

**EVALUASI PROSES OPTIMASI RISIKO, PENGELOLAAN
KEAMANAN, DAN PENGELOLAAN LAYANAN KEAMANAN
MENGUNAKAN KERANGKA KERJA COBIT 5 PADA PT TIRTA
INVESTAMA (AQUA) PANDAAN**

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Vicky Nur Ardianto
NIM: 145150407111071



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

PENGESAHAN

**EVALUASI PROSES OPTIMASI RISIKO, PENGELOLAAN KEAMANAN, DAN
PENGELOLAAN LAYANAN KEAMANAN MENGGUNAKAN KERANGKA KERJA
COBIT 5 PADA PT TIRTA INVESTAMA (AQUA) PANDAAN**

SKRIPSI


Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

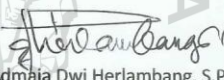
Disusun Oleh :
Vicky Nur Ardianto
NIM: 145150407111071

Skripsi ini telah diuji dan dinyatakan lulus pada
12 Juli 2018
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I

Dosen Pembimbing 2


Suprpto, S.T, M.T
NIP: 197107271996031001


Admaja Dwi Herlambang, S.Pd., M.Pd.
NIK: 2016098908021001

Mengetahui:
Ketua Jurusan Sistem Informasi




Dr. Eng. Herman Tolle, S.T, M.T.
NIP: 197408232000121001



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 didalam 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, 12 Juli 2018



Vicky Nur Ardianto

NIM: 145150407111071

DAFTAR RIWAYAT HIDUP



VICKY NUR ARDIANTO

CURRICULUM VITAE
INFORMATION SYSTEM LABORATORY GRADUATE

NOMOR INDUK MAHASISWA

145150407111071

TEMPAT, TANGGAL LAHIR

Pasuruan, 30 Maret 1996

ALAMAT

Jl. Mangga No. 138 RT 05 RW 09 Dsn. Jetak, Ds. Karang Jati
Kec. Pandaan, Kab. Pasuruan, 67156

RIWAYAT PENDIDIKAN

- 2001 - 2002 TK Kusuma Bangsa
- 2002 - 2008 SDN Jogosari 1
- 2008 - 2011 SMPN 2 Pandaan
- 2011 - 2014 SMKN 1 Purwosari
- 2014 - 2018 Universitas Brawijaya

PRESTASI PRIBADI

- 2016 Finalis Kompetisi i-Fest 2.0 se-Universitas Brawijaya
- 2016 Finalis Kompetisi Beyond se-Jawa Timur

PENGALAMAN PRIBADI

- 2015 Asisten Dosen Mata Kuliah Desain Web
- 2016 Volunteer of Teaching & Traveling ke-5 1000 Guru Malang
- 2016 Volunteer of Teaching & Giving ke-3 1000 Guru Malang (Spesial Ramadhan)
- 2016 Ketua Divisi Publikasi, Dekorasi, dan Desain (PDD) Silaturrahmi Cup FILKOM ke-4
- 2016 Anggota Divisi Publikasi, Dekorasi, dan Desain (PDD) Olimpiade FILKOM
- 2016 Wakil Ketua Divisi Acara i-Fest 3.0 Tingkat Nasional

BAHASA

Indonesia (Bahasa Pokok)
Inggris

PASSION

Sport
Music
Traveling

KONTAK

- +62 812 9001 6686
- vickynurardianto@gmail.com
- vickynurardianto



KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadiran Tuhan yang Maha Esa, Allah Subhanahu Wa Ta'ala atas segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir yang berjudul "Evaluasi Proses Optimasi Risiko, Pengelolaan Keamanan, dan Pengelolaan Layanan Keamanan Menggunakan Kerangka Kerja COBIT 5 Pada PT Tirta Investama (AQUA) Pandaan" dengan baik dan lancar.

Penyusunan tugas akhir diajukan penulis untuk memenuhi sebagian persyaratan dalam memperoleh gelar Sarjana Komputer dari Fakultas Ilmu Komputer (FILKOM) Universitas Brawijaya Malang. Dalam penyusunannya, tentu tidak lepas dari dukungan berupa do'a dan bimbingan dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Wayan Firdaus Mahmudy, S.Si, M.T, Ph.D selaku Dekan Fakultas Ilmu Komputer (FILKOM) Universitas Brawijaya Malang.
2. Dr. Eng. Herman Tolle, S.T, M.T. selaku Ketua Jurusan Sistem Informasi pada Fakultas Ilmu Komputer (FILKOM) Universitas Brawijaya Malang.
3. Suprpto, S.T, M.T. selaku Ketua Program Studi Sistem Informasi dan dosen pembimbing I yang telah memberikan waktu, ilmu, nasihat, dan masukan untuk membimbing dalam menyelesaikan tugas akhir ini.
4. Admaja Dwi Herlambang, S.Pd., M.Pd. selaku dosen pembimbing II yang juga telah memberikan waktu, ilmu, nasihat, dan masukan untuk membimbing dalam menyelesaikan tugas akhir ini.
5. Ibu Misnatin dan Bapak Mochammad Mahmudianto selaku kedua orang tua yang senantiasa memberikan kasih sayang berupa nasihat, semangat dan do'a sehingga tugas akhir ini dapat terselesaikan dengan baik dan tepat waktu.
6. Bapak Nadhif selaku Kepala *Human Resource Department* (HRD) yang telah menerima dan memberikan izin untuk melaksanakan penelitian tugas akhir di PT Tirta Investama (AQUA) Pandaan.
7. Bapak Andrie selaku Staf *DAN'IS Network Analyst* yang telah bersedia menjadi responden dalam penelitian tugas akhir ini.
8. Bapak Udin selaku Staf *IT Onsite* yang juga bersedia menjadi responden dalam penelitian tugas akhir ini.
9. Pihak lain yang tidak dapat disebutkan satu-persatu.

Semoga seluruh dukungan yang telah diberikan mendapat ridha dan keberkahan dari Allah Subhanahu Wa Ta'ala. Dalam penyusunan tugas akhir ini, penulis menyadari masih banyak kekurangan dari beberapa aspek. Oleh karena itu, penulis bersedia menerima saran yang bersifat membangun untuk memperbaiki kekurangan yang ada. Semoga tugas akhir ini bermanfaat dan mengedukasi bagi pihak perusahaan, peneliti selanjutnya dan para pembaca lain.

Malang, 12 Juli 2018

Penulis

vickynurardianto@gmail.com



ABSTRAK

Vicky Nur Ardianto, Evaluasi Proses Optimasi Risiko, Pengelolaan Keamanan, dan Pengelolaan Layanan Keamanan Menggunakan Kerangka Kerja COBIT 5 Pada PT Tirta Investama (AQUA) Pandaan

Dosen Pembimbing: Suprpto, S.T, M.T dan Admaja Dwi Herlambang, S.Pd., M.Pd.

PT Tirta Investama (AQUA) Pandaan merupakan salah satu perusahaan yang telah memanfaatkan teknologi informasi (TI) sebagai penunjang proses bisnisnya. Segala aktivitasnya dikelola langsung oleh divisi *Danone Information Systems* (DAN'IS) selaku penanggung jawab atas penyediaan serta pengembangan fasilitas teknologi dan sistem informasi perusahaan. Adanya pemanfaatan, tentu menimbulkan bahan evaluasi guna menjaga fungsionalitas teknologi agar terus stabil. Penelitian ini bertujuan mengevaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan. Dua dari tiga proses yang ada merupakan proses yang berkaitan dengan sistem keamanan informasi. Keamanan informasi dipilih sebagai objek evaluasi karena terdapat kebijakan perusahaan yang mengatur hal ini. Kebijakan terlampir dalam dokumen yang bernama *IS Security Policy* dan diperkuat dengan adanya bidang keamanan informasi pada struktur organisasi divisi.

Penelitian ini menggunakan kerangka kerja COBIT 5 sebagai referensi utama. Metode penelitian dilakukan melalui observasi, wawancara, dan analisis menggunakan lembar penilaian guna mendeskripsikan kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) dari proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*). Sehingga diketahui tingkat kapabilitas dan pencapaian dari setiap proses yang dimaksud. Setelah dilakukan analisis, diketahui ketiga proses yang ada memiliki tingkat kapabilitas yang sama dengan tingkat kesenjangan yang berbeda-beda. Setiap proses memiliki tingkat kapabilitas pada *level 3 (established process)*, yang mana proses EDM03 (*Ensure Risk Optimization*) memiliki tingkat kesenjangan sebesar 1 dan APO13 (*Manage Security*) serta DSS05 (*Manage Security Services*) sebesar 2.

Selain itu, diperoleh beberapa hasil temuan yang salah satunya belum adanya *management team* yang fokus bertanggung jawab atas pengelolaan risiko teknologi informasi (TI) pada divisi DAN'IS. Sebab, pengelolaan risiko cenderung dilimpahkan kepada tim *IT Support*. Oleh karena itu, diberikan rekomendasi sebagai langkah dalam memperbaiki dan meningkatkan kualitas proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan sehingga meraih tingkat pencapaian seperti yang diharapkan perusahaan.

Kata kunci: evaluasi, optimasi risiko, pengelolaan keamanan, pengelolaan layanan keamanan, COBIT 5

ABSTRACT

Vicky Nur Ardianto, Evaluasi Proses Optimasi Risiko, Pengelolaan Keamanan, dan Pengelolaan Layanan Keamanan Menggunakan Kerangka Kerja COBIT 5 Pada PT Tirta Investama (AQUA) Pandaan

Supervisors: Suprpto, S.T, M.T dan Admaja Dwi Herlambang, S.Pd., M.Pd.

PT Tirta Investama (AQUA) Pandaan is one company that has been utilizing information technology (IT) to support its business process. All activities are managed directly by the division of Danone Information Systems (DAN'IS) as responsible for the provision and development of technology facilities and corporate information systems. The existence of utilization, certainly raises the evaluation materials in order to maintain the functionality of technology to continue to be stable. This study aims to evaluate the process of ensure risk optimization, manage security, and manage security services. Two of the three existing processes are related to information security systems. Information security is selected as an evaluation object, because there is a company policy that governed. The policy is enclosed in a document called IS Security Policy and is reinforced by the field of information security on the organizational structure of the division.

The research method is doing through observation, interview, and analysis using assessment sheet to describe the condition of Base Practices (BP), Work Product (WP), Generic Practices (GP), and Generic Work Product (GWP) of EDM03 (Ensure Risk Optimization), APO13 (Manage Security), and DSS05 (Manage Security Services). So as to know the capability level and targeted level of each process in question. After doing analysis, it's known that the three existing processes have the same level of capability level with different gap levels. Each process has a capability level at level 3 (established process), where the EDM03 (Ensure Risk Optimization) has a gap of 1 and APO13 (Manage Security) and DSS05 (Manage Security Services) has a gap of 2.

In addition, there are several findings, one of which is the absence of a management team that focuses on the management of information technology (IT) risk in the DAN'IS division. Therefore, risk management tends to be assigned to the IT Support team. Therefore, it's recommended as a step in improving the quality of ensure risk optimization, manage security, and manage security services, so as to achieve the targeted level as expected by the company.

Keywords: evaluation, ensure risk optimization, manage security, manage security services, COBIT 5

DAFTAR ISI

PENGESAHAN	ii
PERNYATAAN ORISINALITAS	iii
DAFTAR RIWAYAT HIDUP	iv
KATA PENGANTAR.....	v
ABSTRAK.....	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	6
1.3 Tujuan	6
1.4 Manfaat.....	7
1.5 Batasan Masalah.....	7
1.6 Sistematika Pembahasan.....	8
BAB 2 LANDASAN KEPUSTAKAAN	9
2.1 Kajian Pustaka	9
2.2 Profil PT Tirta Investama (AQUA) Pandaan	12
2.3 Profil DAN'IS.....	13
2.4 Visi, Misi dan Tujuan DAN'IS.....	13
2.5 Struktur Organisasi Divisi DAN'IS.....	14
2.6 Profil <i>Information System and Technology</i>	15
2.7 Pengertian Evaluasi.....	16
2.8 Pengertian Tata Kelola	17
2.9 Manajemen Keamanan Informasi	19
2.10 Pengertian COBIT	20
2.11 Pengertian COBIT 5	21
2.12 Komponen COBIT 5	22
2.13 Area dan Domain COBIT 5	23
2.14 Dasar Proses Keamanan Informasi pada COBIT 5	26



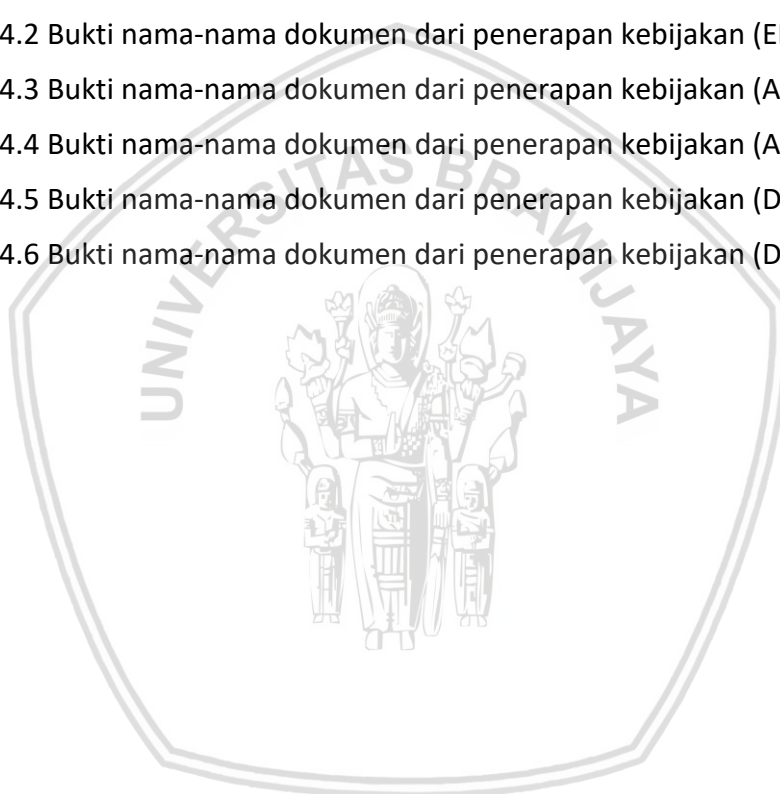
2.15 Pengertian RACI <i>Chart</i>	34
2.16 Pengertian <i>Self Assessment</i>	41
2.17 Indikator Proses Kapabilitas COBIT 5.....	43
BAB 3 METODOLOGI PENELITIAN	46
3.1 Metode Penelitian	46
3.2 Studi Literatur dan Studi Kasus.....	48
3.3 Analisis Profil Perusahaan dan RACI <i>Chart</i>	48
3.4 Pembuatan Pedoman Pengumpulan Data	49
3.5 Pengumpulan Data	49
3.6 Triangulasi Data	49
3.7 <i>Self Assessment</i>	50
3.8 Rekomendasi.....	50
3.9 Kesimpulan dan Saran	50
BAB 4 ANALISIS DAN HASIL	51
4.1 Analisis dan Pemetaan RACI <i>Chart</i>	51
4.2 <i>Ensure Risk Optimization</i> (EDM03).....	57
4.3 <i>Manage Security</i> (APO13).....	68
4.4 <i>Manage Security Services</i> (DSS05).....	78
4.5 Analisis Kesenjangan (<i>Gap Analysis</i>).....	89
4.6 Hasil Temuan	92
BAB 5 PEMBAHASAN.....	94
5.1 <i>Ensure Risk Optimization</i> (EDM03).....	94
5.2 <i>Manage Security</i> (APO13).....	96
5.3 <i>Manage Security Services</i> (DSS05).....	99
BAB 6 KESIMPULAN DAN SARAN	103
6.1 Kesimpulan.....	103
6.2 Saran	104
DAFTAR PUSTAKA.....	105
LAMPIRAN A HASIL WAWANCARA.....	107
LAMPIRAN B HASIL OBSERVASI.....	118
LAMPIRAN C HASIL PENILAIAN	138

DAFTAR TABEL

Tabel 2.1 Proses dari EDM	23
Tabel 2.2 Proses dari APO	24
Tabel 2.3 Proses dari BAI.....	25
Tabel 2.4 Proses dari DSS	25
Tabel 2.5 Proses dari MEA	26
Tabel 2.6 Pihak dari proses EDM03	35
Tabel 2.7 Pihak dari proses APO13	37
Tabel 2.8 Pihak dari proses DSS05	38
Tabel 2.9 Kategori pencapaian tiap <i>level</i>	44
Tabel 4.1 Penentuan peran dari proses EDM03	52
Tabel 4.2 Pemetaan peran pada proses EDM03.....	53
Tabel 4.3 Penentuan peran dari proses APO13	54
Tabel 4.4 Pemetaan peran pada proses APO13	55
Tabel 4.5 Penentuan peran dari proses DSS05.....	55
Tabel 4.6 Pemetaan peran pada proses DSS05	57
Tabel 4.7 Pemetaan kebijakan/dokumen (EDM03).....	65
Tabel 4.8 Perhitungan dari lembar penilaian (EDM03)	67
Tabel 4.9 Hasil tingkat kapabilitas dari proses EDM03	67
Tabel 4.10 Pemetaan kebijakan/dokumen (APO13).....	75
Tabel 4.11 Perhitungan dari lembar penilaian (APO13)	77
Tabel 4.12 Hasil tingkat kapabilitas dari proses APO13.....	77
Tabel 4.13 Pemetaan kebijakan/dokumen (DSS05).....	86
Tabel 4.14 Perhitungan dari lembar penilaian (DSS05)	89
Tabel 4.15 Hasil tingkat kapabilitas dari proses DSS05.....	89
Tabel 4.16 Tingkat kesenjangan dari proses EDM03	91
Tabel 4.17 Tingkat kesenjangan dari proses APO13	91
Tabel 4.18 Tingkat kesenjangan dari proses DSS05.....	92
Tabel 5.1 Rekomendasi (EDM03).....	96
Tabel 5.2 Rekomendasi (APO13).....	98
Tabel 5.3 Rekomendasi (DSS05).....	102

DAFTAR GAMBAR

Gambar 2.1 Struktur organisasi divisi DAN'IS	15
Gambar 2.2 <i>Roadmap IT Governance Implementation Guide</i>	16
Gambar 2.3 RACI <i>Chart</i> dari proses EDM03	34
Gambar 2.4 RACI <i>Chart</i> dari proses APO13	36
Gambar 2.5 RACI <i>Chart</i> dari proses DSS05	38
Gambar 3.1 Tahap penelitian	47
Gambar 4.1 Bukti nama-nama dokumen dari penerapan kebijakan (EDM03)	63
Gambar 4.2 Bukti nama-nama dokumen dari penerapan kebijakan (EDM03)	64
Gambar 4.3 Bukti nama-nama dokumen dari penerapan kebijakan (APO13)	73
Gambar 4.4 Bukti nama-nama dokumen dari penerapan kebijakan (APO13)	74
Gambar 4.5 Bukti nama-nama dokumen dari penerapan kebijakan (DSS05)	84
Gambar 4.6 Bukti nama-nama dokumen dari penerapan kebijakan (DSS05)	86





BAB 1 PENDAHULUAN

1.1 Latar Belakang

Peran teknologi informasi (TI) menjadi bagian penting bagi perusahaan saat ini. Teknologi informasi (TI) mendukung tujuan bisnis dengan menyediakan wadah komunikasi yang cepat, akurat, dan mudah. Selain itu, meningkatkan efektifitas dan efisiensi operasional untuk mendukung inovasi perusahaan agar terus berkembang. Adanya teknologi informasi (TI), seolah mengubah gaya perusahaan dalam mengambil keputusan. Jenis keputusan dapat dipengaruhi oleh kualitas informasi. Sebab, kualitas yang ada menentukan keberhasilan program kerja dari perusahaan. Selain itu, evaluasi terhadap pengelolaan juga diperlukan guna mempertahankan dan meningkatkan performa teknologi informasi (TI) pada perusahaan. Sehingga mendukung keselarasan antara tujuan bisnis dan organisasi. Menurut ITGI (2007), tujuan utama evaluasi tata kelola teknologi informasi (TI) adalah mengelola fungsionalitasnya guna memastikan dan meyakini bahwa aktivitas perusahaan telah selaras dengan tujuan bisnis.

Berdasarkan penelitian sebelumnya, banyak ditemukan masalah ketika melakukan evaluasi tata kelola teknologi informasi (TI), seperti keamanan informasi. Sumber informasi bisa datang dari mana saja, salah satunya penggunaan teknologi informasi (TI). Akan sangat berbahaya bila terjadi manipulasi. Semakin berkembangnya teknologi informasi (TI), maka semakin banyak pula ancaman yang mendekati. Ancaman juga bisa bersumber dari mana saja, contohnya dari hasil pemrosesan data. Akan menjadi bahaya bila terjadi kerusakan bahkan kehilangan data. Hal ini akan berimbas pada operasional perusahaan. Dibalik ancaman tentu ada penyebabnya, seperti peluang, rasionalisasi pikiran, dan tekanan dari dalam maupun luar perusahaan. Oleh karena itu, dibutuhkan evaluasi tata kelola teknologi informasi (TI) menggunakan kerangka kerja yang baik dan relevan sebagai pedoman dalam memperbaiki dan meningkatkan kualitas penerapan teknologi informasi (TI) yang diharapkan.

Terdapat beberapa jenis kerangka kerja yang dapat digunakan sebagai referensi dalam melakukan evaluasi tata kelola teknologi informasi (TI), salah satunya menggunakan kerangka kerja *Control Objective for Information and Related Technology* (COBIT). Kerangka kerja ini berasal dari *IT Governance Institute* (ITGI) yang merupakan bagian dari *Information System Audit and Control Assosiation* (ISACA). Menurut Sarno (2009), kerangka kerja COBIT memberikan standar umum berupa domain dan sekumpulan proses mengenai pengelolaan teknologi informasi (TI). Setiap domain mempresentasikan aktivitas terstruktur yang bisa dikendalikan. Hasil akhir dari penerapan kerangka kerja COBIT akan diketahui tingkat kapabilitas (*capability level*) dari kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) pada objek penelitian. Setelah itu, direkomendasikan perbaikan bilamana diketahui tingkat kesenjangan (*gap level*).

Kerangka kerja COBIT telah banyak mengalami perubahan versi dari tahun ke tahun. Versi kelima merupakan versi terakhir dari kerangka kerja ini. Pihak ISACA merilis COBIT 1 pada tahun 1996 dan COBIT 5 pada tahun 2012. Kerangka kerja COBIT 5 melengkapi seluruh cakupan isi dari versi-versi sebelumnya. Selain itu, kerangka kerja COBIT 5 dipilih karena memiliki dua proses yang terkait dengan penelitian ini. Dua proses yang dimaksud antara lain APO13 (*Manage Security*) sebagai pengelola keamanan dan DSS05 (*Manage Security Services*) sebagai pengelola layanan keamanan. Namun, kedua proses itu tidak lantas maksimal bila tidak diintegrasikan dengan proses lain dari kerangka kerja COBIT 5. Dalam penelitian ini, penulis menyertakan EDM03 (*Ensure Risk Optimization*) sebagai proses tambahan. Proses ini dipilih untuk memastikan optimasi risiko dari pengelolaan keamanan dan pengelolaan layanan keamanan.

Sebelum menentukan COBIT 5 sebagai kerangka kerja tunggal dalam penelitian ini, tentu harus memahami kelebihan dan kekurangan dari kerangka kerja lain yang dianggap relevan dalam melakukan evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan. Sehingga memudahkan dalam menentukan kerangka kerja mana yang sesuai dengan topik dan metode penelitian ini. Jenis kerangka kerja yang dianalisis antara lain *Control Objective for Information and Related Technology* (COBIT), *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), *Information Technology Infrastructure Library* (ITIL), dan ISO/IEC 20000. Berikut penjelasan dari keempat kerangka kerja yang dimaksud. Menurut Alfafara (2008), secara umum COBIT merupakan kerangka kerja tata kelola teknologi informasi (TI) yang memberikan arahan lengkap dari perencanaan, manajemen proyek, pengembangan, sistem mutu, pengelolaan layanan, dan keamanan.

Seiring berjalannya waktu, bentuk arahan didetailkan kembali oleh beberapa kerangka kerja lain mengikuti perkembangan keilmuan. Dalam pelaksanaannya, pengguna utama dari kerangka kerja ini adalah seorang manajer, operator, dan auditor sistem informasi. Sudut pandang dari kerangka kerja ini adalah terkait pengendalian internal organisasi yang mengintegrasikan antara penerapan kebijakan atau prosedur dengan struktur organisasi. Sehingga akan menciptakan suatu sistem yang baik untuk mencapai tujuan organisasi. Selain itu, juga akan tersedia informasi yang kredibilitas melalui dokumen yang dihasilkan dari penerapan kebijakan atau prosedur.

Jenis komponen yang disediakan oleh kerangka kerja ini antara lain perencanaan dan pengorganisasian, penerapan dan pemanduan, serta pengawasan dan pendistribusian. Pengendalian kerangka kerja difokuskan pada penggunaan teknologi informasi (TI). Beberapa hal yang dimaksud merupakan definisi dan kelebihan dari kerangka kerja COBIT. Adapun kekurangan dari kerangka kerja ini adalah hanya memberikan panduan kendali tanpa panduan implementasi. Selain itu, panduan kendali terkesan fokus pada pengukuran tingkatan saja.

Selanjutnya, definisi dari kerangka kerja COSO. Menurut Alfafara (2008), kerangka kerja ini merupakan suatu inisiatif dari sektor swasta yang dibentuk pada tahun 1985. Tujuannya adalah mengidentifikasi faktor-faktor yang menyebabkan penggelapan laporan keuangan dan membuat rekomendasi untuk mengurangi kejadian. Kerangka kerja ini telah menyusun suatu definisi umum untuk standar, pengendalian, dan kriteria internal yang dapat digunakan organisasi untuk menilai sistem pengendalian mereka. Seiring berjalannya waktu, terjadi perkembangan dalam kerangka kerja ini sehingga tercipta kerangka kerja baru bernama COSO *Enterprise Risk Management*, yang mulai meluaskan fokus pada pengelolaan risiko. Dalam pelaksanaannya, pengguna utama dari kerangka kerja ini adalah seorang manajer.

Kerangka kerja ini memberikan keyakinan atau jaminan yang wajar berkaitan dengan pencegahan atau deteksi dini terhadap pengambilan, penggunaan, atau penghilangan yang tidak terotorisasi terhadap aset entitas. Sehingga dapat memberikan pengaruh material terhadap laporan keuangan. Selain itu, aktivitas pengendalian merupakan kebijakan atau prosedur yang membantu menjamin bahwa arahan manajemen telah dilaksanakan. Beberapa hal yang dimaksud merupakan definisi dan kelebihan dari kerangka kerja COSO. Adapun kekurangan dari kerangka kerja ini adalah terkesan fokus dalam hal desain dan implementasi teknologi informasi (TI) sehingga kurang dalam hal pelayanan organisasi. Kerangka kerja ini lebih mengutamakan kualitas internal organisasi daripada pelayanannya.

Kemudian, definisi dari kerangka kerja ITIL. Menurut Alfafara (2008), kerangka kerja ini merupakan serangkaian dengan konsep infrastruktur, pengembangan, serta operasi teknologi informasi (TI). Kerangka kerja ini juga mendeskripsikan sejumlah praktik penting dari teknologi informasi (TI) dan menyediakan daftar komprehensif tugas dan prosedur yang dapat disesuaikan dengan kebutuhan setiap organisasi. Kerangka kerja ini bukan merupakan standar yang memberikan resep (*prescription*), namun fokus terhadap rekomendasi. Oleh karena itu, bentuk implementasi antar organisasi terkadang mengalami perbedaan.

Dengan demikian, siapa pun akan kesulitan dalam membandingkan atau melakukan patokan (*benchmark*) secara pasti. Beberapa hal yang dimaksud merupakan definisi dan kelebihan dari kerangka kerja ITIL. Adapun kekurangan dari kerangka kerja ini adalah sumber referensi yang sulit terjangkau bagi pengguna non-komersial. Akan kurang sesuai bila digunakan oleh seorang pemula dalam melakukan evaluasi, sebab kerangka kerja ini bersifat menyeluruh (*holistic*) yang mencakup semua kerangka kerja untuk tata kelola teknologi informasi (TI) sehingga akan membutuhkan banyak referensi dalam pemahamannya. Selain itu, dalam pelaksanaan pedoman buku ITIL memerlukan pelatihan dan sertifikasi khusus dengan biaya yang relatif besar.

Terakhir, definisi dari kerangka kerja ISO/IEC 20000. Menurut Alfafara (2008), kerangka kerja ini merupakan suatu standar internasional yang diperuntukkan bagi manajemen layanan teknologi informasi (TI). Kerangka kerja ini menggantikan standar sebelumnya yang bernama BS 15000 dan dibuat oleh British. Kerangka kerja ISO/IEC 20000 dipublikasikan oleh *International Organization for Standardization (ISO)* dan *International Electorol Commision (IEC)*. Standar umum pertama yang digunakan dalam manajemen layanan teknologi informasi (TI) adalah kerangka kerja ISO/IEC 20000. Standar ini secara spesifik menentukan persyaratan bagi institusi (merujuk kepada BUMN, Swasta, dan *Government*) sebagai penyedia layanan teknologi informasi (TI) untuk merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, *me-review*, memelihara, dan meningkatkan sistem manajemen layanan teknologi informasi (TI). Beberapa hal yang dimaksud merupakan definisi dan kelebihan dari kerangka kerja ISO/IEC 20000.

Adapun kekurangan dari kerangka kerja ini adalah kurangnya tingkat kesadaran dari *stakeholder* ISO/IEC 20000. Sehingga proses audit hanya untuk memenuhi persyaratan tanpa adanya pemahaman dan rasa kepemilikan dalam menjalankan setiap proses dalam *IT Service Management*. Berdasarkan definisi, kelebihan, dan kekurangan dari keempat kerangka kerja tadi, disimpulkan bahwa COBIT merupakan kerangka kerja yang paling sesuai untuk membantu penelitian ini. Kesesuaian itu berasal dari fokus pengendalian pada sisi teknologi informasi (TI), yang mana pengguna utamanya berasal dari seorang manajer, operator, dan auditor sistem informasi. Selain itu, kerangka kerja ini menyediakan proses khusus yang relevan dengan topik penelitian ini.

Dalam menentukan objek penelitian, dilakukan pemahaman profil instansi terlebih dahulu agar studi kasus yang diperoleh sesuai dengan topik penelitian. PT Tirta Investama (AQUA) Pandaan merupakan salah satu perusahaan yang telah memanfaatkan teknologi informasi (TI) dalam mendukung kegiatan bisnis dan operasionalnya. Seluruh aset teknologi informasi (TI) dikelola langsung oleh divisi *Danone Information Systems (DAN'IS)*. Hal ini menjadi alasan utama dalam menentukan lokasi penelitian. Divisi DAN'IS memiliki seluruh tanggung jawab atas semua penyediaan dan pengembangan fasilitas teknologi informasi (TI) untuk seluruh kegiatan perusahaan Danone. Jenis kegiatan yang dilakukan beragam, seperti pengembangan sumber daya manusia, keuangan, dan penjaminan mutu perusahaan.

Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui Danone telah memiliki dua puluh perusahaan air mineral di seluruh Indonesia. Jadi, disimpulkan bahwa Danone merupakan salah satu instansi besar saat ini. Sehingga banyak informasi yang dikelola, disimpan, dan dibagikan antar anak perusahaan. Risiko terjadinya kerusakan, kehilangan, dan tereksposnya data ke pihak lain akan selalu berpotensi. Oleh karena itu, keamanan informasi sangat dibutuhkan dalam setiap aktivitas perusahaan.

Dalam praktiknya, divisi DAN'IS berfokus dalam penyediaan infrastruktur teknologi informasi (TI) seperti perangkat lunak dan keras. Selain itu, memberi dukungan teknis berupa layanan terhadap peningkatan kualitas pengetahuan dan informasi serta manajemen bisnis dan operasional perusahaan. Keamanan informasi dipilih sebagai objek evaluasi karena terdapat kebijakan perusahaan yang mengatur hal ini. Kebijakan terlampir dalam dokumen yang bernama *IS Security Policy*. Dokumen ini dikelola oleh salah satu bidang divisi DAN'IS yang berfokus terhadap sistem keamanan informasi bernama *DAN'IS Security Analyst*. Evaluasi dilakukan sebagai salah satu aktivitas perbaikan (*improvement*) guna menjaga kondisi keamanan informasi agar terus stabil.

Berdasarkan hasil observasi dan wawancara, ditemukan beberapa masalah yang sering mengganggu performa sistem teknologi informasi (TI) perusahaan. Jenis masalah yang muncul antara lain terjadinya penurunan performa sistem karena kurangnya manajemen data. Hal ini berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI). Sebab, divisi DAN'IS telah menerapkan sistem informasi berbasis *Enterprise Resources Planing* (ERP) untuk beberapa perusahaan Danone, termasuk PT Tirta Investama (AQUA) Pandaan. Selain itu, belum terjaminnya seluruh keamanan data. Terkadang data dapat diakses oleh pihak luar. Akan berakibat fatal bila jenis data yang terekspos sangat vital bagi perusahaan. Sebab, risiko penyalahgunaan data akan terus terjadi. Kemudian, beberapa aset juga pernah mengalami kerusakan bahkan kehilangan data akibat serangan *malware*, seperti virus, *worm spyware*, dan *spam*. Seperti masalah pertama, hal ini juga berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI).

Oleh karena itu, perlu adanya evaluasi tata kelola teknologi informasi (TI) guna mengantisipasi dan menanggulangi permasalahan yang datang. Sebab, dengan adanya evaluasi akan dilakukan proses perbaikan bilamana terjadi permasalahan. Sehingga menjadi pedoman dalam meningkatkan kualitas tata kelola teknologi (TI) di lain hari. Untuk mengevaluasi paparan masalah yang ditemukan, dilakukan penelitian skripsi yang berjudul "**Evaluasi Proses Optimasi Risiko, Pengelolaan Keamanan, dan Pengelolaan Layanan Keamanan Menggunakan Kerangka Kerja COBIT 5 Pada PT Tirta Investama (AQUA) Pandaan**".

1.2 Rumusan Masalah

Berdasarkan paparan latar belakang, diperoleh identifikasi masalah sebagai berikut.

1. Bagaimana kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) pada proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan?
2. Bagaimana kondisi kesenjangan (*gap*) antara tingkat kapabilitas (*capability level*) dengan tingkat pencapaian (*targeted level*) pada proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan?
3. Bagaimana rekomendasi yang diberikan untuk proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) agar meraih tingkat pencapaian (*targeted level*) yang diharapkan perusahaan?

1.3 Tujuan

Berdasarkan paparan rumusan masalah, diperoleh identifikasi tujuan sebagai berikut.

1. Menganalisis dan mendeskripsikan kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) pada proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan.
2. Menghitung dan mendeskripsikan kesenjangan (*gap*) antara tingkat kapabilitas (*capability level*) dengan tingkat pencapaian (*targeted level*) dari proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan.
3. Mengetahui dan mendeskripsikan rekomendasi untuk memperbaiki dan meningkatkan kualitas sistem keamanan informasi berdasarkan proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*) agar meraih tingkat pencapaian (*targeted level*) seperti yang diharapkan divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan.

1.4 Manfaat

Penelitian ini diharapkan memberi manfaat pada divisi dan perusahaan terkait serta pembaca lainnya.

1. Dengan adanya penelitian ini, diharapkan memberi edukasi bagi divisi *Danone Information Systems* (DAN'IS) dan PT Tirta Investama (AQUA) Pandaan serta pembaca lain tentang pentingnya menjaga dan mengembangkan kualitas optimasi risiko dan keamanan informasi perusahaan.
2. Dengan adanya penelitian ini, diharapkan memperkaya kajian keilmuan tentang proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan.
3. Dengan adanya penelitian ini, diharapkan menjadi acuan atau referensi untuk penelitian selanjutnya dan dikembangkan sebagai penerapan *IT Governance* yang tepat bagi perusahaan.

1.5 Batasan Masalah

Berikut batasan masalah terkait penelitian ini.

1. Objek penelitian hanya berfokus pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan, selaku divisi yang bertanggung jawab dan mengelola teknologi informasi (TI) perusahaan dalam mendukung proses bisnis dan operasionalnya.
2. Penelitian ini menggunakan kerangka kerja COBIT 5 sebagai kerangka kerja tunggal dalam melakukan evaluasi. Sebab, kerangka kerja ini memberikan layanan komprehensif untuk mencapai tujuan perusahaan. Selain itu, terdapat dua proses dari salah satu domain yang sesuai dengan topik penelitian ini.
3. Penelitian ini menggunakan tiga proses dari domain kerangka kerja COBIT 5. Jenis proses terdiri dari dua proses utama yang berkaitan tentang pengelolaan keamanan dan pengelolaan layanan keamanan, serta satu proses pendukung sebagai pedoman dalam pemastian optimasi risiko perusahaan. Ketiga proses yang dimaksud antara lain APO13 (*Manage Security*), DSS05 (*Manage Security Services*), dan EDM03 (*Ensure Risk Optimization*).
4. Pemilihan responden ditentukan melalui analisis dan perhitungan tabel RACI *Chart* dari setiap proses. Kemudian, dipetakan terhadap struktur organisasi divisi *Danone Information Systems* (DAN'IS). RACI *Chart* digunakan agar pemilihan responden sesuai dengan kebutuhan penelitian.
5. Kesesuaian data dari lembar *checklist* akan diuji melalui proses triangulasi data beserta hasil temuan (*evidence*) berdasarkan *Base Practices* (BP) dan *Work Product* (WP) dari setiap proses yang digunakan.

6. Penelitian ini tidak membangun sebuah aplikasi sebagai media meningkatkan kualitas optimasi risiko dan keamanan informasi. Sebab, penelitian ini berjenis non-implementatif atau dikerjakan secara deskriptif. Hasil akhir dari penelitian berupa dokumen tertulis secara sistematis dan terstruktur yang berisi rekomendasi perbaikan dari jenis masalah yang telah ditemukan pada objek penelitian.

1.6 Sistematika Pembahasan

Sistematika penulisan skripsi ditujukan untuk memberikan gambaran dan uraian dari keseluruhan skripsi secara sistematis dan terstruktur seperti keenam bab berikut.

BAB 1 PENDAHULUAN

Bab ini mendeskripsikan latar belakang, rumusan masalah, tujuan, manfaat, dan batasan masalah penelitian serta sistematika pembahasan secara ringkas atas keseluruhan isi dokumen.

BAB 2 LANDASAN KEPUSTAKAAN

Bab ini mendeskripsikan kajian pustaka, konsep, dan teori dari literatur ilmiah sebagai pendukung penelitian. Selain itu, terdapat profil perusahaan dan divisi sebagai wawasan penulis dalam melakukan penelitian.

BAB 3 METODOLOGI PENELITIAN

Bab ini mendeskripsikan aktivitas yang dilakukan dalam penelitian. Setiap aktivitas didasari oleh kerangka kerja dan jenis metode yang digunakan dalam penelitian ini.

BAB 4 ANALISIS DAN HASIL

Bab ini mendeskripsikan analisis dan pemetaan RACI *Chart* sebagai pedoman dalam menentukan responden. Selain itu, mendeskripsikan hasil pengolahan data dari setiap proses untuk mengetahui tingkat kapabilitas (*capability level*) dan tingkat kesenjangan (*gap level*) perusahaan. Kemudian, mendeskripsikan hasil temuan (*evidence*) yang diketahui dari hasil observasi dan wawancara.

BAB 5 PEMBAHASAN

Bab ini mendeskripsikan rekomendasi sebagai pedoman untuk memperbaiki dan meningkatkan kualitas optimasi risiko dan keamanan informasi perusahaan. Bentuk rekomendasi didasarkan atas jenis masalah dan tingkat kesenjangan (*gap level*) dari setiap proses yang digunakan.

BAB 6 KESIMPULAN DAN SARAN

Bab ini mendeskripsikan kesimpulan dan saran dari seluruh proses penelitian yang telah dilakukan sehingga menjadi gambaran umum dan referensi bagi penelitian selanjutnya.

BAB 2 LANDASAN KEPUSTAKAAN

Bab ini membahas kajian pustaka dan dasar teori yang digunakan dalam penelitian. Kajian pustaka membahas beberapa penelitian yang telah dilakukan sebelumnya, dimana jenis penelitian memiliki topik dan kerangka kerja yang sama dengan penelitian ini. Kajian pustaka merupakan acuan atau referensi penulis dalam melakukan evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan. Sedangkan dasar teori membahas mengenai segala teori yang digunakan peneliti untuk menunjang penulisan skripsi yang berjudul **“Evaluasi Proses Optimasi Risiko, Pengelolaan Keamanan, dan Pengelolaan Layanan Keamanan Menggunakan Kerangka Kerja COBIT 5 Pada PT Tirta Investama (AQUA) Pandaan”**. Berdasarkan paparan latar belakang dan rumusan masalah, dasar teori yang digunakan meliputi profil perusahaan, struktur organisasi divisi, pengertian tata kelola, manajemen keamanan informasi, kerangka kerja COBIT 5, dan *self assessment*.

2.1 Kajian Pustaka

Penelitian ini mempelajari dan mengkaji beberapa jurnal ilmiah dengan topik dan permasalahan yang relevan. Selain itu, uraian kerangka kerja yang digunakan didasarkan atas penelitian sebelumnya. Kajian pustaka bertujuan membandingkan antara penelitian sekarang dengan penelitian sebelumnya, yang dijadikan penulis sebagai acuan atau referensi dalam melakukan evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan. Pada kajian pustaka terdapat tiga referensi jurnal ilmiah yang digunakan sebagai acuan atau referensi dalam merancang dan melaksanakan penelitian ini. Salah satu jurnal ilmiah berasal dari kolaborasi penelitian antara pihak Universitas Mercu Buana dengan Universitas Indonesia.

Menurut Fitriyah (2018), masalah yang sering timbul di Universitas XYZ meliputi kasus kehilangan data, kesalahan dalam pengambilan keputusan, kebocoran data, penyalahgunaan komputer, dan nilai investigasi teknologi informasi (TI) yang tinggi namun tidak diimbangi dengan pengembalian nilai yang sesuai. Beberapa hal yang dimaksud menjadi alasan penulis untuk mengevaluasi teknologi informasi (TI) di Universitas XYZ. Selain itu, penulis juga menyebutkan istilah lain audit teknologi dan sistem informasi (TI/SI) dalam kerangka kerja *Control Objectives for Information and related Technology* (COBIT) dengan *IT Assurance*. Hal ini bukan sekedar memberikan evaluasi, namun juga memberikan rekomendasi yang digunakan sebagai acuan dalam memperbaiki dan mengembangkan kualitas tata kelola teknologi informasi (TI) di Universitas XYZ.

Kemudian, dalam metodologi penelitiannya juga dijelaskan bahwa sebelum menentukan COBIT sebagai kerangka kerjanya, penulis terlebih dahulu melakukan beberapa pertimbangan melalui beberapa jenis kerangka kerja yang lain seperti *Ron Weber, Queensland Audit Office*, dan *Jack Champlain*. Semua kerangka kerja audit dipetakan sehingga diperoleh kesimpulan bahwa COBIT merupakan kerangka kerja audit yang paling lengkap. Selain itu, penulis juga melakukan perbandingan antara kerangka kerja *Control Objectives for Information and related Technology (COBIT)* dengan *Information Technology Infrastructure Library (ITIL)* untuk memperoleh kajian wawasan yang luas dari domain *Delivery and Support*. Setelah melakukan pertimbangan dalam memilih kerangka kerja, penulis menjelaskan tentang dasar metodologi audit (*assurance*) yang digunakan dalam penelitiannya. Teknik yang digunakan dengan cara pengumpulan data.

Metodologinya terdiri dari empat alur, antara lain yang pertama penelaahan dokumentasi kebijakan teknis maupun non-teknis yang menjadi dasar pengembangan teknologi informasi (TI) Universitas XYZ. Kedua, observasi dan wawancara dengan pihak terkait seperti kepala pusat Unit *Cybernet* dan pengembangan sistem, staf *Cybernet* dan pengajar, direktur akademik, dan mahasiswa. Ketiga, analisis basis data. Terakhir, analisis jaringan. Selain empat alur metodologi yang disebutkan, penulis juga menjelaskan mengenai alur dalam pelaksanaan evaluasinya, antara lain penentuan rencana dan tujuan audit, penentuan lingkup, melakukan kajian di Universitas XYZ, dan melakukan analisis hasil audit. Referensi jurnal ilmiah kedua berasal dari Institut Teknologi Sepuluh Nopember Surabaya (ITS). Menurut Desy (2014), PT Bank XYZ Surabaya merupakan salah satu bank nasional terbesar di Indonesia yang berkantor pusat di Surabaya, yang bertujuan konsisten dalam memberi pelayanan terbaik kepada nasabahnya.

Banyaknya aktivitas proses bisnis yang dilakukan, membuat teknologi informasi (TI) rentan terhadap risiko keamanan informasi. Pemanfaatan teknologi informasi (TI) mempermudah jalannya proses bisnis perbankan, namun juga berpotensi menimbulkan risiko dan ancaman terhadap keamanan informasi perbankan dari waktu ke waktu. Oleh karena itu, untuk meningkatkan perlindungan terhadap aset informasi, dilakukan penilaian risiko terhadap keamanan informasi. Metode yang digunakan penulis dalam penilaian adalah *Failure Mode & Effect Analysis (FMEA)*. Menurut penulis, metode ini digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial serta menentukan tingkat risiko dari kegagalan dan skala prioritas untuk mengambil tindakan yang diperlukan. Hasil akhir dari penelitian penulis berupa dokumen manajemen risiko yang di dalamnya terdapat *Risk Register*. Dokumen yang dimaksud merupakan laporan hasil manajemen risiko yang berisikan daftar analisis dan pengendalian risiko yang dapat digunakan sebagai acuan atau referensi untuk menangani setiap masalah yang terjadi pada divisi Teknologi Informasi (TI) dari PT Bank XYZ Surabaya.

Selain itu, penulis juga menjelaskan alur penelitiannya berdasarkan metode FMEA seperti *me-review* proses, *brainstorm* risiko potensial, menentukan *severity level* untuk menganalisis risiko, menentukan *occurrence level* untuk menilai peluang (probabilitas) frekuensi mekanisme yang akan terjadi, menentukan *detection level* yang diasosiasikan dengan pengendalian saat itu, dan menghitung *Risk Priority Number* (RPN). Referensi jurnal ilmiah ketiga berasal dari Universitas Brawijaya Malang. Menurut Mufti (2017), departemen *Corporate IT* pada PT Martina Berto Tbk diperlukan evaluasi karena mekanisme pengamanannya belum terlampir dalam Standar Operasional Prosedur (SOP) perusahaan. Selain itu, departemen ini belum memiliki unit khusus yang menangani keamanan informasi. Kemudian, *security incident* juga kerap muncul berupa *broadcast* dari salah satu *web server* perusahaan serta serangan yang mengarah pada *server* perusahaan. Kondisi *server* perusahaan berada dalam *ip public* karena belum terinstalasi *virtual private network* (vpn). Perusahaan pernah menggunakan jasa *freelancer audit security*, namun kegiatan ini tidak dilanjutkan oleh manajemen. Terakhir, belum pernah dilakukannya evaluasi tata kelola teknologi informasi (TI) menggunakan kerangka kerja COBIT 5 pada perusahaan. Oleh karena itu, perlu dilakukan evaluasi untuk mengetahui sejauh mana kualitas dan kuantitas departemen *Corporate IT* dalam mengelola keamanan informasi perusahaan.

Kegiatan evaluasi juga digunakan untuk menghasilkan rekomendasi dalam meraih tingkat pencapaian yang optimal sehingga meraih visi dan misi perusahaan. Penelitian ini bertujuan menilai sejauh mana tingkat kapabilitas (*capability level*) teknologi informasi (TI) yang berfokus pada keamanan informasi departemen *Corporate IT* dari PT Martina Berto Tbk. Selain itu, penulis juga menjelaskan alur penelitiannya seperti studi literatur, analisis *RACI Chart*, pengumpulan data melalui metode wawancara dan kuesioner, analisis tingkat kapabilitas (*capability level*), analisis kesenjangan (*gap analysis*), analisis *Strengths, Weaknesses, Opportunities, dan Threats* (SWOT), membuat rekomendasi, serta menyimpulkan hasil dari penelitiannya. Dari ketiga jurnal ilmiah, masing-masing membahas keterkaitan topik yang relevan dengan rancangan penelitian sekarang. Ketiga jurnal ilmiah memiliki topik yang sama mengenai evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan. Selain itu, alasan memilih teknik pengumpulan data yang berbeda adalah mengkaji dan membandingkan setiap proses yang digunakan. Sehingga diperoleh gambaran luas terkait penyelesaian masalah yang ada di lapangan. Dari ketiga jurnal ilmiah, terdapat satu jurnal ilmiah yang menggunakan kerangka kerja sama dengan apa yang digunakan penelitian sekarang. Jenis proses yang digunakan juga sama dengan apa yang digunakan pada penelitian sekarang. Dengan demikian, diharapkan mampu mengadaptasi penelitian sebelumnya agar lebih baik lagi.

Berdasarkan jurnal ilmiah yang telah dikaji, dijelaskan bahwa penelitian dilakukan dengan menganalisis dan menghitung tingkat kapabilitas (*capability level*) dari kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) dari objek penelitian. Penelitian juga bertujuan mengetahui tingkat kesenjangan (*gap level*) dari kondisi nyata saat itu berdasarkan hasil temuan (*evidence*) yang muncul. Sehingga diberikan rekomendasi sebagai pedoman untuk memperbaiki dan meningkatkan kualitas optimasi risiko dan keamanan informasi pada perusahaan.

2.2 Profil PT Tirta Investama (AQUA) Pandaan

Pada tahun 1973, PT Golden Mississippi didirikan sebagai pelopor perusahaan air minum dalam kemasan (AMDK) pertama di Indonesia. Pabrik pertama didirikan di Bekasi. Setahun berikutnya, pabrik meluncurkan produk AQUA pertama dalam bentuk kemasan botol kaca berukuran 950 ml dengan harga Rp.75,-. Pada tahun 1984, pabrik kedua didirikan di Pandaan-Jawa Timur sebagai upaya untuk mendekati diri pada konsumen yang berada di sekitar wilayah Jawa Timur dengan nama PT Tirta Investama (AQUA) Pandaan. Pabrik ini merupakan salah satu instansi yang berada di bawah naungan *Danone Group*. Sebelum dikenal dengan nama PT Tirta Investama (AQUA) Pandaan, perusahaan ini beberapa kali mengalami perubahan nama. Didirikan pertama kali dengan nama PT Tirta Jaya Utama, namun berubah menjadi PT Tirta Jayamas Unggul pada tahun 1985. Selang beberapa tahun, perusahaan mengalami perubahan nama menjadi PT Tirta Investama (AQUA) Pandaan hingga sekarang. Perusahaan ini mengawali aktivitas produksinya pada tanggal 28 April 1984.

Melalui produksinya, PT Tirta Investama (AQUA) Pandaan menghasilkan beberapa jenis produk yang diklasifikasikan dalam dua kategori, antara lain kategori produk *returnable* dan *non returnable*. Produk *returnable* menghasilkan jenis AQUA 5 Gallon, sedangkan *non returnable* menghasilkan jenis AQUA 600 ml, AQUA 1500 ml, AQUA 240 ml dan AQUA Mizone. Dalam menghasilkan dan meluncurkan produk, PT Tirta Investama (AQUA) Pandaan dilengkapi dengan berbagai sertifikasi. Terdapat lima sertifikasi yang telah diperoleh perusahaan, antara lain yang pertama sertifikasi *Good Manufacturing Process* (GMP) mengenai mutu dan keamanan produk. Kedua, sertifikasi ISO 9001-2000 mengenai sistem manajemen mutu. Ketiga, sertifikasi ISO 14001 mengenai sistem manajemen lingkungan. Keempat, sertifikasi ISO 22000 mengenai manajemen keamanan pangan. Terakhir, sertifikasi halal yang diberikan oleh Majelis Ulama' Indonesia (MUI).

2.3 Profil DAN'IS

Danone Information Systems (DAN'IS) merupakan salah satu divisi di bawah naungan departemen *Country Business Support* (CBS), yang memiliki seluruh tanggung jawab atas penyediaan dan pengembangan fasilitas teknologi dan sistem informasi (TI/SI) untuk menunjang operasional perusahaan. Setiap operasional terbagi dalam beberapa unit yang terdiri dari pengembangan sumber daya manusia, keuangan, hingga penjaminan mutu (*quality control*) pada seluruh perusahaan Danone. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, beberapa perangkat yang disediakan dan dikembangkan oleh divisi DAN'IS seperti *Personal Computer* (PC), perangkat lunak, layanan jaringan dan basis data, yang keseluruhan ditunjang oleh sistem keamanan selama 24 jam. Selain itu, divisi DAN'IS juga mendorong, mengaktifkan, dan mentransformasi pertumbuhan Danone melalui proses inovasi dan solusi bisnis yang efisien. Setiap hari, mereka memastikan semua bahan dan sistem beroperasi dengan benar. Mereka menyediakan dukungan dan bantuan untuk mengoptimalkan proses dan solusi.

2.4 Visi, Misi dan Tujuan DAN'IS

Divisi *Danone Information Systems* (DAN'IS) memiliki visi, misi, dan tujuan dalam menjalankan peran sebagai pengelola teknologi dan sistem informasi pada perusahaan Danone. Berikut visi, misi, dan tujuan dari divisi DAN'IS.

Visi:

“Menjadi pusat teknologi informasi (TI) yang mampu memberikan layanan optimal dalam mendukung seluruh proses bisnis dan operasional pada perusahaan Danone”. Hal ini dimaksudkan bahwa, divisi DAN'IS senantiasa meningkatkan dan memperhatikan kualitas jasa yang diberikan untuk para pemangku kepentingan (*stakeholders*) perusahaan sehingga meraih tujuan yang telah ditetapkan perusahaan. Dalam meraih visi tentu bukan hal mudah, namun melalui komitmen tinggi para pimpinan, divisi ini akan terus berkembang menjadi pusat pelayanan teknologi informasi (TI) yang optimal untuk seluruh kepentingan perusahaan.

Misi:

Menyediakan infrastruktur teknologi informasi (TI) seperti perangkat lunak dan keras. Selain itu, memberikan dukungan teknis berupa layanan terhadap peningkatan kualitas tata kelola teknologi dan sistem informasi perusahaan.

Tujuan:

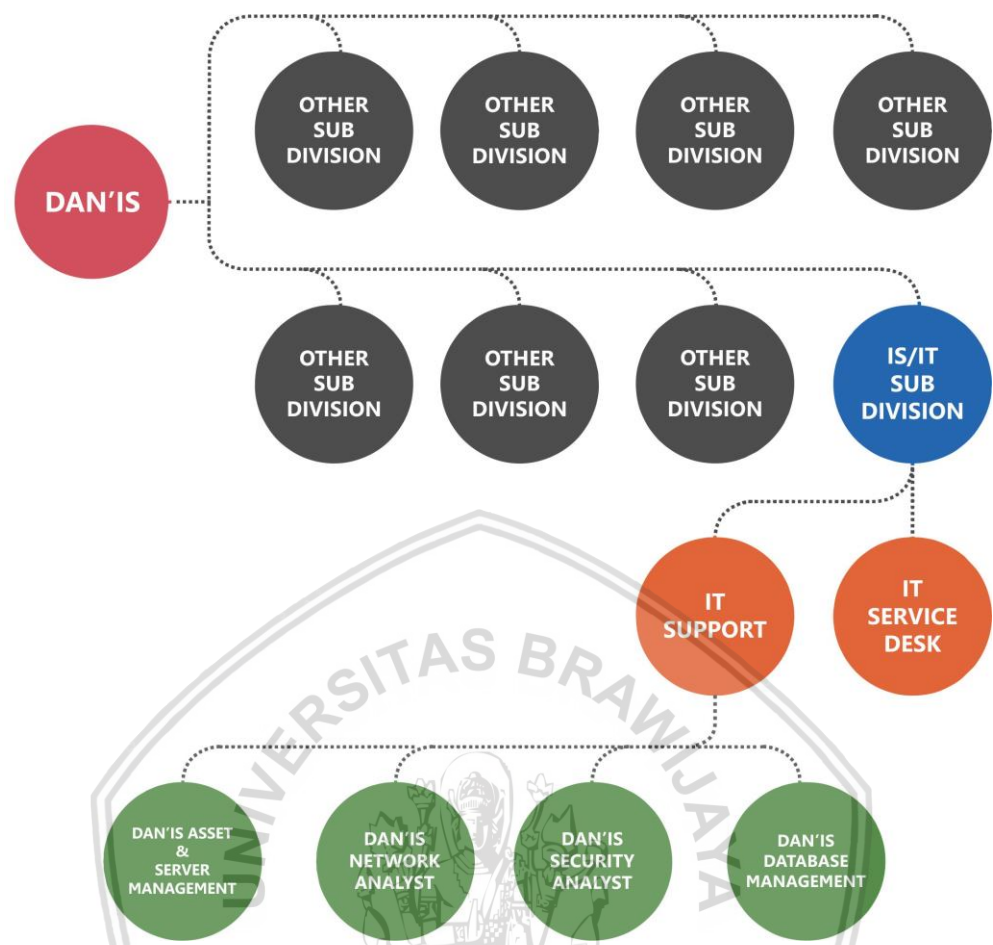
Dalam mewujudkan visi divisi DAN'IS, disusun tujuan strategis agar menjadi acuan dalam pengelolaan dan pengembangan teknologi dan sistem informasi. Jenis tujuan yang dimaksud antara lain menyediakan, mengembangkan, dan memelihara infrastruktur teknologi informasi (TI) untuk mendukung akses manajemen informasi perusahaan. Kedua, menyediakan dan mengembangkan perangkat lunak untuk keperluan manajemen, operasional, dan proses bisnis.

Ketiga, membentuk dan mengelola tingkat keahlian para staf untuk menjadi profesional di bidang teknologi informasi dan komunikasi (TIK) melalui pelatihan staf. Keempat, memastikan perencanaan anggaran yang efektif untuk pengembangan infrastruktur teknologi informasi (TI). Kelima, merencanakan, mengimplementasi, dan mengevaluasi aktifitas pelayanan teknologi informasi (TI). Keenam, menyusun struktur manajemen dan organisasi yang tepat untuk mencapai tujuan dan sasaran divisi DAN'IS. Ketujuh, menciptakan lingkungan, peluang, dan kondisi yang tepat agar dapat meraih dan menjaga kinerja yang optimal untuk kemajuan karir para staf. Kedelapan, menciptakan dan memelihara komunikasi dua arah, baik di luar maupun di dalam unit kerja. Terakhir, mengoptimalkan berbagai sumber daya dan jaringan lokal, regional, dan internasional.

2.5 Struktur Organisasi Divisi DAN'IS

Struktur organisasi divisi *Danone Information Systems* (DAN'IS) ditunjukkan pada Gambar 2.1. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, divisi DAN'IS terbagi dalam delapan sub divisi. Namun, hanya satu sub divisi yang memiliki kewenangan dalam mengelola seluruh aset teknologi informasi (TI) pada perusahaan Danone. Sub divisi ini bernama *Information System and Technology (IT/IS)* yang terbagi menjadi tim *IT Support* dan *IT Service Desk*. Kedua tim memiliki tugas pokok yang berbeda. Dalam praktiknya, tim *IT Support* bertanggung jawab mengelola dan mengawasi proses teknologi informasi (TI) secara terpusat. Sedangkan tim *Service Desk* bertanggung jawab atas perbaikan dan perawatan fasilitas teknologi informasi (TI) secara desentralisasi. Oleh karena itu, tim *IT Service Desk* bertugas pada setiap perusahaan Danone agar penanganan masalah yang muncul lebih cepat.

Agar lebih fokus dalam hal perbaikan dan pengawasan, tim *IT Support* terbagi dalam empat bidang kerja, antara lain yang pertama *DAN'IS Asset & Server Management*. Bidang ini bertanggung jawab menyediakan dan merawat setiap aset yang berkaitan dengan teknologi informasi (TI). Selain itu, bertanggung jawab terhadap seluruh aktivitas *server* dari awal dikembangkan hingga perawatan. Kedua adalah *DAN'IS Network Analyst*. Bidang ini bertanggung jawab terhadap seluruh fasilitas jaringan antar perusahaan Danone. Ketiga adalah *DAN'IS Security Analyst*. Bidang ini bertanggung jawab atas tingkat keamanan seluruh komponen sistem dan jaringan teknologi informasi (TI) pada perusahaan Danone. Terakhir adalah *DAN'IS Database Management*. Bidang ini bertanggung jawab mengelola integritas basis data dan keamanan basis data.



Gambar 2.1 Struktur organisasi divisi DAN'IS

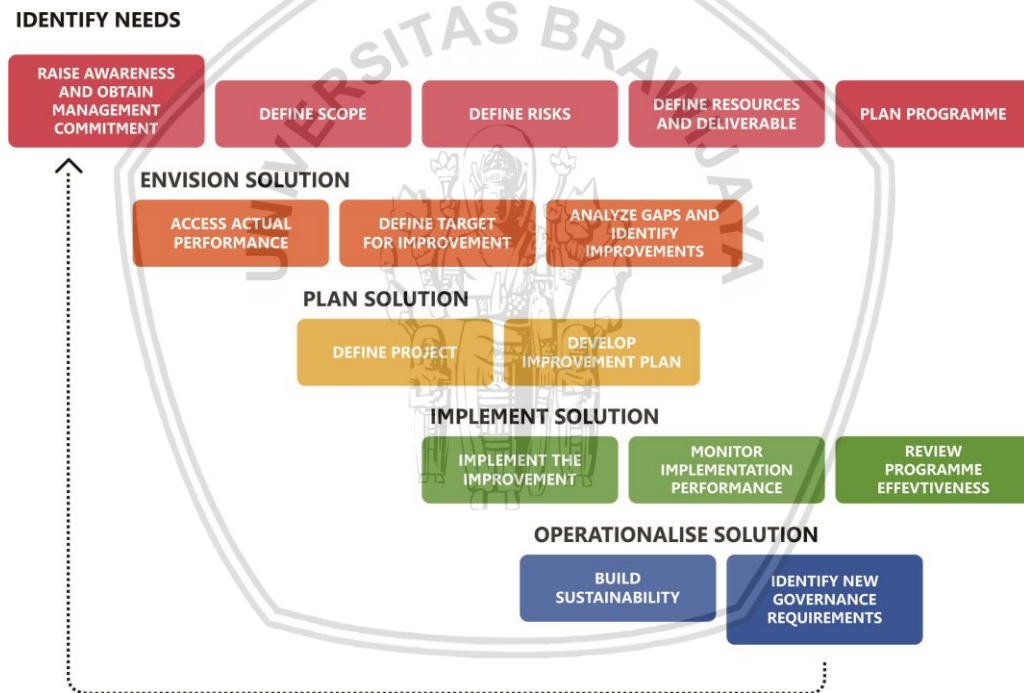
Sumber: wawancara bersama pihak DAN'IS Network Analyst.

2.6 Profil Information System and Technology

Dalam mendukung tata kelola teknologi dan sistem informasi yang terstruktur, divisi *Danone Information Systems* (DAN'IS) membagi konsentrasi kerja dalam delapan sub divisi. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, divisi DAN'IS terbagi dalam delapan sub divisi. Namun, hanya satu sub divisi yang memiliki kewenangan dalam mengelola seluruh aset teknologi informasi (TI) pada perusahaan Danone. Sub divisi ini bernama *Information System and Technology (IT/IS)* yang terbagi menjadi tim *IT Support* dan *IT Service Desk*. Kedua tim memiliki tugas pokok yang berbeda. Dalam praktiknya, tim *IT Support* bertanggung jawab mengelola dan mengawasi proses teknologi informasi (TI) secara terpusat. Sedangkan tim *Service Desk* bertanggung jawab atas perbaikan dan perawatan fasilitas teknologi informasi (TI) secara desentralisasi. Oleh karena itu, tim *Service Desk* bertugas pada setiap perusahaan Danone agar penanganan masalah yang muncul lebih cepat.

2.7 Pengertian Evaluasi

Menurut Arikunto (dalam Sulistya, 2013), evaluasi merupakan kegiatan untuk mengumpulkan informasi mengenai kinerja suatu hal. Kemudian, menggunakan informasi yang diperoleh sebagai alternatif dalam menentukan keputusan. Fungsi utama dari evaluasi adalah menyediakan informasi yang berguna bagi pihak pengambil keputusan (*decision maker*) untuk menentukan kebijakan atau prosedur yang akan diambil berdasarkan hasil temuan sebelumnya. Selanjutnya, menurut Worthen & Sanders (dalam Sulistya, 2013), evaluasi merupakan bentuk kegiatan dalam mencari temuan berharga (*worth*). Temuan berharga meliputi informasi mengenai suatu program dan kebijakan tertentu. Dalam hakikatnya, evaluasi bukan tergolong hal baru dalam kehidupan manusia, sebab setiap proses kehidupan membutuhkan evaluasi agar menjadi lebih baik. Kemudian, menurut Stufflebeam (dalam Sulistya, 2013), evaluasi merupakan kegiatan untuk memperoleh dan menyajikan informasi sebagai alternatif dalam menentukan keputusan.



Gambar 2.2 Roadmap IT Governance Implementation Guide

Sumber: diadaptasi dari *Information Technology Governance Institute*, 2007.

Beberapa pendapat yang dikemukakan para ahli, disimpulkan bahwa evaluasi merupakan kegiatan untuk mengumpulkan informasi melalui berbagai jenis metode sebagai bahan menentukan keputusan yang akan diambil selanjutnya. Evaluasi juga sebagai wadah penilaian untuk mengetahui kondisi saat itu sehingga dapat dilakukan perbaikan bilamana kondisi yang dimaksud tidak sesuai harapan. Sebelum melakukan evaluasi, tentu dilakukan perencanaan agar evaluasi dapat berjalan sistematis dan saling berkesinambungan antar proses yang sedang dijalankan.

Banyak hal yang berkaitan dengan proses evaluasi, salah satunya dalam kehidupan manusia sehari-hari. Setiap perilaku tentu membutuhkan evaluasi sebagai cara menjaga dan memperbaiki diri. Sebab, hakikatnya segala keputusan yang diambil saat ini akan menentukan kondisi di masa mendatang. Sebelum melakukan evaluasi, dianjurkan memahami setiap tahapan yang ada. Pemahaman dilakukan agar proses yang dijalankan lebih terstruktur sehingga memperoleh hasil yang baik. Secara teori, kerangka kerja COBIT 5 tidak memberikan langkah khusus dalam melakukan evaluasi tata kelola teknologi informasi (TI), namun menurut ITGI (2007), disediakan alur (*roadmap*) dalam pelaksanaan evaluasi tata kelola teknologi informasi (TI). Jenis alur (*roadmap*) yang dimaksud ditunjukkan pada Gambar 2.2, yang meliputi identifikasi kebutuhan (*identify needs*), membuat visi tentang solusi (*envision solution*), merencanakan solusi (*plan the solution*), menerapkan solusi (*implement the solution*), dan mengelola solusi (*operationalise solution*). Kelima alur (*roadmap*) merupakan contoh persiapan dalam melakukan evaluasi tata kelola teknologi informasi (TI).

2.8 Pengertian Tata Kelola

Istilah tata kelola atau tata pemerintahan di Indonesia merupakan terjemahan dari "*Corporate Governance*". Secara etimologis, kata "*Governance*" berasal dari bahasa Perancis kuno "*Gouvernance*", yang berarti pengendalian (*regulated*). Selain itu, diartikan sebagai kondisi yang terkendali (*the state of being governed*). Menurut Farrar (dalam Ningsih, 2001), esensi dalam tata kelola sering dikaitkan dengan cara menahkodai kapal (*the idea of steering or captaining a ship*). Secara harfiah, *governance* di Indonesia kerap diterjemahkan sebagai 'aturan', akan tetapi diperlukan kajian untuk mencari istilah yang tepat dalam bahasa Indonesia. Sedangkan menurut Winarno (dalam Ningsih, 2001), *governance* tidak tepat diterjemahkan sebagai pemerintahan, meskipun telah banyak orang yang mengartikan demikian. Dalam konteks tata kelola yang baik (*good corporate governance*) disebut sebagai tata pamong atau penadbiran. Kata terakhir mungkin terasa janggal di telinga, sebab istilah ini berasal dari bahasa Melayu.

Sedangkan secara etimologis, istilah "*Corporate*" merupakan turunan dari bahasa latin *Corpus* yang berarti sekumpulan peraturan atau undang-undang, sedangkan "*Erate*" yang berarti sesuatu yang dipatuhi atau dihargai. Beberapa pendapat yang dikemukakan para ahli, disimpulkan bahwa tata kelola yang baik (*good corporate governance*) merupakan struktur yang mengatur pola hubungan harmonis pada struktur organisasi. Kemudian, terdapat sistem *check and balance* yang mencakup keseimbangan kewenangan atas pengendalian perusahaan yang membatasi munculnya pengelolaan yang salah dan penyalahgunaan aset perusahaan. Selain itu, diartikan juga sebagai proses yang transparan untuk menentukan tujuan perusahaan dan pengukuran kinerjanya. Terdapat pula prinsip-prinsip dasar dalam menjalankan tata kelola yang baik. Menurut Daniri (2005), terdapat lima prinsip dasar dalam tata kelola yang baik (*good corporate governance*).

Kelima prinsip meliputi transparansi, akuntabilitas, responsibilitas, independensi, dan kesetaraan atau kewajaran. Namun dalam Permendagri No. 61 tahun 2007, hanya empat prinsip pertama yang diwajibkan untuk dilakukan. Berikut merupakan definisi rinci dari prinsip dasar yang telah disebutkan sebelumnya, antara lain yang pertama transparansi (*transparency*). Merupakan keterbukaan informasi baik dalam proses pengambilan keputusan maupun mengungkapkan informasi material dan relevan mengenai perusahaan. Keuntungan melakukan prinsip ini agar menghindari benturan kepentingan (*conflict of interest*) dari berbagai pihak manajemen. Kedua adalah akuntabilitas (*accountability*). Merupakan kejelasan fungsi, struktur, sistem, dan pertanggungjawaban organ lembaga sehingga pengelolaannya terlaksana dengan baik. Dengan terlaksananya prinsip ini, lembaga akan terhindar dari konflik atau benturan kepentingan. Ketiga adalah responsibilitas (*responsibility*). Merupakan kesesuaian dalam pengelolaan lembaga terhadap prinsip korporasi yang sehat dan peraturan yang berlaku, termasuk masalah pajak, hubungan industrial, perlindungan lingkungan hidup, kesehatan atau keselamatan kerja, standar penggajian, dan persaingan yang sehat.

Keempat adalah independensi (*independency*). Merupakan keadaan dimana lembaga dikelola secara profesional tanpa benturan kepentingan dan pengaruh dari pihak manapun yang tidak sesuai dengan perundang-undangan yang berlaku serta prinsip korporasi yang sehat. Terakhir adalah kesetaraan atau kewajaran (*fairness*). Merupakan perlakuan yang adil dan setara dalam memenuhi hak pemangku kepentingan (*stakeholder*) yang timbul berdasarkan perjanjian dan perundang-undangan yang berlaku. Dalam teori tata kelola, terdapat hubungan antara risiko dan pengendalian. Hal ini menjadi alasan dalam memilih EDM03 (*Ensure Risk Optimization*) sebagai proses pendukung untuk melengkapi kedua proses yang digunakan dalam penelitian ini. Proses EDM03 (*Ensure Risk Optimization*) bertujuan memastikan optimasi risiko. Bila diartikan secara luas, merupakan pendekatan dari pemangku kepentingan (*stakeholder*) perusahaan terhadap risiko yang diartikulasikan untuk membantu perusahaan dalam menangani setiap risiko yang ditemui. Audit internal perlu menyadari bahwa tata kelola bukanlah himpunan proses dan struktur yang berdiri sendiri.

Tata kelola juga memiliki keterkaitan dengan manajemen risiko dan pengendalian internal. Tata kelola yang efektif mempertimbangkan risiko pada saat menyusun strategi. Sebaliknya, manajemen risiko didasarkan pada tata kelola yang efektif (seperti, *tone at the top*, selera risiko dan toleransi risiko, budaya risiko, dan pengawasan manajemen risiko). Tata kelola yang efektif juga bergantung pada pengendalian internal dan komunikasi dari struktur organisasi. Selain itu, pengendalian dan risiko juga saling terkait, mengingat pengendalian merupakan tindakan yang diambil oleh manajemen, dewan, dan pihak-pihak lain untuk mengelola risiko serta meningkatkan keyakinan bahwa tujuan yang ditetapkan dapat diraih. Dalam penerapannya, *Chief Audit Executive* harus mempertimbangkan pola hubungan struktur organisasi dalam merencanakan penilaian terhadap proses tata kelola.

Penerapan terbagi dalam tiga hal yang masing-masing memiliki contoh studi kasus, antara lain yang pertama suatu penugasan audit harus melihat setiap pengendalian dalam proses tata kelola yang dirancang untuk mencegah atau mendeteksi kejadian yang berdampak negatif terhadap pencapaian strategi organisasi, tujuan, dan sasaran seperti efisiensi dan efektivitas operasional, pelaporan keuangan serta kepatuhan terhadap hukum dan perundang-undangan yang berlaku. Kedua, setiap pengendalian tata kelola terkesan kurang maksimal dalam mengelola beberapa risiko. Sebagai contoh, pengendalian seperti penerapan kode etik dapat dilakukan untuk memitigasi berbagai jenis risiko. Hal ini perlu dipertimbangkan ketika mengembangkan ruang lingkup audit terhadap proses tata kelola. Terakhir, menganjurkan setiap auditor untuk menerapkan hasil dari penilaian tata kelola sebagai pedoman untuk meningkatkan kualitas dari setiap kondisi yang telah dikelola.

2.9 Manajemen Keamanan Informasi

Menurut Sarno & Iffano (2009), keamanan informasi merupakan proteksi terhadap data dan aset teknologi dari ancaman dan penyalahgunaan pihak yang tidak bertanggung jawab sehingga menjamin kontinuitas bisnis, mengurangi jenis risiko yang terjadi, dan mengoptimalkan pengembalian investasi. Semakin banyak informasi perusahaan yang disimpan, dikelola, dan dibagikan, maka semakin besar risiko, kehilangan, kerusakan, hingga tereksposnya data ke pihak luar. Saat ini, banyak perusahaan yang memanfaatkan teknologi informasi (TI) berbasis jaringan, baik lokal maupun global untuk mendukung tujuan perusahaan. Namun, masih banyak yang meremehkan tentang pentingnya keamanan terhadap akses jaringan. Keamanan informasi bertujuan memastikan kerahasiaan, ketersediaan, dan integritas dalam sumber daya informasi perusahaan. Manajemen keamanan informasi terdiri dari dua jenis, antara lain Sistem Manajemen Keamanan Informasi (*Information Security Management System*), yang mengani keamanan sehari-hari dan Manajemen Kesiambungan Bisnis (*Business Continuity Management*) sebagai pedoman dalam menghadapi kondisi pasca bencana.

Selain itu, terdapat tujuan dari keamanan informasi. Setiap tujuan diciptakan untuk meraih tiga sasaran utama, antara lain yang pertama tentang kerahasiaan. Berfungsi melindungi data dan informasi perusahaan dari penyingkapan pengguna yang tidak memiliki akses resmi. Kedua, tentang ketersediaan. Berfungsi meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh pengguna yang memiliki hak akses. Terakhir, tentang integritas. Berfungsi melindungi kelengkapan dan ketelitian informasi. Semua tujuan memberi jaminan bahwa data tidak akan diubah tanpa izin atau perintah dari pihak yang berwenang. Manajemen keamanan informasi sangat penting diterapkan agar segala informasi perusahaan dapat dikelola dengan benar sehingga memberikan kenyamanan dalam menerima dan menggunakan informasi untuk melakukan pelayanan kepada lingkungan internal maupun eksternal perusahaan.

Dalam penerapannya, pengelolaan keamanan informasi terdiri dari empat langkah, antara lain yang pertama mengidentifikasi ancaman (*threats*) yang dapat menyerang sumber daya informasi perusahaan. Kedua, mendefinisikan risiko dari ancaman (*threats*) yang dapat memaksakan. Ketiga, menetapkan kebijakan keamanan informasi. Terakhir, menerapkan kontrol yang tertuju pada suatu risiko. Maksud dari pengontrolan adalah memberikan mekanisme untuk melindungi dan mengurangi berbagai risiko yang dapat mengganggu kenyamanan perusahaan. Bentuk ancaman keamanan bisa bersumber dari mana saja, seperti individu, organisasi, kebijakan, atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan. Jenis ancaman dapat dibuat dengan sengaja maupun tidak dan bersumber dari internal maupun eksternal. Terdapat jenis tindakan yang dapat menimbulkan risiko, antara lain pencurian dan penyingkapan, penggunaan suatu hal secara ilegal, pembinasaaan dan pengingkaran layanan secara ilegal, serta memodifikasi hak akses secara ilegal. Namun, keamanan informasi bisa diimplementasikan menggunakan lima tahap antara lain pengenalan *project*, pengembangan kebijakan, konsultasi dan penyetujuan, kesadaran dan pendidikan, serta penyebaran kebijakan.

2.10 Pengertian COBIT

Kerangka kerja *Control Objective for Information and related Technology* (COBIT) merupakan sekumpulan dokumentasi dalam bentuk *Base Practices* (BP) dan panduan untuk mengimplementasikan *IT Governance*. Menurut ISACA (2012), kerangka kerja ini membantu seorang manajer, operator, auditor, dan pengguna lain dalam menjembatani kesenjangan (*gap*) antara kebutuhan, risiko bisnis, dan permasalahan teknis organisasi. Kerangka kerja ini dikeluarkan dan dikembangkan oleh *IT Governance Institute* (ITGI), dimana telah diakui dan diimplementasikan secara lingkup internasional sebagai sebuah praktik dalam pengendalian atas seluruh hal mengenai teknologi informasi (TI) dan risiko yang terkait. Kerangka kerja COBIT merupakan bagian dari *Information System Audit and Control Association* (ISACA). Dalam situs resmi ITGI, dijelaskan bahwa kerangka kerja COBIT memudahkan *Chief Information Officer* dan membantu pemangku kepentingan (*stakeholder*) dalam memahami proses dan layanan teknologi informasi (TI).

Hal ini menjadi alasan bahwa kerangka kerja COBIT dapat berintegrasi dengan berbagai kerangka kerja lainnya seperti *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), *Information Technology Infrastructure Library* (ITIL), dan ISO/IEC 20000. Menurut Jogiyanto (2011), kerangka kerja COBIT memberikan seorang manajer, operator, auditor, dan para pengguna teknologi informasi (TI) berupa serangkaian kerangka kerja dari langkah umum, proses, indikator, dan *Base Practices* (BP) untuk membantu dalam memaksimalkan seluruh manfaat yang diperoleh perusahaan melalui penggunaan teknologi informasi (TI) dan pengembangan *IT Governance* yang sesuai dalam kebijakan organisasi. Kerangka kerja ini telah mengalami beberapa perubahan versi hingga enam kali. Pihak ISACA merilis kerangka kerja COBIT 1 pada tahun 1996. Versi ini berfokus pada pekerjaan audit.

Selang dua tahun, berkembanglah menjadi kerangka kerja COBIT 2 yang merefleksikan pengelolaan sejumlah sumber dokumen dan langkah implementasi yang dipublikasikan pada tahun 1998. Kerangka kerja COBIT 3 ditandai dengan adanya ITGI yang dibentuk oleh ISACA pada tahun 1998, yang memperluas fokusnya untuk mengelola teknologi informasi (TI). Kemudian, terdapat peningkatan sisi *IT Governance* pada kerangka kerja COBIT 4. Pada tahun 2007, ISACA kembali merilis kerangka kerja COBIT 4.1 dengan menambahkan *IT value 2.0* yang merupakan nilai investasi dari penilaian risiko teknologi informasi (TI). Hingga saat ini, COBIT 5 merupakan versi terakhir dengan melengkapi seluruh cakupan isi dari kerangka kerja COBIT versi sebelumnya. Menurut Jogiyanto (2011), untuk menjadi kerangka kerja yang mampu menerapkan *IT Governance of Enterprise*, kerangka kerja ini telah mengalami berbagai perubahan untuk mengikuti perkembangan zaman dan keilmuan.

2.11 Pengertian COBIT 5

Menurut ISACA (2012), COBIT 5 merupakan kerangka kerja versi terbaru dalam panduan *Information System Audit and Control Assosiation* (ISACA) yang membahas mengenai tata kelola, manajemen, dan semua hal yang berhubungan dengan pengelolaan teknologi informasi (TI). Selain itu, kerangka kerja ini juga menyediakan alat analisis, praktik, prinsip, dan model yang diterima secara luas (*global*) dengan tujuan untuk meningkatkan nilai-nilai implementasi teknologi informasi (TI). Kerangka kerja ini mendefinisikan beberapa proses dari setiap domain yang disediakan. Setiap proses dirancang untuk membantu pengelolaan aktivitas dan tujuan organisasi.

Kerangka kerja ini membantu sebuah organisasi untuk memperoleh nilai maksimal dari pemanfaatan teknologi informasi (TI) melalui pemastian optimasi risiko, penggunaan sumber daya, dan kesadaran akan setiap manfaat. Kerangka kerja ini membahas area fungsional dan bisnis pada teknologi informasi (TI), baik secara internal maupun eksternal untuk para pemangku kepentingan (*stakeholder*). Menurut ISACA (2012), kerangka kerja COBIT 5 terbagi menjadi dua area fungsional, antara lain tata kelola (*governance*) dan manajemen (*management*). Penerapan tata kelola (*governance*) digunakan untuk memastikan segala aktivitas organisasi yang dilakukan tetap berada dalam cakupan kerangka kerja COBIT 5, sedangkan penerapan manajemen (*management*) mendeskripsikan pengelolaan dasar untuk mendefinisikan tujuan dan strategi organisasi.

2.12 Komponen COBIT 5

Kerangka kerja COBIT 5 memiliki lima prinsip (*principles*) dan tujuh pemicu (*enablers*) yang bersifat umum untuk digunakan berbagai organisasi berbasis teknologi informasi (TI). Menurut ISACA (2012), terdapat lima prinsip pada kerangka kerja COBIT 5, antara lain *meeting stakeholder needs, covering enterprise end-to-end, applying a single integrated framework, enabling a holistic approach*, dan *separating governance from management*. Berikut definisi dari kelima prinsip yang ada. Prinsip *meeting stakeholder needs* (pemenuhan kebutuhan dari pemangku kepentingan), mendefinisikan bahwa setiap organisasi berusaha dalam menciptakan nilai-nilai positif bagi para pemangku kepentingan. Selain itu, prinsip ini juga berguna dalam pengelolaan prioritas untuk implementasi dan perbaikan. Segala kebutuhan dari pemangku kepentingan (*stakeholder*) dirancang sebagai strategi organisasi. Sistem tata kelola akan melibatkan seluruh pemangku kepentingan (*stakeholder*) dalam membuat keputusan mengenai penilaian sumber daya, manfaat, dan pengelolaan risiko.

Kedua, prinsip *covering enterprise end-to-end* (mencakup seluruh area perusahaan), mendeskripsikan bahwa kerangka kerja COBIT 5 mencakup semua proses dari organisasi. Selain itu, juga mengatur proses integrasi antara aktivitas perusahaan dengan aktivitas yang terdapat pada kerangka kerja melalui setiap domain dan proses yang disediakan. Ketiga, prinsip *applying a single integrated framework* (penerapan kerangka kerja tunggal yang terintegrasi), mendeskripsikan bahwa kerangka kerja COBIT 5 menyelaraskan standar dengan kerangka kerja lain dari *Information System Audit and Control Association (ISACA)* seperti manajemen risiko teknologi informasi (*Risk IT*), *Business Model for Information Security (BMIS)*, penilaian manfaat investasi teknologi informasi (*VAL IT*), dan lain-lain. Sehingga memudahkan organisasi dalam mengintegrasikan antar kerangka kerja. Keempat, prinsip *enabling a holistic approach* (pendekatan yang menyeluruh), mendeskripsikan bahwa kerangka kerja COBIT 5 memiliki beberapa pemicu (*enablers*) yang saling terkait satu sama lain untuk mendukung aktivitas tata kelola (*governance*) dan manajemen (*management*) organisasi.

Menurut ISACA (2012), pemicu (*enabler*) merupakan sekumpulan faktor yang mempengaruhi segala aktivitas yang sedang dikerjakan. Kerangka kerja COBIT 5 memiliki tujuh pemicu (*enablers*). Ketujuh pemicu (*enablers*) antara lain yang pertama adalah *principles, policies, and framework*. Merupakan pendorong untuk menerjemahkan perilaku menjadi panduan praktis untuk pengelolaan sehari-hari. Kedua adalah *processes*. Merupakan definisi tentang pengelolaan berbagai kegiatan untuk meraih tujuan tertentu sehingga menghasilkan keluaran (*output*) dalam mendukung strategi organisasi. Ketiga adalah *organizational structures*. Merupakan entitas dalam organisasi sebagai kunci dalam pembuatan keputusan. Keempat adalah *culture, ethics, and behavior*. Merupakan faktor dalam tata kelola dan manajemen sebagai pemicu keberhasilan. Kelima adalah *information*. Menjadi kebutuhan penting bagi seluruh aspek organisasi dimanapun dan kapanpun.

Jenis informasi dibedakan menjadi informasi yang dibutuhkan atau dihasilkan. Keenam adalah *service, infrastructure, and applications*. Menyediakan berbagai aset teknologi informasi (TI) untuk mendukung proses dan layanan organisasi. Terakhir adalah *people, skills, and competencies*. Memiliki definisi bahwa pencapaian kesuksesan harus disertai dengan penentuan langkah-langkah yang tepat. Selain itu, dibutuhkan setiap individu yang berkompoten untuk menjalankan aktivitas organisasi. Kelima, prinsip *separating governance from management* (pemisahan tata kelola dari manajemen), mendeskripsikan bahwa kerangka kerja COBIT 5 sangat membedakan antara tata kelola (*governance*) dengan manajemen (*management*). Kedua hal memiliki cakupan dari struktur organisasi, kegiatan, dan pelayanan yang berbeda. Tata kelola dipertanggung jawabi oleh direksi di bawah kepemimpinan ketua. Kegiatan ini melibatkan pengambilan keputusan tingkat tinggi (*high level*). Sedangkan manajemen dipertanggung jawabi oleh manajemen eksekutif di bawah kepemimpinan *Chief Executive Officer*.

2.13 Area dan Domain COBIT 5

Menurut ISACA (2012), kerangka kerja COBIT 5 terbagi menjadi dua area fungsional, seperti tata kelola (*governance*) dan manajemen (*management*). Setiap area memiliki proses yang terbagi menjadi lima domain. Kelima domain lantas terdiri dari tiga puluh tujuh proses. Berikut definisi berdasarkan area tata kelola (*governance*). Terdapat lima proses tata kelola pada domain EDM (*Evaluate, Direct and Monitor*) seperti Tabel 2.1. Domain ini mendefinisikan proses tata kelola dengan para pemangku kepentingan (*stakeholder*) dalam melakukan penilaian, optimasi risiko, dan sumber daya. Selain itu, terdapat aktivitas yang bertujuan mengevaluasi pilihan strategis, memberikan arahan teknologi informasi (TI), dan pemantauan hasil.

Tabel 2.1 Proses dari EDM

KODE	PROSES
EDM01	<i>Ensure governance framework setting and maintenance</i> (memastikan pengaturan dan pemeliharaan tata kelola dari kerangka kerja).
EDM02	<i>Ensure benefits delivery</i> (memastikan penyampaian hal yang bermanfaat).
EDM03	<i>Ensure risk Optimization</i> (memastikan optimasi risiko).
EDM04	<i>Ensure resource Optimization</i> (memastikan optimasi sumber daya).
EDM05	<i>Ensure stakeholder transparency</i> (memastikan bentuk transparansi dari pemangku kepentingan).

Sumber: diadaptasi dari *Information System Audit and Control Association*) ISACA, 2012.



Selanjutnya, definisi berdasarkan area manajemen (*management*). Kerangka kerja COBIT 5 mensejajarkan empat domain berdasarkan setiap fungsionalitas pada area manajemen (*management*). Jenis fungsionalitas yang dimaksud seperti tanggung jawab perencanaan, pembangunan, dan pengawasan. Sedangkan keempat domain, antara lain yang pertama *Align, Plan, and Organise* (APO). Kedua, *Build, Acquire, and Implement* (BAI). Ketiga, *Deliver, Service, and Support* (DSS). Terakhir, *Monitor, Evaluate, and Assess* (MEA).

Secara keseluruhan, keempat domain yang dimaksud memiliki tiga puluh dua proses. Domain APO mencakup strategi yang berfokus pada identifikasi praktik teknologi informasi (TI) terhadap pencapaian tujuan organisasi. Penerapan tujuan strategis tentu harus direncanakan sebaik mungkin oleh para pemangku kepentingan (*stakeholder*) melalui proses yang terstruktur. Berikut tiga belas jenis proses berdasarkan domain APO pada Tabel 2.2.

Tabel 2.2 Proses dari APO

KODE	PROSES
APO01	<i>Manage the IT management framework</i> (mengelola kerangka kerja dari manajemen teknologi informasi).
APO02	<i>Manage strategy</i> (mengelola bentuk strategi).
APO03	<i>Manage enterprise architecture</i> (mengelola bentuk arsitektur perusahaan).
APO04	<i>Manage innovation</i> (mengelola bentuk inovasi).
APO05	<i>Manage portfolio</i> (mengelola bentuk portofolio).
APO06	<i>Manage budget and costs</i> (mengelola bentuk anggaran dan biaya).
APO07	<i>Manage human resources</i> (mengelola sumber daya manusia).
APO08	<i>Manage relationships</i> (mengelola pola hubungan).
APO09	<i>Manage service agreements</i> (mengelola persetujuan layanan).
APO10	<i>Manage suppliers</i> (mengelola jenis <i>suppliers</i>).
APO11	<i>Manage quality</i> (mengelola jenis kualitas).
APO12	<i>Manage risk</i> (mengelola risiko).
APO13	<i>Manage security</i> (mengelola keamanan).

Sumber: diadaptasi dari (*Information System Audit and Control Association* (ISACA), 2012).

Definisi kedua adalah mendeskripsikan domain BAI. Domain ini memberikan solusi untuk menjadikannya bentuk layanan. Dalam penerapan strategi organisasi, tentu mempertimbangkan beberapa langkah strategis seperti penerapan dan pengembangan yang semua didasarkan pada tujuan organisasi. Selain itu, domain ini juga mencakup pemeliharaan dan perubahan sistem untuk memastikan solusi yang diciptakan sesuai dengan tujuan bisnis. Berikut sepuluh jenis proses berdasarkan domain BAI pada Tabel 2.3.

Tabel 2.3 Proses dari BAI

KODE	PROSES
BAI01	<i>Manage programmes and projects</i> (mengelola jenis proyek dan program).
BAI02	<i>Manage requirements definition</i> (mengelola definisi suatu persyaratan).
BAI03	<i>Manage solutions identification and build</i> (mengidentifikasi solusi dan bentuk pembangunan).
BAI04	<i>Manage availability and capacity</i> (mengelola kapasitas dan ketersediaan).
BAI05	<i>Manage organisational change enablement</i> (mengelola perubahan organisasi).
BAI06	<i>Manage changes</i> (mengelola bentuk perubahan).
BAI07	<i>Manage change acceptance and transitioning</i> (menerima segala bentuk transisi dan perubahan).
BAI08	<i>Manage knowledge</i> (mengelola berbagai pengetahuan).
BAI09	<i>Manage assets</i> (mengelola jenis aset/benda).
BAI10	<i>Manage configuration</i> (mengelola bentuk konfigurasi).

Sumber: diadaptasi dari *Information System Audit and Control Association* (ISACA), 2012.

Definisi ketiga adalah mendeskripsikan domain DSS. Domain ini berfokus pada proses *actual delivery* dan *support of required services*. Contoh penerapan *service delivery* seperti pelayanan bagi pengguna, pengelolaan keamanan secara kontinuitas, pengelolaan data, dan fasilitas operasional. Berikut enam jenis proses berdasarkan domain DSS pada Tabel 2.4.

Tabel 2.4 Proses dari DSS

KODE	PROSES
DSS01	<i>Manage operations</i> (mengelola operasional).
DSS02	<i>Manage service requests and incidents</i> (mengelola permintaan layanan).

Tabel 2.4 Proses dari DSS (lanjutan)

KODE	PROSES
DSS03	<i>Manage problems</i> (mengelola berbagai jenis masalah).
DSS04	<i>Manage continuity</i> (mengelola suatu kontinuitas).
DSS05	<i>Manage security services</i> (mengelola pelayanan keamanan).
DSS06	<i>Manage business process controls</i> (mengelola pengendalian proses bisnis).

Sumber: diadaptasi dari *Information System Audit and Control Association* (ISACA), 2012.

Definisi terakhir adalah mendeskripsikan domain MEA. Domain ini berfokus pada hal pengawasan dari seluruh proses. Selain itu, memastikan seluruh bentuk arahan berjalan dengan tepat. Untuk memastikan kualitas tetap stabil, maka dilakukan pengawasan melalui jadwal yang telah ditetapkan. Berikut tiga jenis proses berdasarkan domain MEA pada Tabel 2.5.

Tabel 2.5 Proses dari MEA

KODE	PROSES
MEA01	<i>Monitor, evaluate, and assess performance and conformance</i> (mengawasi, mengevaluasi, dan mengukur kesesuaian kinerja).
MEA02	<i>Monitor, evaluate, and assess the system of internal control</i> (mengawasi, mengevaluasi, dan mengukur sistem pengendalian internal).
MEA03	<i>Monitor, evaluate, and assess compliance with external requirements</i> (mengawasi, mengevaluasi, dan mengukur kesesuaian dari kebutuhan luar).

Sumber: diadaptasi dari *Information System Audit and Control Association* (ISACA), 2012.

2.14 Dasar Proses Keamanan Informasi pada COBIT 5

Terdapat dua proses utama dan satu proses pendukung yang digunakan dalam penelitian ini. Dua proses utama terdiri dari APO13 (*Manage Security*) dan DSS05 (*Manage Security Services*). Sedangkan satu proses pendukung berasal dari EDM03 (*Ensure Risk Optimization*). Menurut ISACA (2012), APO13 (*Manage Security*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang mendefinisikan, mengoperasikan, dan mengawasi keamanan informasi. Selain itu, bertujuan agar risiko keamanan informasi dapat diterima oleh perusahaan sesuai batas yang telah ditentukan. Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada APO13 (*Manage Security*).

Proses ini memiliki tiga macam *Base Practices* (BP), antara lain yang pertama APO13.01 atau menetapkan dan memelihara sistem manajemen keamanan informasi. Sesuai dengan artinya, proses ini bertujuan membangun dan memelihara *Information Security Management System* (ISMS) yang menyediakan pendekatan standar maupun formal secara terus menerus untuk manajemen keamanan informasi. Selain itu, memastikan keamanan teknologi dan proses bisnis selaras dengan kebutuhan bisnis dan manajemen keamanan. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat tujuh *Base Practices* (BP) dari proses ini, antara lain yang pertama menentukan ruang lingkup dan batas-batas sistem manajemen keamanan informasi berdasarkan karakteristik dari perusahaan. Kedua, mengidentifikasi sistem manajemen keamanan informasi agar selaras dengan kebijakan perusahaan. Ketiga, menyelaraskan sistem manajemen keamanan informasi melalui pendekatan perusahaan secara keseluruhan untuk manajemen keamanan.

Keempat, mendapatkan otorisasi manajemen untuk menerapkan atau mengubah sistem manajemen keamanan informasi. Kelima, mempersiapkan dan mempertahankan keadaan dari lingkup sistem manajemen keamanan informasi. Keenam, menentukan dan mengkomunikasikan peran serta tanggung jawab dari manajemen keamanan informasi. Terakhir, terus melakukan pendekatan komunikasi pada sistem manajemen keamanan informasi. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain kebijakan dan lingkup pernyataan tentang sistem manajemen keamanan informasi. Kedua adalah APO13.02 atau menentukan dan merencanakan penanganan risiko keamanan informasi. Sesuai dengan artinya, proses ini bertujuan mempertahankan rencana keamanan informasi dan menjelaskan bagaimana menyelaraskan antara strategi dan arsitektur perusahaan dengan pengelolaan risiko keamanan informasi. Selain itu, memastikan rekomendasi perbaikan keamanan didasarkan atas kasus bisnis yang telah disetujui dan dilaksanakan sebagai cara untuk mengembangkan solusi dan layanan bisnis.

Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat tujuh *Base Practices* (BP) dari proses ini, antara lain yang pertama merumuskan dan mempertahankan rencana perawatan risiko keamanan informasi agar selaras dengan tujuan strategis dan arsitektur perusahaan. Kedua, mempertahankan solusi terbaik agar konsisten dalam mengelola risiko keamanan. Ketiga, mengembangkan metode untuk menerapkan rencana perawatan risiko keamanan informasi berdasarkan studi kasus yang ada melalui alokasi peran dan tanggung jawab terlebih dahulu. Keempat, memberikan masukan sebagai pengembangan solusi untuk rencana perawatan keamanan informasi. Kelima, mendefinisikan bagaimana cara yang efektif untuk pengelolaan risiko keamanan agar hasil yang diperoleh sesuai harapan. Keenam, menyarankan program-program pelatihan dan kesadaran dari keamanan informasi.

Terakhir, mengintegrasikan perencanaan, desain, implementasi, dan pengawasan terhadap prosedur serta pengelolaan keamanan sebagai pencegahan risiko keamanan. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain rencana perawatan risiko keamanan informasi dan rangkuman studi kasus dari keamanan informasi. Terakhir adalah APO13.03 atau mengawasi dan meninjau ulang (*review*) sistem manajemen keamanan informasi. Sesuai dengan artinya, proses ini bertujuan mempertahankan manfaat dari hasil perbaikan keamanan informasi secara terus menerus. Selain itu, mengumpulkan dan menganalisis data tentang sistem manajemen keamanan informasi serta meningkatkan efektivitas dari sistem yang ada. Kemudian, aktif dalam menjaga budaya keamanan dengan cara rutin melakukan perbaikan sehingga mencegah risiko keamanan yang datang. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan.

Terdapat lima *Base Practices* (BP) dari proses ini, antara lain yang pertama menerapkan kebijakan dan tujuan sistem manajemen keamanan informasi secara berkala. Kedua, melakukan audit sistem manajemen keamanan informasi secara internal pada jangka waktu yang telah direncanakan sebelumnya. Ketiga, meninjau ulang sistem (*review*) manajemen keamanan informasi secara teratur untuk memastikan lingkungan sekitar tetap memadai. Selain itu, melakukan perbaikan terhadap sistem manajemen keamanan informasi yang telah diidentifikasi. Keempat, memberikan masukan kepada pemelihara rencana keamanan untuk memperhitungkan hasil pengawasan dan meninjau setiap aktivitasnya. Terakhir, mendokumentasikan setiap tindakan dan peristiwa yang dapat berdampak pada efektivitas kinerja sistem manajemen keamanan informasi. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain laporan audit dari sistem manajemen keamanan informasi dan rekomendasi untuk meningkatkan sistem manajemen keamanan informasi.

Selanjutnya, definisi dari proses utama yang kedua, yaitu DSS05 (*Manage Security Services*). Menurut ISACA (2012), DSS05 (*Manage Security Services*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang melindungi informasi perusahaan untuk mempertahankan tingkat keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijaksanaan keamanan. Selain itu, menetapkan dan mempertahankan peran keamanan informasi dan hak akses serta melakukan pengawasan keamanan. Proses ini bertujuan mengurangi dampak risiko dari manajemen keamanan informasi. Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada DSS05 (*Manage Security Services*). Terdapat tujuh *Base Practices* (BP) dari proses ini, antara lain yang pertama DSS05.01 atau melindungi terhadap risiko dari virus komputer. Sesuai dengan artinya, proses ini bertujuan memberikan perlindungan dari virus komputer (*malware*). Praktik tata kelola yang dilakukan adalah menerapkan dan memelihara pencegahan serta langkah-langkah perbaikan pada unit organisasi untuk melindungi aset teknologi informasi (TI) dari serangan *malware* seperti virus, *worm spyware*, dan *spam*.

Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat enam *Base Practices* (BP) dari proses ini, antara lain yang pertama menciptakan kesadaran dari bahaya perangkat lunak yang tidak dikenali dan menegakkan prosedur pencegahan dan tanggung jawab. Kedua, menginstal dan mengaktifkan aplikasi perlindungan dari perangkat lunak yang berbahaya, kemudian melakukan pembaharuan perangkat lunak untuk versi terbaru. Ketiga, mendistribusikan semua perlindungan dari perangkat lunak secara terpusat. Keempat, secara teratur meninjau dan mengevaluasi informasi terhadap ancaman baru. Kelima, selektif dalam mengirim atau menerima pesan *online* seperti *email* dan berhati-hati dalam mengunduh sesuatu agar segala informasi pribadi tetap terlindungi. Terakhir, melakukan pemahaman tentang perangkat lunak negatif secara periodik melalui sumber terpercaya. Memahami agar tidak menginstal perangkat lunak sembarangan.

Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain kebijakan pencegahan terhadap perangkat lunak negatif dan mengevaluasi potensi ancaman. Kedua adalah DSS05.02 atau mengelola keamanan jaringan dan konektivitas. Sesuai dengan artinya, proses ini bertujuan mengelola jaringan dan keamanan konektivitas. Praktik tata kelola yang dilakukan adalah menggunakan keamanan dan prosedur yang terkait untuk melindungi keamanan informasi dari segi konektivitas. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat sembilan *Base Practices* (BP) dari proses ini, antara lain yang pertama membangun dan mempertahankan kebijakan untuk keamanan konektivitas berdasarkan penilaian risiko dan kebutuhan bisnis. Kedua, membatasi akses terhadap informasi dan jaringan perusahaan untuk beberapa perangkat lunak. Ketiga, menerapkan mekanisme pemilihan jaringan seperti *firewall* dan beberapa perangkat lunak tambahan.

Keempat, mengenkripsi transit informasi menurut klasifikasinya. Kelima, menerapkan persetujuan terhadap protokol keamanan untuk konektivitas jaringan. Keenam, mengkonfigurasi peralatan jaringan sesuai aturan yang tepat. Ketujuh, membentuk mekanisme yang dipercaya untuk mendukung dan menerima informasi yang aman. Kedelapan, melaksanakan pengujian secara periodik untuk menentukan kecukupan dari perlindungan jaringan. Terakhir, melaksanakan pengujian sistem keamanan secara berkala untuk menentukan kecukupan dari sistem perlindungan. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain kebijakan konektivitas keamanan dan hasil dari pengujian tingkat keamanan. Ketiga adalah DSS05.03 atau mengelola titik akhir dari suatu keamanan. Sesuai dengan artinya, proses ini bertujuan mengelola keamanan pada titik akhir. Praktik tata kelola yang dilakukan adalah memastikan perangkat titik akhir (*endpoint*) seperti *laptop*, *dekstop*, dan *server* agar tetap aman sesuai kebijakan yang ditetapkan.

Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat sembilan *Base Practices* (BP) dari proses ini, antara lain yang pertama mengkonfigurasi sistem operasi menggunakan cara yang tepat. Kedua, menerapkan mekanisme dari penguncian perangkat. Ketiga, mengenkripsi penyimpanan informasi sesuai klasifikasinya. Keempat, mengelola akses. Kelima, mengelola konfigurasi jaringan menggunakan cara yang tepat. Keenam, menerapkan penyaringan pada perangkat *endpoint* seperti *laptop, desktop, server, handphone*, dan perangkat jaringan lainnya. Ketujuh, melindungi integritas sistem. Kedelapan, memberikan perlindungan fisik pada perangkat *endpoint* seperti *laptop, desktop, server, handphone*, dan perangkat jaringan lainnya. Terakhir, menentukan perangkat *endpoint* (*laptop, desktop, server, handphone*, dan perangkat jaringan lainnya) yang aman. Selanjutnya, terdapat sebuah *Work Product* (WP) yang dihasilkan dari proses ini, yaitu kebijakan menjaga keamanan pada perangkat *endpoint* seperti *laptop, desktop, server, handphone*, dan perangkat jaringan lainnya.

Keempat adalah DSS05.04 atau mengelola identitas pengguna dan hak akses. Sesuai dengan artinya, proses ini bertujuan mengelola identitas pengguna dan hak akses. Praktik tata kelola yang dilakukan adalah memastikan semua pengguna memiliki hak akses informasi yang sesuai dengan kebutuhan mereka. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat delapan *Base Practices* (BP) dari proses ini, antara lain yang pertama mempertahankan hak akses pengguna berdasarkan kebutuhan fungsi dan proses bisnis. Kedua, mengidentifikasi semua pengolahan informasi berdasarkan peran dan fungsional. Kemudian, mengkoordinasikan dengan unit usaha untuk memastikan semua peran telah didefinisikan secara konsisten. Ketiga, Mengautentikasi semua akses terhadap aset informasi berdasarkan klasifikasi keamanan mereka. Keempat, mengelola semua perubahan hak akses yang meliputi penciptaan, modifikasi, dan penghapusan yang diterapkan pada waktu yang tepat.

Kelima, memisahkan dan mengelola pengguna akun yang memiliki hak akses lebih. Keenam, melakukan peninjauan ulang dari semua akun yang memiliki hak akses lebih. Ketujuh, memastikan semua pengguna (internal, eksternal, dan sementara) dan aktivitas pada sistem teknologi informasi (TI) telah teridentifikasi. Terakhir, mengaudit akses terhadap informasi yang tergolong sensitif. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain persetujuan dari hak akses pengguna dan laporan hasil dari ulasan pengguna akun biasa dan istimewa. Kelima adalah DSS05.05 atau mengelola akses fisik terhadap aset teknologi informasi (TI). Sesuai dengan artinya, proses ini bertujuan mendefinisikan dan menerapkan prosedur, membatasi, dan mencabut akses sesuai dengan kebutuhan bisnis dalam keadaan darurat.

Selain itu, mengelola keamanan akses pada tempat yang berwenang atas akses yang dimaksud. Kemudian, memantau orang-orang yang memasuki tempat akses termasuk staf, klien, vendor, dan pengunjung atau pihak ketiga. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat tujuh *Base Practices* (BP) dari proses ini, antara lain yang pertama mengelola permintaan dan pemberian hak akses terhadap fasilitas komputasi. Kedua, memastikan akses terhadap profil masih tepat. Ketiga, memantau semua kegiatan yang merujuk terhadap akses informasi. Keempat, memerintahkan agar semua personil menampilkan identifikasi setiap saat. Kelima, dianjurkan untuk mengarahkan setiap aktivitas pengunjung lain pada sistem. Keenam, membatasi akses terhadap situs-situs yang tergolong sensitif dengan mendirikan perangkat keamanan yang dianggap tepat. Terakhir, melakukan pelatihan untuk kesadaran keamanan. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain menyetujui terhadap permintaan akses dan memasuki sistem yang telah diakses.

Keenam adalah DSS05.06 atau mengelola dokumen-dokumen penting dan perangkat keluaran lainnya. Sesuai dengan artinya, proses ini bertujuan mengelola keamanan dokumen. Praktik tata kelola yang dilakukan adalah membangun pengamanan fisik yang sesuai, kemudian menginventarisasi dokumen penting atas aset teknologi informasi (TI) seperti surat berharga dan token keamanan. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat lima *Base Practices* (BP) dari proses ini, antara lain yang pertama menetapkan prosedur untuk mengatur penerimaan, penggunaan, dan penghapusan terhadap keluaran dari sebuah perangkat dalam maupun luar perusahaan. Kedua, menetapkan hak akses terhadap dokumen yang sensitif berdasarkan prinsip hak istimewa. Selain itu, menyeimbangkan risiko dan persyaratan dari bisnis. Ketiga, membangun inventaris dokumen yang sensitif dan melakukan rekonsiliasi.

Keempat, membangun pengamanan fisik yang memadai atas bentuk khusus dan perangkat yang sensitif. Terakhir, memindahkan informasi rahasia dan melindungi keluaran dari sebuah perangkat. Selanjutnya, terdapat dua *Work Product* (WP) yang dihasilkan dari proses ini, antara lain menyediakan dokumen dan hak akses terhadap perangkat yang tergolong sensitif. Terakhir adalah DSS05.07 atau memantau infrastruktur untuk segala kegiatan yang berhubungan dengan keamanan. Sesuai dengan artinya, proses ini bertujuan menggunakan alat deteksi instruksi dan mengawasi infrastruktur untuk akses yang tidak sah serta memastikan setiap peristiwa yang terintegrasi dengan cara mengelola dan mengawasi risiko. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat lima *Base Practices* (BP) dari proses ini, antara lain yang pertama menentukan peristiwa terkait keamanan dan mengidentifikasi tingkat informasi sebagai bahan dokumentasi berdasarkan pertimbangan risiko.

Kemudian, menyimpan hasil dokumentasi dalam jangka panjang sehingga membantu dalam penyelidikan suatu saat. Kedua, menentukan sifat dan karakteristik dari potensi insiden terkait keamanan sehingga memudahkan untuk mengenali dan melakukan respon yang tepat. Ketiga, secara rutin meninjau daftar peristiwa untuk mempersiapkan potensi insiden. Keempat, mempertahankan prosedur pengumpulan bukti sesuai dengan peraturan bukti forensik dan memastikan semua staf sadar akan persyaratan. Terakhir, memastikan insiden keamanan diciptakan pada waktu yang tepat ketika melakukan identifikasi terhadap potensi insiden keamanan. Selanjutnya, terdapat tiga *Work Product* (WP) yang dihasilkan dari proses ini, antara lain yang pertama daftar dari peristiwa keamanan. Kedua, karakteristik insiden keamanan. Terakhir, alur penyelesaian dari insiden keamanan. Terakhir, definisi dari proses pendukung, yaitu EDM03 (*Ensure Risk Optimization*).

Menurut ISACA (2012), EDM03 (*Ensure Risk Optimization*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang bertujuan memastikan risiko perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI) tidak melampaui *risk appetite* yang telah ditetapkan. *Risk appetite* merupakan suatu keadaan dimana perusahaan memilih untuk menerima, memantau, mempertahankan diri, atau memaksimalkan diri melalui peluang-peluang yang ada. Selain itu, tujuan lain dari proses EDM03 (*Ensure Risk Optimization*) adalah memastikan dampak risiko penggunaan teknologi informasi (TI) dapat diidentifikasi dan potensi kegagalan dapat diminimalisasi. Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada EDM03 (*Ensure Risk Optimization*). Terdapat tiga *Base Practices* (BP) dari proses ini, antara lain yang pertama EDM03.01 atau evaluasi manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengevaluasi dan membuat penilaian tentang dampak langsung maupun jangka panjang dari risiko penggunaan teknologi informasi (TI) pada perusahaan.

Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat enam *Base Practices* (BP) dari proses ini, antara lain yang pertama menentukan tingkat risiko dari penggunaan teknologi informasi (TI) pada perusahaan untuk membantu pencapaian strategi perusahaan. Kedua, mengevaluasi dan menyetujui batasan risiko teknologi informasi (TI) yang dapat diterima oleh perusahaan. Ketiga, menentukan keselarasan antara strategi risiko teknologi informasi (TI) dengan strategi risiko perusahaan. Keempat, mengevaluasi faktor risiko teknologi informasi (TI) yang dapat mengganggu pengambilan keputusan perusahaan dan memastikan keputusan pencegahan risiko telah diambil. Kelima, menentukan risiko teknologi informasi (TI) untuk dinilai dan dievaluasi sesuai dengan standar nasional maupun internasional yang relevan. Terakhir, mengevaluasi aktivitas manajemen risiko untuk memastikan kesesuaian dengan kerugian yang terkait dengan teknologi informasi (TI) dan kemampuan perusahaan dalam mengatasinya.

Selanjutnya, terdapat tiga *Work Products* (WP) yang dihasilkan dari proses ini, antara lain yang pertama panduan terhadap pertumbuhan risiko teknologi informasi (TI). Kedua, mendefinisikan batasan risiko teknologi informasi (TI) yang disetujui. Terakhir, laporan evaluasi dari aktivitas manajemen risiko. Kedua adalah EDM03.02 atau pengarahan manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengarahkan pengelolaan risiko untuk memastikan pengelolaannya tidak melebihi batas pertumbuhan risiko perusahaan. Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat enam *Base Practices* (BP) dari proses ini, antara lain yang pertama mempromosikan budaya sadar risiko teknologi informasi (TI) dan meningkatkan kemampuan perusahaan dalam mengidentifikasi risiko, keuntungan, dan dampak teknologi informasi (TI) untuk perusahaan. Kedua, mengarahkan integrasi strategi dan pelaksanaan risiko teknologi informasi (TI) pada perusahaan.

Ketiga, mengarahkan pengembangan komunikasi risiko yang meliputi seluruh area perusahaan berdasarkan rencana pengelolaan risiko. Keempat, mengarahkan mekanisme yang layak untuk merespon risiko dan melaporkannya pada manajemen perusahaan. Kelima, mengarahkan risiko, kesempatan, dan masalah risiko teknologi informasi (TI) untuk diidentifikasi dan dilaporkan kepada pengambil keputusan di perusahaan. Terakhir, mengidentifikasi dan mengawasi tujuan serta manajemen risiko. Selain itu, menyetujui pendekatan, metode teknik, dan prosesnya. Selanjutnya, terdapat tiga *Work Products* (WP) yang dihasilkan dari proses ini, antara lain yang pertama kebijakan manajemen risiko. Kedua, daftar aktivitas yang dipantau dalam manajemen risiko. Terakhir, proses pengukuran manajemen risiko. Terakhir adalah EDM03.03 atau mengawasi manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengawasi tujuan dan matriks proses manajemen risiko serta menyusun bagaimana masalah risiko teknologi informasi (TI) diidentifikasi, dilacak, dan dilaporkan.

Penilaian tingkat kapabilitas (*capability level*) dilakukan terhadap kegiatan yang telah dilakukan (*base practices*) beserta bukti (*evidence*) yang telah dihasilkan (*work product*) oleh perusahaan. Terdapat empat *Base Practices* (BP) pada proses ini, antara lain yang pertama mengawasi profil risiko yang dikelola sesuai dengan batas pertumbuhan risiko. Kedua, mengawasi tujuan dan matriks proses tata kelola serta manajemen risiko sesuai target. Selain itu, menganalisis penyebab dari ketidaksesuaian dan menetapkan langkah-langkah perubahan. Ketiga, memastikan pihak yang bertanggung jawab meninjau ulang (*review*) pelaksanaan manajemen risiko dalam mencapai tujuan yang telah ditetapkan. Terakhir, melaporkan setiap masalah manajemen risiko kepada pimpinan perusahaan. Selanjutnya, terdapat dua *Work Products* (WP) yang dihasilkan dari proses ini, antara lain laporan perbaikan untuk mengatasi ketidaksesuaian manajemen risiko dan laporan setiap permasalahan manajemen risiko kepada pimpinan perusahaan.

2.15 Pengertian RACI Chart

Memahami seluruh aturan dan pertanggung jawaban pada setiap kinerja merupakan sebuah kunci efektifitas dalam pengendalian. Kerangka kerja COBIT 5 menyediakan sebuah wadah analisis peran dan fungsi pada RACI Chart. RACI Chart merupakan singkatan dari *Responsible, Accountable, Consulted, dan Informed*, yang merupakan sebuah matriks dari seluruh wewenang atau aktivitas dalam mengambil keputusan dari sebuah organisasi pada setiap individu dan proses. Berikut definisi dari empat komponen RACI Chart, antara lain yang pertama *Responsible* (pelaksana). Komponen ini bertanggung jawab secara langsung dalam pelaksanaan aktivitas organisasi. Kedua, definisi *Accountable* (penanggung jawab). Komponen ini memiliki tanggung jawab dan otoritas penuh dalam menentukan kebijakan atau keputusan pada organisasi. Ketiga, definisi *Consulted* (penasihat). Komponen ini berkontribusi untuk memberikan umpan balik (*feedback*) berupa saran atas aktivitas yang telah dilaksanakan. Terakhir, definisi *Informed* (terinformasi). Komponen ini bertugas menerima informasi keseluruhan aktivitas organisasi yang telah dilakukan.

EDM03 RACI CHART																											
GOVERNANCE PRACTICE	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer	
EDM 03.01 Evaluate risk management	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C								C
EDM 03.02 Direct risk management	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I	I
EDM 03.03 Monitor risk management	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	I	C

Gambar 2.3 RACI Chart dari proses EDM03

Sumber: diadaptasi dari COBIT 5 *Enabling Processes*, 2012.

Diketahui sekumpulan aktivitas berdasarkan proses EDM03 (*Ensure Risk Optimization*) yang terdiri dari tiga *Base Practices* (BP) pada Gambar 2.3. Setiap *Base Practices* (BP) memiliki tujuan berbeda-beda, antara lain yang pertama *evaluate risk management*. *Base Practices* (BP) ini bertujuan mengevaluasi dan membuat penilaian tentang dampak langsung maupun jangka panjang dari risiko penggunaan teknologi informasi (TI) organisasi. Kedua, definisi *direct risk management*. *Base Practices* (BP) ini bertujuan mengarahkan pengelolaan risiko agar tidak melebihi batas pertumbuhan risiko organisasi.

Terakhir, definisi *monitor risk management. Base Practices* (BP) ini bertujuan mengawasi tujuan dan matriks proses manajemen risiko serta menyusun bagaimana masalah risiko teknologi informasi (TI) diidentifikasi, dilacak, dan dilaporkan. Berdasarkan Gambar 2.3, diketahui peran yang terlibat dalam penerapan ketiga *Base Practices* (BP) dari proses EDM03 (*Ensure Risk Optimization*). Setiap peran memiliki golongan komponen yang berbeda-beda. Berikut pembagian komponen beserta peran yang terlibat pada Tabel 2.6.

Tabel 2.6 Peran dari proses EDM03

KOMPONEN	PERAN YANG TERLIBAT
Responsible (Penasihat)	<ul style="list-style-type: none"> ○ Chief Executive Officer ○ Business Executive ○ Strategy Executive Committee ○ Chief Risk Officer ○ Chief Information Officer
Accountable (Penanggung Jawab)	Board
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ Chief Financial Officer ○ Chief Operating Officer ○ Business Process Owner ○ Head Human Resources ○ Compliance ○ Auditor ○ Head Architecture
Informed (Terinformasi)	<ul style="list-style-type: none"> ○ Value Management Officer ○ Enterprise Risk Committee

Selanjutnya, diketahui sekumpulan aktivitas berdasarkan proses APO13 (*Manage Security*) yang terdiri dari tiga *Base Practices* (BP) pada Gambar 2.4. Setiap *Base Practices* (BP) memiliki tujuan berbeda-beda, antara lain yang pertama *establish and maintain an Information Security Management System (ISMS)*. *Base Practices* (BP) ini bertujuan membangun dan memelihara *Information Security Management System (ISMS)* yang menyediakan pendekatan standar maupun formal secara terus menerus untuk manajemen keamanan informasi. Selain itu, memastikan keamanan teknologi dan proses bisnis selaras dengan kebutuhan bisnis dan manajemen keamanan. Kedua, definisi *define and manage an information security risk treatment plan*.



Base Practices (BP) ini bertujuan mempertahankan rencana keamanan informasi dan menjelaskan bagaimana menyelaraskan antara strategi dan arsitektur perusahaan dengan pengelolaan risiko keamanan informasi. Selain itu, memastikan rekomendasi perbaikan keamanan didasarkan atas kasus bisnis yang telah disetujui dan dilaksanakan sebagai cara untuk mengembangkan solusi dan layanan bisnis. Terakhir, definisi *monitor and review the Information Security Management System (ISMS)*. *Base Practices* (BP) ini bertujuan mempertahankan manfaat dari hasil perbaikan keamanan informasi secara terus menerus. Selain itu, mengumpulkan dan menganalisis data tentang sistem manajemen keamanan informasi serta meningkatkan efektivitas dari sistem yang ada. Kemudian, aktif dalam menjaga budaya keamanan dengan cara rutin melakukan perbaikan sehingga mencegah risiko keamanan yang datang.

APO13 RACI CHART

KEY MANAGEMENT PRACTISE	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO 13.01 Establish and maintain an ISMS	C	C	C	C	I	C	I	I	C	A	C	C	C	C	C	R	I	I	I	R	I	R	C	C		
APO 13.02 Define and manage an information security risk treatment plan	C	C	C	C	C	I	I	C	A	C	C	C	C	R	C	C	C	R	C	C	R	C	R	C	C	
APO 13.03 Monitor and review the ISMS					C	R	C	R			A				C	C	R	R	R	R	R	R	R	R	R	

Gambar 2.4 RACI Chart dari proses APO13

Sumber: diadaptasi dari COBIT 5 *Enabling Processes*, 2012.

Berdasarkan Gambar 2.4, diketahui peran yang terlibat dalam penerapan ketiga *Base Practices* (BP) dari proses APO13 (*Manage Security*). Setiap peran memiliki golongan komponen yang berbeda-beda. Berikut pembagian komponen beserta peran yang terlibat pada Tabel 2.7.

Tabel 2.7 Peran dari proses APO13

KOMPONEN	PERAN YANG TERLIBAT
Responsible (Penasihat)	<ul style="list-style-type: none"> ○ Chief Information Officer ○ Head IT Administration ○ Information Security Manager



Tabel 2.7 Peran dari proses APO13 (lanjutan)

KOMPONEN	PERAN YANG TERLIBAT
Accountable (Penanggung Jawab)	<i>Chief Information Security Officer</i>
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ <i>Business Executive</i> ○ <i>Strategy Executive Committee</i> ○ <i>Compliance</i> ○ <i>Auditor</i>
Informed (Terinformasi)	<ul style="list-style-type: none"> ○ <i>Steering (Programmes/Projects) Committee</i> ○ <i>Project Management Office</i>

Terakhir, diketahui sekumpulan aktivitas berdasarkan proses DSS05 (*Manage Security Services*) yang terdiri dari tujuh *Base Practices* (BP) pada Gambar 2.5. Setiap *Base Practices* (BP) memiliki tujuan berbeda-beda, antara lain yang pertama *protect against malware*. *Base Practices* (BP) ini bertujuan memberikan perlindungan dari virus komputer (*malware*). Praktik tata kelola yang dilakukan adalah menerapkan dan memelihara pencegahan serta langkah-langkah perbaikan pada unit organisasi untuk melindungi aset teknologi informasi (TI) dari serangan *malware* seperti virus, *worm spyware*, dan *spam*. Kedua, definisi *manage network and connectivity security*. *Base Practices* (BP) ini bertujuan mengelola jaringan dan keamanan konektivitas. Praktik tata kelola yang dilakukan adalah menggunakan keamanan dan prosedur yang terkait untuk melindungi keamanan informasi dari segi konektivitas. Ketiga, definisi *manage endpoint security*. *Base Practices* (BP) ini bertujuan mengelola keamanan pada titik akhir.

Praktik tata kelola yang dilakukan adalah memastikan perangkat titik akhir (*endpoint*) seperti *laptop*, *dekstop*, dan *server* agar tetap aman sesuai kebijakan yang ditetapkan. Keempat, definisi *manage user identity and logical access*. *Base Practices* (BP) ini bertujuan mengelola identitas pengguna dan hak akses. Praktik tata kelola yang dilakukan adalah memastikan semua pengguna memiliki hak akses informasi yang sesuai dengan kebutuhan mereka. Kelima, definisi *manage physical access to IT assets*. *Base Practices* (BP) ini bertujuan mendefinisikan dan menerapkan prosedur, membatasi, dan mencabut akses sesuai dengan kebutuhan bisnis dalam keadaan darurat. Selain itu, mengelola keamanan akses pada tempat yang berwenang atas akses yang dimaksud. Kemudian, memantau orang yang memasuki tempat akses termasuk staf, klien, vendor, dan pengunjung atau pihak ketiga. Keenam, definisi *manage sensitive documents and output devices*. *Base Practices* (BP) ini bertujuan mengelola keamanan dokumen.

Praktik tata kelola yang dilakukan adalah membangun pengamanan fisik yang sesuai, kemudian menginventarisasi dokumen penting atas aset teknologi informasi (TI) seperti surat berharga dan token keamanan. Terakhir, definisi *monitor the infrastructure for security-related events*. *Base Practices* (BP) ini bertujuan menggunakan alat deteksi instruksi dan mengawasi infrastruktur untuk akses yang tidak sah serta memastikan setiap peristiwa yang terintegrasi dengan cara mengawasi dan mengelola risiko.

DSS05 RACI CHART																										
KEY MANAGEMENT PRACTISE	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS 05.01 Protect against malware					R	I					C	A			R	C	C	C	I	R	R		I	R		
DSS 05.02 Manage network and connectivity security											C	A				C	C	C	I	R	R			R		
DSS 05.03 Manage endpoint security											C	A				C	C	C	I	R	R		I	R		
DSS 05.04 Manage user identity and logical access						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS 05.05 Manage physical access to IT assets											C	A				C	C	C	I	C	R		I	R	I	
DSS 05.06 Manage sensitive documents and output devices																C	C	A			R					
DSS 05.07 Monitor the infrastructure for security-related events				I		C						I	A			C	C	C	I	C	R		I	R	I	I

Gambar 2.5 RACI Chart dari proses DSS05

Sumber: diadaptasi dari COBIT 5 *Enabling Processes*, 2012.

Berdasarkan Gambar 2.5, diketahui peran yang terlibat dalam penerapan ketujuh *Base Practices* (BP) dari proses DSS05 (*Manage Security Services*). Setiap peran memiliki golongan komponen yang berbeda-beda. Berikut pembagian komponen beserta peran yang terlibat pada Tabel 2.7.

Tabel 2.8 Peran dari proses DSS05

KOMPONEN	PERAN YANG TERLIBAT
<i>Responsible</i> (Penasihat)	<i>Head IT Operations</i>



Tabel 2.8 Peran dari proses DSS05 (lanjutan)

KOMPONEN	PERAN YANG TERLIBAT
Accountable (Penanggung Jawab)	<i>Chief Information Security Officer</i>
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ <i>Compliance</i> ○ <i>Auditor</i>
Informed (Terinformasi)	<ul style="list-style-type: none"> ○ <i>Head Architect</i> ○ <i>Service Manager</i>

Setelah mengetahui peran apa saja yang terlibat dari setiap komponen RACI Chart, berikut definisi keseluruhan peran yang terdapat pada kerangka kerja COBIT 5. Peran yang pertama adalah *Board*. Merupakan individu atau kelompok eksekutif senior dari organisasi yang bertanggung jawab tata kelola organisasi, memiliki pengelolaan dan pengawasan terhadap aktivitas serta sumber daya perusahaan. Kedua, definisi *Chief Executive Officer*. Merupakan pimpinan perusahaan yang memiliki kedudukan tinggi dalam bertanggung jawab atas keberhasilan maupun kegagalan perusahaan serta pengelolaan organisasi. Ketiga, definisi *Chief Financial Officer*. Merupakan individu yang bertanggung jawab atas pengelolaan dan perencanaan keuangan, dokumentasi, dan pengelolaan risiko serta pelaporan keuangan organisasi. Keempat, definisi *Chief Operating Officer*. Merupakan individu dengan tingkatan senior pada organisasi yang bertanggung jawab operasional internal perusahaan, seperti operasional kantor, karyawan hingga bisnis. Kelima, definisi *Business Executive*. Merupakan individu yang melakukan transaksi terhadap anak organisasi atau unit bisnis tertentu dan membina hubungan baik dengan pihak ketiga.

Keenam, definisi *Business Process Owner*. Merupakan individu yang bertanggung jawab atas performansi proses atau kinerja, menyetujui perubahan proses, dan mendorong perbaikan proses. Ketujuh, definisi *Strategy Executive Committee*. Merupakan eksekutif senior yang ditunjuk oleh dewan direksi untuk bertanggung jawab menyusun dan mengelola strategi. Selain itu, memastikan dewan direksi terlibat dalam pengambilan keputusan yang berkaitan dengan teknologi informasi (TI). Kedepalan, definisi *Steering (Programmes/Projects) Committee*. Merupakan pemangku kepentingan (*stakeholder*) dan individu yang berkompeten untuk mengelola program atau proyek perusahaan. Kesembilan, definisi *Project Management Office*. Merupakan departemen atau divisi dalam organisasi yang menjaga, mengelola, dan menentukan standar manajemen proyek organisasi agar mendapat keuntungan maksimal. Selain itu, mengarahkan program atau proyek yang dijalankan agar sesuai aturan. Kesepuluh, definisi *Value management office*. Merupakan departemen atau divisi yang bertindak sebagai sekretariat dalam menangani pengelolaan anggaran untuk berinvestasi terhadap hasil karya.

Kesebelas, definisi *Chief Risk Officer*. Merupakan individu yang memiliki tingkatan senior pada organisasi untuk bertanggung jawab mengembangkan dan memantau pengelolaan serta pengawasan risiko yang berkaitan dengan teknologi informasi (TI). Kedua belas, definisi *Chief Information Security Officer*. Merupakan individu yang bertanggung jawab atas keamanan informasi dan mempertahankan strategi, visi, dan program perusahaan untuk memastikan seluruh aset teknologi informasi (TI) telah terlindungi. Ketiga belas, definisi *Architecture Board*. Merupakan penasihat teknis mengenai jenis keputusan yang ditetapkan sebagai standar arsitektur dan kebijakan. Keempat belas, definisi *Enterprise Risk Committee*. Merupakan pemantau kebijakan dan pengelolaan mitigasi risiko yang diambil oleh organisasi. Kelima belas, definisi *Head Human Resources*. Merupakan pimpinan yang bertanggung jawab memajukan organisasi melalui perencanaan dan pemberian kebijakan mengenai sumber daya manusia.

Keenam belas, definisi *Compliance*. Merupakan individu yang bertanggung jawab mengelola kualitas sistem dan memberikan pengarahan mengenai aturan dan hukum yang berlaku. Selain itu, memastikan seluruh kegiatan produksi dan transaksi berjalan dengan tepat. Ketujuh belas, definisi *Auditor*. Merupakan individu yang bertanggung jawab atas pelaksanaan audit internal dan laporan keuangan. Kedelapan belas, definisi *Chief Information Officer*. Merupakan individu yang bertanggung jawab dalam sistem informasi organisasi dalam mendukung tujuan organisasi. Kesembilan belas, definisi *Head of Architecture*. Merupakan pimpinan yang berwenang melakukan proses *architecture enterprise* dan bertanggung jawab memimpin perancangan arsitektur teknologi informasi (TI) yang diterapkan organisasi. Kedua puluh, definisi *Head of Development*. Merupakan individu yang bertanggung jawab atas perkembangan teknologi informasi (TI) untuk menunjang strategi dan tujuan organisasi.

Kedua puluh satu, definisi *Head IT Operation*. Merupakan individu yang bertanggung jawab memelihara infrastruktur teknologi informasi (TI) sebagai aset penting dari organisasi. Kedua puluh dua, definisi *Head of IT Administration*. Merupakan individu yang bertanggung jawab atas pengelolaan terhadap administrasi yang berkaitan dengan teknologi informasi (TI). Kedua puluh tiga, definisi *Service Manager*. Merupakan individu yang bertanggung jawab atas kepuasan pengguna atau konsumen mengenai layanan yang diterapkan. Selain itu, memastikan layanan dikelola oleh individu yang berkompeten. Kedua puluh empat, definisi *Information Security Manager*. Merupakan individu yang bertanggung jawab atas penerapan, pengelolaan, dan pengawasan keamanan informasi organisasi. Kedua puluh lima, definisi *Business Continuity Manager*. Merupakan individu yang bertanggung jawab atas kelangsungan bisnis organisasi. Kedua puluh enam, definisi *Privacy Officer*. Merupakan individu yang bertanggung jawab mengelola dan memantau risiko serta menjaga segala bentuk privasi organisasi.

2.16 Pengertian *Self Assessment*

Menurut ISACA (2013), *self assessment* merupakan sebuah pendekatan sederhana untuk melakukan penilaian yang tidak didasarkan pada bukti, tidak memerlukan penilai independen atau bersertifikat, dan dapat dilakukan staf manajemen perusahaan sehingga menjadi pendahuluan untuk melakukan penilaian secara formal. *Self assessment* dapat mengidentifikasi kesenjangan proses yang memerlukan perbaikan sebelum penilaian formal dan digunakan sebagai investasi kecil namun membantu manajemen dalam menetapkan tingkat kapabilitas (*capability level*) perusahaan. Menurut ISACA (2013), terdapat lima tahapan dalam pelaksanaan *self assessment*, antara lain yang pertama *decide on processes to asses*. Pada tahap ini, dilakukan penentuan proses apa saja yang akan dinilai. Penilai mencatat proses yang dipilih sesuai pencapaian dari pihak perusahaan. Hal ini bertujuan memberikan pemetaan mengenai sasaran bisnis dan teknologi informasi (TI). Selain itu, diketahui tingkat kapabilitas (*capability level*) yang diraih.

Kerangka kerja COBIT 5 memberikan format khusus yang dapat digunakan untuk menganalisis tingkat kapabilitas (*capability level*) perusahaan. Format yang dimaksud berisi jenis dan definisi setiap proses yang digunakan dalam penilaian. Penilaian dilakukan dengan menganalisis setiap proses yang telah diterapkan dan menentukan tingkat kapabilitas (*capability level*) melalui kategori nilai seperti N (*Not Achieved*), P (*Partially Achieved*), L (*Largely Achieved*), dan F (*Fully Achieved*). Dalam menentukan tingkat kapabilitas (*capability level*), tentu mempertimbangkan bukti pelaksanaan sehingga hasil penilaian sesuai dengan kondisi saat itu. Terdapat beberapa *level* yang dikategorikan berdasarkan hasil penerapan kebijakan perusahaan. Pada *level 1*, memiliki satu atribut proses pada *Process Performance* (PA 1.1). Pencapaian ini didasarkan bilamana suatu proses tercapai dan tidak memiliki suatu produk. Pada *level 2*, memiliki dua atribut proses, antara lain *Performance Management* (PA 2.1) dan *Work Product Management* (PA 2.2).

Performance Management (PA 2.1) adalah suatu proses yang muncul bilamana terjadi permasalahan pada tanggung jawab seperti penggunaan sumber daya dan kurangnya pengelolaan biaya dan waktu. Kemudian, *Work Product Management* (PA 2.2) terjadi bilamana kualitas dan integritas produk tidak dapat diprediksi, meningkatnya biaya pendukung, dan kesalahan dalam komunikasi. Pada *level 3*, juga memiliki dua atribut proses, antara lain *Process Definition* (PA 3.1) dan *Process Deployment* (PA 3.2). *Process Definition* (PA 3.1) tercapai bilamana perusahaan ingin mengidentifikasi praktik dan mempelajari hasil kinerja sebelumnya. Selain itu, mendefinisikan segala kinerja organisasi bilamana belum adanya pondasi dalam meningkatkan kualitas proses perusahaan. Selanjutnya, *Process Deployment* (PA 3.2) terjadi bilamana proses yang diimplementasikan tidak terdapat praktik yang telah diidentifikasi dari kinerja sebelumnya. Pada *level* ini, suatu proses cenderung sulit diidentifikasi sehingga menyebabkan kehilangan peluang.

Pada *level 4*, juga memiliki dua atribut proses, antara lain *Process Management* (PA 4.1) dan *Process Control* (PA 4.2). *Process Management* (PA 4.1) merupakan keadaan dimana perusahaan tidak memiliki pemahaman kuantitatif tentang seberapa baik suatu proses, tujuan, dan bisnis yang tercapai. Kemudian, tidak ada kemampuan kuantitatif untuk mendeteksi masalah kinerja sejak dini. Selanjutnya, *Process Control* (PA 4.2) merupakan keadaan dimana proses tidak dapat diprediksi dalam batas yang ditentukan. Selain itu, belum terpenuhinya tujuan kuantitatif dan bisnis perusahaan. Pada *level 5*, juga memiliki dua atribut proses, antara lain *Process Innovation* (PA 5.1) dan *Process Optimization* (PA 5.2). *Process Innovation* (PA 5.1) merupakan proses pertimbangan bilamana tujuan perbaikan tidak didefinisikan dengan jelas. Selanjutnya, *Process Optimization* (PA 5.2) terjadi bilamana perusahaan tidak mampu mengubah proses secara efektif untuk mencapai tujuan dari perbaikan proses.

Tahap kedua adalah *determine level 1 capability*. Pada tahap ini, ditentukan apakah sebuah proses telah dilakukan dan mencapai hasil. Dalam *worksheet self assessment*, disediakan tabel untuk setiap proses. Indikator tingkat kapabilitas (*capability level*) pertama ditunjukkan secara spesifik sehingga setiap proses diharapkan mampu menilai apakah atribut proses telah tercapai atau belum. Tahap ketiga adalah *determine capability for levels 2 to 5*. Pada tahap ini, setiap proses harus dibuat untuk mengetahui apakah kriteria telah tercapai atau belum. Kemudian, hasil keputusan diterjemahkan dalam bentuk penilaian dan digunakan sebagai pedoman untuk menilai proses lain. Penilaian dilakukan secara berulang hingga meraih kategori nilai L (*Largely Achieved*) maupun F (*Fully Achieved*). Tahap keempat adalah *record and summarise capability levels*. Pada tahap ini, dianjurkan untuk mendokumentasikan hasil penilaian. Nantinya, tingkat kapabilitas (*capability level*) akan ditentukan berdasarkan atribut proses yang meraih kategori nilai L (*Largely Achieved*) maupun F (*Fully Achieved*).

Tahap terakhir adalah *plan process improvement*. Menurut ISACA (2013), jenis pertimbangan harus diberikan terhadap rencana perbaikan dan pengembangan proses. Pilihan pertama memulai rencana perbaikan berdasarkan *risk assessment*. Hal ini mampu mengatasi area penting bagi sasaran bisnis perusahaan yang kemudian berfokus pada area yang memiliki *gap* (kesenjangan) antara kondisi saat ini dengan kondisi yang diharapkan perusahaan. Pilihan kedua melakukan penilaian independen yang lebih formal berdasarkan kerangka kerja COBIT 5 dan panduan dari *asesor*. Hal ini akan memberikan hasil dan panduan perbaikan yang tepat. Pada tahap ini, akan dibuat rekomendasi agar perusahaan mampu meraih tingkat pencapaian (*targeted level*) yang diharapkan.

2.17 Indikator Proses Kapabilitas COBIT 5

Menurut ISACA (2012), indikator proses kapabilitas merupakan sebuah kemampuan suatu proses dalam meraih tingkat kapabilitas (*capability level*) yang telah ditetapkan oleh setiap atribut proses. Penilaian dari pencapaian atribut proses didukung dalam bukti dari seluruh indikator proses kapabilitas. Menurut ISACA (2013), ada enam *level* yang menunjukkan tingkat kapabilitas (*capability level*). Keenam *level* yang dimaksud antara lain yang pertama pada *level 0 (Incomplete Process)*. *Level* ini mengindikasikan proses teknologi informasi (TI) tidak diterapkan atau gagal mencapai tujuan. Selain itu, *level* ini tidak memiliki atribut proses sama sekali. Kedua adalah *level 1 (Performed Process)* yang memiliki satu atribut proses. *Level* ini mengindikasikan proses telah diterapkan dan mencapai tujuan. Ketiga adalah *level 2 (Managed Process)* yang juga memiliki dua atribut proses. *Level* ini mengindikasikan proses yang telah diterapkan harus dikelola (perencanaan, pengawasan, dan penerapan) dan hasil dari pengelolaan dipelihara dengan baik.

Keempat adalah *level 3 (Established Process)* yang memiliki dua atribut proses. *Level* ini mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Kelima adalah *level 4 (Predictable Process)* yang juga memiliki dua atribut proses. *Level* ini mengindikasikan proses teknologi informasi (TI) dilakukan secara konsisten dengan batasan yang telah ditentukan. Terakhir adalah *level 5 (Optimizing Process)* yang juga memiliki dua atribut proses. *Level* ini mengindikasikan proses teknologi informasi (TI) ditingkatkan secara berkelanjutan untuk memenuhi kebutuhan bisnis saat ini dan akan datang. *Level 1* merupakan indikator khusus bagi organisasi untuk mengukur tingkat keberhasilan dalam menjalankan setiap proses yang telah ditetapkan berdasarkan kerangka kerja COBIT 5. Pada *level 2* hingga 5, penilaian kapabilitas didasarkan atas indikator kinerja dari proses generik. Disebut generik, sebab berlaku untuk semua proses, namun tetap berbeda dari satu *level* ke *level* lainnya.

Secara umum dapat dipahami ketika semakin tinggi *level* proses kapabilitas (*capability process*) yang dicapai, maka semakin rendah risiko proses gagal dalam memenuhi tujuan. Kemudian, ketika semakin tinggi tingkat kapabilitas (*capability level*), maka semakin mahal proses operasinya. Menurut ISACA (2013), setiap atribut proses terdapat label atau kode berupa Proses Atribut (PA). Berdasarkan paragraf sebelumnya, *level 0 (Incomplete Process)* tidak memiliki atribut proses sama sekali. Sebab, *level* ini mengindikasikan suatu proses tidak atau belum diterapkan sehingga dinilai gagal dalam meraih tujuan proses. Sedangkan *level 1* memiliki satu atribut proses yaitu *Process Performance (PA 1.1)*. Atribut proses ini merupakan pengukuran mengenai seberapa jauh suatu proses mampu mencapai tujuan yang telah didefinisikan atau direncanakan. Oleh karena itu, diperlukan beberapa bukti (*evidences*) untuk memastikan proses setiap *level* telah berjalan. Selanjutnya terdapat dua atribut proses pada *level 2*, antara lain yang pertama *Performance Management (PA 2.1)*. Merupakan pengukuran mengenai performa proses yang dikelola.

Kedua adalah *Work Product Management* (PA 2.2). Merupakan pengukuran kinerja dari jenis proses yang telah dikelola. Kemudian, *level 3* memiliki dua atribut proses pula, antara lain yang pertama *Process Definition* (PA 3.1). Merupakan pengukuran sejauh mana standar proses dikelola untuk mendukung proses yang telah didefinisikan. Kedua adalah *Process Deployment* (PA 3.2). Merupakan pengukuran standar proses secara efektif untuk mengetahui kondisi proses yang telah berjalan. Selanjutnya, *level 4* memiliki dua atribut proses pula, antara lain yang pertama *Process Measurement* (PA 4.1). Merupakan proses pengukuran mengenai seberapa jauh hasil pengukuran yang digunakan untuk memastikan performa proses mendukung pencapaian tujuan proses dan organisasi.

Kedua adalah *Process Control* (PA 4.2). Merupakan pengukuran secara kuantitatif tentang seberapa jauh suatu proses dapat menghasilkan proses yang stabil dan diprediksi dalam batasan telah ditentukan. Terakhir, *level 5* yang memiliki dua atribut proses pula, antara lain yang pertama *Process Innovation* (PA 5.1). Merupakan pengukuran atas perubahan proses yang telah diidentifikasi dari penyebab adanya variasi dalam performa. Selain itu, menginvestigasi pendekatan inovatif untuk mendefinisikan dan melaksanakan proses. Kedua adalah *Process Optimization* (PA 5.2). Merupakan pengukuran perubahan definisi, manajemen, dan performa proses agar memiliki hasil yang efektif untuk mencapai tujuan dari peningkatan proses.

Tabel 2.9 Kategori pencapaian tiap level

KATEGORI	PERSENTASE KATEGORI
<i>Not Achieved</i>	0 sampai 15 %.
<i>Partially Achieved</i>	> 15 % sampai 50 %.
<i>Largely Achieved</i>	> 50 % sampai 85 %.
<i>Fully Achieved</i>	> 85 % sampai 100 %.

Sumber: diadaptasi dari buku *Self Assessment Guide Using COBIT 5*, 2012.

Menurut ISACA (2013), penilaian pada setiap *level* akan diklasifikasikan dalam empat kategori seperti Tabel 2.9, antara lain yang pertama keterangan N (*Not Achieved* (tidak tercapai)), yang artinya *range* atau batasan pada kategori ini berkisar 0-15%. Kategori ini tidak ada atau hanya sedikit bukti terkait pencapaian atribut proses. Kedua adalah keterangan P (*Partially Achieved* (tercapai hanya sebagian)), yang artinya *range* atau batasan pada kategori ini berkisar 15-50%. Kategori ini telah terdapat beberapa bukti (*evidences*) mengenai pendekatan proses serta beberapa pencapaian dari atribut proses. Ketiga adalah keterangan L (*Largely Achieved* (secara garis besar tercapai)), yang artinya *range* atau batasan pada kategori ini berkisar 50-85%.

Pada kategori ini akan terlihat pencapaian signifikan atas setiap proses dan ditemukan beberapa bukti (*evidences*) mengenai pendekatan yang sistematis, meskipun diketahui kelemahan yang tidak signifikan. Terakhir adalah keterangan F (*Fully Achieved* (tercapai sepenuhnya)), yang artinya *range* atau batasan pada kategori ini berkisar 85-100%. Kategori ini telah terdapat pencapaian penuh atas atribut proses dan ditemukan beberapa bukti (*evidences*) mengenai pendekatan yang sistematis dan lengkap. Kategori ini telah tidak ditemukan kelemahan berarti mengenai atribut proses. Dalam menentukan pencapaian tiap *level*, terdapat pola yang telah ditetapkan. Menurut ISACA (2012), perpindahan tiap *level* hanya dapat dilakukan bilamana kondisi proses telah mencapai *Largely Achieved* atau *Fully Achieved*.



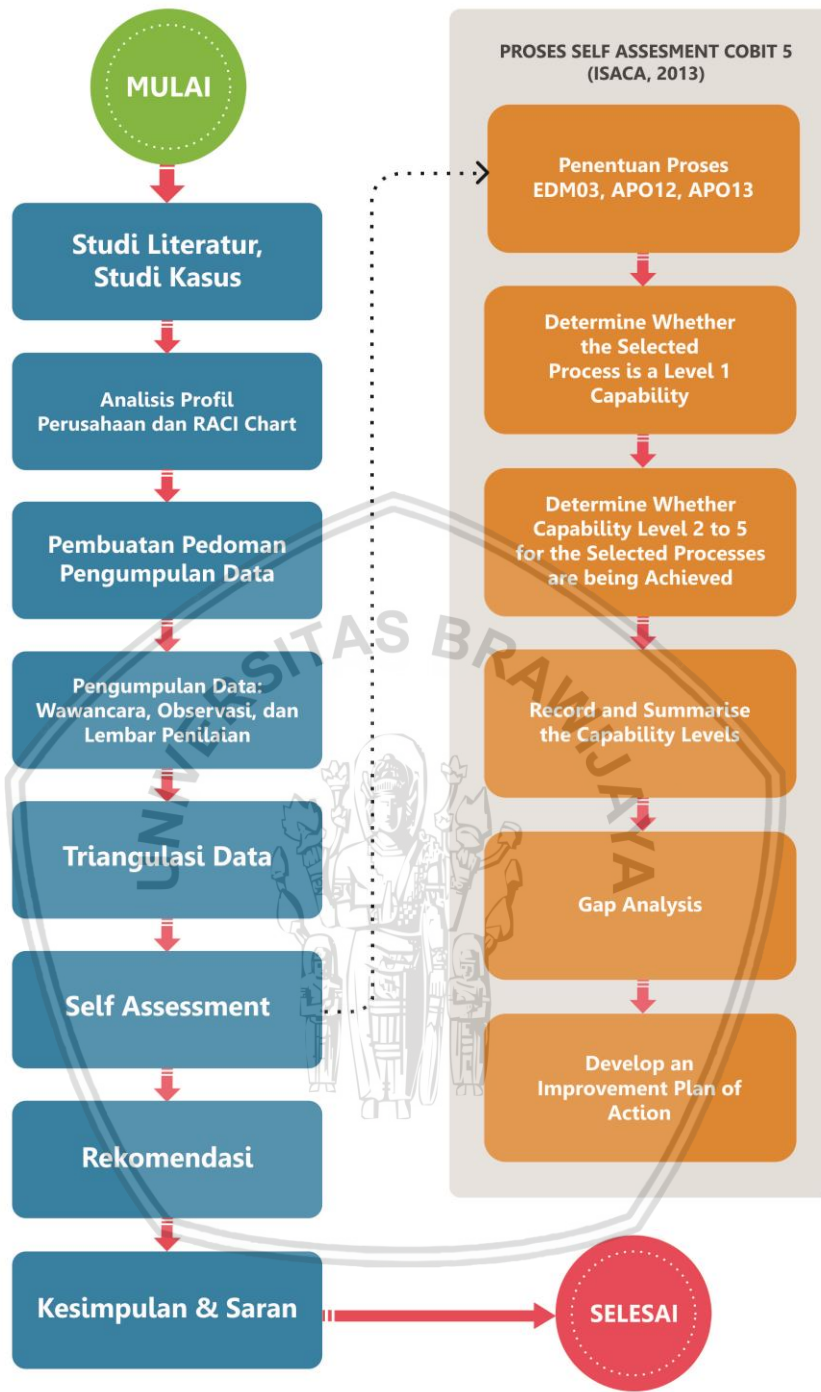
BAB 3 METODOLOGI PENELITIAN

3.1 Metode Penelitian

Jenis metode yang digunakan dalam penelitian ini adalah kualitatif. Metode ini dirancang untuk membantu peneliti memahami beberapa fenomena dari setiap konteks. Menurut Recker (2013), metode kualitatif merupakan strategi investigasi yang menyelidiki fenomena dalam konteks kehidupan nyata. Metode ini cocok untuk penelitian eksplorasi, dimana contoh fenomena yang dimaksud belum sepenuhnya dipahami. Dengan menggunakan metode ini, fokus penelitian diarahkan terhadap interpretasi data. Beberapa data diperoleh dari hasil wawancara, observasi, dan lembar penilaian. Dari data yang diperoleh, dilakukan analisis guna mendapatkan tingkat kapabilitas (*capability level*) sehingga menghasilkan rekomendasi.

Dalam teknik pengumpulan data, metode kualitatif memiliki berbagai cara, antara lain yang pertama menggunakan wawancara deskriptif. Cara ini digunakan untuk memberikan gambaran yang jelas tentang fenomena yang dirasakan oleh setiap individu. Dengan cara ini pula, pemahaman subjektif dapat dihasilkan. Wawancara deskriptif memberikan keuntungan karena berfokus pada topik yang dipilih sehingga memberikan kesimpulan kausal seperti yang dirasakan oleh responden sebagai objek wawancara. Cara kedua menggunakan *direct observation*. Cara ini dilakukan dengan mengamati langsung dan melibatkan peneliti sebagai pengamat pasif dan netral. Cara terakhir menganalisis kondisi *Base Practices* (BP) dan *Work Product* (WP) menggunakan lembar *checklist* yang disediakan oleh peneliti.

Beberapa cara pengumpulan data yang telah dilakukan, dilanjutkan proses triangulasi data. Hal ini bertujuan memastikan data yang diperoleh memiliki kredibilitas sehingga data berkualitas dan disaksikan oleh kedua responden terpilih sebagai bentuk validasi data pada penelitian ini. Setelah dilakukan proses triangulasi, maka data diolah menggunakan lembar penilaian guna mengetahui tingkat kapabilitas (*capability level*) dari proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan perusahaan. Lembar penilaian disusun berdasarkan kriteria dari tiap *level* pada kerangka kerja COBIT 5, kemudian dilakukan pemetaan hasil pengisian lembar *checklist* terhadap setiap kriteria sehingga diketahui kondisi *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP) dari setiap *level* yang ada. Setelah diketahui tingkat kapabilitas (*capability level*), diberikan rekomendasi sebagai langkah untuk melakukan perbaikan dan meningkatkan *level* saat ini menuju *level* yang diharapkan perusahaan guna menghilangkan tingkat kesenjangan (*gap level*) yang diketahui dari hasil wawancara. Berikut tahap penelitian yang ditunjukkan pada Gambar 3.1.



Gambar 3.1 Tahap penelitian

Pada Gambar 3.1, diketahui tahap penelitian mengacu pada kerangka kerja COBIT 5. Berikut penjelasan dari masing-masing tahap penelitian yang terbagi menjadi delapan tahap, antara lain yang pertama tentang studi literatur. Pada alur ini, digunakan literatur mengenai kerangka kerja COBIT 5 yang difokuskan pada keamanan informasi melalui proses APO13 (*Manage Security*) dan DSS05 (*Manage Security Services*), serta satu proses pendukung yaitu EDM03 (*Ensure Risk Optimization*). Selain itu, digunakan jurnal maupun artikel ilmiah yang berkaitan dengan kerangka kerja COBIT 5 dan penerapan manajemen keamanan informasi. Studi kasus ini dilakukan guna mengetahui batas dari penelitian ini. Kedua adalah melakukan analisis profil perusahaan dan RACI *Chart* untuk mengetahui gambaran umum tentang perusahaan dan peran mana saja yang terlibat dalam penelitian ini. Ketiga adalah melakukan pembuatan pedoman pengumpulan data seperti penyusunan daftar pertanyaan wawancara, observasi, dan tabel lembar penilaian.

Keempat adalah pengumpulan data melalui proses wawancara, observasi, dan pengisian lembar penilaian. Kelima adalah melakukan analisis triangulasi data guna memastikan data yang diperoleh memiliki kredibilitas. Keenam adalah melakukan penilaian pribadi (*self assessment*) untuk setiap proses yang digunakan seperti EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*). Ketujuh adalah pembuatan rekomendasi bagi perusahaan guna meningkatkan tingkat kapabilitas (*capability level*) sesuai dengan tingkat pencapaian (*targeted level*) yang diharapkan melalui hasil wawancara. Terakhir, keseluruhan penelitian ini menghasilkan kesimpulan dan saran yang dapat dikembangkan dan digunakan sebagai referensi bagi peneliti selanjutnya.

3.2 Studi Literatur dan Studi Kasus

Pada tahap ini, mencari dan mempelajari literatur baik dari buku, jurnal, laporan penelitian sebelumnya maupun artikel yang berkaitan dengan kerangka kerja COBIT 5. Subjek dari penelitian ini mengenai evaluasi menggunakan penilaian tingkat kapabilitas (*capability level*) pada proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan. Sedangkan objek penelitian ini dilakukan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan.

3.3 Analisis Profil Perusahaan dan RACI *Chart*

Sebelum melakukan wawancara dan observasi, peneliti menganalisis RACI *Chart* terlebih dahulu guna mengetahui pihak responden yang terlibat berdasarkan proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*). Sehingga hasil analisis dapat digunakan mengetahui dan memetakan pihak responden yang tepat berdasarkan struktur organisasi divisi *Danone Information Systems* (DAN'IS). Struktur organisasi diperoleh dari hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4.

3.4 Pembuatan Pedoman Pengumpulan Data

Pembuatan pedoman pengumpulan data dilakukan sebagai acuan dalam melakukan wawancara, observasi, dan lembar penilaian. Lembar penilaian disusun berdasarkan kerangka kerja COBIT 5. Sebelum melakukan wawancara, dilakukan penyusunan pertanyaan untuk memperoleh data dan informasi penting dari perusahaan. Sedangkan kegiatan observasi difokuskan untuk meneliti dan menemukan suatu hal yang berharga dari pelaksanaan wawancara, seperti adanya program atau kebijakan tertentu dari perusahaan.

3.5 Pengumpulan Data

Pada tahap ini, terdapat tiga jenis metode pengumpulan data yang dilakukan pada penelitian ini, antara lain wawancara, observasi, dan pengisian lembar penilaian. Lembar penilaian digunakan untuk mengetahui tingkat kapabilitas (*capability level*) dari proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan. Lembar penilaian ini disusun berdasarkan kerangka kerja COBIT 5.

Selanjutnya adalah metode wawancara. Metode ini dilakukan untuk memperoleh data dan informasi dari pihak yang terpilih berdasarkan pemetaan RACI *Chart* pada struktur organisasi perusahaan. Selain itu, metode wawancara juga sebagai acuan dalam verifikasi hasil temuan dari kegiatan observasi. Terakhir adalah metode observasi. Metode ini dilakukan dengan cara *direct observation* dan pengamatan langsung yang melibatkan peneliti sebagai pengamat pasif dan netral. Dari hasil pengamatan, diketahui bagaimana kondisi penerapan tata kelola teknologi informasi (TI) divisi DAN'IS untuk PT Tirta Investama (AQUA) Pandaan secara umum.

3.6 Triangulasi Data

Triangulasi data merupakan tahap mencari konvergensi (keadaan menuju satu titik pusat) dan menguatkan hasil dari berbagai metode yang sudah dilakukan dalam pengumpulan data. Pada sub bab sebelumnya, dijelaskan bahwa tiga jenis metode yang dilakukan dalam penelitian ini antara lain wawancara, observasi, dan lembar penilaian. Menurut Recker (2013), melalui triangulasi data, peneliti dapat memperoleh gambaran situasi yang lebih bernuansa dan meningkatkan ketepatan serta validitas dari temuan peneliti. Sehingga akan mencapai kredibilitas dan menjaga rantai bukti serta memperoleh catatan yang jelas mengenai keputusan yang dibuat selama proses penelitian.

3.7 Self Assessment

Pada tahap ini, terdapat lima langkah yang dilakukan, antara lain yang pertama menentukan proses apa saja yang dinilai berdasarkan proses EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*), dan DSS05 (*Manage Security Services*). Setelah itu, menentukan tingkat pencapaian (*targeted level*) yang ingin diraih oleh perusahaan. Kedua adalah menentukan setiap proses yang mampu mencapai *level 1*. Ketiga adalah melakukan penilaian pada setiap proses untuk mencapai *level 2* hingga 5.

Keempat adalah melakukan pencatatan akan hasil yang diperoleh dari penentuan *level 1* hingga 5 dan dianalisis melalui tingkat pencapaian (*targeted level*) sehingga mampu diketahui tingkat kesenjangan (*gap level*) antar keduanya. Kelima adalah menentukan langkah-langkah apa saja yang perlu diambil untuk meningkatkan kondisi seperti yang diharapkan. Terakhir adalah melakukan pertimbangan untuk rencana perbaikan proses sehingga mampu memenuhi tingkat pencapaian (*targeted level*) yang diharapkan.

3.8 Rekomendasi

Rekomendasi dihasilkan melalui beberapa analisis yang telah dilakukan, seperti wawancara, observasi, dan lembar penilaian. Rekomendasi bertujuan memperbaiki permasalahan yang ada dan meningkatkan kualitas proses optimasi risiko, pengelolaan keamanan, serta pengelolaan layanan keamanan perusahaan dari *level* saat ini menuju *level* yang diharapkan. Selain itu, bertujuan menghilangkan tingkat kesenjangan (*gap level*) yang diketahui dari hasil wawancara.

3.9 Kesimpulan dan Saran

Kesimpulan dibuat berdasarkan rumusan masalah yang telah dipaparkan pada penelitian ini. Sedangkan saran diberikan bagi peneliti selanjutnya untuk mengembangkan penelitian menggunakan metode dan kerangka kerja lain. Sehingga karya penelitian akan lebih variatif dan bermanfaat untuk setiap objek penelitian.

BAB 4 ANALISIS DAN HASIL

4.1 Analisis dan Pemetaan RACI Chart

Dalam melakukan wawancara dan observasi, tentu ada pihak responden yang terlibat. Penentuan siapa dan berapa jumlah responden harus diperhitungkan secara tepat agar data dan informasi yang diperoleh juga akurat. Kerangka kerja COBIT 5 menyediakan sebuah wadah analisis pada RACI Chart. RACI Chart merupakan singkatan dari *Responsible*, *Accountable*, *Consulted*, dan *Informed*, yang merupakan sebuah matriks dari seluruh wewenang atau aktivitas dalam mengambil keputusan dari sebuah organisasi pada setiap individu dan proses. Berikut definisi dari empat komponen RACI Chart, antara lain yang pertama *Responsible* (pelaksana). Komponen ini bertanggung jawab secara langsung dalam pelaksanaan aktivitas organisasi.

Kedua, definisi *Accountable* (penanggung jawab). Komponen ini memiliki tanggung jawab dan otoritas penuh dalam menentukan kebijakan atau keputusan pada organisasi. Ketiga, definisi *Consulted* (penasihat). Komponen ini berkontribusi untuk memberikan umpan balik (*feedback*) berupa saran atas aktivitas yang telah dilaksanakan. Terakhir, definisi *Informed* (terinformasi). Komponen ini bertugas menerima informasi keseluruhan aktivitas organisasi yang telah dilakukan. Dengan menggunakan fungsi RACI Chart akan diketahui siapa dan berapa jumlah responden yang terlibat dalam pelaksanaan wawancara dan observasi. Berikut tabel analisis dan perhitungan peran RACI Chart berdasarkan proses EDM03 (*Ensure Risk Optimization*).

Tabel 4.1 Penentuan peran dari proses EDM03

NO	PERAN	KOMPONEN			
		R	A	C	I
1	<i>Board</i>		3		
2	<i>Chief Executive Officer</i>	3			
3	<i>Chief Financial Officer</i>			3	
4	<i>Chief Operating Officer</i>			3	
5	<i>Business Executive</i>	3			
6	<i>Business Process Owners</i>			3	
7	<i>Strategy Executive Committee</i>	3			
8	<i>Steering (Programmes/Projects) Committee</i>				2
9	<i>Project Management Office</i>	1			2
10	<i>Value Management Office</i>				3
11	<i>Chief Risk Officer</i>	3			
12	<i>Chief Information Security Officer</i>	1		1	1

Tabel 4.1 Penentuan peran dari proses EDM03 (lanjutan)

NO	PERAN	KOMPONEN			
		R	A	C	I
13	<i>Architecture Board</i>				2
14	<i>Enterprise Risk Committee</i>				3
15	<i>Head Human Resource</i>			3	
16	<i>Compliance</i>			3	
17	<i>Audit</i>			3	
18	<i>Chief Information Officer</i>	3			
19	<i>Head Architect</i>			3	
20	<i>Head Development</i>				2
21	<i>Head IT Operation</i>				2
22	<i>Head IT Administration</i>				2
23	<i>Service Manager</i>				2
24	<i>Information Security Manager</i>				2
25	<i>Business Continuity Manager</i>				2
26	<i>Privacy Officer</i>			2	1

Jika menganalisis nilai setiap peran pada Tabel 4.1, *Chief Executive Officer*, *Business Executive*, *Strategy Executive Committee*, *Chief Risk Officer*, dan *Chief Information Officer* memiliki nilai tertinggi sebagai komponen *Responsible* (pelaksana) dengan angka 3. Kemudian, terdapat *Board* yang memiliki nilai tertinggi sebagai komponen *Accountable* (penanggung jawab) dengan angka 3. Terdapat pula *Chief Financial officer*, *Chief Operating Officer*, *Business Process Owner*, *Head Human Resources*, *Compliance*, *Auditor*, dan *Head Architecture* yang memiliki nilai tertinggi sebagai komponen *Consulted* (penasihat) dengan angka 3. Sedangkan *Value Management Officer* dan *Enterprise Risk Committee* memiliki nilai tertinggi sebagai komponen *Informed* (terinformasi) dengan angka 3. Berikut tabel pemetaan peran RACI Chart yang terpilih berdasarkan struktur organisasi divisi *Danone Information Systems* (DAN'IS) melalui proses EDM03 (*Ensure Risk Optimization*).

Tabel 4.2 Pemetaan peran pada proses EDM03

KOMPONEN	PERAN	JABATAN PERUSAHAAN
<i>Responsible</i> (Penasihat)	<ul style="list-style-type: none"> ○ <i>Chief Risk Officer</i> ○ <i>Chief Information Officer</i> 	<i>DAN'IS Network Analyst</i> dan <i>DAN'IS Asset & Server Management</i>



Tabel 4.2 Pemetaan peran pada proses EDM03 (lanjutan)

KOMPONEN	PERAN	JABATAN PERUSAHAAN
Accountable (Penanggung Jawab)	<i>Board</i>	-
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ <i>Chief Financial Officer</i> ○ <i>Chief Operating Officer</i> ○ <i>Business Process Owner</i> ○ <i>Head Human Resources</i> ○ <i>Compliance</i> ○ <i>Auditor</i> ○ <i>Head Architecture</i> 	-
Informed (PENGinformasi)	<ul style="list-style-type: none"> ○ <i>Value Management Officer</i> ○ <i>Enterprise Risk Committee</i> 	-

Jika menganalisis hasil pemetaan pada Tabel 4.2, disimpulkan bahwa jabatan *DAN'IS Network Analyst* dan *DAN'IS Asset & Server Management* mengisi dua peran RACI Chart dari *Chief Risk Officer* dan *Chief Information Officer* sebagai responden *Responsible* (pelaksana). Sedangkan tiga komponen lainnya tidak ditemukan deskripsi peran yang sesuai dengan nama jabatan pada divisi DAN'IS. Hasil pemetaan ini diperoleh berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.1 dan A.2. Selanjutnya merupakan tabel analisis dan perhitungan peran RACI Chart berdasarkan proses APO13 (*Manage Security*).

Tabel 4.3 Penentuan peran dari proses APO13

NO	PERAN	KOMPONEN			
		R	A	C	I
1	<i>Board</i>				
2	<i>Chief Executive Officer</i>			2	
3	<i>Chief Financial Officer</i>				
4	<i>Chief Operating Officer</i>			2	
5	Business Executive			3	
6	<i>Business Process Owners</i>	1		1	1
7	Strategy Executive Committee			3	
8	Steering (Programmes/Projects) Committee				2
9	<i>Project Management Office</i>	1			2



Tabel 4.3 Penentuan peran dari proses APO13 (lanjutan)

NO	PERAN	KOMPONEN			
		R	A	C	I
10	<i>Value Management Office</i>				
11	<i>Chief Risk Officer</i>			2	
12	Chief Information Security Officer		3		
13	<i>Architecture Board</i>			2	
14	<i>Enterprise Risk Committee</i>			2	
15	<i>Head Human Resource</i>				
16	Compliance			3	
17	Audit			3	
18	Chief Information Officer	3			
19	<i>Head Architect</i>	1		1	1
20	<i>Head Development</i>	1		1	1
21	<i>Head IT Operation</i>	1		1	1
22	Head IT Administration	3			
23	<i>Service Manager</i>	1		1	1
24	Information Security Manager	3			
25	<i>Business Continuity Manager</i>	1		2	
26	<i>Privacy Officer</i>	1		2	

Jika menganalisis nilai setiap peran pada Tabel 4.3, *Chief Information Officer*, *Head IT Administration*, dan *Information Security Manager* memiliki nilai tertinggi sebagai komponen *Responsible* (pelaksana) dengan angka 3. Kemudian, terdapat *Chief Information Security Officer* yang memiliki nilai tertinggi sebagai komponen *Accountable* (penanggung jawab) dengan angka 3. Terdapat pula *Business Executive*, *Strategy Executive Committee*, *Compliance*, dan *Auditor* yang memiliki nilai tertinggi sebagai komponen *Consulted* (penasihat) dengan angka 3. Sedangkan *Steering (Programmes/Projects) Committee* dan *Project Management Office* memiliki nilai tertinggi sebagai komponen *Informed* (terinformasi) dengan angka 2. Berikut tabel pemetaan peran RACI Chart yang terpilih berdasarkan struktur organisasi divisi *Danone Information Systems (DAN'IS)* melalui proses APO13 (*Manage Security*).

Tabel 4.4 Pemetaan peran pada proses APO13

KOMPONEN	PERAN	JABATAN PERUSAHAAN
Responsible (Penasihat)	<i>Information Security Manager</i>	<i>DAN'IS Security Analyst</i>
Accountable (Penanggung Jawab)	<i>Chief Information Security Officer</i>	<i>DAN'IS Security Analyst</i>
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ <i>Business Executive</i> ○ <i>Strategy Executive Committee</i> ○ <i>Compliance</i> ○ <i>Auditor</i> 	-
Informed (PENGinformasi)	<ul style="list-style-type: none"> ○ <i>Steering (Programmes/Projects) Committee</i> ○ <i>Project Management Office</i> 	-

Jika menganalisis hasil pemetaan pada Tabel 4.4, disimpulkan bahwa jabatan *DAN'IS Security Analyst* mengisi dua peran *RACI Chart* yang antara lain *Information Security Manager* sebagai *Responsible* (pelaksana) dan *Chief Information Security Officer* sebagai *Accountable* (penanggung jawab). Sedangkan dua komponen lainnya tidak ditemukan deskripsi peran yang sesuai dengan nama jabatan pada divisi *DAN'IS*. Hasil pemetaan ini diperoleh berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.1 dan A.2. Selanjutnya merupakan tabel analisis dan perhitungan peran *RACI Chart* berdasarkan proses *DSS05 (Manage Security Services)*.

Tabel 4.5 Penentuan peran dari proses DSS05

NO	PERAN	KOMPONEN			
		R	A	C	I
1	<i>Board</i>				
2	<i>Chief Executive Officer</i>				
3	<i>Chief Financial Officer</i>				
4	<i>Chief Operating Officer</i>				1
5	<i>Business Executive</i>				
6	<i>Business Process Owners</i>	2		1	3
7	<i>Strategy Executive Committee</i>				1
8	<i>Steering (Programmes/Projects) Committee</i>				



Tabel 4.5 Penentuan peran dari proses DSS05 (lanjutan)

NO	PERAN	KOMPONEN			
		R	A	C	I
9	<i>Project Management Office</i>				
10	<i>Value Management Office</i>				
11	<i>Chief Risk Officer</i>			5	2
12	Chief Information Security Officer		6		
13	<i>Architecture Board</i>				
14	<i>Enterprise Risk Committee</i>				
15	<i>Head Human Resource</i>	1			1
16	Compliance			7	
17	Audit			7	
18	<i>Chief Information Officer</i>		1	6	
19	Head Architect				6
20	<i>Head Development</i>	3		3	
21	Head IT Operation	7			
22	<i>Head IT Administration</i>				
23	Service Manager				6
24	<i>Information Security Manager</i>	6			
25	<i>Business Continuity Manager</i>				2
26	<i>Privacy Officer</i>			1	1

Jika menganalisis nilai setiap peran pada Tabel 4.5, *Head IT Operations* memiliki nilai tertinggi sebagai komponen *Responsible* (pelaksana) dengan angka 7. Kemudian, terdapat *Chief Information Security Officer* yang memiliki nilai tertinggi sebagai komponen *Accountable* (penanggung jawab) dengan angka 6. Terdapat pula *Compliance* dan *Auditor* yang memiliki nilai tertinggi sebagai komponen *Consulted* (penasihat) dengan angka 7. Sedangkan *Head Architect* dan *Service Manager* memiliki nilai tertinggi sebagai komponen *Informed* (terinformasi) dengan angka 6. Berikut tabel pemetaan peran RACI Chart yang terpilih berdasarkan struktur organisasi divisi *Danone Information Systems* (DAN'IS) melalui proses DSS05 (*Manage Security Services*).

Tabel 4.6 Pemetaan peran pada proses DSS05

KOMPONEN	PERAN	JABATAN PERUSAHAAN
Responsible (Penasihat)	<i>Head IT Operations</i>	<i>IT Onsite</i>
Accountable (Penanggung Jawab)	<i>Chief Information Security Officer</i>	<i>DAN'IS Security Analyst</i>
Consulted (Penasihat)	<ul style="list-style-type: none"> ○ <i>Compliance</i> ○ <i>Auditor</i> 	-
Informed (Pengeinformasi)	<ul style="list-style-type: none"> ○ <i>Head Architect</i> ○ <i>Service Manager</i> 	-

Jika menganalisis hasil pemetaan pada Tabel 4.6, disimpulkan bahwa jabatan *IT Onsite* dan *DAN'IS Security Analyst* mengisi dua peran RACI Chart yang antara lain *Head IT Operations* sebagai *Responsible* (pelaksana) dan *Chief Information Security Officer* sebagai *Accountable* (penanggung jawab). Sedangkan dua komponen lainnya tidak ditemukan deskripsi peran yang sesuai dengan nama jabatan pada divisi DAN'IS. Hasil pemetaan ini diperoleh berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.1 dan A.2.

4.2 Ensure Risk Optimization (EDM03)

Menurut ISACA (2012), EDM03 (*Ensure Risk Optimization*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang bertujuan memastikan risiko perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI) tidak melebihi *risk appetite* yang telah ditetapkan. *Risk appetite* merupakan suatu keadaan dimana perusahaan memilih untuk menerima, memantau, mempertahankan diri, atau memaksimalkan diri melalui peluang-peluang yang ada. Selain itu, tujuan lain dari proses EDM03 (*Ensure Risk Optimization*) adalah memastikan dampak risiko penggunaan teknologi informasi (TI) dapat diidentifikasi dan potensi kegagalan dapat diminimalisasi.

Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada EDM03 (*Ensure Risk Optimization*). Terdapat tiga *Base Practices* (BP) dari proses ini, antara lain yang pertama EDM03.01 atau mengevaluasi manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengevaluasi dan membuat penilaian tentang dampak langsung maupun jangka panjang dari risiko penggunaan teknologi informasi (TI) pada perusahaan. Kedua adalah EDM03.02 atau pengarahan manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengarahkan pengelolaan risiko untuk memastikan pengelolaannya tidak melebihi batas pertumbuhan risiko perusahaan.

Terakhir adalah EDM03.03 atau mengawasi manajemen risiko. Sesuai dengan artinya, proses ini bertujuan mengawasi tujuan dan matriks proses manajemen risiko, serta menyusun bagaimana masalah risiko teknologi informasi (TI) diidentifikasi, dilacak, dan dilaporkan. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, dijelaskan bahwa terjadi penurunan performa sistem karena kurangnya manajemen data. Hal ini berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI). Sebab, divisi *DAN'IS* telah menerapkan sistem informasi berbasis *Enterprise Resources Planing* (ERP) untuk beberapa perusahaan Danone, termasuk PT Tirta Investama (AQUA) Pandaan. Oleh karena itu, dilakukan observasi sebagai cara menganalisis permasalahan lebih dalam melalui studi lapangan secara langsung. Selanjutnya, melakukan wawancara dengan beberapa responden terpilih berdasarkan hasil pemetaan RACI *Chart* dari proses EDM03 (*Ensure Risk Optimization*).

Masing-masing responden terpilih antara lain pihak *DAN'IS Network Analyst* dan *DAN'IS Asset & Server Management* yang berperan sebagai *Responsible* (pelaksana). Namun, hanya pihak *DAN'IS Network Analyst* yang bersedia diwawancarai karena terhalangnya waktu dan tempat dari pihak *DAN'IS Asset & Server Management*. Proses wawancara ini, dilakukan secara langsung (tatap muka) sebanyak dua kali menggunakan lembar *checklist* dari proses EDM03 (*Ensure Risk Optimization*). Lembar *checklist* yang dimaksud terlampir pada Lampiran B.1. Wawancara pertama dilakukan sebagai pencarian data atau bukti (*evidence*) dengan pihak *DAN'IS Network Analyst*, sedangkan wawancara kedua dilakukan dengan pihak *IT Onsite* sebagai validasi data berdasarkan hasil wawancara pertama. Setelah memperoleh data atau bukti (*evidence*) yang valid, dilakukan penilaian tingkat kapabilitas (*capability level*) melalui lembar penilaian dari proses EDM03 (*Ensure Risk Optimization*). Lembar penilaian terlampir pada Lampiran C.1.

Pengisian lembar penilaian dilakukan secara individu (*self assessment*) yang hasilnya dilaporkan pada dua responden terkait sebagai proses triangulasi data. Pengisian dilakukan secara individu (*self assessment*) karena keterbatasan waktu yang dimiliki oleh setiap responden. Pada lembar penilaian terdapat sepuluh kolom tabel yang masing-masing terdiri dari tingkat indikator proses kapabilitas, proses atribut, kriteria, validasi kriteria, kategori penilaian (*Not Achieved*, *Partially Achieved*, *Largely Achieved*, dan *Fully Achieved*) dan keterangan dari *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP). Pengisian sepuluh kolom tabel didasarkan atas hasil temuan pada lembar *checklist* melalui analisis, perhitungan, dan pemetaan pada kategori penilaian (*Not Achieved*, *Partially Achieved*, *Largely Achieved*, dan *Fully Achieved*) maupun keterangan dari *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP). Setelah dilakukan pengisian lembar penilaian untuk proses EDM03 (*Ensure Risk Optimization*), diketahui tingkat kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved* (F) dari dua atribut proses yang ada.

Pada *level 3 (established process)*, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Berdasarkan Lampiran C.1 pada *level 1 (performed process)*, divisi DAN'IS telah menerapkan *Base Practices (BP)* berdasarkan dua kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil mencapai kategori *Fully Achieved (F)* pada *level* ini. Dua kriteria yang dimaksud merupakan atribut proses pertama (PA 1.1) dari *level 1 (performed process)*. *Base Practices (BP)* yang telah diterapkan pada *level* ini antara lain yang pertama penerapan kebijakan *IS User Access Authorization*. Kebijakan ini berisi tentang tata cara atau panduan dalam membuat dan menjaga akun pengguna untuk mengakses informasi perusahaan berdasarkan hak akses masing-masing. Dengan adanya kebijakan ini, memudahkan para staf atau pegawai dalam membuat dan mengubah jenis karakter akun mereka melalui tata cara atau panduan yang ada. Selain itu, juga memudahkan divisi DAN'IS dalam menggolongkan akun berdasarkan jenis identitas setiap pengguna.

Work Product (WP) yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Kedua adalah penerapan kebijakan dari *SAP user* beserta *T-Code*. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, *SAP user* merupakan kependekan dari *System Analysis and Program Development*, yaitu suatu perangkat lunak (*software*) yang dikembangkan untuk mendukung suatu organisasi dalam menjalankan kegiatan operasionalnya agar lebih efisien dan efektif. Sedangkan *T-Code* adalah sebuah modul mengenai tata cara atau panduan khusus yang dibuat oleh divisi DAN'IS untuk mengelola setiap aktivitas teknologi informasi (TI) sehingga meminimalisir risiko yang datang. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *Danone Government (DanGo)* pada Bab *IT Operations Control*. Ketiga adalah penerapan kebijakan terkait pengawasan manajemen risiko pada seluruh perusahaan Danone.

Salah satu contoh kebijakan ini adalah membatasi dan menyesuaikan jumlah pengguna aset teknologi informasi (TI) pada setiap perusahaan Danone. Sehingga memudahkan divisi DAN'IS dalam melacak jumlah dan aktivitas dari setiap pengguna yang telah ditetapkan. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *Danone Government (DanGo)* pada Bab *IS Interconnection Authorization*. Terakhir adalah kebijakan dalam mendokumentasikan hasil pelaksanaan kegiatan dalam bentuk dokumen resmi perusahaan. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *Danone Government (DanGo)* pada Bab *Archiving Procedures*. Selanjutnya pada *level 2 (managed process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 2.1) dari *level 2 (managed process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi setiap tujuan dari proses kinerja perusahaan.

Kedua adalah kebijakan merencanakan dan memantau proses kinerja untuk memenuhi setiap tujuan yang telah diidentifikasi sebelumnya. Ketiga adalah kebijakan menyesuaikan performa proses dari setiap kinerja, seperti mengetahui tindakan apakah yang diambil ketika sebuah kinerja belum tercapai. Keempat adalah kebijakan menentukan tanggung jawab dan pihak yang berwenang untuk melakukan setiap proses kinerja. Kelima adalah kebijakan mengidentifikasi dan membuat ketersediaan sumber daya untuk melakukan proses kinerja sesuai dengan rencana. *Generic Work Product (GWP)* yang dihasilkan dari kelima *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Terakhir adalah kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat, seperti individu dan kelompok yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *IS Interconnection Authorization*.

Setelah mendeskripsikan hasil atribut proses pertama pada *level 2 (managed process)*, selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 2.2) pada *level 2 (managed process)*. Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan empat kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menentukan persyaratan untuk hasil atau produk kerja, termasuk konten, struktur, dan kualitas dari suatu kriteria. Kedua adalah kebijakan menentukan persyaratan untuk pendokumentasian dan pengelolaan hasil atau produk kerja. Ketiga adalah mengidentifikasi, mendokumentasikan, dan mengelola hasil atau produk kerja. Terakhir adalah kebijakan meninjau dan menyesuaikan hasil atau produk kerja agar memenuhi kriteria yang ditetapkan. *Generic Work Product (GWP)* yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *Production Systems Management*.

Kemudian pada *level 3 (established process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* sesuai lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Lima kriteria yang dimaksud merupakan atribut proses pertama (PA 3.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menetapkan sebuah standar proses yang mendukung pendefinisian setiap proses. Kedua adalah kebijakan menentukan urutan dan interaksi antar proses sebagai pembuktian bahwa mereka saling terintegrasi. Ketiga adalah kebijakan mengidentifikasi setiap peran dan kompetensi untuk melakukan standar proses kinerja. Keempat adalah kebijakan mengidentifikasi lingkungan kerja dan infrastruktur yang dibutuhkan untuk melakukan standar proses. *Generic Work Product (GWP)* yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Global Information Policy*.

Terakhir adalah kebijakan menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses, termasuk menyesuaikan proses yang telah didefinisikan sebelumnya dan menyiapkan kebutuhan untuk audit internal dan pengelolaan ulang. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*. Setelah mendeskripsikan hasil atribut proses pertama pada *level 3 (established process)*, selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 3.2) pada *level 3 (established process)*. Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria. Kedua adalah menetapkan dan mengkomunikasikan peran, tanggung jawab, serta otoritas untuk melakukan pendefinisian proses.

Ketiga adalah memastikan kompetensi yang diperlukan untuk melakukan pendefinisian proses. *Generic Work Product (GWP)* yang dihasilkan dari ketiga *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Human Resources Security*. Keempat adalah kebijakan menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Kelima adalah kebijakan menyediakan infrastruktur yang memadai untuk mendukung proses kinerja. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *IS-IT Critical Asset*. Terakhir adalah kebijakan mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*.

Terakhir pada *level 4 (predictable process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 4.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi kebutuhan proses informasi berdasarkan tujuan bisnis. Kedua adalah kebijakan memperoleh hasil pengukuran tujuan dari kebutuhan informasi. Ketiga adalah menetapkan tujuan kuantitatif untuk proses kinerja yang telah didefinisikan agar dapat berguna bagi perusahaan. Keempat adalah kebijakan mengidentifikasi hasil atau produk dan tata cara proses yang mendukung pencapaian tujuan kuantitatif untuk proses kinerja. Kelima adalah kebijakan mengumpulkan hasil atau produk dan pengukuran proses melalui pendefinisian proses. Terakhir adalah kebijakan menggunakan hasil pengukuran untuk memantau dan memverifikasi pencapaian tujuan dari proses kinerja.

Generic Work Product (GWP) yang dihasilkan dari keenam *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Setelah mendeskripsikan hasil atribut proses pertama pada 4 (*predictable process*), selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 4.2) pada level 4 (*predictable process*). Pada atribut proses ini, divisi DAN'IS hanya dapat menerapkan satu *Generic Practices (GP)* dari lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini hanya dapat meraih kategori *Partially Achieved (P)*. Kategori ini diperoleh dari hasil pembagian persentase penuh (100%) dengan lima kriteria yang ada dan dikalikan pada satu *Generic Practices (GP)* yang telah diterapkan. Maka, perhitungan itu akan menghasilkan persentase sebesar 20% dan termasuk pada kategori *Partially Achieved (P)*. Menurut ISACA (2013), kategori *Partially Achieved (P)* tidak memenuhi syarat untuk bertahan maupun berlanjut dari *level* saat itu. Sehingga hasil penilaian proses ini berada pada *level 3 (established process)*.

Terdapat beberapa bukti (*evidences*) yang diperoleh dari hasil wawancara dengan pihak *DAN'IS Network Analyst*. Namun, tampilan bukti (*evidence*) yang diperoleh sangat terbatas karena bersifat rahasia (*confidential*). Beberapa bukti (*evidences*) itu ditunjukkan pada Gambar 4.1 dan 4.2. Diketahui kedua gambar merupakan kumpulan *file* yang mewakili seluruh *Work Product (WP)* dan *Generic Work Product (GWP)* dari penerapan *Base Practices (BP)* dan *Generic Practices (GP)* oleh divisi DAN'IS. Pada Gambar 4.1, merupakan *Work Product (WP)* dan *Generic Work Product (GWP)* dari penerapan *IS Security Policy*. Berdasarkan hasil pemetaan pada Tabel 4.7, dokumen Bab *Controlling Access to Information* merupakan *Work Product (WP)* dari proses EDM03 (*Ensure Risk Optimization*). Dokumen ini tercantum pada Gambar 4.1a. Dokumen Bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan.

Sedangkan dokumen Bab *Business Continuity Plan*, *Global Information Policy*, *Asset Management and Data Classification*, *Human Resources Security*, dan *Controlling Access to Information* merupakan *Generic Work Product (GWP)* dari proses EDM03 (*Ensure Risk Optimization*). Setiap dokumen *Generic Work Product (GWP)* memiliki definisi masing-masing. Dokumen Bab *Business Continuity Plan* mendefinisikan hasil kebijakan dan identifikasi dari setiap tujuan dan risiko bisnis. Setiap aktivitas diselaraskan dengan teknologi informasi (TI) sehingga menunjang proses bisnis agar lebih efektif. Dokumen ini tercantum pada Gambar 4.1d. Selanjutnya, dokumen Bab *Global Information Policy* mendefinisikan keseluruhan informasi tentang prosedur aktivitas yang dilakukan pada setiap unit perusahaan, termasuk pengelolaan aset teknologi informasi (TI) secara garis besar. Dokumen ini tercantum pada Gambar 4.1b.

Kemudian, dokumen Bab *Asset Management and Data Classification* mendefinisikan hasil kebijakan dan panduan mengelola aset teknologi informasi (TI), serta klasifikasi data (*mining data*). Dokumen ini tercantum pada Gambar 4.1c. Setelah itu, dokumen Bab *Human Resources Security* mendefinisikan hasil kebijakan dan identifikasi keamanan dari setiap sumber daya manusia pada perusahaan. Dokumen ini tercantum pada Gambar 4.1e. Terakhir, dokumen Bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan. Dokumen ini tercantum pada Gambar 4.1a.

	Date modified	Type	Size
- Endpoints Security Policy.pdf	5/19/2016 4:40 PM	Adobe Acrobat D...	76 KB
- DMZ Security Policy.html	5/19/2016 4:39 PM	HTML Document	35 KB
- Protection against malicious and mobile cod...	5/19/2016 4:39 PM	HTML Document	11 KB
a - Controlling Access to Information.html	5/19/2016 4:39 PM	HTML Document	36 KB
- Sever Security Policy - DRAFT.html	5/19/2016 4:40 PM	HTML Document	35 KB
1 - VMWare Security guidelines.html	5/19/2016 4:40 PM	HTML Document	21 KB
- Network Access Policy.html	5/19/2016 4:40 PM	HTML Document	42 KB
1 - Internal Network Segmentation Policy.html	5/19/2016 4:41 PM	HTML Document	29 KB
2 - Network Access Control.html	5/19/2016 4:41 PM	HTML Document	14 KB
- Application Security.html	5/19/2016 4:41 PM	HTML Document	10 KB
- Backup and Restore Policy.html	5/19/2016 4:41 PM	HTML Document	49 KB
- Password Management Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
- Mobile Devices.html	5/19/2016 4:42 PM	HTML Document	13 KB
- Datacenter Security.html	5/19/2016 4:36 PM	HTML Document	204 KB
- Extranet Access Policy(1).html	5/19/2016 4:43 PM	HTML Document	35 KB
- Extranet Access Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
b - Global Information Policy.doc	5/19/2016 4:38 PM	Microsoft Word 9...	102 KB
- Sending Electronic Email.doc	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
- Incoming Electronic Email.doc	5/19/2016 4:39 PM	Microsoft Word 9...	66 KB
- Setting up an Internet Access.doc	5/19/2016 4:39 PM	Microsoft Word 9...	69 KB
- Setting up an Extranet.doc	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
c - Asset Management and Data Classification.d...	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
d - Business Continuity Plan.doc	5/19/2016 4:41 PM	Microsoft Word 9...	63 KB
- Staff Security Training.doc	5/19/2016 4:42 PM	Microsoft Word 9...	63 KB
- Communication softwares and Internet Dow...	5/19/2016 4:42 PM	Microsoft Word 9...	75 KB
e - Human Resource Security.doc	5/19/2016 4:42 PM	Microsoft Word 9...	72 KB

Gambar 4.1 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak *DAN'IS Network Analyst*.

Selanjutnya, Gambar 4.2 merupakan *Work Product* (WP) dan *Generic Work Product* (GWP) dari penerapan dokumen *Danone Government* (DanGo) yang meliputi kebijakan *IS User Access Authorization, System Analysis and Program Development* (SAP) user beserta modul *T-Code*, dan beberapa kebijakan lainnya pada Lampiran B.1. Berdasarkan hasil pemetaan pada Tabel 4.7, dokumen Bab *IT Operations Control, IS Interconnection Authorization, dan Archiving Procedures* merupakan *Work Product* (WP) dari proses EDM03 (*Ensure Risk Optimization*). Setiap dokumen *Work Product* (WP) memiliki definisi masing-masing. Dokumen Bab *IT Operations Control* mendefinisikan hasil kebijakan dan panduan mengelola setiap aktivitas yang berkaitan dengan teknologi informasi (TI). Dokumen ini tercantum pada Gambar 4.2d.



Selanjutnya, dokumen Bab *IS Interconnection Authorization* mendefinisikan hasil kebijakan dan panduan terhadap konektivitas antar unit teknologi informasi (TI) maupun unit-unit yang lain. Dokumen ini tercantum pada Gambar 4.2c. Terakhir, dokumen Bab *Archiving Procedures* mendefinisikan hasil penerapan dari kebijakan pendokumentasian hasil pelaksanaan kebijakan dalam bentuk dokumen resmi perusahaan. Dokumen ini tercantum pada Gambar 4.2e. Sedangkan dokumen Bab *IS Interconnection Authorization, Production Systems Management, dan Critical IS-IT Asset* merupakan *Generic Work Product (GWP)* dari proses EDM03 (*Ensure Risk Optimization*). Setiap dokumen *Generic Work Product (GWP)* memiliki definisi masing-masing.

Dokumen Bab *IS Interconnection Authorization* mendefinisikan hasil kebijakan dan panduan terhadap konektivitas antar unit teknologi informasi (TI) maupun unit-unit yang lain. Dokumen ini tercantum pada Gambar 4.2c. Selanjutnya, dokumen Bab *Production Systems Management* mendefinisikan hasil kebijakan dan panduan mengelola hasil akhir dari setiap aktivitas teknologi informasi (TI) pada perusahaan. Sehingga pengemasan dari setiap produk selaras dalam satu *template* yang telah ditetapkan perusahaan. Dokumen ini tercantum pada Gambar 4.2b. Terakhir, dokumen Bab *Critical IS-IT Asset* mendefinisikan hasil kebijakan dan informasi setiap aset penting dari teknologi informasi (TI). Tujuannya untuk dirawat dan dikelola dengan bijaksana. Dokumen ini tercantum pada Gambar 4.2a.

Name	Date modified	Type	Size
- SLA	3/22/2017 6:27 AM	File folder	
- IS Security Officer	3/22/2017 6:39 AM	File folder	
- Critical IS-IT Asset	3/22/2017 6:39 AM	File folder	
- IS Backup	3/22/2017 6:39 AM	File folder	
- IT Vulnerability	3/22/2017 6:40 AM	File folder	
- Data Network Management	3/22/2017 6:41 AM	File folder	
- IS Authentication policy	3/22/2017 6:43 AM	File folder	
- IS User Access Authorization	3/22/2017 6:45 AM	File folder	
- Production systems management	3/22/2017 6:45 AM	File folder	
- DRP	3/22/2017 6:49 AM	File folder	
- IS Local Legislation	3/22/2017 6:49 AM	File folder	
- Intrusion Followup	3/22/2017 6:50 AM	File folder	
- Internet access	3/22/2017 6:50 AM	File folder	
- Public Servers	3/22/2017 6:50 AM	File folder	
- Remote Access	3/22/2017 6:50 AM	File folder	
- IS Security Policy	3/22/2017 6:50 AM	File folder	
- IS Protection Mobile Devices	3/22/2017 6:51 AM	File folder	
- IS Interconnection authorization	3/22/2017 6:51 AM	File folder	
- IT Problem Tracking	3/22/2017 6:55 AM	File folder	
- IT operations control	3/22/2017 5:13 AM	File folder	
- Archiving Procedures	3/22/2017 6:56 AM	File folder	

Gambar 4.2 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak *DAN'IS Network Analyst*.

Berikut adalah hasil pemetaan dari jenis kebijakan atau dokumen pada proses EDM03 (*Ensure Risk Optimization*). Hasil pemetaan ini berdasarkan proses analisis menggunakan lembar *checklist* dan penilaian yang kemudian ditulis pada Tabel 4.7. Terdapat dua kolom tabel yang terdiri dari kolom jenis kebijakan atau dokumen dan nama kebijakan atau dokumen.

Tabel 4.7 Pemetaan kebijakan/dokumen (EDM03)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
Base Practices (BP)	<ul style="list-style-type: none"> ○ Kebijakan <i>IS User Access Authorization</i>. ○ Kebijakan <i>SAP user & T-Code</i>. ○ Kebijakan pembatasan dan penyesuaian jumlah pengguna aset teknologi informasi (TI) pada masing-masing perusahaan Danone.
Work Product (WP)	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IT Operations Control</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Archiving Procedures</i>.
Generic Practices (GP)	<ul style="list-style-type: none"> ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan setiap tujuan dari proses kinerja pada perusahaan. ○ Kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif. ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan hasil atau produk kerja. ○ Kebijakan untuk mengidentifikasi dan menentukan standar proses kinerja. ○ Kebijakan untuk menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses kinerja. ○ Kebijakan untuk memastikan dan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria. ○ Kebijakan untuk menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses kinerja. ○ Kebijakan untuk menyediakan infrastruktur yang memadai untuk



Tabel 4.7 Pemetaan kebijakan/dokumen (EDM03) (lanjutan)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
	<p>mendukung proses kinerja.</p> <ul style="list-style-type: none"> ○ Kebijakan untuk mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. ○ Kebijakan untuk mengidentifikasi, memperoleh, dan menetapkan kebutuhan proses informasi berdasarkan tujuan bisnis. ○ Kebijakan untuk menentukan teknik-teknik yang tepat untuk mengendalikan proses kinerja.
<p>Generic Work Product (GWP)</p>	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Business Continuity Plan</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IS Interconnection Authorization</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Production Systems Management</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Global Information Policy</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Asset Management and Data Classification</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Human Resources Security</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. <p>Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Critical IS-IT Asset</i>.</p>

Setelah dilakukan analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian, maka diketahui hasil tingkat kapabilitas (*capability level*) dari proses EDM03 (*Ensure Risk Optimization*) seperti Tabel 4.8. Diketahui pengisian kategori penilaian berhenti pada *level 4 (predictable process)* dengan kategori *Partially Achieved (P)* pada atribut proses kedua.

Menurut ISACA (2013), bila terdapat kategori *Partially Achieved* (P) pada salah satu atribut proses, maka hasil penilaian akan berhenti pada *level* sebelumnya. Hal ini menunjukkan bahwa pencapaian tingkat kapabilitas (*capability level*) dari proses EDM03 (*Ensure Risk Optimization*) terletak pada *level 3 (established process)*. Seperti deskripsi paragraf sebelumnya, hasil penilaian ini telah dilaporkan pada dua responden terkait sebagai proses triangulasi data.

Tabel 4.8 Perhitungan dari lembar penilaian (EDM03)

NAMA PROSES	LEVEL 0	LEVEL 1	LEVEL 2		LEVEL 3		LEVEL 4		LEVEL 5	
		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 Berdasarkan Kriteria		F	F	F	F	F	F	P	-	-
Pencapaian Tingkat Kapabilitas					3					
Keterangan: N (<i>Not Achieved</i> , 0%-15%), P (<i>Partially Achieved</i> , >15%-50%), L (<i>Largely Achieved</i> , >50%-85%), F (<i>Fully Achieved</i> , >85%-100%)										

Berikut hasil tingkat kapabilitas (*capability level*) dari proses EDM03 (*Ensure Risk Optimization*) pada Tabel 4.9. Seperti deskripsi paragraf sebelumnya, hasil tingkat kapabilitas (*capability level*) ini diperoleh dari analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian. Sehingga diketahui tingkat kapabilitas (*capability level*) dari proses EDM03 (*Ensure Risk Optimization*) terletak pada *level 3 (established process)*. Sedangkan nilai *targeted level* diperoleh dari hasil wawancara bersama dua responden terkait berdasarkan proses ini. Pada Tabel 4.9, diketahui *targeted level* divisi DAN'IS dari proses EDM03 (*Ensure Risk Optimization*) berada pada *level 4 (predictable process)*. Pada *level* ini, proses teknologi informasi (TI) dilakukan secara konsisten dengan batasan yang telah ditentukan.

Tabel 4.9 Hasil tingkat kapabilitas dari proses EDM03

NAMA PROSES	TARGET LEVEL	TINGKAT KAPABILITAS					
		0	1	2	3	4	5
EDM03	4				3		



4.3 Manage Security (APO13)

Menurut ISACA (2012), APO13 (*Manage Security*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang mendefinisikan, mengoperasikan, dan mengawasi keamanan informasi. Selain itu, bertujuan agar risiko keamanan informasi masih bisa diterima oleh perusahaan sesuai batas yang telah ditentukan. Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada APO13 (*Manage Security*). Proses ini memiliki tiga macam *Base Practices* (BP), antara lain yang pertama APO13.01 atau menetapkan dan memelihara sistem manajemen keamanan informasi. Sesuai dengan artinya, proses ini bertujuan membangun dan memelihara *Information Security Management System* (ISMS) yang menyediakan pendekatan standar maupun formal secara terus menerus untuk manajemen keamanan informasi. Selain itu, memastikan keamanan teknologi dan proses bisnis selaras dengan kebutuhan bisnis dan manajemen keamanan. Kedua adalah APO13.02 atau menentukan dan merencanakan penanganan risiko keamanan informasi.

Sesuai dengan artinya, proses ini bertujuan mempertahankan rencana keamanan informasi dan menjelaskan bagaimana menyelaraskan antara strategi dan arsitektur perusahaan dengan pengelolaan risiko keamanan informasi. Selain itu, memastikan rekomendasi perbaikan keamanan didasarkan atas kasus bisnis yang telah disetujui dan dilaksanakan sebagai cara untuk mengembangkan solusi dan layanan aktivitas bisnis. Terakhir adalah APO13.03 atau mengawasi dan meninjau ulang (*review*) sistem manajemen keamanan informasi. Sesuai dengan artinya, proses ini bertujuan mempertahankan manfaat dari hasil perbaikan keamanan informasi secara terus menerus. Selain itu, mengumpulkan dan menganalisis data tentang sistem manajemen keamanan informasi, serta meningkatkan efektivitas dari sistem yang ada. Kemudian, aktif dalam menjaga budaya keamanan dengan cara rutin melakukan perbaikan sehingga mencegah risiko keamanan yang datang. Berdasarkan hasil pemetaan responden menggunakan *RACI Chart*, pihak *DAN'IS Security Analyst* merupakan responden utama dari proses APO13 (*Manage Security*).

Namun, pihak ini berhalangan dalam kegiatan wawancara sehingga diwakili oleh pihak *DAN'IS Network Analyst*. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, dijelaskan bahwa belum terjaminnya seluruh keamanan data. Terkadang data dapat diakses oleh pihak luar. Akan berakibat fatal bila jenis data yang terekspos sangat vital bagi perusahaan. Sebab, risiko penyalahgunaan data akan terus terjadi. Oleh karena itu, dilakukan observasi sebagai cara untuk menganalisis permasalahan lebih dalam melalui studi lapangan secara langsung. Selanjutnya, melakukan wawancara dengan beberapa responden terpilih berdasarkan hasil pemetaan *RACI Chart* dari proses APO13 (*Manage Security*). Dalam hal ini, pihak responden diwakili oleh *DAN'IS Network Analyst* yang berperan sebagai *Responsible* (pelaksana) dan *Accountable* (penanggung jawab). Proses wawancara ini, dilakukan secara langsung (tatap muka) sebanyak dua kali menggunakan lembar *checklist* dari proses APO13 (*Manage Security*).

Lembar *checklist* ini terlampir pada Lampiran B.2. Wawancara pertama dilakukan sebagai pencarian data atau bukti (*evidence*) dengan pihak *DAN'IS Network Analyst*, sedangkan wawancara kedua dilakukan dengan pihak *IT Onsite* sebagai validasi data berdasarkan hasil wawancara pertama. Setelah memperoleh data atau bukti (*evidence*) yang valid, dilakukan penilaian tingkat kapabilitas (*capability level*) melalui lembar penilaian dari proses APO13 (*Manage Security*). Lembar penilaian ini terlampir pada Lampiran C.2. Pengisian lembar penilaian dilakukan secara individu (*self assessment*) yang hasilnya dilaporkan pada dua responden terkait sebagai proses triangulasi data. Pengisian dilakukan secara individu (*self assessment*) karena keterbatasan waktu yang dimiliki oleh setiap responden. Pada lembar penilaian terdapat sepuluh kolom tabel yang masing-masing terdiri dari tingkat indikator proses kapabilitas, proses atribut, kriteria, validasi kriteria, kategori penilaian (*Not Achieved, Partially Achieved, Largely Achieved, dan Fully Achieved*) dan keterangan dari *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP).

Pengisian sepuluh kolom tabel didasarkan atas hasil temuan pada lembar *checklist* melalui analisis, perhitungan, dan pemetaan pada kategori penilaian (*Not Achieved, Partially Achieved, Largely Achieved, dan Fully Achieved*) maupun keterangan dari *Base Practices* (BP), *Work Product* (WP), *Generic Practices* (GP), dan *Generic Work Product* (GWP). Setelah dilakukan pengisian lembar penilaian pada proses APO13 (*Manage Security*), diketahui tingkat indikator proses kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved* (F) dari dua atribut proses yang ada. Pada *level 3 (established process)*, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Berdasarkan Lampiran C.2 pada *level 1 (performed process)*, divisi *DAN'IS* telah menerapkan *Base Practices* (BP) berdasarkan dua kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved* (F) pada *level* ini.

Dua kriteria yang dimaksud merupakan atribut proses pertama (PA 1.1) dari *level 1 (performed process)*. *Base Practices* (BP) yang telah diterapkan pada *level* ini antara lain yang pertama penerapan kebijakan *IS Security Policy*. Kebijakan ini berisi tentang tata cara atau panduan dalam menjaga privasi informasi dari setiap aset yang digunakan oleh seluruh perusahaan Danone dengan standar yang telah ditentukan. Selain itu, kebijakan itu mendorong agar keamanan informasi selaras dengan kebutuhan bisnis dari setiap perusahaan Danone. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *IS Security Policy* pada Bab *Data Center Security*. Kedua, juga dilakukan penerapan yang sama pada kebijakan *IS Security Policy*. Namun, penerapannya difokuskan untuk mempertahankan rencana keamanan informasi dari seluruh perusahaan Danone. Rencana yang ada tentu diselaraskan dengan strategi dan arsitektur dari setiap perusahaan Danone. Selain itu, kebijakan *IS Security Policy* juga mendeskripsikan mengenai rekomendasi perbaikan keamanan bilamana terjadi sesuatu hal yang tidak diinginkan.

Work Product (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Ketiga adalah penerapan kebijakan *IS User Access Authorization*. Kebijakan ini berisi tentang data dan informasi dari hasil perbaikan keamanan informasi pada seluruh perusahaan Danone. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *IS Security Policy* pada Bab *Data Center Security*. Terakhir adalah kebijakan dalam mendokumentasikan hasil pelaksanaan kegiatan dalam bentuk dokumen resmi perusahaan. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *Danone Government* (DanGo) pada Bab *Archiving Procedures*. Selanjutnya pada *level 2* (*managed process*), divisi DAN'IS telah menerapkan *Generic Practices* (GP) berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved* (F) pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 2.1) dari *level 2* (*managed process*).

Generic Practices (GP) yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi setiap tujuan dari proses kinerja perusahaan. Kedua adalah kebijakan merencanakan dan memantau proses kinerja untuk memenuhi setiap tujuan yang telah diidentifikasi sebelumnya. Ketiga adalah kebijakan menyesuaikan performa proses dari setiap kinerja, seperti mengetahui tindakan apakah yang diambil ketika sebuah kinerja belum tercapai. Keempat adalah kebijakan menentukan tanggung jawab dan pihak yang berwenang untuk melakukan setiap proses kinerja. Kelima adalah kebijakan mengidentifikasi dan membuat ketersediaan sumber daya untuk melakukan proses kinerja sesuai dengan rencana. *Generic Work Product* (GWP) yang dihasilkan dari kelima *Generic Practices* (GP) itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Terakhir adalah kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat, seperti individu dan kelompok yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif.

Generic Work Product (GWP) yang dihasilkan dari *Generic Practices* (GP) itu adalah dokumen *Danone Government* (DanGo) pada Bab *IS Interconnection Authorization*. Setelah mendeskripsikan hasil atribut proses pertama pada *level 2* (*managed process*), selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 2.2) pada *level 2* (*managed process*). Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices* (GP) berdasarkan empat kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved* (F) pada *level* ini. *Generic Practices* (GP) yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menentukan persyaratan untuk hasil atau produk kerja, termasuk konten, struktur, dan kualitas dari suatu kriteria. Kedua adalah kebijakan menentukan persyaratan untuk pendokumentasian dan pengelolaan hasil atau produk kerja. Ketiga adalah mengidentifikasi, mendokumentasikan, dan mengelola hasil atau produk kerja. Terakhir adalah kebijakan meninjau dan menyesuaikan hasil atau produk kerja agar memenuhi kriteria yang ditetapkan.

Generic Work Product (GWP) yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *Production Systems Management*. Kemudian pada *level 3 (established process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* sesuai lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Lima kriteria yang dimaksud merupakan atribut proses pertama (PA 3.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menetapkan sebuah standar proses yang mendukung pendefinisian setiap proses. Kedua adalah kebijakan menentukan urutan dan interaksi antar proses sebagai pembuktian bahwa mereka saling terintegrasi. Ketiga adalah kebijakan mengidentifikasi setiap peran dan kompetensi untuk melakukan standar proses kinerja. Keempat adalah kebijakan mengidentifikasi lingkungan kerja dan infrastruktur yang dibutuhkan untuk melakukan standar proses.

Generic Work Product (GWP) yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Global Information Policy*. Terakhir adalah kebijakan menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses, termasuk menyesuaikan proses yang telah didefinisikan sebelumnya dan menyiapkan kebutuhan untuk audit internal dan pengelolaan ulang. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*. Setelah mendeskripsikan hasil atribut proses pertama pada *level 3 (established process)*, selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 3.2) pada *level 3 (established process)*. Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria.

Kedua adalah menetapkan dan mengkomunikasikan peran, tanggung jawab, serta otoritas untuk melakukan pendefinisian proses. Ketiga adalah memastikan kompetensi yang diperlukan untuk melakukan pendefinisian proses. *Generic Work Product (GWP)* yang dihasilkan dari ketiga *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Human Resources Security*. Keempat adalah kebijakan menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Kelima adalah kebijakan menyediakan infrastruktur yang memadai untuk mendukung proses kinerja. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *IS-IT Critical Asset*. Terakhir adalah kebijakan mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*.

Terakhir pada *level 4 (predictable process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 4.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi kebutuhan proses informasi berdasarkan tujuan bisnis. Kedua adalah kebijakan memperoleh hasil pengukuran tujuan dari kebutuhan informasi. Ketiga adalah menetapkan tujuan kuantitatif untuk proses kinerja yang telah didefinisikan agar dapat berguna bagi perusahaan. Keempat adalah kebijakan mengidentifikasi hasil atau produk dan tata cara proses yang mendukung pencapaian tujuan kuantitatif untuk proses kinerja. Kelima adalah kebijakan mengumpulkan hasil atau produk dan pengukuran proses melalui pendefinisian proses. Terakhir adalah kebijakan menggunakan hasil pengukuran untuk memantau dan memverifikasi pencapaian tujuan dari proses kinerja.

Generic Work Product (GWP) yang dihasilkan dari keenam *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Setelah mendeskripsikan hasil atribut proses pertama pada 4 (*predictable process*), selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 4.2) pada *level 4 (predictable process)*. Pada atribut proses ini, divisi DAN'IS hanya dapat menerapkan satu *Generic Practices (GP)* dari lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini hanya dapat meraih kategori *Partially Achieved (P)*. Kategori ini diperoleh dari hasil pembagian persentase penuh (100%) dengan lima kriteria yang ada dan dikalikan pada satu *Generic Practices (GP)* yang telah diterapkan. Maka, perhitungan itu akan menghasilkan persentase sebesar 20% dan termasuk pada kategori *Partially Achieved (P)*. Menurut ISACA (2013), kategori *Partially Achieved (P)* tidak memenuhi syarat untuk bertahan maupun berlanjut dari *level* saat itu. Sehingga hasil penilaian proses ini berada pada *level 3 (established process)*.

Terdapat beberapa bukti (*evidences*) yang diperoleh dari hasil wawancara dengan pihak *DAN'IS Network Analyst*. Namun, tampilan bukti (*evidence*) yang diperoleh sangat terbatas karena bersifat rahasia (*confidential*). Beberapa bukti (*evidences*) itu ditunjukkan pada Gambar 4.3 dan 4.4. Diketahui kedua gambar merupakan kumpulan *file* yang mewakili seluruh *Work Product (WP)* dan *Generic Work Product (GWP)* dari penerapan *Base Practices (BP)* dan *Generic Practices (GP)* oleh divisi DAN'IS. Pada Gambar 4.3, merupakan *Work Product (WP)* dan *Generic Work Product (GWP)* dari penerapan *IS Security Policy*. Berdasarkan hasil pemetaan pada Tabel 4.10, dokumen Bab *Data Center Security* dan *Controlling Access to Information* merupakan *Work Product (WP)* dari proses APO13 (*Manage Security*). Setiap dokumen *Work Product (WP)* memiliki definisi masing-masing. Dokumen Bab *Data Center Security* mendefinisikan hasil kebijakan dan panduan mengelola keamanan dari seluruh data yang ada, termasuk hasil klasifikasi data (*mining data*). Dokumen ini tercantum pada Gambar 4.3c.

Terakhir, dokumen Bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan. Dokumen ini tercantum pada Gambar 4.3a. Sedangkan dokumen Bab *Business Continuity Plan, Global Information Policy, Asset Management and Data Classification, Human Resources Security*, dan *Controlling Access to Information* merupakan *Generic Work Product (GWP)* dari proses APO13 (*Manage Security*). Setiap dokumen *Generic Work Product (GWP)* memiliki definisi masing-masing. Dokumen Bab *Business Continuity Plan* mendefinisikan hasil kebijakan dan identifikasi dari setiap tujuan dan risiko bisnis. Setiap aktivitas diselaraskan dengan teknologi informasi (TI) sehingga menunjang proses bisnis agar lebih efektif. Dokumen ini tercantum pada Gambar 4.3e.

	Date modified	Type	Size
- Endpoints Security Policy.pdf	5/19/2016 4:40 PM	Adobe Acrobat D...	76 KB
- DMZ Security Policy.html	5/19/2016 4:39 PM	HTML Document	35 KB
- Protection against malicious and mobile cod...	5/19/2016 4:39 PM	HTML Document	11 KB
a - Controlling Access to Information.html	5/19/2016 4:39 PM	HTML Document	36 KB
- Sever Security Policy - DRAFT.html	5/19/2016 4:40 PM	HTML Document	35 KB
1 - VMWare Security guidelines.html	5/19/2016 4:40 PM	HTML Document	21 KB
- Network Access Policy.html	5/19/2016 4:40 PM	HTML Document	42 KB
1 - Internal Network Segmentation Policy.html	5/19/2016 4:41 PM	HTML Document	29 KB
2 - Network Access Control.html	5/19/2016 4:41 PM	HTML Document	14 KB
- Application Security.html	5/19/2016 4:41 PM	HTML Document	10 KB
- Backup and Restore Policy.html	5/19/2016 4:41 PM	HTML Document	49 KB
- Password Management Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
- Mobile Devices.html	5/19/2016 4:42 PM	HTML Document	13 KB
b - Datacenter Security.html	5/19/2016 4:35 PM	HTML Document	204 KB
- Extranet Access Policy(1).html	5/19/2016 4:43 PM	HTML Document	35 KB
- Extranet Access Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
c - Global Information Policy.doc	5/19/2016 4:38 PM	Microsoft Word 9...	102 KB
- Sending Electronic Email.doc	5/19/2016 4:38 PM	Microsoft Word 9...	67 KB
- Incoming Electronic Email.doc	5/19/2016 4:39 PM	Microsoft Word 9...	66 KB
- Setting up an Internet Access.doc	5/19/2016 4:39 PM	Microsoft Word 9...	69 KB
- Setting up an Extranet.doc	5/19/2016 4:38 PM	Microsoft Word 9...	67 KB
d - Asset Management and Data Classification.d...	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
e - Business Continuity Plan.doc	5/19/2016 4:41 PM	Microsoft Word 9...	63 KB
- Staff Security Training.doc	5/19/2016 4:42 PM	Microsoft Word 9...	63 KB
- Communication softwares and Internet Dow...	5/19/2016 4:42 PM	Microsoft Word 9...	75 KB
f - Human Resource Security.doc	5/19/2016 4:42 PM	Microsoft Word 9...	72 KB

Gambar 4.3 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak *DAN'IS Network Analyst*.

Selanjutnya, dokumen Bab *Global Information Policy* mendefinisikan keseluruhan informasi tentang prosedur aktivitas yang dilakukan pada setiap unit perusahaan, termasuk pengelolaan aset teknologi informasi (TI) secara garis besar. Dokumen ini tercantum pada Gambar 4.3c. Kemudian, dokumen Bab *Asset Management and Data Classification* mendefinisikan hasil kebijakan dan panduan mengelola aset teknologi informasi (TI) serta klasifikasi data (*mining data*). Dokumen ini tercantum pada Gambar 4.3d. Setelah itu, dokumen Bab *Human Resources Security* mendefinisikan hasil kebijakan dan identifikasi keamanan dari setiap sumber daya manusia pada perusahaan. Dokumen ini tercantum pada Gambar 4.3f.



Terakhir, dokumen Bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan. Dokumen ini tercantum pada Gambar 4.3a. Selanjutnya, Gambar 4.4 merupakan *Work Product* (WP) dan *Generic Work Product* (GWP) dari penerapan dokumen *Danone Government* (DanGo) pada Lampiran B.2. Berdasarkan hasil pemetaan pada Tabel 4.10, dokumen Bab *Archiving Procedures* merupakan *Work Product* (WP) dari proses APO13 (*Manage Security*). Dokumen ini tercantum pada Gambar 4.4e. Dokumen Bab *Archiving Procedures* mendefinisikan hasil penerapan dari kebijakan pendokumentasian hasil pelaksanaan kebijakan dalam bentuk dokumen resmi perusahaan. Sedangkan dokumen Bab *IS Interconnection Authorization*, *Production Systems Management* dan *Critical IS-IT Asset* merupakan *Generic Work Product* (GWP) dari proses APO13 (*Manage Security*).

Name	Date modified	Type	Size
- SLA	3/22/2017 6:27 AM	File folder	
- IS Security Officer	3/22/2017 6:39 AM	File folder	
- Critical IS-IT Asset	3/22/2017 6:39 AM	File folder	
- IS Backup	3/22/2017 6:39 AM	File folder	
- IT Vulnerability	3/22/2017 6:40 AM	File folder	
- Data Network Management	3/22/2017 6:41 AM	File folder	
- IS Authentication policy	3/22/2017 6:43 AM	File folder	
- IS User Access Authorization	3/22/2017 6:45 AM	File folder	
- Production systems management	3/22/2017 6:45 AM	File folder	
- DRP	3/22/2017 6:49 AM	File folder	
- IS Local Legislation	3/22/2017 6:49 AM	File folder	
- Intrusion Followup	3/22/2017 6:50 AM	File folder	
- Internet access	3/22/2017 6:50 AM	File folder	
- Public Servers	3/22/2017 6:50 AM	File folder	
- Remote Access	3/22/2017 6:50 AM	File folder	
- IS Security Policy	3/22/2017 6:50 AM	File folder	
- IS Protection Mobile Devices	3/22/2017 6:51 AM	File folder	
- IS Interconnection authorization	3/22/2017 6:51 AM	File folder	
- IT Problem Tracking	3/22/2017 6:55 AM	File folder	
- IT operations control	3/19/2017 5:13 AM	File folder	
- Archiving Procedures	3/22/2017 6:56 AM	File folder	

Gambar 4.4 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak *DAN'IS Network Analyst*.

Setiap dokumen *Generic Work Product* (GWP) memiliki definisi masing-masing. Dokumen Bab *IS Interconnection Authorization* mendefinisikan hasil kebijakan dan panduan terhadap konektivitas antar unit teknologi informasi (TI) maupun unit-unit yang lain. Dokumen ini tercantum pada Gambar 4.4c. Selanjutnya, dokumen Bab *Production Systems Management* mendefinisikan hasil kebijakan dan panduan mengelola hasil akhir dari setiap aktivitas teknologi informasi (TI) pada perusahaan. Sehingga pengemasan dari setiap produk selaras dalam satu *template* yang telah ditetapkan perusahaan. Dokumen ini tercantum pada Gambar 4.4b. Terakhir, dokumen Bab *Critical IS-IT Asset* mendefinisikan hasil kebijakan dan informasi setiap aset penting dari teknologi informasi (TI).



Tujuannya untuk dirawat dan dikelola dengan bijaksana. Dokumen ini tercantum pada Gambar 4.4a. Berikut adalah hasil pemetaan dari jenis kebijakan atau dokumen pada proses APO13 (*Manage Security*). Hasil pemetaan ini berdasarkan proses analisis menggunakan lembar *checklist* dan penilaian yang kemudian ditulis pada Tabel 4.10. Terdapat dua kolom tabel yang terdiri dari kolom jenis kebijakan atau dokumen dan nama kebijakan atau dokumen.

Tabel 4.10 Pemetaan kebijakan/dokumen (APO13)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
Base Practices (BP)	<ul style="list-style-type: none"> ○ Kebijakan <i>IS Security Policy</i>. ○ Kebijakan <i>IS User Authorization</i>. ○ Kebijakan untuk mendokumentasikan hasil pelaksanaan kebijakan dalam bentuk dokumen resmi perusahaan.
Work Product (WP)	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Data Center Security</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Archiving Procedures</i>.
Generic Practices (GP)	<ul style="list-style-type: none"> ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan setiap tujuan dari proses kinerja pada perusahaan. ○ Kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif. ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan hasil atau produk kerja. ○ Kebijakan untuk mengidentifikasi dan menentukan standar proses kinerja. ○ Kebijakan untuk menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses kinerja. ○ Kebijakan untuk memastikan dan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria. ○ Kebijakan untuk menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses kinerja. ○ Kebijakan untuk menyediakan infrastruktur yang memadai untuk



Tabel 4.10 Pemetaan kebijakan/dokumen (APO13) (lanjutan)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
	<p>mendukung proses kinerja.</p> <ul style="list-style-type: none"> ○ Kebijakan untuk mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. ○ Kebijakan untuk mengidentifikasi, memperoleh, dan menetapkan kebutuhan proses informasi berdasarkan tujuan bisnis. ○ Kebijakan untuk menentukan teknik-teknik yang tepat untuk mengendalikan proses kinerja.
<p>Generic Work Product (GWP)</p>	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Business Continuity Plan</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IS Interconnection Authorization</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Production Systems Management</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Global Information Policy</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Asset Management and Data Classification</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Human Resources Security</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. <p>Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Critical IS-IT Asset</i>.</p>

Setelah dilakukan analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian, maka diketahui hasil tingkat kapabilitas (*capability level*) dari proses APO13 (*Manage Security*) seperti Tabel 4.11. Diketahui pengisian kategori penilaian berhenti pada *level 4 (predictable process)* dengan kategori *Partially Achieved (P)* pada atribut proses kedua.



Menurut ISACA (2013), bila terdapat kategori *Partially Achieved* (P) pada salah satu atribut proses, maka hasil penilaian akan berhenti pada *level* sebelumnya. Hal ini menunjukkan bahwa pencapaian tingkat kapabilitas (*capability level*) dari proses APO13 (*Manage Security*) terletak pada *level 3* (*established process*). Seperti deskripsi paragraf sebelumnya, hasil penilaian ini telah dilaporkan pada dua responden terkait sebagai proses triangulasi data.

Tabel 4.11 Perhitungan dari lembar penilaian (APO13)

NAMA PROSES	LEVEL 0	LEVEL 1			LEVEL 2		LEVEL 3		LEVEL 4		LEVEL 5	
		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		
APO13		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 Berdasarkan Kriteria		F	F	F	F	F	F	P	-	-		
Pencapaian Tingkat Kapabilitas					3							
Keterangan: N (<i>Not Achieved</i> , 0%-15%), P (<i>Partially Achieved</i> , >15%-50%), L (<i>Largely Achieved</i> , >50%-85%), F (<i>Fully Achieved</i> , >85%-100%)												

Berikut hasil tingkat kapabilitas (*capability level*) dari proses APO13 (*Manage Security*) pada Tabel 4.12. Seperti deskripsi paragraf sebelumnya, hasil tingkat kapabilitas (*capability level*) ini diperoleh dari analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian. Sehingga diketahui tingkat kapabilitas (*capability level*) dari proses APO13 (*Manage Security*) terletak pada *level 3* (*established process*). Sedangkan nilai *targeted level* diperoleh dari hasil wawancara bersama dua responden terkait berdasarkan proses ini. Pada Tabel 4.12, diketahui *targeted level* divisi DAN'IS dari proses APO13 (*Manage Security*) berada pada *level 5* (*optimizing process*). Pada *level* ini, proses teknologi informasi (TI) dilakukan secara konsisten dengan batasan yang telah ditentukan.

Tabel 4.12 Hasil tingkat kapabilitas dari proses APO13

NAMA PROSES	TARGET LEVEL	TINGKAT KAPABILITAS					
		0	1	2	3	4	5
APO13	5				3		



4.4 Manage Security Services (DSS05)

Menurut ISACA (2012), DSS05 (*Manage Security Services*) merupakan salah satu proses dari kerangka kerja COBIT 5 yang melindungi informasi perusahaan untuk mempertahankan tingkat keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijaksanaan keamanan. Selain itu, menetapkan dan mempertahankan peran keamanan informasi dan hak akses, serta melakukan pengawasan keamanan. Proses ini bertujuan mengurangi dampak risiko dari manajemen keamanan informasi. Model penilaian disesuaikan berdasarkan setiap proses yang terdapat pada DSS05 (*Manage Security Services*). Terdapat tujuh *Base Practices* (BP) dari proses ini, antara lain yang pertama DSS05.01 atau melindungi terhadap risiko dari virus komputer. Sesuai dengan artinya, proses ini bertujuan memberikan perlindungan dari virus komputer (*malware*). Praktik tata kelola yang dilakukan adalah menerapkan dan memelihara pencegahan, serta langkah-langkah perbaikan pada unit organisasi untuk melindungi aset teknologi informasi (TI) dari serangan *malware* seperti virus, *worm spyware*, dan *spam*.

Kedua adalah DSS05.02 atau mengelola keamanan jaringan dan konektivitas. Sesuai dengan artinya, proses ini bertujuan mengelola jaringan dan keamanan konektivitas. Praktik tata kelola yang dilakukan adalah menggunakan keamanan dan prosedur yang terkait untuk melindungi keamanan informasi dari segi konektivitas. Ketiga adalah DSS05.03 atau mengelola titik akhir dari suatu keamanan. Sesuai dengan artinya, proses ini bertujuan mengelola keamanan pada titik akhir. Praktik tata kelola yang dilakukan adalah memastikan perangkat titik akhir (*endpoint*) seperti *laptop*, *dekstop*, dan *server* agar tetap aman sesuai kebijakan yang ditetapkan. Keempat adalah DSS05.04 atau mengelola identitas pengguna dan hak akses. Sesuai dengan artinya, proses ini bertujuan mengelola identitas pengguna dan hak akses. Praktik tata kelola yang dilakukan adalah memastikan semua pengguna memiliki hak akses informasi yang sesuai dengan kebutuhan mereka. Kelima adalah DSS05.05 atau mengelola akses fisik terhadap aset teknologi informasi (TI).

Sesuai dengan artinya, proses ini bertujuan mendefinisikan dan menerapkan prosedur, membatasi, dan mencabut akses sesuai dengan kebutuhan bisnis dalam keadaan darurat. Selain itu, mengelola keamanan akses pada tempat yang berwenang atas akses yang dimaksud. Kemudian, memantau orang yang memasuki tempat akses termasuk staf, klien, vendor, dan pengunjung atau pihak ketiga. Keenam adalah DSS05.06 atau mengelola dokumen-dokumen penting dan perangkat keluaran lainnya. Sesuai dengan artinya, proses ini bertujuan mengelola keamanan dokumen. Praktik tata kelola yang dilakukan adalah membangun pengamanan fisik yang sesuai, kemudian menginventarisasi dokumen penting atas aset teknologi informasi (TI) seperti surat berharga dan token keamanan. Terakhir adalah DSS05.07 atau memantau infrastruktur untuk segala kegiatan yang berhubungan dengan keamanan.

Sesuai dengan artinya, proses ini bertujuan menggunakan alat deteksi instruksi dan mengawasi infrastruktur untuk akses yang tidak sah serta memastikan setiap peristiwa yang terintegrasi dengan cara mengawasi dan mengelola risiko. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, dijelaskan bahwa belum terjaminnya seluruh keamanan aset teknologi informasi (TI). Beberapa aset juga pernah mengalami kerusakan bahkan kehilangan data akibat serangan *malware*, seperti virus, *worm spyware*, dan *spam*. Seperti masalah pada proses EDM03 (*Ensure Risk Optimization*), hal ini juga berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI). Sebab, divisi *Danone Information Systems (DAN'IS)* telah menerapkan sistem informasi berbasis *Enterprise Resources Planing (ERP)* untuk beberapa perusahaan Danone, termasuk PT Tirta Investama (AQUA) Pandaan. Oleh karena itu, dilakukan observasi sebagai cara untuk menganalisis permasalahan lebih dalam melalui studi lapangan secara langsung.

Selanjutnya, melakukan wawancara dengan beberapa responden terpilih berdasarkan hasil pemetaan RACI *Chart* dari proses DSS05 (*Manage Security Services*). Masing-masing responden antara lain pihak *IT Onsite* sebagai *Responsible* (pelaksana) dan *DAN'IS Security Analyst* sebagai *Accountable* (penanggung jawab). Namun, hanya pihak *IT Onsite* yang bersedia diwawancarai karena terhalangnya waktu dan tempat dari pihak *DAN'IS Security Analyst*. Proses wawancara ini, dilakukan secara langsung (tatap muka) sebanyak dua kali menggunakan lembar *checklist* dari proses DSS05 (*Manage Security Services*). Lembar *checklist* yang dimaksud terlampir pada Lampiran B.3. Wawancara pertama dilakukan sebagai pencarian data atau bukti (*evidence*) dengan pihak *IT Onsite*, sedangkan wawancara kedua dilakukan dengan pihak *DAN'IS Network Analyst* sebagai validasi data berdasarkan hasil wawancara pertama. Setelah memperoleh data atau bukti (*evidence*) yang valid, dilakukan penilaian tingkat kapabilitas (*capability level*) melalui lembar penilaian dari proses DSS05 (*Manage Security Services*).

Lembar penilaian ini terlampir pada Lampiran C.3. Pengisian lembar penilaian dilakukan secara individu (*self assessment*) yang hasilnya dilaporkan pada dua responden terkait sebagai proses triangulasi data. Pengisian dilakukan secara individu (*self assessment*) karena keterbatasan waktu yang dimiliki oleh masing-masing responden. Pada lembar penilaian terdapat sepuluh kolom tabel yang masing-masing terdiri dari tingkat indikator proses kapabilitas, proses atribut, kriteria, validasi kriteria, kategori penilaian (*Not Achieved, Partially Achieved, Largely Achieved, dan Fully Achieved*) dan keterangan dari *Base Practices (BP)*, *Work Product (WP)*, *Generic Practices (GP)*, dan *Generic Work Product (GWP)*. Pengisian sepuluh kolom tabel didasarkan atas hasil temuan pada lembar *checklist* melalui analisis, perhitungan, dan pemetaan pada kategori penilaian (*Not Achieved, Partially Achieved, Largely Achieved, dan Fully Achieved*) maupun keterangan dari *Base Practices (BP)*, *Work Product (WP)*, *Generic Practices (GP)*, dan *Generic Work Product (GWP)*.

Setelah dilakukan pengisian lembar penilaian pada proses DSS05 (*Manage Security Services*), diketahui tingkat indikator proses kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved (F)* dari dua atribut proses yang ada. Pada *level 3 (established process)*, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Berdasarkan Lampiran C.3 pada *level 1 (performed process)*, divisi DAN'IS telah menerapkan *Base Practices (BP)* berdasarkan dua kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil mencapai kategori *Fully Achieved (F)* pada *level* ini. Dua kriteria yang dimaksud merupakan atribut proses pertama (PA 1.1) dari *level 1 (performed process)*. *Base Practices (BP)* yang telah diterapkan pada *level* ini antara lain yang pertama penerapan kebijakan *IS Security Policy*. Kebijakan ini berisi tentang tata cara atau panduan untuk memberikan perlindungan terhadap aset-aset teknologi informasi (TI) dari serangan *malware* seperti virus, *worm spyware*, dan *spam*.

Selain itu, kebijakan ini mendorong agar keamanan informasi selaras dengan kebutuhan bisnis dari setiap perusahaan Danone. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *IS Security Policy* pada Bab *VMWare Security Guidelines*. Kedua, juga dilakukan penerapan yang sama pada kebijakan *IS Security Policy*. Namun, penerapannya difokuskan untuk mempertahankan rencana keamanan informasi dari seluruh perusahaan Danone. Rencana yang ada tentu diselaraskan dengan strategi dan arsitektur dari setiap perusahaan Danone. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Ketiga, masih dilakukan penerapan yang sama pada kebijakan *IS Security Policy*. Dalam hal ini, kebijakan berisi tentang tata cara atau panduan dalam mengelola keamanan pada titik atau perangkat terakhir seperti *laptop*, *dekstop*, dan *server* dari seluruh perusahaan Danone. Setiap aset teknologi informasi (TI) yang ada disesuaikan menurut tingkat keamanan masing-masing.

Tingkat keamanan itu tentunya telah didefinisikan berdasarkan pengalaman risiko yang pernah terjadi sebelumnya. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *IS Security Policy* pada Bab *Endpoints Security Policy*. Keempat adalah penerapan kebijakan *IS User Access Authorization*. Kebijakan ini berisi tentang tata cara atau panduan dalam membuat dan menjaga akun pengguna untuk mengakses informasi perusahaan sesuai hak akses masing-masing. Dengan adanya kebijakan ini, memudahkan para staf atau pegawai dalam membuat dan mengubah jenis karakter akun mereka melalui tata cara atau panduan yang ada. Selain itu, juga memudahkan divisi DAN'IS dalam menggolongkan akun berdasarkan jenis identitas setiap pengguna. *Work Product (WP)* yang dihasilkan dari *Base Practices (BP)* ini adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Kelima, juga dilakukan penerapan yang sama pada kebijakan *IS Security Policy*. Namun, penerapannya difokuskan untuk membatasi dan mencabut akses yang disesuaikan dengan kebutuhan bisnis atau dalam keadaan darurat pada setiap perusahaan Danone.

Selain itu, dengan adanya kebijakan ini akan memudahkan pihak DAN'IS dalam memantau seluruh aktivitas pengguna, baik internal maupun eksternal. Keenam adalah penerapan kebijakan dari dokumen *Danone Government* (DanGo). Kebijakan ini berisi tentang aturan dalam pengelolaan keamanan informasi melalui pembuatan dokumen dari masing-masing kebijakan yang telah dijalankan. Praktik tata kelola yang dilakukan adalah membangun pengamanan fisik yang sesuai, inventarisasi dokumen penting, dan persediaan manajemen atas aset teknologi informasi (TI) seperti surat berharga dan bentuk keamanan lainnya. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *Danone Government* (DanGo) pada Bab *Archiving Procedures*. Ketujuh adalah penerapan kebijakan *IS User Access Authorization*. Kebijakan ini berisi tentang tata cara atau panduan untuk pembatasan dan pencabutan akses yang disesuaikan dengan kebutuhan bisnis atau dalam keadaan darurat pada setiap perusahaan Danone.

Selain itu, dengan adanya kebijakan ini akan memudahkan pihak DAN'IS dalam memantau seluruh aktivitas pengguna, baik internal maupun eksternal. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah *Danone Government* (DanGo) pada Bab *IS Interconnection Authorization*. Terakhir adalah kebijakan dalam mendokumentasikan hasil pelaksanaan kegiatan dalam bentuk dokumen resmi perusahaan. *Work Product* (WP) yang dihasilkan dari *Base Practices* (BP) ini adalah dokumen *Danone Government* (DanGo) pada Bab *Archiving Procedures*. Selanjutnya pada *level 2 (managed process)*, divisi DAN'IS telah menerapkan *Generic Practices* (GP) berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved* (F) pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 2.1) dari *level 2 (managed process)*. *Generic Practices* (GP) yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi setiap tujuan dari proses kinerja perusahaan.

Kedua adalah kebijakan merencanakan dan memantau proses kinerja untuk memenuhi setiap tujuan yang telah diidentifikasi sebelumnya. Ketiga adalah kebijakan menyesuaikan performa proses dari setiap kinerja, seperti mengetahui tindakan apakah yang diambil ketika sebuah kinerja belum tercapai. Keempat adalah kebijakan menentukan tanggung jawab dan pihak yang berwenang untuk melakukan setiap proses kinerja. Kelima adalah kebijakan mengidentifikasi dan membuat ketersediaan sumber daya untuk melakukan proses kinerja sesuai dengan rencana. *Generic Work Product* (GWP) yang dihasilkan dari kelima *Generic Practices* (GP) itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Terakhir adalah kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat, seperti individu dan kelompok yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif. *Generic Work Product* (GWP) yang dihasilkan dari *Generic Practices* (GP) itu adalah dokumen *Danone Government* (DanGo) pada Bab *IS Interconnection Authorization*.

Setelah mendeskripsikan hasil atribut proses pertama pada *level 2 (managed process)*, selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 2.2) pada *level 2 (managed process)*. Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan empat kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menentukan persyaratan untuk hasil atau produk kerja, termasuk konten, struktur, dan kualitas dari suatu kriteria. Kedua adalah kebijakan menentukan persyaratan untuk pendokumentasian dan pengelolaan hasil atau produk kerja. Ketiga adalah mengidentifikasi, mendokumentasikan, dan mengelola hasil atau produk kerja. Terakhir adalah kebijakan meninjau dan menyesuaikan hasil atau produk kerja agar memenuhi kriteria yang ditetapkan. *Generic Work Product (GWP)* yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *Production Systems Management*.

Kemudian pada *level 3 (established process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* sesuai lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Lima kriteria yang dimaksud merupakan atribut proses pertama (PA 3.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menetapkan sebuah standar proses yang mendukung pendefinisian setiap proses. Kedua adalah kebijakan menentukan urutan dan interaksi antar proses sebagai pembuktian bahwa mereka saling terintegrasi. Ketiga adalah kebijakan mengidentifikasi setiap peran dan kompetensi untuk melakukan standar proses kinerja. Keempat adalah kebijakan mengidentifikasi lingkungan kerja dan infrastruktur yang dibutuhkan untuk melakukan standar proses. *Generic Work Product (GWP)* yang dihasilkan dari keempat *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Global Information Policy*.

Terakhir adalah kebijakan menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses, termasuk menyesuaikan proses yang telah didefinisikan sebelumnya dan menyiapkan kebutuhan untuk audit internal dan pengelolaan ulang. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*. Setelah mendeskripsikan hasil atribut proses pertama pada *level 3 (established process)*, selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 3.2) pada *level 3 (established process)*. Pada atribut proses ini, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian. Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria. Kedua adalah menetapkan dan mengkomunikasikan peran, tanggung jawab, serta otoritas untuk melakukan pendefinisian proses. Ketiga adalah memastikan kompetensi yang diperlukan untuk melakukan pendefinisian proses.

Generic Work Product (GWP) yang dihasilkan dari ketiga *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Human Resources Security*. Keempat adalah kebijakan menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Kelima adalah kebijakan menyediakan infrastruktur yang memadai untuk mendukung proses kinerja. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *Danone Government (DanGo)* pada Bab *IS-IT Critical Asset*. Terakhir adalah kebijakan mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. *Generic Work Product (GWP)* yang dihasilkan dari *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Asset Management and Data Classification*. Terakhir pada *level 4 (predictable process)*, divisi DAN'IS telah menerapkan *Generic Practices (GP)* berdasarkan enam kriteria yang ada pada lembar penilaian.

Artinya, divisi ini telah berhasil meraih kategori *Fully Achieved (F)* pada *level* ini. Enam kriteria yang dimaksud merupakan atribut proses pertama (PA 4.1) dari *level 3 (established process)*. *Generic Practices (GP)* yang telah diterapkan pada *level* ini antara lain yang pertama kebijakan mengidentifikasi kebutuhan proses informasi berdasarkan tujuan bisnis. Kedua adalah kebijakan memperoleh hasil pengukuran tujuan dari kebutuhan informasi. Ketiga adalah menetapkan tujuan kuantitatif untuk proses kinerja yang telah didefinisikan agar dapat berguna bagi perusahaan. Keempat adalah kebijakan mengidentifikasi hasil atau produk dan tata cara proses yang mendukung pencapaian tujuan kuantitatif untuk proses kinerja. Kelima adalah kebijakan mengumpulkan hasil atau produk dan pengukuran proses melalui pendefinisian proses. Terakhir adalah kebijakan menggunakan hasil pengukuran untuk memantau dan memverifikasi pencapaian tujuan dari proses kinerja.

Generic Work Product (GWP) yang dihasilkan dari keenam *Generic Practices (GP)* itu adalah dokumen *IS Security Policy* pada Bab *Business Continuity Plan*. Setelah mendeskripsikan hasil atribut proses pertama pada 4 (*predictable process*), selanjutnya mendeskripsikan hasil atribut proses terakhir (PA 4.2) pada *level 4 (predictable process)*. Pada atribut proses ini, divisi DAN'IS hanya dapat menerapkan satu *Generic Practices (GP)* dari lima kriteria yang ada pada lembar penilaian. Artinya, divisi ini hanya dapat meraih kategori *Partially Achieved (P)*. Kategori ini diperoleh dari hasil pembagian persentase penuh (100%) dengan lima kriteria yang ada dan dikalikan pada satu *Generic Practices (GP)* yang telah diterapkan. Maka, perhitungan itu akan menghasilkan persentase sebesar 20% dan termasuk pada kategori *Partially Achieved (P)*. Menurut ISACA (2013), kategori *Partially Achieved (P)* tidak memenuhi syarat untuk bertahan maupun berlanjut dari *level* saat itu. Sehingga hasil penilaian proses ini berada pada *level 3 (established process)*. Terdapat beberapa bukti (*evidences*) yang diperoleh dari hasil wawancara dengan pihak *IT Onsite*. Namun, tampilan bukti (*evidence*) yang diperoleh sangat terbatas karena bersifat rahasia (*confidential*). Beberapa bukti (*evidences*) itu ditunjukkan pada Gambar 4.5 dan 4.6.

Diketahui kedua gambar merupakan kumpulan *file* yang mewakili seluruh *Work Product* (WP) dan *Generic Work Product* (GWP) dari penerapan *Base Practices* (BP) dan *Generic Practices* (GP) oleh divisi DAN'IS. Pada Gambar 4.5, merupakan *Work Product* (WP) dan *Generic Work Product* (GWP) dari penerapan *IS Security Policy*. Berdasarkan hasil pemetaan pada Tabel 4.13, dokumen Bab *VMWare Security Guidelines, Controlling Access to Information* dan *Endpoints Security Policy* merupakan *Work Product* (WP) dari proses DSS05 (*Manage Security Services*). Setiap dokumen *Work Product* (WP) memiliki definisi masing-masing. Dokumen bab *VMWare Security Guidelines* merupakan hasil kebijakan dan panduan memberikan perlindungan terhadap aset-aset teknologi informasi (TI) dari serangan *malware* seperti virus, *worm spyware*, dan *spam*. Dokumen ini tercantum pada Gambar 4.5c.

	Date modified	Type	Size
Endpoints Security Policy.pdf	5/19/2016 4:40 PM	Adobe Acrobat D...	76 KB
- DMZ Security Policy.html	5/19/2016 4:39 PM	HTML Document	35 KB
- Protection against malicious and mobile cod...	5/19/2016 4:39 PM	HTML Document	11 KB
Controlling Access to Information.html	5/19/2016 4:39 PM	HTML Document	36 KB
- Sever Security Policy - DRAFT.html	5/19/2016 4:40 PM	HTML Document	35 KB
- VMWare Security guidelines.html	5/19/2016 4:40 PM	HTML Document	21 KB
- Network Access Policy.html	5/19/2016 4:40 PM	HTML Document	42 KB
1 - Internal Network Segmentation Policy.html	5/19/2016 4:41 PM	HTML Document	29 KB
2 - Network Access Control.html	5/19/2016 4:41 PM	HTML Document	14 KB
- Application Security.html	5/19/2016 4:41 PM	HTML Document	10 KB
- Backup and Restore Policy.html	5/19/2016 4:41 PM	HTML Document	49 KB
- Password Management Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
- Mobile Devices.html	5/19/2016 4:42 PM	HTML Document	13 KB
- Datacenter Security.html	5/19/2016 4:36 PM	HTML Document	204 KB
- Extranet Access Policy(1).html	5/19/2016 4:43 PM	HTML Document	35 KB
- Extranet Access Policy.html	5/19/2016 4:42 PM	HTML Document	35 KB
Global Information Policy.doc	5/19/2016 4:38 PM	Microsoft Word 9...	102 KB
- Sending Electronic Email.doc	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
- Incoming Electronic Email.doc	5/19/2016 4:39 PM	Microsoft Word 9...	66 KB
- Setting up an Internet Accessl.doc	5/19/2016 4:39 PM	Microsoft Word 9...	69 KB
- Setting up an Extranet.doc	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
- Asset Management and Data Classification.d...	5/19/2016 4:39 PM	Microsoft Word 9...	67 KB
- Business Continuity Plan.doc	5/19/2016 4:41 PM	Microsoft Word 9...	63 KB
- Staff Security Training.doc	5/19/2016 4:42 PM	Microsoft Word 9...	63 KB
- Communication softwares and Internet Dow...	5/19/2016 4:42 PM	Microsoft Word 9...	75 KB
- Human Resource Security.doc	5/19/2016 4:42 PM	Microsoft Word 9...	72 KB

Gambar 4.5 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak IT Onsite.

Selanjutnya, dokumen bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan. Dokumen ini tercantum pada Gambar 4.5b. Terakhir, dokumen bab *Endpoints Security Policy* mendefinisikan hasil kebijakan dan panduan mengelola keamanan pada titik atau perangkat terakhir seperti *laptop*, *dekstop*, dan *server* dari seluruh perusahaan Danone. Dokumen ini tercantum pada Gambar 4.5a. Sedangkan dokumen Bab *Business Continuity Plan, Global Information Policy, Asset Management and Data Classification, Human Resources Security*, dan *Controlling Access to Information* merupakan *Generic Work Product* (GWP) dari proses DSS05 (*Manage Security Services*).



Setiap dokumen *Generic Work Product* (GWP) memiliki definisi masing-masing. Dokumen Bab *Business Continuity Plan* mendefinisikan hasil kebijakan dan identifikasi dari setiap tujuan dan risiko bisnis. Setiap aktivitas diselaraskan dengan teknologi informasi (TI) sehingga menunjang proses bisnis agar lebih efektif. Dokumen ini tercantum pada Gambar 4.5f. Selanjutnya, dokumen Bab *Global Information Policy* mendefinisikan keseluruhan informasi tentang prosedur aktivitas yang dilakukan pada setiap unit perusahaan, termasuk pengelolaan aset teknologi informasi (TI) secara garis besar. Dokumen ini tercantum pada Gambar 4.5d. Kemudian, dokumen Bab *Asset Management and Data Classification* mendefinisikan hasil kebijakan dan panduan mengelola aset teknologi informasi (TI) serta klasifikasi data (*mining data*). Dokumen ini tercantum pada Gambar 4.5e. Setelah itu, dokumen Bab *Human Resources Security* mendefinisikan hasil kebijakan dan identifikasi keamanan dari setiap sumber daya manusia pada perusahaan. Dokumen ini tercantum pada Gambar 4.5g.

Terakhir, dokumen Bab *Controlling Access to Information* mendefinisikan tentang hasil kebijakan dan panduan tentang pembagian dan pemberian hak akses terhadap seluruh aktivitas teknologi informasi (TI) perusahaan. Dokumen ini tercantum pada Gambar 4.5b. Selanjutnya, Gambar 4.6 merupakan *Work Product* (WP) dan *Generic Work Product* (GWP) dari penerapan dokumen *Danone Government* (DanGo) pada Lampiran B.3. Berdasarkan hasil pemetaan pada Tabel 4.13, dokumen Bab *IS Interconnection Authorization* dan *Archiving Procedures* merupakan *Work Product* (WP) dari proses DSS05 (*Manage Security Services*). Setiap dokumen *Work Product* (WP) memiliki definisi masing-masing. Dokumen Bab *IS Interconnection Authorization* mendefinisikan hasil kebijakan dan panduan terhadap konektivitas antar unit teknologi informasi (TI) maupun unit-unit yang lain. Dokumen ini tercantum pada Gambar 4.6c. Terakhir, dokumen Bab *Archiving Procedures* mendefinisikan hasil penerapan dari kebijakan pendokumentasian hasil pelaksanaan kebijakan dalam bentuk dokumen resmi perusahaan.

Dokumen ini tercantum pada Gambar 4.6e. Sedangkan dokumen Bab *IS Interconnection Authorization*, *Production Systems Management* dan *Critical IS-IT Asset* merupakan *Generic Work Product* (GWP) dari proses DSS05 (*Manage Security Services*). Setiap dokumen *Generic Work Product* (GWP) memiliki definisi masing-masing. Dokumen Bab *IS Interconnection Authorization* mendefinisikan hasil kebijakan dan panduan terhadap konektivitas antar unit teknologi informasi (TI) maupun unit-unit yang lain. Dokumen ini tercantum pada Gambar 4.6c. Selanjutnya, dokumen Bab *Production Systems Management* mendefinisikan hasil kebijakan dan panduan mengelola hasil akhir dari setiap aktivitas teknologi informasi (TI) pada perusahaan. Sehingga pengemasan dari setiap produk selaras dalam satu *template* yang telah ditetapkan perusahaan. Dokumen ini tercantum pada Gambar 4.6b. Terakhir, dokumen Bab *Critical IS-IT Asset* mendefinisikan hasil kebijakan dan informasi setiap aset penting dari teknologi informasi (TI). Tujuannya untuk dirawat dan dikelola dengan bijaksana. Dokumen ini tercantum pada Gambar 4.6a.

	Date modified	Type	Size
- SLA	3/22/2017 6:27 AM	File folder	
- IS Security Officer	3/22/2017 6:39 AM	File folder	
- Critical IS-IT Asset	3/22/2017 6:39 AM	File folder	
- IS Backup	3/22/2017 6:39 AM	File folder	
- IT Vulnerability	3/22/2017 6:40 AM	File folder	
- Data Network Management	3/22/2017 6:41 AM	File folder	
- IS Authentication policy	3/22/2017 6:43 AM	File folder	
- IS User Access Authorization	3/22/2017 6:45 AM	File folder	
- Production systems management	3/22/2017 6:45 AM	File folder	
- DRP	3/22/2017 6:49 AM	File folder	
- IS Local Legislation	3/22/2017 6:49 AM	File folder	
- Intrusion Followup	3/22/2017 6:50 AM	File folder	
- Internet access	3/22/2017 6:50 AM	File folder	
- Public Servers	3/22/2017 6:50 AM	File folder	
- Remote Access	3/22/2017 6:50 AM	File folder	
- IS Security Policy	3/22/2017 6:50 AM	File folder	
- IS Protection Mobile Devices	3/22/2017 6:51 AM	File folder	
- IS Interconnection authorization	3/22/2017 6:51 AM	File folder	
- IT Problem Tracking	3/22/2017 6:55 AM	File folder	
- IT operations control	3/22/2017 6:56 AM	File folder	
- Archiving Procedures	3/22/2017 6:56 AM	File folder	

Gambar 4.6 Bukti nama-nama dokumen dari penerapan kebijakan

Sumber: wawancara dengan pihak *IT Onsite*.

Berikut adalah hasil pemetaan dari jenis kebijakan atau dokumen pada proses DSS05 (*Manage Security Services*). Hasil pemetaan ini berdasarkan proses analisis menggunakan lembar *checklist* dan penilaian yang kemudian ditulis pada Tabel 4.13. Terdapat dua kolom tabel yang terdiri dari kolom jenis kebijakan atau dokumen dan nama kebijakan atau dokumen.

Tabel 4.13 Pemetaan kebijakan/dokumen (DSS05)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
Base Practices (BP)	<ul style="list-style-type: none"> o Kebijakan <i>IS Security Policy</i>. o Kebijakan <i>IS User Access Authorization</i>. o Dokumen <i>Danone Government</i>. o Kebijakan untuk mendokumentasikan hasil pelaksanaan kebijakan dalam bentuk dokumen resmi perusahaan.



Tabel 4.13 Pemetaan kebijakan/dokumen (DSS05) (lanjutan)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
<p>Work Product (WP)</p>	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>VMWare Security Guidelines</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Endpoints Policy</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IS Interconnection Authorization</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Archiving Procedures</i>.
<p>Generic Practices (GP)</p>	<ul style="list-style-type: none"> ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan setiap tujuan dari proses kinerja pada perusahaan. ○ Kebijakan mengelola aktivitas antarmuka antara pihak yang terlibat pada identifikasi proses melalui tanggung jawab dan komunikasi yang jelas dan efektif. ○ Kebijakan untuk mengidentifikasi, menentukan, dan menyesuaikan hasil atau produk kerja. ○ Kebijakan untuk mengidentifikasi dan menentukan standar proses kinerja. ○ Kebijakan untuk menentukan metode yang cocok untuk memantau efektivitas dan kesesuaian standar proses kinerja. ○ Kebijakan untuk memastikan dan menjalankan hasil pendefinisian proses yang telah memenuhi kriteria. ○ Kebijakan untuk menyediakan sumber daya dan informasi untuk mendukung pelaksanaan proses kinerja. ○ Kebijakan untuk menyediakan infrastruktur yang memadai untuk mendukung proses kinerja. ○ Kebijakan untuk mengumpulkan dan menganalisis data tentang proses kinerja untuk menunjukkan kesesuaian dan efektivitas. ○ Kebijakan untuk mengidentifikasi, memperoleh, dan menetapkan



Tabel 4.13 Pemetaan kebijakan/dokumen (DSS05) (lanjutan)

JENIS KEBIJAKAN ATAU DOKUMEN	NAMA KEBIJAKAN ATAU DOKUMEN
	kebutuhan proses informasi berdasarkan tujuan bisnis. <ul style="list-style-type: none"> ○ Kebijakan untuk menentukan teknik-teknik yang tepat untuk mengendalikan proses kinerja.
Generic Work Product (GWP)	<ul style="list-style-type: none"> ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Business Continuity Plan</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IS Interconnection Authorization</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Production Systems Management</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Global Information Policy</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Asset Management and Data Classification</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Human Resources Security</i>. ○ Dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i>. ○ Dokumen <i>Danone Government (DanGo)</i> pada Bab <i>Critical IS-IT Asset</i>.

Setelah dilakukan analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian, maka diketahui hasil tingkat kapabilitas (*capability level*) dari proses DSS05 (*Manage Security Services*) seperti Tabel 4.14. Diketahui pengisian kategori penilaian berhenti pada *level 4 (predictable process)* dengan kategori *Partially Achieved (P)* pada atribut proses kedua. Menurut ISACA (2013), bila terdapat kategori *Partially Achieved (P)* pada salah satu atribut proses, maka hasil penilaian akan berhenti pada *level* sebelumnya. Hal ini menunjukkan bahwa pencapaian tingkat kapabilitas (*capability level*) dari proses DSS05 (*Manage Security Services*) terletak pada *level 3 (established process)*. Seperti deskripsi paragraf sebelumnya, hasil penilaian ini telah dilaporkan pada dua responden terkait sebagai proses triangulasi data.



Tabel 4.14 Perhitungan dari lembar penilaian (DSS05)

NAMA PROSES	LEVEL 0	LEVEL 1	LEVEL 2			LEVEL 3		LEVEL 4		LEVEL 5	
		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 Berdasarkan Kriteria		F	F	F	F	F	F	P	-	-	
Pencapaian Tingkat Kapabilitas					3						
Keterangan: N (<i>Not Achieved</i> , 0%-15%), P (<i>Partially Achieved</i> , >15%-50%), L (<i>Largely Achieved</i> , >50%-85%), F (<i>Fully Achieved</i> , >85%-100%)											

Berikut adalah hasil tingkat kapabilitas (*capability level*) dari proses DSS05 (*Manage Security Services*) pada Tabel 4.15. Seperti penjelasan pada paragraf sebelumnya, hasil tingkat kapabilitas (*capability level*) diperoleh dari analisis, pemetaan, dan perhitungan pada lembar *checklist* dan penilaian. Sehingga diketahui tingkat kapabilitas (*capability level*) dari proses DSS05 (*Manage Security Services*) terletak pada *level 3* (*established process*). Sedangkan nilai *targeted level* diperoleh dari hasil wawancara bersama dua responden terkait sesuai proses ini. Pada keterangan Tabel 4.15, diketahui *targeted level* divisi DAN'IS dari proses APO13 (*Manage Security*) berada pada *level 5* (*optimizing process*). Pada *level* ini, proses teknologi informasi (TI) ditingkatkan secara berkelanjutan untuk memenuhi kebutuhan bisnis saat ini dan akan datang.

Tabel 4.15 Hasil tingkat kapabilitas dari proses DSS05

NAMA PROSES	TARGET LEVEL	TINGKAT KAPABILITAS					
		0	1	2	3	4	5
DSS05	5				3		

4.5 Analisis Kesenjangan (*Gap Analysis*)

Menurut Adi (2015), analisis kesenjangan (*gap analysis*) digunakan untuk menentukan langkah apa saja yang perlu diambil untuk meraih kondisi yang diharapkan. Banyak orang menyebutnya menjadi analisis kebutuhan dan gap, penilaian kebutuhan atau analisis kebutuhan saja. Analisis kesenjangan (*gap analysis*) dapat juga diartikan sebagai perbandingan kinerja aktual dengan kinerja potensial atau yang diharapkan.



Sebagai metode, analisis kesenjangan (*gap analysis*) digunakan sebagai alat evaluasi bisnis yang menitikberatkan pada kesenjangan kinerja perusahaan saat ini dengan kinerja yang sudah ditargetkan sebelumnya. Analisis ini juga mengidentifikasi tindakan-tindakan apa saja yang diperlukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan pada masa datang. Lebih dari itu analisis ini juga memperkirakan waktu, biaya, dan sumber daya yang dibutuhkan untuk mencapai keadaan perusahaan yang diharapkan. Analisis kesenjangan (*gap analysis*) terdiri dari tiga komponen faktor utama, antara lain yang pertama daftar karakteristik seperti atribut, kompetensi, tingkat kinerja dari situasi saat ini. Kedua, daftar apa yang diperlukan untuk mencapai tujuan masa depan. Terakhir, daftar kesenjangan apa yang ada dan perlu diisi. Analisis kesenjangan (*gap analysis*) akan memicu organisasi atau perusahaan untuk merenung status dan kemampuan apa yang saat ini dimiliki oleh organisasi dan bertanya ingin berada dimana di masa depan.

Dengan demikian, analisis kesenjangan (*gap analysis*) adalah studi yang dibuat untuk mengidentifikasi apakah sistem saat ini telah memenuhi kebutuhan. Analisis *gap* mengidentifikasikan kesenjangan (*gap*) antara bagaimana operasi bisnis diperlukan untuk melawan apa yang diinginkan tetapi belum atau tidak bisa penuhi. Dengan sendirinya, alternatif-alternatif akan dikembangkan pada saat fungsi *gap* ditemukan. *Gap* diubah sesuai dengan proses bisnis, laporan yang diinginkan atau penyesuaian perangkat yang digunakan. Sasaran awal dari analisis kesenjangan (*gap analysis*) adalah mengumpulkan persyaratan (*requirement*) dari perusahaan, menentukan penyesuaian (*customization*) yang diperlukan, memastikan sistem yang baru memenuhi kebutuhan proses bisnis perusahaan, memastikan proses bisnis akan menjadi *Base Practices* (BP), dan mengidentifikasikan permasalahan yang membutuhkan perubahan kebijakan perusahaan.

Berdasarkan hasil analisis, pemetaan, dan perhitungan pada Lampiran B.1 dan C.1, diketahui tingkat kapabilitas (*capability level*) proses EDM03 (*Ensure Risk Optimization*) berada pada *level 3 (established process)*. Pada *level* ini, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Kemudian, berdasarkan hasil wawancara bersama pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui *targeted level* yang diharapkan dari proses EDM03 (*Ensure Risk Optimization*) berada pada *level 4 (predictable process)*. Pada *level* ini, mengindikasikan proses teknologi informasi (TI) dilakukan secara konsisten dengan batasan yang telah ditentukan. Jadi, dapat disimpulkan bahwa tingkat kesenjangan (*gap level*) antara pencapaian saat ini dengan yang diharapkan oleh divisi *Danone Information Systems* (DAN'IS) adalah *1 level*. Hasil ini diperoleh dari selisih antara *level* yang diharapkan dengan *level* yang dicapai pada saat ini. Tingkat kesenjangan (*gap level*) dapat dilihat pada Tabel 4.16.

Tabel 4.16 Tingkat kesenjangan dari proses EDM03

PROSES	TARGET LEVEL	TINGKAT KAPABILITAS	TINGKAT KESENJANGAN
EDM03	4	3	1

Selanjutnya, berdasarkan hasil analisis, pemetaan, dan perhitungan pada Lampiran B.2 dan C.2, diketahui tingkat kapabilitas (*capability level*) proses APO13 (*Manage Security*) berada pada *level 3 (established process)*. Pada *level* ini, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Kemudian, berdasarkan hasil wawancara bersama pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui *targeted level* yang diharapkan dari proses APO13 (*Manage Security*) berada pada *level 5 (optimizing process)*. Pada *level* ini, proses teknologi informasi (TI) ditingkatkan secara berkelanjutan untuk memenuhi kebutuhan bisnis saat ini dan akan datang. Jadi, disimpulkan bahwa tingkat kesenjangan (*gap level*) antara pencapaian saat ini dengan yang diharapkan oleh divisi DAN'IS adalah 2 *level*. Hasil itu diperoleh dari selisih antara *level* yang diharapkan dengan *level* yang dicapai pada saat ini. Tingkat kesenjangan (*gap level*) dapat dilihat pada Tabel 4.17.

Tabel 4.17 Tingkat kesenjangan dari proses APO13

PROSES	TARGET LEVEL	TINGKAT KAPABILITAS	TINGKAT KESENJANGAN
APO13	5	3	2

Terakhir, berdasarkan hasil analisis, pemetaan, dan perhitungan pada Lampiran B.3 dan C.3, diketahui tingkat kapabilitas (*capability level*) proses DSS (*Manage Security Services*) berada pada *level 3 (established process)*. Pada *level* ini, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Kemudian, berdasarkan hasil wawancara bersama pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui *targeted level* yang diharapkan dari proses DSS (*Manage Security Services*) berada pada *level 5 (optimizing process)*. Pada *level* ini, proses teknologi informasi (TI) ditingkatkan secara berkelanjutan untuk memenuhi kebutuhan bisnis saat ini dan akan datang. Jadi, disimpulkan bahwa tingkat kesenjangan (*gap level*) antara pencapaian saat ini dengan yang diharapkan oleh divisi DAN'IS adalah 2 *level*. Hasil itu diperoleh dari selisih antara *level* yang diharapkan dengan *level* yang dicapai pada saat ini. Tingkat kesenjangan (*gap level*) dapat dilihat pada Tabel 4.18.

Tabel 4.18 Tingkat kesenjangan dari proses DSS05

PROSES	TARGET LEVEL	TINGKAT KAPABILITAS	TINGKAT KESEJANGAN
DSS05	5	3	2

4.6 Hasil Temuan

Berdasarkan analisis dari hasil wawancara bersama pihak *DAN'IS Network Analyst* dan *IT Onsite*, diketahui beberapa hasil temuan dari penelitian ini. Hasil temuan didasarkan dari masing-masing proses yang digunakan dalam penelitian ini, antara lain EDM03 (*Ensure Risk Optimization*), APO13 (*Manage Security*) dan DSS05 (*Manage Security Services*). Hasil temuan juga dibedakan menjadi dua jenis, yaitu temuan positif dan negatif. Berdasarkan jenisnya, temuan positif merupakan temuan yang berdampak baik terhadap perkembangan perusahaan. Adapun temuan ditunjukkan melalui suatu kebijakan ataupun dokumen resmi sebagai bentuk dari pelaksanaan tujuan perusahaan. Sedangkan temuan negatif merupakan temuan yang berdampak kurang baik terhadap perkembangan perusahaan. Adapun temuan ditunjukkan melalui suatu permasalahan yang mengganggu perusahaan dalam mencapai tujuan.

Dalam perkembangannya, diketahui beberapa hasil temuan dari divisi *Danone Information Systems (DAN'IS)*, antara lain yang pertama telah memiliki dan menggunakan acuan resmi dalam pelaksanaan setiap prosedur maupun kebijakan perusahaan. Acuan resmi ini terlampir pada dua dokumen penting perusahaan, yaitu dokumen *Danone Government (DanGo)* dan *DAN'IS Policy*. Kedua dokumen ini memiliki peran masing-masing dalam perusahaan. Dokumen *Danone Government (DanGo)* berisi keseluruhan informasi terkait prosedur maupun kebijakan dalam pelaksanaan aktivitas perusahaan. Masing-masing aktivitas ini dikelompokkan berdasarkan jenis dan tujuan perusahaan. Sebab, Danone telah memiliki banyak anak perusahaan hingga saat ini. Secara garis besar, aktivitas yang dimaksud seperti bisnis dan operasional, pengembangan sumber daya manusia, unit keuangan (*finance*), hingga penjaminan mutu (*quality control*) untuk seluruh anak perusahaan Danone.

Sedangkan dokumen *DAN'IS Policy* berisi informasi terkait prosedur maupun kebijakan yang berfokus pada teknologi dan sistem informasi perusahaan. Dokumen ini juga terbagi menjadi beberapa bidang yang masing-masing mengarah pada aktivitas teknologi informasi (TI), seperti sistem keamanan informasi, keamanan jaringan, keamanan aset teknologi informasi (TI), dan masih banyak lagi. Hal ini menjadi temuan positif karena setiap aktivitas yang ada disesuaikan berdasarkan prosedur maupun kebijakan resmi perusahaan. Sehingga aktivitas tiap unit selaras dengan tujuan utama perusahaan. Temuan kedua adalah telah terjalinnya kerja sama dengan dua *provider* besar yaitu Indosat Ooredoo dan Telkomsel sebagai penyedia layanan jaringan pada seluruh anak perusahaan Danone.

Hal ini menjadi temuan positif karena masing-masing perusahaan akan dimudahkan dalam menikmati layanan komunikasi, khususnya jaringan internet. Sehingga seluruh aktivitas perusahaan akan terintegrasi optimal satu sama lain. Temuan ketiga adalah telah terjalannya kerja sama dengan salah satu media sosial besar dunia, yaitu Facebook. Media sosial ini berfungsi sebagai media komunikasi maupun *sharing data* antar staf-staf perusahaan Danone. Pihak Facebook menyediakan sub domain khusus kepada pihak Danone sebagai bentuk kerja samanya. Sub domain ini bernama *danone* yang dapat diakses pada alamat *danone.facebook.com*. Hal ini menjadi temuan positif karena akan memudahkan komunikasi maupun *sharing data* untuk staf-staf Danone di seluruh dunia. Masing-masing aktivitas tentu telah terjamin keamanannya.

Temuan terakhir adalah minimnya staf utama yang bertanggung jawab pada masing-masing bidang dari sub divisi DAN'IS. Hal ini didasarkan dari hasil wawancara bersama pihak *DAN'IS Network Analyst* yang mengatakan bahwa masing-masing bidang ini hanya diperankan oleh satu orang. Tentu sangat berisiko mengingat DAN'IS merupakan divisi besar yang bertanggung jawab atas teknologi informasi (TI) pada seluruh anak perusahaan Danone. Masing-masing bidang yang dimaksud antara lain *DAN'IS Asset & Server Management*, *DAN'IS Network Analyst*, *DAN'IS Security Analyst* dan *DAN'IS Database Management*. Hal ini menjadi temuan negatif karena berdampak pada kurangnya *sharing knowledge* antar personal sehingga jenis keputusan yang dihasilkan dalam penyelesaian masalah akan minim.

BAB 5 PEMBAHASAN

5.1 *Ensure Risk Optimization (EDM03)*

Risiko merupakan bagian yang tidak terpisahkan dari kehidupan, bahkan ada pepatah mengatakan bahwa tidak ada hidup tanpa adanya risiko. Dalam dunia bisnis tentu sangat erat kaitannya dengan suatu risiko. Hal ini akan menjadi ancaman bila tidak ada kecermatan. Menurut Darmawi & Djojosoedarso (dalam Yasa, 2013), risiko merupakan suatu potensi kejadian yang dapat merugikan dan disebabkan karena adanya ketidakpastian atas terjadinya suatu peristiwa, dimana ketidakpastian itu merupakan kondisi yang menyebabkan tumbuhnya risiko yang bersumber dari berbagai aktivitas. Dalam mengatasi risiko tentu dilakukan pengelolaan yang tepat. Pengelolaan ini didasari atas hasil analisis dari suatu permasalahan yang muncul. Menurut Kerzner (dalam Yasa, 2013), manajemen risiko merupakan seperangkat kebijakan, prosedur lengkap yang dimiliki oleh organisasi untuk mengelola, mengawasi, dan mengendalikan risiko yang mungkin muncul.

Sistem manajemen risiko tidak hanya mengidentifikasi tapi juga harus menghitung risiko dan pengaruhnya terhadap proyek, yang hasilnya apakah jenis risiko dapat diterima atau tidak. Ketika melakukan pengelolaan tentu dibarengi dengan identifikasi risiko guna mengenali risiko secara komprehensif. Menurut Godfrey (dalam Yasa, 2013), dalam melakukan identifikasi risiko terlebih dahulu diupayakan untuk menentukan sumber risiko secara komprehensif. Risiko dapat bersumber dari politis (*political*), lingkungan (*environmental*), perencanaan (*planning*), pemasaran (*market*), ekonomi (*economic*), keuangan (*financial*), proyek (*project*), teknik (*technical*), manusia (*human*), kriminal (*criminal*), dan keselamatan (*safety*). Sedangkan menurut Darmawi (dalam Yasa, 2013), melakukan identifikasi risiko merupakan proses penganalisaan untuk menemukan secara sistematis dan berkesinambungan risiko (kerugian yang potensial) yang menantang perusahaan.

Setelah dilakukan identifikasi risiko, dilanjutkan dengan melakukan klasifikasi terhadap risiko dengan tujuan untuk memudahkan dalam melakukan perbedaan dan pemahaman terhadap risiko. Menurut Flanagan & Norman (dalam Yasa, 2013), terdapat tiga cara untuk mengklasifikasikan identifikasi risiko antara lain dengan mengidentifikasi risiko berdasarkan konsekuensi risiko, jenis, dan pengaruh risiko. Setelah dilakukan klasifikasi, dilanjutkan dengan melakukan analisis risiko. Hal itu dapat dilakukan secara kualitatif maupun kuantitatif, dimana risiko harus diidentifikasi dan akibat (*effect*) harus dinilai atau dianalisis. Tujuan dari analisis risiko adalah membantu menghindari kegagalan dan memberikan gambaran tentang apa yang terjadi bila proyek yang dijalankan ternyata tidak sesuai dengan apa yang direncanakan. Terakhir adalah melakukan penanganan risiko (*risk mitigation*).

Menurut Flanagan & Norman (dalam Yasa, 2013), *risk response* adalah tanggapan atau reaksi terhadap risiko yang dilakukan oleh setiap orang atau kelompok dalam pengambilan keputusan, yang dipengaruhi oleh pendekatan risiko (*risk attitude*) dari pengambil keputusan. Jenis-jenis tindakan yang dapat dilakukan dalam menangani risiko antara lain yang pertama menahan risiko (*risk retention*). Tindakan ini dilakukan karena dampak dari suatu kejadian yang merugikan masih dapat diterima (*acceptable*). Kedua adalah mengurangi risiko (*risk reduction*). Tindakan ini dilakukan dengan mempelajari secara mendalam tentang jenis risiko dan melakukan usaha-usaha pencegahan pada sumber risiko atau mengkombinasikan usaha agar risiko yang diterima tidak terjadi secara simultan. Ketiga adalah memindahkan risiko (*risk transfer*). Tindakan ini dilakukan dengan cara mengansurahkan risiko, baik sebagian atau seluruhnya kepada pihak lain.

Terakhir adalah menghindari risiko (*risk avoidance*). Tindakan ini dilakukan dengan menghindari aktivitas yang tingkat kerugiannya sangat tinggi. Hal ini juga sesuai dengan fungsi utama dari proses EDM03 (*Ensure Risk Optimization*). Berdasarkan hasil evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan menggunakan kerangka kerja COBIT 5, diberikan beberapa rekomendasi yang dapat digunakan sebagai optimasi risiko (EDM03). Bentuk rekomendasi didasarkan atas temuan negatif dari proses EDM03 (*Ensure Risk Optimization*). Berikut beberapa rekomendasi yang disarankan untuk proses EDM03 (*Ensure Risk Optimization*), antara lain rekomendasi pertama melakukan pengelolaan data secara kontinuitas agar meminimalisir penurunan performa sistem yang masih terjadi. Hal ini perlu dilakukan guna menindaklanjuti permasalahan dari proses EDM03 (*Ensure Risk Optimization*), yaitu kurangnya manajemen data sehingga menyebabkan penurunan performa sistem.

Hal ini tentu berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI). Sebab, divisi DAN'IS telah menerapkan sistem informasi berbasis *Enterprise Resources Planing* (ERP) untuk beberapa perusahaan Danone, termasuk PT Tirta Investama (AQUA) Pandaan. Rekomendasi kedua adalah mendefinisikan dokumen tertulis yang berisi prosedur ataupun kebijakan tentang *risk appetite* perusahaan. Sehingga risiko perusahaan yang terkait dengan teknologi informasi (TI) tidak melebihi *risk appetite* beserta toleransinya. Selain itu, mengidentifikasi dan mengelola dampak risiko teknologi informasi (TI) terhadap nilai perusahaan dan meminimalisir potensi kegagalannya. *Risk appetite* merupakan suatu keadaan dimana perusahaan memilih untuk menerima, memantau, mempertahankan diri, atau memaksimalkan diri melalui peluang-peluang yang ada. Bentuk rekomendasi kedua merupakan langkah yang diciptakan guna meningkatkan tingkat kapabilitas (*capability level*) perusahaan dari kondisi sekarang menuju kondisi yang diharapkan.

Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4 diketahui *targeted level* perusahaan dari proses ini berada pada *level ke-4 (predictable process)*. Rekomendasi terakhir adalah membentuk *management team* yang bertanggung jawab penuh atas pengelolaan risiko teknologi informasi (TI) pada divisi DAN'IS. Sebab, pengelolaan risiko cenderung dilimpahkan kepada sub divisi *IT Support*. Setelah itu, menetapkan arahan untuk mengintegrasikan strategi dan pelaksanaan risiko yang ada pada divisi DAN'IS.

Tabel 5.1 Rekomendasi (EDM03)

PROSES	REKOMENDASI	ALASAN
EDM03	Melakukan pengelolaan data secara kontinuitas agar meminimalisir penurunan performa sistem yang masih terjadi.	Bentuk rekomendasi didasarkan atas masalah yang ditemukan dari hasil observasi dan wawancara pada pengelolaan risiko teknologi informasi (TI).
	Mendefinisikan dokumen tertulis yang berisi prosedur ataupun kebijakan tentang <i>risk appetite</i> perusahaan.	Bentuk rekomendasi diciptakan untuk meraih tingkat pencapaian (<i>targeted level</i>) yang diharapkan pada <i>level 4 (predictable process)</i> .
	Membentuk <i>management team</i> yang bertanggung jawab penuh atas pengelolaan risiko teknologi informasi (TI) pada divisi DAN'IS.	Bentuk rekomendasi didasarkan atas temuan negatif dari hasil observasi dan wawancara.

5.2 Manage Security (APO13)

Terdapat perbedaan mendasar tentang keamanan yang berkaitan dengan dunia teknologi informasi (TI). Perbedaan ini dapat ditemui dalam dua istilah, antara lain keamanan teknologi informasi (TI) dan keamanan informasi. Menurut Ibrahim & Koswara (2010), keamanan teknologi informasi (TI) atau *IT security* mengacu pada setiap untuk mengamankan infrastruktur informasi dari setiap gangguan akses terlarang seperti penggunaan jaringan yang tidak diizinkan. Sedangkan pengertian dari keamanan informasi atau *information security* adalah mengacu pada setiap usaha untuk fokus terhadap pengamanan data dan informasi dari sebuah instansi. Pada istilah kedua ini, konsep usaha yang dilakukan adalah merencanakan, mengembangkan, dan mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan sesuai fungsinya serta tidak disalahgunakan atau bahkan dibocorkan kepada pihak-pihak yang tidak berkepentingan. Berdasarkan kedua penjelasan tadi, keamanan teknologi informasi (TI) merupakan bagian dari keseluruhan aspek keamanan informasi. Sebab, teknologi informasi (TI) merupakan salah satu media penting yang digunakan untuk mengamankan akses serta penggunaan data dan informasi sebuah instansi.



Dari pemahaman tadi, disimpulkan bahwa teknologi informasi (TI) bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi pada sebuah instansi. Dalam penggunaan teknologi informasi (TI) pada sebuah instansi, membutuhkan suatu operasional yang optimal untuk mendukung proses bisnis yang berjalan. Setiap operasional akan melibatkan banyak hal di dalamnya. Menurut Ibrahim & Koswara (2010), pelibatan yang dimaksud meliputi perangkat keras (*hardware*), perangkat lunak (*software*), prosedur dan sumber daya manusia. Ketergantungan dari setiap komponen sangatlah menentukan keberhasilan operasional yang dilakukan, namun suatu keberhasilan akan terasa kurang tanpa melibatkan faktor keamanan. Hal ini menjadi alasan utama untuk memperhatikan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sehingga setiap informasi yang dimiliki benar-benar diperlakukan sebagai aset yang berharga bagi sebuah instansi. Dalam menjamin keamanan operasional tidak hanya terkait teknologi pelindungnya, namun kebijakan yang jelas dalam melakukan keamanan operasional sangat penting karena ancaman sebenarnya berasal dari sumber daya internal instansi.

Untuk meminimalisasi ancaman, keamanan operasional distandarisasi dan melakukan tata cara atau panduan yang tepat guna mengurangi dan menjaga dari ancaman risiko. Jadi, tanpa kebijakan dan prosedur yang baik maka segala ancaman akan mudah mengganggu. Untuk setiap divisi teknologi informasi (TI) disarankan untuk menjalankan kebijakan *corporate user* dalam menggunakan aset teknologi informasi (TI). Kebijakan ini berisi tiga aktivitas untuk dijalankan, antara lain yang pertama *control and protection*. Aktivitas ini berfungsi untuk mengatur dan melindungi operasional untuk mencapai tingkat keamanan yang optimal. Kedua, *monitoring and auditing*. Aktivitas ini berfungsi untuk mengetahui dan menjamin sejauh mana keamanan yang telah dicapai. Terakhir, *threat and vulnerabilities*. Aktivitas ini berisi pemahaman tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang telah dilakukan. Jadi, secara garis besar keamanan informasi adalah aset untuk semua individu dan proses bisnis yang wajib dikelola agar tidak menghambat atau merugikan tujuan sebuah instansi.

Hal ini juga sesuai dengan fungsi utama dari proses APO13 (*Manage Security*). Berdasarkan hasil evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan menggunakan kerangka kerja COBIT 5, diberikan beberapa rekomendasi yang dapat digunakan sebagai pengelola keamanan (APO13). Bentuk rekomendasi didasarkan atas temuan negatif dari proses APO13 (*Manage Security*). Berikut beberapa rekomendasi yang disarankan untuk proses APO13 (*Manage Security*), antara lain rekomendasi pertama memberikan edukasi terhadap seluruh pengguna terkait bagaimana cara untuk membuat *password* agar mudah diingat. Rekomendasi kedua adalah menjadwalkan pengguna untuk senantiasa mengganti *password* secara berkala maksimal satu bulan sekali.

Rekomendasi ketiga adalah mencegah usaha *login* ilegal yang dilakukan secara berturut-turut dengan lebih meningkatkan tingkat keamanan aplikasi. Rekomendasi keempat adalah mendokumentasikan usaha *login* yang tidak berhasil dan setiap komunikasi yang dilakukan oleh pengguna. Menambah fasilitas bantuan (*help*) yang dapat mempermudah penggunaan aset teknologi khususnya keamanan informasi. Rekomendasi kelima adalah melakukan *backup* data dan informasi secara rutin seperti 8 atau 12 jam sekali dalam sehari. Rekomendasi keenam adalah menjalankan program audit internal keamanan sebagai salah satu usaha untuk memantau dan menilai apakah peningkatan efektivitas prosedur dan kebijakan informasi yang telah dibuat pada dokumen *DAN'IS Policy* tentang *IS Security Policy* telah sesuai atau belum.

Keenam rekomendasi merupakan usaha dalam menindaklanjuti permasalahan dari proses APO13 (*Manage Security*), yaitu belum terjaminnya seluruh keamanan data. Terkadang data dapat diakses oleh pihak luar yang sebenarnya tidak boleh terjadi. Akan berakibat fatal bila data yang terekspos sangat penting bagi perusahaan. Sebab, risiko penyalahgunaan data akan terus berpotensi. Rekomendasi ketujuh adalah mendefinisikan dokumen tertulis yang berisi prosedur ataupun kebijakan tentang manfaat dari manajemen keamanan informasi. Dalam kebijakan atau dokumen yang dimaksud perlu diidentifikasi tujuan dari tiap proses, mendefinisikan individu-individu yang bertanggung jawab pada tiap proses, serta mengalokasikan sumber daya dan informasi yang dibutuhkan dalam melaksanakan proses-proses yang dimaksud.

Rekomendasi terakhir adalah mendefinisikan hasil tiap proses yang telah dilakukan dengan cara mendokumentasikan kegiatan manajemen keamanan informasi serta mengawasi dan menerapkan manfaat yang diperoleh. Bentuk kedua rekomendasi merupakan langkah yang diciptakan guna meningkatkan tingkat kapabilitas (*capability level*) perusahaan dari kondisi sekarang menuju kondisi yang diharapkan. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui *targeted level* perusahaan dari proses ini berada pada *level* ke-5 (*optimizing process*).

Tabel 5.2 Rekomendasi (APO13)

PROSES	REKOMENDASI	ALASAN
APO13	Memberikan edukasi terhadap seluruh pengguna terkait bagaimana cara untuk membuat <i>password</i> agar mudah diingat.	Bentuk rekomendasi didasarkan atas masalah yang ditemukan dari hasil observasi dan wawancara pada pengelolaan keamanan informasi.
	Menjadwalkan pengguna untuk senantiasa mengganti <i>password</i> secara berkala maksimal satu bulan sekali.	

Tabel 5.2 Rekomendasi (APO13) (lanjutan)

PROSES	REKOMENDASI	ALASAN
	Mencegah usaha <i>login</i> ilegal yang dilakukan secara berturut-turut dengan lebih meningkatkan tingkat keamanan aplikasi.	
	Mendokumentasikan usaha <i>login</i> yang tidak berhasil dan setiap komunikasi yang dilakukan oleh pengguna.	
	Melakukan <i>backup</i> data dan informasi secara rutin seperti 8 atau 12 jam sekali dalam sehari.	
	Menjalankan program audit internal keamanan sebagai salah satu usaha untuk memantau dan menilai apakah peningkatan efektivitas prosedur dan kebijakan informasi yang telah dibuat pada dokumen <i>DAN'IS Policy</i> tentang <i>IS Security Policy</i> telah sesuai atau belum.	
	Mendefinisikan dokumen tertulis yang berisi prosedur ataupun kebijakan tentang manfaat dari manajemen keamanan informasi.	Bentuk rekomendasi diciptakan untuk meraih tingkat pencapaian (<i>targeted level</i>) yang diharapkan pada level 5 (<i>optimizing process</i>).
	Mendefinisikan hasil tiap proses yang telah dilakukan dengan cara mendokumentasikan kegiatan manajemen keamanan informasi serta mengawasi dan menerapkan manfaat yang diperoleh.	

5.3 Manage Security Services (DSS05)

Terkait sub bab ini, pembahasan materi akan difokuskan terhadap pengelolaan layanan keamanan informasi. Suatu layanan akan menciptakan sebuah sistem yang menjadi acuan dalam pengelolaan. Sistem ini dikenal dengan istilah *Information Security Management System (ISMS)*. Menurut Ibrahim & Koswara (2010), *Information Security Management System (ISMS)* merupakan sebuah kesatuan sistem yang disusun berdasarkan pendekatan risiko bisnis, pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan, dan peningkatan keamanan informasi perusahaan.



Sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut, antara lain yang pertama struktur organisasi. Hal ini merupakan keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi seperti *Chief Security Officer* dan beberapa lainnya. Kedua adalah kebijakan keamanan. Contoh dari kebijakan ini adanya kejadian pelanggaran keamanan dan kelemahan sistem informasi yang harus segera dilaporkan. Setelah itu, pihak administrator mengambil dan menjalankan keputusan secara cepat dan tepat. Akses terhadap sumber daya jaringan harus dikendalikan secara ketat untuk mencegah akses yang tidak diinginkan. Ketiga adalah prosedur dan proses. Kedua hal ini berkaitan pada usaha pengimplementasian keamanan informasi pada perusahaan. Terakhir adalah tentang tanggung jawab. Hal ini mencerminkan konsep dan aspek-aspek keamanan informasi perusahaan pada *job description* dari setiap jabatan. Begitu pula dengan adanya program-program pelatihan dan pembinaan tanggung jawab keamanan informasi perusahaan untuk staf dan karyawannya.

Selain mengevaluasi keamanan dari setiap aset teknologi, dibutuhkan pula ketahanan terhadap keamanan organisasi. Menurut Ibrahim & Koswara (2010), setiap staf keamanan teknologi informasi (TI) harus mengerti dan menerapkan kontrol manajemen, operasional, dan teknis. Penerapan semua jenis kontrol membutuhkan staf keamanan teknologi informasi (TI) yang berkompeten. Para staf memiliki dua fungsi utama, antara lain sebagai spesialis pengadaan barang yang meninjau spesifikasi dari sebuah *system upgrade* dan sebagai pengajar tentang kesadaran akan keamanan teknologi informasi (TI). Namun kenyataannya, banyak organisasi yang dihadapkan oleh kurangnya sumber daya dalam menjalankan dua peran. Oleh karena itu, kebijakan dalam penentuan staf ini harus direncanakan sedini mungkin sebagai pondasi awal organisasi untuk berinvestasi tentang kemajuan keamanan teknologi informasi (TI), khususnya pada layanan keamanan informasi. Hal ini juga sesuai dengan fungsi utama dari proses DSS05 (*Manage Security Services*).

Berdasarkan hasil evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan pada divisi *Danone Information Systems* (DAN'IS) untuk PT Tirta Investama (AQUA) Pandaan menggunakan kerangka kerja COBIT 5, diberikan beberapa rekomendasi yang dapat digunakan sebagai pengelola layanan keamanan informasi (DSS05). Bentuk rekomendasi didasarkan atas temuan negatif dari ketiga proses. Berikut beberapa rekomendasi yang disarankan untuk proses DSS05 (*Manage Security Services*), antara lain rekomendasi pertama adalah meningkatkan intensitas pelaksanaan kebijakan terhadap penggunaan perangkat lunak (*software*) yang belum sepenuhnya dikenali guna menghindari ancaman dari *malware*. Kebijakan ini telah terlampir pada dokumen *IS Security Policy* pada Bab *VMWare Security Guidelines*. Rekomendasi kedua adalah meningkatkan intensitas pelaksanaan kebijakan keamanan konektivitas sebagai prinsip dasar kegiatan mengelola keamanan konektivitas. Selain itu, melakukan *penetration test* secara berkala untuk menilai kecukupan keamanan jaringan dan hasilnya didokumentasikan dengan baik.

Menurut Octavianus (2014), *penetration test* merupakan suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan perusahaan untuk menemukan kelemahan yang ada pada sistem jaringan. Orang yang melakukan kegiatan ini disebut sebagai *penetration tester*. Kebijakan ini telah terlampir pada dokumen *IS Security Policy* pada Bab *Controlling Access to Information*. Rekomendasi ketiga adalah menerapkan secara rutin tentang kebijakan keamanan perangkat akhir (*endpoint*) sebagai prinsip dasar kegiatan mengelola keamanan seperti *laptop*, *dekstop*, dan *server*. Hal ini dapat dilakukan dalam kurun waktu minimal sekali dalam 1 hari. Kebijakan ini telah terlampir pada dokumen *IS Security Policy* pada Bab *Endpoints Security Policy*. Rekomendasi keempat adalah meninjau ulang tentang kelengkapan dokumen yang berisi pembagian hak akses pengguna sesuai dengan kebutuhan unit bisnis perusahaan. Hal ini telah terlampir pada dokumen *Danone Government (DanGo)* pada Bab *IS Interconnection Authorization*.

Rekomendasi kelima adalah mengganti atau menambah jenis antivirus bertipe *full edition* dan membeli anti *malware* pendukung. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui jenis antivirus yang digunakan pada PT Tirta Investama (AQUA) Pandaan saat ini adalah *Symantec Endpoint Protection (SEP)* versi 14 atau yang terbaru. Setelah itu, memperbarui detektor suhu ruang *server* menjadi bentuk digital yang dapat memberikan perubahan suhu dan memperbarui resolusi *Closed Circuit Television (CCTV)* menjadi bentuk digital pula serta mengatur ulang tingkat warna video sehingga citra ruang aset teknologi informasi (TI) terlihat lebih jelas. Kelima rekomendasi ini merupakan usaha dalam menindaklanjuti permasalahan dari proses *DSS05 (Manage Security Services)*, yaitu belum terjaminnya seluruh keamanan aset teknologi informasi (TI). Beberapa aset pernah mengalami pernah mengalami kerusakan bahkan kehilangan data akibat serangan *malware* seperti virus, *worm spyware*, dan *spam*.

Seperti masalah pada proses *EDM03 (Ensure Risk Optimization)*, hal ini tentu berimbas terhadap seluruh aktivitas perusahaan yang berkaitan dengan penggunaan teknologi informasi (TI). Sebab, divisi *DAN'IS* telah menerapkan sistem informasi berbasis *Enterprise Resources Planing (ERP)* untuk beberapa perusahaan Danone, termasuk PT Tirta Investama (AQUA) Pandaan. Rekomendasi terakhir adalah mendefinisikan dokumen tertulis yang berisi tentang pengelolaan jalannya proses kinerja yang digunakan sebagai prosedur atau panduan dalam mengoperasikan kegiatan layanan keamanan informasi, dimana standar ini juga mendefinisikan urutan interaksi dari satu proses ke proses lainnya, mendefinisikan kompetensi dan infrastruktur yang dibutuhkan serta metode yang cocok untuk pemantauan proses kinerja. Bentuk rekomendasi terakhir merupakan langkah yang diciptakan guna meningkatkan tingkat kapabilitas (*capability level*) perusahaan dari kondisi sekarang menuju kondisi yang diharapkan. Berdasarkan hasil wawancara dengan pihak *DAN'IS Network Analyst* pada Lampiran A.3 dan A.4, diketahui *targeted level* perusahaan dari proses ini berada pada *level ke-5 (optimizing process)*.

Tabel 5.3 Rekomendasi (DSS05)

PROSES	REKOMENDASI	ALASAN
DSS05	Meningkatkan intensitas pelaksanaan kebijakan dari dokumen <i>IS Security Policy</i> pada Bab <i>VMWare Security Guidelines</i> terhadap penggunaan perangkat lunak (<i>software</i>) yang belum sepenuhnya dikenali guna menghindari ancaman dari <i>malware</i> .	Bentuk rekomendasi didasarkan atas masalah yang ditemukan dari hasil observasi dan wawancara pada pengelolaan keamanan informasi.
	Meningkatkan intensitas pelaksanaan kebijakan pada dokumen <i>IS Security Policy</i> pada Bab <i>Controlling Access to Information</i> terhadap keamanan konektivitas sebagai prinsip dasar kegiatan mengelola keamanan konektivitas.	
	Menerapkan secara rutin tentang kebijakan dokumen <i>IS Security Policy</i> pada Bab <i>Endpoints Security Policy</i> terhadap keamanan perangkat akhir (<i>endpoint</i>) sebagai prinsip dasar kegiatan mengelola keamanan seperti <i>laptop</i> , <i>dekstop</i> dan <i>server</i> .	
	Meninjau ulang tentang kelengkapan dokumen yang berisi pembagian hak akses pengguna sesuai dengan kebutuhan unit bisnis perusahaan. Hal ini terlampir pada dokumen <i>Danone Government (DanGo)</i> pada Bab <i>IS Interconnection Authorization</i> .	
	Mengganti atau menambah jenis antivirus bertipe <i>full edition</i> dan membeli anti <i>malware</i> pendukung.	
	Mendefinisikan dokumen tertulis yang berisi tentang pengelolaan jalannya proses kinerja yang digunakan sebagai prosedur atau panduan dalam mengoperasikan kegiatan layanan keamanan informasi, dimana standar yang dimaksud juga mendefinisikan urutan interaksi dari satu proses ke proses lainnya, mendefinisikan kompetensi dan infrastruktur yang dibutuhkan serta metode yang cocok untuk pemantauan proses kinerja yang dimaksud.	





BAB 6 KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan menggunakan kerangka kerja COBIT 5 pada PT Tirta Investama (AQUA) Pandaan, dipaparkan kesimpulan sebagai berikut. Pada proses EDM03 (*Ensure Risk Optimization*), diketahui tingkat indikator proses kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved (F)* dari dua atribut proses yang ada. Pada *level 3 (established process)*, mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Kemudian, pada proses APO13 (*Manage Security*), diketahui tingkat indikator proses kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved (F)* dari dua atribut proses yang ada. Seperti deskripsi sebelumnya, *level 3 (established process)* mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik. Terakhir, pada proses DSS05 (*Manage Security Services*), diketahui tingkat indikator proses kapabilitasnya berada pada *level 3 (established process)*. Hal ini disebabkan pada *level 4 (predictable process)* hanya meraih sekali *Fully Achieved (F)* dari dua atribut proses yang ada. Seperti penjelasan sebelumnya, *level 3 (established process)* mengindikasikan proses teknologi informasi (TI) telah terdefinisi dan terstandarisasi dengan baik.

Selanjutnya, pada proses EDM03 (*Ensure Risk Optimization*), diketahui tingkat kesenjangan (*gap level*) antara pencapaian perusahaan saat ini dengan yang diharapkan oleh divisi *Danone Information Systems (DAN'IS)* adalah 1 *level*. Hasil ini diperoleh dari selisih antara target pencapaian (*targeted level*) pada *level 4 (predictable process)* dengan tingkat kapabilitas (*capability level*) pada *level 3 (established process)*. Sedangkan pada proses APO13 (*Manage Security*), diketahui tingkat kesenjangan (*gap level*) antara pencapaian perusahaan saat ini dengan yang diharapkan oleh divisi *DAN'IS* adalah 2 *level*. Hasil ini diperoleh dari selisih antara target pencapaian (*targeted level*) pada *level 5 (optimizing process)* dengan tingkat kapabilitas (*capability level*) pada *level 3 (established process)*. Terakhir, pada proses DSS05 (*Manage Security Services*), diketahui tingkat kesenjangan (*gap level*) antara pencapaian perusahaan saat ini dengan yang diharapkan oleh divisi *DAN'IS* adalah 2 *level*. Hasil ini diperoleh dari selisih antara target pencapaian (*targeted level*) pada *level 5 (optimizing process)* dengan tingkat kapabilitas (*capability level*) pada *level 3 (established process)*. Terakhir, pada proses EDM03 (*Ensure Risk Optimization*), diberikan tiga rekomendasi dari proses ini. Pada proses APO13 (*Manage Security*), diberikan delapan rekomendasi dari proses ini. Pada proses DSS05 (*Manage Security Services*), diberikan enam rekomendasi dari proses ini. Ketiga rekomendasi ini diperoleh dari analisis lembar penilaian yang bertujuan mencapai *targeted level* yang diharapkan oleh perusahaan.

6.2 Saran

Setelah dipaparkan beberapa kesimpulan dari penelitian ini, diberikan saran sebagai penunjang aktivitas evaluasi proses optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan di kemudian hari. Saran ini ditujukan kepada peneliti selanjutnya untuk menggunakan metode lain, seperti indeks Keamanan Informasi (KAMI), ISO 27001, *Information Technology Infrastructure Library* (ITIL), dan metode lainnya. Sehingga memperkaya kajian keilmuan tentang optimasi risiko, pengelolaan keamanan, dan pengelolaan layanan keamanan.



DAFTAR PUSTAKA

- Adi, Suroto. 2015. Gap Analysis (Analisa Kesenjangan), [online]. Tersedia di: <<https://sis.binus.ac.id/2015/07/28/gap-analysis-analisa-kesenjangan/>> [Diakses 5 Maret 2018]
- Afrianto, Budi. 2013. Pengertian Risk Appetite, Risk Tolerance, dan Risk Attitude, [online]. Tersedia di: <<http://www.akademiasuransi.org/2013/05/pengertian-risk-appetite-risk-tolerance.html>> [Diakses 2 Februari 2018]
- Alfara, Jennifer F. 2008. *Overview of Frameworks: COBIT, COSO, ITIL, ISO, and more*. [e-book] Resources Global Professionals.
- Daniri, Achmad. 2005. *Good Corporate Governance Konsep dan Penerapannya*. Jakarta: Ray Indonesia.
- Desy, Innike. 2014. *Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis Di Divisi TI PT Bank XYZ Surabaya*, [e-journal]. Tersedia melalui: <<http://is.its.ac.id/pubs/oajis/index.php/home/detail/1432/PENILAIAN-RISIKO-KEAMANAN-INFORMASI-MENGGUNAKANMETODE-FAILURE-MODE-AND-EFFECTS-ANALYSIS-DI-DIVISI-TIPT-BANK-XYZ-SURABAYA>> [Diakses 9 April 2018]
- Fitriah, Devi. 2018. *Jurnal Sistem Informasi. Audit Sistem Informasi/Teknologi Informasi Dengan Kerangka Kerja COBIT Untuk Evaluasi Manajemen Teknologi Informasi Di Universitas XYZ*, [e-journal]. Tersedia melalui: <<http://jsi.cs.ui.ac.id/index.php/jsi/article/view/243>> [Diakses 9 April 2018]
- Ibrahim, R.N., & Hadi Koswara. 2010. *Jurnal Computech & Bisnis. Kerangka Kerja Manajemen Keamanan Berdasar ISO 27000 Beserta Turunannya Untuk Sistem Pada E-Government*, [e-journal] 4(1). Tersedia melalui: <<http://jurnal.stmik-mi.ac.id/index.php/jcb/article/view/45>> [Diakses 9 April 2018]
- ISACA. 2012a. *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. USA: IT Governance Institute.
- ISACA. 2012b. *COBIT 5 Enabling Processes*. USA: IT Governance Institute.
- ISACA. 2013a. *COBIT 5 for Risk*. USA: IT Governance Institute.
- ISACA. 2013b. *COBIT 5 Processes Assessment*. USA: IT Governance Institute.
- ISACA. 2013c. *COBIT 5 Self-Assessment Guide: Using COBIT 5*. USA: IT Governance Institute.
- IT Governance Institute. 2007. *COBIT 4.1 Framework Control Objective, Management Guidelines, Maturity Models*. IT Governance Institute.



- Jogiyanto. Abdillah. 2011. *Sistem Tata Kelola Teknologi Informasi*. Jakarta: Penerbit ANDI.
- Mufti, Raja Gantino. 2017. JPTIHK. *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk)*, [e-journal] 1(12). Tersedia melalui: <<http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/580>> [Diakses 9 April 2018]
- Ningsih, Erna. 2001. *Pemahaman Tata Kelola*, [online]. Tersedia di: <<https://www.scribd.com/doc/111637278/1-Pemahaman-Tata-Kelola>> [Diakses 10 Mei 2018]
- Octavianus, Boni. 2014. COOLNETKID. *Apa itu Penetration Testing?*, [online]. Tersedia di: <<https://coolnetkid.wordpress.com/2014/05/24/penetration-testing/>> [Diakses 12 Mei 2018]
- PT TIRTA INVESTAMA. AQUA. DANONE, [online]. Tersedia di: <http://aqua.com/tentang_aqua> [Diakses 1 Februari 2018]
- Riadi, Fransisca Tiarawati, Augie David Manuputty, dan Ahadi Saputra. 2018. JUTEI (Jurnal Teknologi Informasi). *Evaluasi Manajemen Risiko Keamanan Informasi dengan Menggunakan COBIT 5 Subdomain EDM03 (Ensure Risk Optimization): Studi Kasus : Satuan Organisasi XYZ – Lembaga ABC*, [e-journal] 2(1). Tersedia melalui: <<https://jutei.ukdw.ac.id/index.php/jurnal/article/view/53>> [Diakses 9 April 2018]
- Sarno, Ritanarto. 2009. *Audit Sistem dan Teknologi Informasi*. Surabaya: ITS Press.
- Sarno, Ritanarto. Iffano. Irsyat. 2009. *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. Surabaya: ITS Press.
- Sulistya, Anggun. 2013. *Evaluasi Program dan Penyelenggaraan Pelatihan*, [online]. Tersedia di: <<https://goenable.wordpress.com/2014/04/03/evaluasi-program-dan-penyelenggaraan-pelatihan/>> [Diakses 11 Mei 2018]
- Surendro, Kridanto. 2009. *Implementasi Tata kelola sistem keamanan informasi*. Bandung: Informatika.
- Yasa, I.W.W., I.G. B Sila Dharma, dan I Gst. Ketut Sudipta. 2013. *Manajemen Risiko Operasional Dan Pemeliharaan Tempat Pembuangan Akhir (TPA) Regional Bangli Di Kabupaten Bangli*, [e-journal] 1(2). Tersedia melalui: <<https://ojs.unud.ac.id/index.php/jsn/article/view/5795>> [Diakses 9 April 2018]