakterisasi sistem informasi *(hardware, software dan interface)*	Karena sesuai dengan latar belakang peneilitian mengenai meningkatkan kehandalan terkait aset yang dimiliki.
	Melakukan analisis dampak untuk tetap menjaga kerahasiaan, integritas dan ketersediaan informasi.	Karena untuk mengurangi risiko dan dampak yang terjadi terkait dengan keamanan informasi.

BAB 6 PENUTUP

6.1 Kesimpulan

Kesimpulan yang dapat ditarik dari penelitian ini yaitu, pertama kondisi dari *base practices* dan *generic practices* yaitu di mana keduanya merupakan indikator untuk masing-masing proses yang memberikan definisi tugas dan aktivitas yang dibutuhkan untuk mencapai tujuan dari proses dan memenuhi hasil dari proses. *Base practices* merupakan istilah yang digunakan pada penilaian *level* 1 sedangkan untuk *level* 2-5 menggunakan istilah *generic practices*. Pada subdomain EDM03 *(Ensure Risk Optimisation)* PDAM Kota Malang telah melakukan evaluasi, identifikasi dan pemantauan dari manajemen risiko. Perusahaan telah memiliki dokumen yang menjelaskan aktivitas dan proses mengenai optimasi risiko. Pada APO12 *(Manage Risk)* perusahaan telah melakukan aktivitas yang berulang guna mencapai pengelolaan risiko dengan baik. Perusahaan telah mengumpulkan data yang digunakan untuk analisis risiko namun hanya bersifat insidental, mempertahankan sumber daya dalam pengelolaan risiko, dan menang*gap*i secara cepat untuk langkah efektif risiko walupun selama ini yang ada pada *software* yang digunakan hanya sekitar risiko yang sifatnya teknis. Dan untuk APO13 *(Manage Security)* perusahaan telah menetapkan dan memelihara keamanan informasi walaupun belum secara khusus dibentuk tim yang menangani masalah keamanan. Perusahaan telah menjaga dan mengenalkan budaya keamanan dan perbaikan. Ini didapati dari bocornya informasi mengenai *business plan* yang seharusnya tidak boleh diakses oleh publik.

Untuk kondisi *work product* dan *generic work products* yaitu di mana keduanya berfungsi sebagai pemberi panduan objektif untuk mencari masukan dan keluaran yang potensial, dan bukti objektif untuk mendukung penilaian berdasarkan dokumentasi. Mereka membelikan rekamanan dan jejak audit dari aktivitas proses dan memungkinkan tindak lanjut jika terjadi insiden. Pada subdomain EDM03 *(Ensure Risk Optimisation)* PDAM Kota Malang telah memiliki panduan mengenai rekamanan dan jejak audit dari aktivitas optimasi risiko. Namun, tetap hanya beberapa kategori risiko yang diidenfitikasi. Perusahaan belum mempertimbangkan kategori risiko yang mungkin saja terjadi di masa depan. Subdomain APO12 *(Mengelola Risiko)* dokumen WPs yang dimiliki masih belum sempurna dikarenakan tidak mendetail terutama mengenai bagaimana pengelolaan risiko, karena ada beberapa pihak yang memiliki tugas ganda sesuai dengan deskripsi ISACA. Dan untuk subdomain APO13 *(Manage Security)* belum adanya dokumen khusus membahas mengenai keamanan menjadikan kondisi di mana pengelolaan keamanan masih butuh banyak perbaikan.

Kesimpulan kedua, kondisi dari *gap* (kesenjangan) antara *capability level* dengan *targeted level* pada subdomain EDM03 memiliki kesenjangan 1. Ini dikarenakan *targeted level* yang diharapkan yaitu berada pada *capability level* 2 sedangkan menurut hasil penilaian perusahaan berada pada *capability level* 1. Subdomain APO12 memiliki kesenjangan 1 *level*. Ini dikarenakan *targeted level*

yang diharapkan yaitu berada pada *capability level* 2 sedangkan menurut hasil penilaian perusahaan berada pada *capability level* 1. Dan *subdomain* APO12 memiliki kesenjangan 1 *level*. Ini dikarenakan *targeted level* yang diharapkan yaitu berada pada *capability level* 2 sedangkan menurut hasil penilaian perusahaan berada pada *capability level* 1.

Kesimpulan ketiga, rekomendasi pertama untuk subdomain EDM03 yaitu melakukan kategori risiko sesuai dengan kategori *IT Risk* ISACA yaitu *IT Benefit/Value Enablement*, *IT Programmer and Project Delivery Risk*, dan *IT Operations and Service Delivery*. Rekomendasi kedua, perusahaan mampu membentuk tim sendiri untuk manajemen risiko dan pembagian tugas dan tanggung jawab sesuai dengan deskripsi ISACA. Rekomendasi ketiga, melakukan analisis dan membuat daftar terkait ancaman yang mungkin terjadi di masa depan dari teknologi informasi. Rekomendasi keempat, menerapkan persyaratan dalam hal dokumentasi terkait konten, rincian, ruang lingkup, siapa yang bertanggung jawab dan lain sebagainya. Dan rekomendasi kelima, perusahaan mampu menetapkan kompetensi yang dibutuhan staff dalam melakukan proses. Kompetensi disini yaitu kemampuan atau pengalaman staff. Rekomendasi pertama untuk subdomain APO12 yaitu memiliki dokumen terkait saran yang dibutuhkan ketika ancaman terkait penerapan teknologi informasi terjadi. Rekomendasi kedua, perusahaan melakukan identifikasi dan penilaian risiko sehingga merumuskan bagaimana cara untuk mengurangi risiko yang berhubungan dengan teknologi informasi. Disatukan kedalam satu dokumen di mana di dalamnya memiliki pertimbangan dalam biaya serta manfaat dari pengelolaan risiko TI. Rekomendasi ketiga pemisahan antara tanggung jawab dan tugas seperti yang telah ditentukan oleh ISACA pada RACI *Chart*. Sehingga penggunaan sumber daya khususnya manusia mampu dimanfaatkan dengan baik dan teratur. Rekomendasi keempat, perusahaan mampu menentukan kompetensi terkait sumber daya manusia seperti apa yang dibutuhkan dalam pengelolaan risiko. Dan rekomendasi kelima, perusahaan harus mampu menentukan metode yang tepat dan sesuai untuk memantau hasil dari pengelolaan risiko sehingga risiko TI tersebut tetap berada dalam risiko yang mampu diterima oleh perusahaan.

Dan rekomendasi pertama untuk subdomain APO13 yaitu, mampu membentuk tim khusus untuk keamanan informasi dan pemisahan tugas dan tanggung jawab. Rekomendasi kedua, mendokumentasikan seluruh kasus mengenai keamanan informasi dan bagaimana lingkup dari manajemen keamanan sistem informasi tersebut. Sehingga manajemen atau tim yang dibentuk mengetahui lingkup mereka dalam mengelola keamanan. Rekomendasi ketiga, melakukan identifikasi dan analisis dari risiko yang mampu terjadi dari keamanan informasi dan disesuaikan dengan strategi perusahaan dan arsitektur perusahaan yang disimpan kedalam sebuah dokumen dengan menentapkan persyaratan akan konten dari dokumen tersebut sehingga pihak yang membutuhkan informasi terkait mampu memanfaatkannya dengan baik. Rekomendasi keempat, membuat dokumen mengenai kebijakan keamanan. Berisi mengenai berbagai kendali yang dilakukan dalam mengontrol manajemennya,

mekanismenya, prosedur serta tata cara dalam mengamankan informasi. Rekomendasi kelima, menetapkan serangkaian kontrol dan pedoman untuk memastikan bahwa prosedur keamanan yang mengatur penggunaan aset dan sumber daya TI organisasi ditegakkan dengan benar dan diterapkan sesuai dengan tujuan dan misi organisasi. Rekomendasi keenam, menetapkan tanggung jawab keamanan untuk memastikan bahwa keamanan yang memadai disediakan untuk sistem TI. Rekomendasi ketujuh, melakukan kesadaran akan keamanan dan pelatihan teknik untuk memastikan bahwa pengguna akhir dan pengguna sistem sadar akan aturan perilaku dan tanggung jawab mereka dalam melindungi tujuan dari organisasi. Rekomenadi kedelapan, melakukan karakterisasi sistem informasi. Dimulai dengan identifikasi batas-batas sistem informasi, sumber daya dan informasi. Minimal, karakterisasi sistem menggambarkan masing-masing komponen sistem *hardware, software, interface.* Dan rekomendasi keesembilan, melakukan analisis dampak. Karena pada dasarnya keamanan informasi dilakukan demi menjaga kerahasiaan,integritas dan ketersediaan informasi. Diberikan tingkat *low*, *moderate* dan *high* dan dampaknya kepada kerahasiaan, integritas dan ketersediaan seperti apa.

6.2 Saran

Penelitian ini hanya berfokus kepada penilaian *capability level* dan memberikan rekomendasi untuk mencapai *level* yang diharapkan. Saran yang diberikan penulis dalam penelitian selanjutnya khususnya terkait manajemen risiko teknologi informasi dengan menggunakan *framework* COBIT 5 yaitu kedepannya mampu melakukan *risk assessment* dengan mempertimbangkan beberapa hal yang berasal dari internal perusahaan dan eksternal perusahaan. Sehingga menghasilkan penilaian risiko dari seluruh kategori risiko. Dan mampu menyusun dokumen seperti apa yang dibutuhkan oleh perusahaan. Terkait konten dari dokumen, isi, dan analisis serta lainnya yang mampu mendukung perusahaan dalam mencapai tujuan proses.

DAFTAR PUSTAKA

Astuti, H. M., et al., 2017. Risk Assessment of Information Technology Process Based on COBIT 5 Framework: A Case Study of ITS Service Desk. In: Information Systems International Conference (ISICO), 2017. *4th Information Systems International Conference.* Bali, Indonesia, 6-8 November 2017. Amsterdam: Elsevier B.V.

Arief, M. H., 2018. *Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang).* Malang: Universitas Brawijaya Malang

Bachri, B. S., 2010. *Meyakinkan Validitas Data Melalui Triangulasi Pada Penelitian Kualitatif.* Surabaya: Universitas Negeri Surabaya

Djajalaksana, Y. M., & Gantini, T., 2013. *Kebutuhan Kompetensi Tenaga Kerja Teknologi Informasi di Indonesia.* Yogyakarta: Universitas Kristen Maranatha

Datta, S. P., 2010. *Risk Management Process for Information Security System.* India: Kalyani University

Elky, S., 2006. *An Introduction to Information System Risk Management.* U.S: SANS Insititute.

IACOP., 2014. *Risk Assessment In Audit Planning.* IACOP: Ukraine

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

ISACA., 2012b. *COBIT 5: Enabling Processess.* USA: Rolling Meadows

ISACA., 2013a. *COBIT 5: for Risk.* USA: Rolling Meadows

ISACA., 2013b. *COBIT 5: Self-Assessment Guide: Using COBIT 5.* USA: Rolling Meadows

ISACA., 2013c. *Process Assessment Model (PAM): Using COBIT 5.* USA: Rolling Meadows

ISO/IEC 27000., 2016. *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.* Switzerland: ISO

Mufti, R. G., 2017. *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk).* Malang: Universitas Brawijaya

Pithcard, C. L., 2015. *Risk Management Concepts and Guidance Fifth Edition.* New York: CRC Press

Recker, J., 2013. *Scientific Research in Information Systems.* Australia: Springer Heidelberg

Rezwinda, 2015. *Pentingnya Kebijakan Keamanan Informasi (Security Policy).* [online] Proxsis. Tersedia di: <https://it.proxsisgroup.com/pentingnya-kebijakan-keamanan-informasi-security-policy/> [Diakses 22 April 2018]

Suminar, S., Fitroh & Ratnawati, S., 2015. *Evaluation of Information Technology Governance using COBIT 5 Framework Focus APO13 and DSS05 in PPIKSIN-BATAN.* Jakarta: University of Islam Negeri Syarif Hidayatullah.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems.* Gaithersburg: U.S Department of Commerce.