

**EVALUASI TATA KELOLA KEAMANAN INFORMASI
MENGUNAKAN COBIT 5 PADA DOMAIN APO13 DAN
DSS05
(STUDI PADA PT GAGAS ENERGI INDONESIA)**

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Yauma Dzikri Imany
NIM: 155150407111026



PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2019

PENGESAHAN

EVALUASI TATA KELOLA KEAMANAN INFORMASI MENGGUNAKAN COBIT 5 PADA
DOMAIN APO13 DAN DSS05 (STUDI PADA PT GAGAS ENERGI INDONESIA)

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Yauma Dzikri Imany
NIM: 155150407111026

Skripsi ini telah diuji dan dinyatakan lulus pada
11 Juli 2019

Telah diperiksa dan disetujui oleh:

Pembimbing I

Pembimbing II

Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.
NIK: 2017128704092001

Admaja Dwi Herlambang, S.Pd., M.Pd.
NIP: 198908022019031007

Mengetahui
Ketua Jurusan Sistem Informasi



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 referensi.

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, 11 Juli 2019



Yauma Dzikri Imany

NIM: 155150407111026

PRAKATA

Puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat, taufik serta hidayah-Nya sehingga laporan skripsi dengan judul “Evaluasi Tata Kelola Keamanan Informasi Menggunakan Framework COBIT 5 Pada Domain APO13 dan DSS05 (Studi Kasus : PT Gagas Energi Indonesia)” dapat terselesaikan dengan baik.

Penulis menyadari tanpa adanya bantuan dari berbagai pihak, maka skripsi ini tidak akan mampu penulis selesaikan sendiri. Oleh karenanya penulis ingin menyampaikan rasa hormat dan terima kasih kepada :

1. Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom. sebagai pembimbing 1 penulis dan Admaja Dwi Herlambang, S.Pd., M.Pd sebagai pembimbing 2 penulis yang dengan sabar membimbing dan mengarahkan penulis untuk menyelesaikan skripsi ini.
2. Fajar Pradana S.ST., M.Eng sebagai pembimbing akademik penulis yang selalu mendampingi dan memberikan nasihat akademik selama menempuh masa studi.
3. Yusi Tyroni Mursityo, S.Kom., M.AB. sebagai Ketua Program Studi Sistem Informasi.
4. Dr. Eng., Herman Tolle, S.T, M.T. sebagai Ketua Jurusan Sistem Informasi.
5. Wayan Firdaus Mahmudy., S.Si., M.T, PhD sebagai Dekan Fakultas Ilmu Komputer Universitas Brawijaya
6. Bapak Moch. Rashid Ridho, Bapak Andika Agustafia dan Ibu Herlina serta seluruh pihak dari PT Gagas Energi Indonesia yang telah memberikan izin serta membantu penulis untuk melakukan penelitian ini.
7. Keluarga penulis terutama kedua orang tua penulis yang telah membesarkan penulis serta memberikan dukungan dan doa bagi penulis untuk menyelesaikan skripsi.
8. Teman-teman penulis yang tidak bisa disebutkan satu persatu yang telah banyak membantu dan mendorong penulis untuk menyelesaikan skripsi.

Penulis menyadari bahwa skripsi yang telah disusun ini masih memiliki banyak kekurangan. Oleh karena itu, penulis mengharapkan adanya kritik dan saran yang membangun bagi skripsi ini. Akhir kata penulis berharap agar skripsi ini mampu memberikan manfaat bagi pihak yang membutuhkannya.

Malang, 11 Juli 2019

Penulis

imanyauma@student.ub.ac.id

ABSTRAK

Yauma Dzikri Imany, Evaluasi Tata Kelola Keamanan Informasi Menggunakan Framework COBIT 5 Pada Domain APO13 dan DSS05 (Studi Pada PT Gagas Energi Indonesia)

Pembimbing: Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom dan Admaja Dwi Herlambang S.Pd., M.Pd.

PT Gagas Energi Indonesia merupakan salah satu perusahaan yang menerapkan Teknologi Informasi (TI) untuk menunjang proses bisnisnya. Aktivitas pengelolaan TI di lingkungan PT Gagas Energi Indonesia dilakukan dibawah *HR & IT Department* melalui Satuan Kerja TI. Pemanfaatan TI membutuhkan banyak data dan informasi untuk mendukung proses bisnis yang berjalan. Banyaknya data dan informasi penting yang disimpan dalam TI maka perlu dipastikan data dan informasi yang tersimpan pada TI yang diterapkan telah diamankan dengan baik untuk mencegah adanya ancaman terhadap sistem yang merugikan bisnis. Kualitas pengelolaan keamanan informasi perlu untuk diukur untuk memastikan teknologi informasi yang diterapkan benar-benar aman.

Untuk mengukur kualitas keamanan pengelolaan keamanan informasi, maka perlu dilakukan evaluasi dan analisis untuk mengetahui sejauh mana pencapaian keamanan informasi yang telah diterapkan. Secara umum, evaluasi keamanan informasi dilakukan dengan membandingkan antara pencapaian yang telah dicapai oleh perusahaan dan pencapaian yang diinginkan oleh perusahaan. Penelitian ini menggunakan kerangka kerja COBIT 5 dengan fokus pada proses APO13 (Mengelola Keamanan) dan DSS05 (Mengelola Layanan Keamanan) dengan menggunakan pendekatan kualitatif deskriptif untuk pengumpulan data. Pengumpulan data dilakukan dengan melakukan observasi serta menggunakan instrumen lembar penilaian dan wawancara. Berdasarkan hasil penelitian, kedua proses tersebut telah mencapai level 2 (*Managed Process*), dengan tingkat pencapaian yang diinginkan perusahaan berada pada level 3 (*Established Process*). Sehingga terjadi kesenjangan (*gap level*) sebesar 1 level pada masing-masing proses. Berikutnya akan diberikan sejumlah rekomendasi yang difokuskan pada pengelolaan keamanan dan layanan keamanan, serta perbaikan dokumen dan prosedur yang dibutuhkan berdasarkan hasil temuan penelitian dengan mempertimbangkan kesenjangan (*gap level*) yang ada.

Kata kunci: evaluasi, keamanan informasi, pengelolaan keamanan, pengelolaan layanan keamanan, COBIT 5

ABSTRACT

Yauma Dzikri Imany, Evaluation of Information Security Governance Using COBIT 5 in APO13 and DSS05 Domains (Study at PT Gagas Energi Indonesia)

Supervisors: Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom and Admaja Dwi Herlambang S.Pd., M.Pd.

PT Gagas Energi Indonesia is one of the company that implemented information technology (IT) to support their business process. IT activity in PT Gagas Energi Indonesia environment is managed under IT task force under HR & IT Department. IT utilization needs many of data and information to support running business process. The amount of data and information stored in IT systems is need to be secured better to ensure there is no threat to a business. Information security quality measurement is needed to ensure implemented information technology is still safe.

To measure the quality of information security management, the company is need to do evaluation and analyze to measure how far the company achievement for information security. Information security measure is doing by comparing current achievement that achieve by a company with achievement that desired by company. This research using COBIT 5 framework focusing on APO13 (Manage Security) and DSS05 (Manage Security Services) process with qualitative approach methodology for data gathering. Data gathering is doing by observation and using assessment sheet and interview instrument. Based on result, both of process is achieved at level 2 (Managed Process) while achievement level desired by company is at level 3 (Established Process). So that gap level is 1 level at each process. The next step is giving some recommendation with focused on manage security and security services, improvement of the document and procedure with based on research evidence considering gap level exist.

Keywords : evaluation, information security, manage security, manage security services, COBIT 5

DAFTAR ISI

PENGESAHAN	ii
PERNYATAAN ORISINALITAS	iii
PRAKATA.....	iv
ABSTRAK.....	v
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMPIRAN	xii
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan	4
1.4 Manfaat.....	4
1.5 Batasan Masalah.....	4
1.6 Sistematika Pembahasan.....	5
BAB 2 LANDASAN KEPUSTAKAAN	6
2.1 Penelitian Sebelumnya	6
2.2 Profil PT Gas Energi Indonesia	7
2.2.1 Visi	8
2.2.2 Misi	8
2.2.3 Struktur Organisasi.....	8
2.3 Evaluasi	9
2.4 Tata Kelola	9
2.5 Keamanan Informasi.....	10
2.6 Manajemen Keamanan Informasi	11
2.7 Pengelolaan Keamanan	13
2.8 Pengelolaan Layanan Keamanan	13
2.9 COBIT 5.....	13
2.10 Model Proses dan Domain dalam COBIT 5.....	16

2.10.1 Evaluate, Direct and Monitor (EDM).....	17
2.10.2 Align, Plan and Organize (APO).....	17
2.10.3 Build, Acquire and Implement (BAI).....	18
2.10.4 Deliver, Service and Support (DSS).....	19
2.10.5 Monitor, Evaluate and Assess	19
2.11 COBIT 5 Process Capability Model	20
2.12 COBIT 5 Self Assessment	29
2.13 Keamanan Informasi Pada COBIT 5	30
2.13.1 Manage Security (APO13).....	30
2.13.2 Manage Security Services (DSS05).....	32
2.14 RACI Chart.....	34
BAB 3 METODOLOGI	39
3.1 Metodologi Penelitian	39
3.2 Studi Literatur	40
3.3 RACI Chart.....	41
3.4 Pengumpulan Data	41
3.5 Triangulasi Data	42
3.6 Self Assesment	42
3.7 Pemberian Rekomendasi.....	42
3.8 Kesimpulan dan Saran	43
BAB 4 HASIL EVALUASI	44
4.1 Manage Security (APO13).....	44
4.2 Manage Security Services (DSS05).....	52
BAB 5 PEMBAHASAN.....	64
5.1 Manage Security (APO13).....	64
5.2 Manage Security Services (DSS05).....	67
BAB 6 PENUTUP	73
6.1 Kesimpulan.....	73
6.2 Saran	74
DAFTAR REFERENSI	75
LAMPIRAN A PEMETAAN RESPONDEN	78
LAMPIRAN B HASIL OBSERVASI DOKUMEN	81





DAFTAR TABEL

Tabel 2.1 Perbedaan Tata Kelola dan Manajemen	15
Tabel 2.2 Domain EDM.....	17
Tabel 2.3 Domain APO	17
Tabel 2.4 Domain BAI.....	18
Tabel 2.5 Domain DSS	19
Tabel 2.6 Domain MEA.....	19
Tabel 2.7 Penilaian Level 2 pada COBIT 5	20
Tabel 2.8 Penilaian Level 3 COBIT 5	23
Tabel 2.9 Penilaian Level 4 COBIT 5	25
Tabel 2.10 Penilaian Level 5 COBIT 5	27
Tabel 2.11 Kategori Penilaian Kapabilitas	29
Tabel 2.12 Penjelasan <i>Outcome</i> Proses APO13	30
Tabel 2.13 Penjelasan <i>Outcome</i> Proses DSS05	32
Tabel 4.1 Analisis RACI <i>Chart</i> APO13	44
Tabel 4.2 Pemetaan RACI <i>Chart</i> Terhadap Proses APO13	45
Tabel 4.3 Hasil Pemetaan Dokumen/Kebijakan Proses APO13	47
Tabel 4.4 Penilaian Level 1 Proses APO13	50
Tabel 4.5 Perhitungan Kapabilitas Proses APO13	51
Tabel 4.6 Penilaian Pada Proses APO13.....	52
Tabel 4.7 Analisis Kesenjangan Proses APO13.....	52
Tabel 4.8 Analisis RACI <i>Chart</i> DSS05	53
Tabel 4.9 Pemetaan RACI <i>Chart</i> Terhadap Proses DSS05	54
Tabel 4.10 Pemetaan Kebijakan/Dokumen Proses DSS05.....	57
Tabel 4.11 Penilaian Level 1 Proses DSS05	60
Tabel 4.12 Penilaian Kapabilitas Proses DSS05	62
Tabel 4.13 Penilaian Pada Proses DSS05.....	62
Tabel 4.14 Analisis Kesenjangan Proses DSS05.....	63
Tabel 5.1 Pemetaan Rekomendasi Proses APO13	66
Tabel 5.2 Pemetaan Rekomendasi Proses DSS05	70

DAFTAR GAMBAR

Gambar 2.1 Struktur Organisasi.....	8
Gambar 2.2 Aspek Utama Keamanan Informasi.....	11
Gambar 2.3 Prinsip COBIT 5.....	14
Gambar 2.4 <i>Enabler</i> pada COBIT 5.....	15
Gambar 2.5 Model Proses pada COBIT 5.....	16
Gambar 2.6 RACI <i>Chart</i> APO13.....	35
Gambar 2.7 RACI <i>Chart</i> DSS05.....	36
Gambar 3.1 Alur Penelitian.....	40



DAFTAR LAMPIRAN

LAMPIRAN A PEMETAAN RESPONDEN	78
A.1 Pemetaan Responden APO13.....	78
A.2 Pemetaan Responden DSS05	79
A.3 Hasil Wawancara	80
LAMPIRAN B HASIL OBSERVASI DOKUMEN	81
B.1 Dokumen Pedoman Tata Kelola Teknologi Informasi	81
B.2 Prosedur Pengamanan IT.....	82
B.3 Tampilan Dokumen Prosedur Operasi Permasalahan IT.....	83
B.4 Tampilan Prosedur Pengelolaan Permasalahan IT	84
B.5 Tampilan Dokumen Prosedur Pengelolaan Hak Akses.....	85
B.6 Tampilan Prosedur Operasi Instalasi <i>Software</i>	88
B.7 Tampilan Dokumen <i>Grand Design (Roadmap)</i> IT.....	91
B.8 Tampilan Konsep Integrasi ICT	92
B.9 Tampilan Pengelolaan Manajemen Resiko	93
LAMPIRAN C HASIL PENILAIAN	94
C.1 Hasil Penilaian Proses APO13	94
C.2 Hasil Penilaian Proses DSS05	110

BAB 1 PENDAHULUAN

1.1 Latar Belakang

PT Gagas Energi Indonesia merupakan perusahaan yang bergerak dalam bidang usaha penjualan produk berbasis gas bumi dan merupakan anak usaha dari PT Perusahaan Gas Negara (Tbk). Untuk mempermudah penerapan proses bisnis dalam hal penjualan gas ke pelanggan dan membantu kegiatan administrasi sehari-hari dalam perusahaan. Dalam hal penjualan gas, penerapan Teknologi Informasi (TI) dilakukan dengan mengimplementasikan aplikasi *point of sales* (POS) dan aplikasi untuk memonitor pengiriman gas ke pelanggan. Sedangkan dalam hal administrasi, penerapan TI dilakukan dengan mengimplementasikan sistem persuratan, sistem monitor karyawan dan penyimpanan dokumen digital. Penerapan TI di PT Gagas Energi Indonesia membutuhkan data dan informasi yang disimpan sebagai dasar untuk pengambilan keputusan yang sesuai dari masing-masing sistem informasi yang diterapkan. Karena sebagian besar data dan informasi yang disimpan dalam sistem informasi tersebut memiliki sifat yang rahasia, maka pengamanan data dan informasi dalam sistem teknologi informasi merupakan hal yang penting.

Dalam mendukung penerapan TI, PT Gagas Energi Indonesia memiliki unit khusus untuk mendukung pengelolaan TI yang terdiri dari dua unit. Unit pertama yaitu *Information and System Development* yang bertugas untuk mengembangkan sistem dan teknologi informasi yang digunakan sesuai dengan kebutuhan PT Gagas Energi Indonesia. Selain itu, unit ini memiliki tanggungjawab pada pengelolaan TI. Unit lainnya adalah *Infrastructure and Network* yang bertugas untuk menangani permasalahan dalam hal infrastruktur TI yang digunakan di lingkungan PT Gagas Energi Indonesia.

Masalah keamanan menjadi hal yang penting dalam penyimpanan data dan informasi dalam sebuah sistem informasi untuk mencegah adanya ancaman terhadap sistem (Kadir, 2014). Hal tersebut sangat penting mengingat sebagian data yang disimpan dalam sistem informasi memiliki sifat rahasia dan hanya boleh diketahui oleh yang memiliki hak akses. Sehingga, sebuah sistem informasi seharusnya memiliki keamanan yang baik agar data dan informasi yang tersimpan di dalamnya tetap terjaga kerahasiaannya. Berpindahannya informasi ke pihak lain yang tidak memiliki hak akses dapat menimbulkan kerugian bagi pemegang informasi yang bersangkutan (Rahardjo, 1999). Oleh karena itu, keamanan sistem informasi perlu diperhatikan bagi setiap organisasi atau perusahaan yang menerapkan sistem teknologi informasi.

PT Gagas Energi Indonesia sebagai perusahaan yang menerapkan sistem informasi sudah seharusnya memperhatikan masalah keamanan dalam sistem informasi yang digunakan. Dengan semakin banyaknya penggunaan sistem informasi, maka semakin banyak data dan informasi yang disimpan yang sebagian dari data dan informasi tersebut memiliki sifat rahasia. Sehingga dalam hal ini aspek keamanan informasi menjadi penting untuk mengamankan data

yang dimiliki PT Gagas Energi Indonesia. Oleh karena itu, pengukuran pengelolaan keamanan informasi penting dilakukan untuk mengetahui tingkat keamanan informasi pada PT Gagas Energi Indonesia.

Permasalahan keamanan informasi tidak hanya perlu diperhatikan dari sisi teknisnya saja, tetapi juga perlu diperhatikan dari sisi manajemen dan tata kelolanya sehingga tujuan dari penerapan keamanan informasi akan mampu dirasakan oleh perusahaan. Dalam hal ini, PT Gagas Energi Indonesia telah menerapkan pengamanan informasi secara teknis salah satunya dalam bentuk sistem *fileshare*, yaitu sistem penyimpanan dan berbagi data yang digunakan perusahaan untuk menyimpan dokumen kerja dari masing-masing satuan kerja secara *online*. Sistem tersebut secara teknis telah mampu membagi data sesuai dengan kebutuhan dari satuan kerja, sehingga dari setiap satuan kerja hanya mampu mengakses satu direktori atau *file* dari satuan kerja. Hal ini dilakukan untuk menjaga kerahasiaan data dan informasi yang disimpan pada setiap satuan kerja karena sebagian data dan informasi tersebut bersifat rahasia dan tidak boleh diakses oleh departemen atau satuan kerja lain. Tetapi, dalam penerapannya, pernah terjadi kebocoran informasi yang bersifat rahasia secara internal yang disimpan dalam sistem *fileshare*. Sehingga pihak satuan kerja lain yang seharusnya tidak berhak untuk mengetahui informasi tersebut dapat mengetahui informasi yang memiliki sifat rahasia tersebut. Berpindahnya informasi yang bersifat rahasia pada sistem yang sudah memiliki keamanan cukup baik menunjukkan adanya kekurangan pada pengelolaan prosedur pengamanan informasi yang dilakukan oleh perusahaan. Selain itu, terdapat juga permasalahan lain pada aspek keamanan informasi yaitu adanya serangan pada *website* resmi perusahaan yang apabila kondisi ini terus dibiarkan maka data dan informasi yang disimpan tidak memiliki jaminan yang cukup baik.

Berdasarkan kondisi tersebut, perbaikan tidak cukup hanya dengan memperhatikan aspek teknis, tetapi juga perlu dilakukan perbaikan dari sisi tata kelola dan manajerial. Dalam hal ini, evaluasi pada tata kelola keamanan informasi dapat digunakan sebagai salah satu langkah untuk mengetahui penyebab permasalahan dan memberikan solusi dari masalah yang telah terjadi. Evaluasi memberikan solusi dari sebuah permasalahan dengan memberikan rekomendasi atau saran dari sebuah permasalahan yang ada. Selain itu, evaluasi dapat dilakukan sebagai langkah preventif untuk menanggulangi masalah. Evaluasi yang dilakukan dapat memberikan rekomendasi atau saran yang dapat dilakukan untuk mengurangi atau mencegah permasalahan yang terjadi. Hal ini perlu dilakukan oleh perusahaan dalam rangka mengurangi atau mencegah risiko dari sebuah permasalahan. Dalam hal pengelolaan keamanan informasi, evaluasi perlu dilakukan untuk mengidentifikasi permasalahan dan menanggulangi risiko keamanan dari penerapan TI dalam perusahaan. Evaluasi menjadi penting jika dilihat dari banyak tersimpannya data dan informasi yang bersifat rahasia pada PT Gagas Energi Indonesia sehingga apabila terjadi masalah dalam hal keamanan informasi, maka data yang bersifat rahasia dapat dengan mudah diketahui oleh .

Terdapat beberapa cara untuk evaluasi tata kelola informasi. Pengukuran pada tata kelola keamanan informasi salah satunya adalah dengan menggunakan kerangka kerja (*Control Objectives for Information and related Technology*). COBIT 5 merupakan kerangka kerja yang diterbitkan oleh ISACA untuk membantu manajemen TI dalam perusahaan atau organisasi untuk mencapai tujuan yang diharapkan. COBIT 5 memberikan panduan mengenai pengukuran tata kelola dan manajemen penerapan teknologi informasi untuk membantu penggunaan sumber daya teknologi informasi dan menyeimbangkannya dengan risiko dalam rangka mencapai tujuan organisasi. Kerangka kerja COBIT 5 menyediakan domain yang merupakan kumpulan proses teknologi informasi yang merepresentasikan aktivitas terstruktur dan dapat dikendalikan. COBIT juga dapat memberikan beberapa rekomendasi bagi organisasi untuk melakukan perbaikan, pengembangan dan pengelolaan TI kedepannya.

COBIT 5 dapat mengukur pengelolaan keamanan informasi dengan menyediakan domain dan proses. Domain dan proses tersebut didasarkan pada sektor *IT Goals* ke sepuluh yaitu *Security of Information* yang terdiri dari subdomain EDM03 (Memastikan Optimasi Resiko), APO12 (Mengelola Resiko), APO13 (Mengelola Keamanan), BAI06 (Mengelola Perubahan) dan DSS05 (Mengelola Layanan Keamanan) (Matin, et al., 2017). Terdapatnya domain tersebut menjadikan COBIT 5 dapat digunakan untuk mengevaluasi tata kelola keamanan informasi pada PT Gagas Energi Indonesia. Namun, berdasarkan penjelasan yang telah dijabarkan, maka proses yang digunakan adalah APO13 dan DSS05 karena kedua domain tersebut dapat digunakan untuk melakukan evaluasi manajemen keamanan informasi (ISACA, 2013b).

Berdasarkan penjabaran dari kondisi yang ada pada PT Gagas Energi Indonesia, maka penulis mengajukan penelitian yang berjudul "**Evaluasi Tata Kelola Keamanan Informasi Menggunakan COBIT 5 Domain APO13 dan DSS05 (Studi Pada PT Gagas Energi Indonesia)**". Judul tersebut diambil penulis dengan maksud untuk melakukan evaluasi keamanan informasi pada PT Gagas Energi Indonesia dengan menggunakan COBIT 5, khususnya pada domain APO pada proses APO13 dan DSS pada proses DSS05 untuk mengukur tata kelola keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah dijelaskan pada latar belakang, didapatkan rumusan masalah penelitian sebagai berikut :

1. Bagaimana hasil dari evaluasi tata kelola keamanan informasi pada PT Gagas Energi Indonesia menggunakan kerangka kerja COBIT 5 pada proses APO13 dan DSS05?
2. Bagaimana tingkat pencapaian keamanan informasi saat ini dan yang diinginkan oleh perusahaan pada PT Gagas Energi Indonesia jika diukur menggunakan kerangka kerja COBIT 5 pada proses APO13 dan DSS05?

3. Apa rekomendasi yang diberikan untuk memperbaiki keamanan informasi berdasarkan hasil evaluasi menggunakan kerangka kerja COBIT 5 pada proses APO13 dan DSS05?

1.3 Tujuan

Tujuan dari penelitian yang dilakukan yaitu :

1. Mengetahui hasil evaluasi keamanan informasi pada PT Gagas Energi Indonesia dengan menggunakan COBIT 5 pada proses APO13 dan DSS05.
2. Mengukur tingkat kesenjangan antara keamanan informasi yang telah dicapai dan yang diinginkan oleh PT Gagas Energi Indonesia dengan menggunakan COBIT 5 pada proses APO13 dan DSS05.
3. Memberikan rekomendasi untuk meningkatkan keamanan informasi pada PT Gagas Energi Indonesia berdasarkan hasil penelitian yang dilakukan menggunakan COBIT 5 pada proses APO13 dan DSS05.

1.4 Manfaat

Manfaat yang diharapkan dari penelitian yang dilakukan adalah :

1. Membantu perusahaan mengevaluasi tata kelola keamanan informasi dari sistem informasi yang diterapkan oleh PT Gagas Energi Indonesia.
2. Memberikan rekomendasi perbaikan keamanan informasi pada Gagas Energi Indonesia sehingga terjadi peningkatan kualitas keamanan sistem informasi.
3. Menerapkan ilmu yang telah dipelajari dan menambah ilmu dalam hal evaluasi dan tata kelola sistem informasi, khususnya evaluasi tata kelola keamanan sistem informasi.

1.5 Batasan Masalah

Penelitian ini memiliki beberapa batasan masalah untuk mendapatkan fokus dari penelitian yang dilakukan. Sehingga dalam penelitian ini memiliki batasan sebagai berikut :

1. Evaluasi tata kelola keamanan informasi dilakukan pada PT Gagas Energi Indonesia.
2. Fokus dari penelitian berada dalam ruang lingkup tata kelola manajemen keamanan informasi yang diimplementasikan oleh PT Gagas Energi Indonesia.
3. Penelitian ini akan berfokus pada dokumen dan kebijakan yang telah diterapkan oleh PT Gagas Energi Indonesia.
4. Penelitian yang dilakukan hanya akan memberikan rekomendasi secara deskriptif pada kebijakan keamanan informasi yang diterapkan oleh perusahaan.

1.6 Sistematika Pembahasan

Sistematika dari penelitian ini adalah sebagai berikut :

1. BAB I : PENDAHULUAN

Bab 1 berisikan penjelasan mengenai permasalahan dari penelitian yang dalam bentuk penjabaran latar belakang yang mendukung pelaksanaan penelitian serta merumuskan masalah, tujuan dan manfaat penelitian serta membatasi masalah yang dibahas jika diperlukan.

2. BAB II : LANDASAN KEPUSTAKAAN

Bab II berisikan berbagai teori pendukung dan penelitian sebelumnya yang digunakan sebagai landasan dalam melakukan penelitian ini yang diambil dari berbagai referensi ilmiah.

3. BAB III : METODOLOGI PENELITIAN

Menjelaskan tahapan-tahapan yang dilakukan untuk mencapai tujuan dari penelitian mulai dari tahap perumusan masalah, pengumpulan data, metode analisis data sampai tahap memberikan rekomendasi berdasarkan hasil analisis dan membuat kesimpulan penelitian.

4. BAB IV : HASIL EVALUASI

Menjelaskan hasil evaluasi yang telah dilakukan. Pada bab ini data penelitian akan diolah sehingga dapat dijadikan pembahasan.

5. BAB V : PEMBAHASAN

Bab pembahasan berisikan rekomendasi yang didapatkan dari hasil evaluasi.

6. BAB VI : PENUTUP

Bab VI berisikan kesimpulan penelitian yang berisikan garis besar hasil penelitian yang merupakan jawaban dari rumusan masalah yang ada dalam penelitian ini serta saran berisikan masukan yang membangun terkait penelitian ini dan dapat digunakan untuk mengembangkan penelitian ini lebih lanjut.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Penelitian Sebelumnya

Literatur pertama yang digunakan berasal dari penelitian yang berjudul Analisis Keamanan Data Center Menggunakan COBIT 5 yang dilakukan oleh Matin et.al (2017) menjelaskan bahwa keamanan informasi menjadi hal yang penting untuk menjamin keamanan aset TI pada institusi. Penelitian ini dilandasi oleh adanya peretasan terhadap *data center* beberapa tahun sebelum penelitian ini dilakukan. Selain itu, organisasi juga belum pernah melakukan audit terkait keamanan *data center*. Penelitian difokuskan pada proses APO13 dan DSS05 yang terdapat pada COBIT 5. Penelitian ini menunjukkan jika proses APO13 memiliki nilai 1,54 dan DSS05 bernilai 1,70 yang berarti proses tersebut telah mencapai level 2 (*Managed Process*). Artinya, proses pengelolaan keamanan informasi telah dijalankan, dikontrol dan dikelola dengan tepat. Sedangkan rekomendasi yang diberikan untuk dapat mencapai level berikutnya (level 3), maka hal yang perlu dilakukan adalah dengan membuat kebijakan dengan detil dan dikelola dengan standar tertentu. Selain itu, implementasi dan standar yang telah dibuat harus dapat diimplementasikan.

Referensi kedua yaitu penelitian yang dilakukan oleh Suminar et.al (2014) yang berjudul "*Evaluation of Information Technology Governance Using COBIT 5 Framework Focus APO13 and DSS05 in PPIKSN-BATAN*" menjelaskan bahwa COBIT 5 dapat digunakan untuk mengukur pengelolaan keamanan informasi pada organisasi dengan fokus pada proses APO13 dan DSS05. Hasil dari penelitian yang dilakukan menunjukkan bahwa pada kedua proses berada pada level 2 (*Managed*) dengan nilai 1,96 pada APO13 dan 1,71 pada DSS05. Berdasarkan hasil yang didapatkan, rekomendasi yang dapat dilakukan untuk mencapai level berikutnya adalah dengan membuat kebijakan untuk mengimplementasikan standar dan prosedur pengamanan informasi pada PPIKSN-BATAN.

Penelitian ketiga yang digunakan berasal Ciptaningrum et.al (2015) yang berjudul "*Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5*". Jurnal ini mengangkat permasalahan perlunya pada aplikasi-aplikasi pendukung layanan TI seperti situs resmi Pemerintah Kota Yogyakarta dan aplikasi-aplikasi pendukung lainnya untuk menerapkan standar dan prosedur pengamanan informasi. Berdasarkan permasalahan tersebut maka dilakukan audit tata kelola keamanan sistem informasi pada domain EDM03, APO12, APO13, BAI06 dan DSS05. Dari hasil audit yang dilakukan diketahui bahwa kapabilitas dari keseluruhan domain yang dipilih berada pada level 1 (*Performed Process*). Penelitian ini memberikan rekomendasi perbaikan yaitu dengan mendokumentasikan SOP terkait keamanan informasi sehingga pengelolaan keamanan informasi dapat mencapai tingkat yang diharapkan.

Referensi keempat didapatkan dari penelitian yang dilakukan oleh Wolden et.al (2015) yang berjudul "*The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management Systems*". Penelitian tersebut dilakukan untuk mengetahui efektivitas penanganan manajemen keamanan informasi menggunakan COBIT 5 pada *Supply Chain Management Systems* (SCMS) pada salah satu perusahaan di Inggris. Hasil penelitian yang dilakukan menunjukkan bahwa COBIT 5 secara efektif dapat digunakan sebagai kerangka kerja dalam mengukur manajemen keamanan informasi.

2.2 Profil PT Gagas Energi Indonesia

PT Gagas Energi Indonesia didirikan Di Jakarta pada tanggal 27 Juni 2011 oleh para pemegang saham yaitu PT Perusahaan Gas Negara (PGN) (Persero) Tbk. dan PT PGN Solution, salah satu anak perusahaan PT Perusahaan Gas Negara (Persero) Tbk. berdasarkan Akta Pendirian No.125 Tahun 2011 yang dibuat di hadapan Fatimah Helmi, SH. Notaris di Jakarta, dan telah mendapatkan pengesahan dari Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor : AHU-42487.AH.01.01 dan beralamat di Jalan K.H Zainul Arifin Nomor 20, Jakarta. Sesuai dengan Anggaran Dasarnya, PT Gagas Energi Indonesia bergerak di bidang pengolahan, pengangkutan dan niaga minyak dan gas bumi. PT Gagas Energi Indonesia didirikan dengan tujuan memperkuat bisnis hilir PGN di bidang perniagaan gas bumi. Bisnis hilir PGN diperkuat oleh PT Gagas Energi Indonesia dengan melakukan pengusahaan di bidang pengolahan, penyimpanan, pengangkutan dan perniagaan gas bumi dalam berbagai bentuk.

Pada awal 2012, Gagas memulai komersialisasi gas bumi melalui pipa dengan menjual gas kepada 3 pelanggan industri dan terus meningkat hingga mencapai 109 pelanggan pada akhir tahun. Pada Desember 2012, Gagas mulai mengembangkan bisnis baru penjualan gas, yaitu menjual *Compressed Natural Gas* (CNG) kepada pelanggan yang tidak terjangkau jaringan pipa gas.

Pada tahun 2013, Gagas memulai penjualan gas bumi kepada masyarakat umum yang ditandai dengan beroperasinya *Mobile Refueling Unit* (MRU) pertama di lapangan IRTI Monas. MRU dipilih sebagai model pengisian bahan bakar gas karena tidak membutuhkan banyak lahan untuk mendirikannya dan dapat dipindahkan sesuai dengan kebutuhan pengisian bahan bakar. Tetapi, kapasitas penyimpanan MRU tidak sebesar kapasitas SPBG, sehingga perlu pengisian bahan bakar yang lebih sering.

Seiring dengan bertambahnya konsumen yang membutuhkan CNG, Gagas kemudian melakukan upaya untuk dapat memiliki mother station sendiri dan melayani kebutuhan pelanggannya melalui mother station miliknya, baik pelanggan sektor transportasi maupun sektor industri. Hal tersebut ditandai dengan diresmikannya stasiun pengisian bahan bakar gas yang pertama bagi GAGAS pada tanggal 24 Desember 2013, yaitu Stasiun Pengisian Bahan Bakar Gas di Pondok Ungu – Bekasi. SPBG Pondok Ungu merupakan SPBG hybrid, yang

berarti bahwa selain berfungsi sebagai mother station, SPBG Pondok Ungu juga melayani kebutuhan pengisian bahan bakar gas bagi konsumen transportasi.

2.2.1 Visi

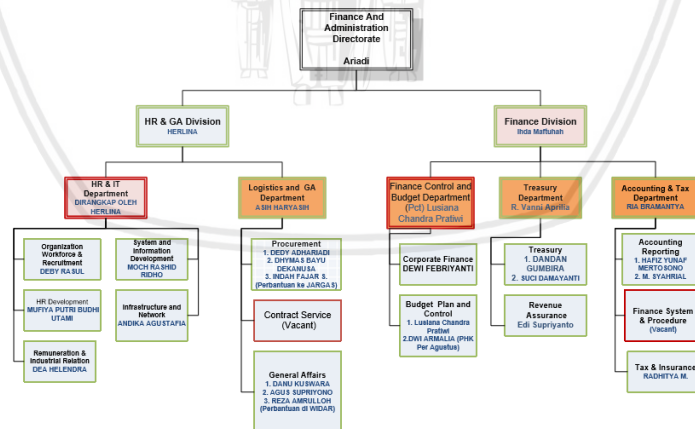
Menjadi penyedia energi terkemuka di Indonesia di bidang gas bumi dan produk turunannya

2.2.2 Misi

Untuk Meningkatkan nilai Perusahaan bagi *stakeholder* melalui :

1. Mendukung PGN Group dengan menghasilkan portofolio usaha baru yang menguntungkan dan berkelanjutan di sektor hilir gas bumi dan mensinergikan serta mengintegrasikan sumber daya yang tersedia untuk memberi nilai tambah bagi gas bumi sebagai bahan bakar pilihan.
2. Mendukung inisiatif pemerintah dalam memperkenalkan gas bumi sebagai energi yang bersih, efisien dan ramah lingkungan melalui penyediaan infrastruktur dan sistem pasokan energi yang berguna bagi mitra dan pemangku kepentingan.
3. Meningkatkan kompetensi melalui pengembangan Sumber Daya Manusia, dan memberikan kesempatan yang sama bagi seluruh Pekerja untuk mengembangkan keahlian dan kompetensi masing-masing.

2.2.3 Struktur Organisasi



Gambar 2.1 Struktur Organisasi

Berdasarkan Gambar 2.1, dapat dilihat bahwa unit yang menangani masalah TI berada di bawah naungan Direktorat *Finance and Administration*, lebih tepatnya dibawah departemen HR & IT. Unit TI dibagi menjadi 2 bagian, yaitu bagian *System and Information Development* dan *Infrastructure and Network*

yang masing-masing unit tersebut memiliki 1 staf untuk menangani masalah TI pada perusahaan.

2.3 Evaluasi

Evaluasi adalah membandingkan sesuatu dengan suatu ukuran tertentu yang telah ditetapkan. Kegiatan evaluasi dilakukan dengan mengukur objek terlebih dahulu dengan sebuah standar (Arikunto, 2015). Secara umum, evaluasi memiliki tujuan untuk mengetahui kesuksesan suatu program dengan tujuannya. Selain itu, tujuan dari evaluasi adalah memberikan bahan pertimbangan dalam menentukan keputusan dan kebijakan dalam organisasi (Wirawan, 2012). Dalam artian lain, evaluasi memiliki tujuan untuk menilai suatu objek dengan sebuah standar tertentu yang telah ditetapkan sebelumnya. Hasil dari evaluasi dapat memberikan rekomendasi perbaikan pada objek yang dilakukan evaluasi. Dalam hal ini evaluasi dapat diartikan sebagai kegiatan untuk mengetahui kondisi sebuah objek dengan menggunakan instrumen yang hasilnya akan dibandingkan dengan sebuah standar sehingga memperoleh kesimpulan (Yunanda, 2009). Selain itu evaluasi digunakan dalam menentukan kesuksesan dari sebuah tugas atau pekerjaan. Tujuan dari evaluasi adalah memberikan bahan pertimbangan dalam menentukan keputusan dan kebijakan dalam organisasi

Penjelasan tentang evaluasi di atas menunjukkan bahwa evaluasi adalah sebuah langkah untuk menilai sebuah pencapaian kerja secara sistematis dan terstruktur dengan membandingkan antara hasil dan perencanaan awal menggunakan instrumen tertentu. Evaluasi dapat juga dilakukan untuk menemukan permasalahan dari sebuah pencapaian kerja. Hasil dari pelaksanaan evaluasi kemudian dapat digunakan oleh organisasi sebagai ukuran dari kesuksesan dari sebuah hasil kerja. Selain itu, hasil dari evaluasi dapat digunakan untuk memperbaiki proses kerja yang berjalan sehingga diharapkan menjadi lebih baik dibandingkan sebelumnya.

2.4 Tata Kelola

Tata kelola adalah proses untuk mengatasi masalah yang terjadi di masyarakat (Jogiyanto, 2011). Tata kelola dibutuhkan oleh organisasi untuk mengatasi masalah yang terjadi dalam organisasi atau perusahaan. Tata kelola mencakup hubungan antara *stakeholder* dalam organisasi dengan tujuan dari organisasi. Dalam penerapan teknologi informasi (TI), tata kelola dibutuhkan untuk memastikan penerapan TI telah sesuai dengan tujuan dari organisasi tersebut. Hal tersebut harus dilakukan sebab biaya investasi TI dalam perusahaan terkadang membutuhkan biaya yang besar, sehingga memerlukan pengelolaan baik untuk memastikan investasi teknologi sesuai dengan tujuan bisnis dari perusahaan (Omari, 2016). Selain itu, pengelolaan TI dibutuhkan oleh organisasi untuk memastikan tidak ada masalah dalam penerapan TI.

Tata kelola TI memiliki tujuan untuk menyeimbangkan teknologi informasi yang digunakan dengan tujuan bisnis perusahaan. Dalam artian, penggunaan teknologi informasi dapat memenuhi strategi bisnis yang dilakukan. Dalam hal

ini, strategi TI akan disesuaikan dengan strategi bisnis perusahaan sehingga penerapan TI dapat mendatangkan manfaat atau keuntungan bagi organisasi atau perusahaan. Selain itu, tata kelola TI memiliki tujuan menyelaraskan penggunaan teknologi informasi agar sesuai dengan proses bisnis perusahaan. Tata kelola TI menjadi bagian dari tata kelola perusahaan yang terdiri dari kepemimpinan, struktur organisasi TI dan pengembangan strategi organisasi. Tata kelola TI menggambarkan penerapan prinsip organisasi dengan fokus pada kegiatan manajemen dan penggunaan TI dalam organisasi. Eksekutif pimpinan suatu perusahaan memiliki tanggung jawab terhadap berlangsungnya tata kelola TI.

Berdasarkan penjabaran di atas, tata kelola diartikan sebagai sebuah proses mengarahkan dan mengatur untuk mengatasi permasalahan dalam organisasi dengan melibatkan *stakeholder* di dalamnya. Dalam penerapan TI, tata kelola merupakan sebuah proses untuk memastikan apakah penerapan TI sesuai dengan tujuan yang diharapkan. Dalam hal penerapan tata kelola TI, penggunaan TI akan disesuaikan dengan tujuan bisnis yang diharapkan, sehingga penerapan TI dapat memberikan manfaat bagi organisasi/perusahaan yang menerapkannya.

2.5 Keamanan Informasi

Keamanan informasi adalah usaha untuk melindungi akses informasi dari pihak yang tidak berwenang terhadap informasi tersebut (Andress, 2014). Secara umum hal ini diartikan sebagai salah satu bentuk pengamanan informasi dari gangguan seperti akses yang tidak berhak terhadap informasi. Pengamanan informasi dapat dilakukan dengan merencanakan, mengembangkan dan mengawasi segala aktivitas terkait bagaimana penggunaan data dan informasi untuk bisnis dapat dimanfaatkan sesuai dengan kebutuhannya tanpa adanya penyalahgunaan atau kebocoran data kepada pihak yang tidak berhak atas data dan informasi tersebut.

Secara umum, keamanan informasi memiliki 3 aspek utama menurut Andress (2014) seperti yang dijelaskan dalam gambar 2.2



Gambar 2.2 Aspek Utama Keamanan Informasi

Sumber : Andress (2014)

1. *Confidentiality* (Kerahasiaan)
Kerahasiaan adalah kemampuan informasi dan data yang disimpan agar tidak diakses oleh yang tidak memiliki hak akses.
2. *Integrity* (Integritas)
Integritas adalah pencegahan terhadap perubahan informasi dari pihak yang tidak berhak untuk melakukan perubahan informasi. Hal ini dapat diartikan sebagai perubahan data
3. *Availability* (Ketersediaan)
Diartikan sebagai ketersediaan informasi saat pihak yang sah atas informasi tersebut membutuhkannya.

2.6 Manajemen Keamanan Informasi

Manajemen keamanan informasi diartikan sebagai pengelolaan, standar, aturan dan kebijakan penjaminan keamanan informasi pada perusahaan atau organisasi. Manajemen keamanan informasi dibutuhkan oleh perusahaan karena penanganan keamanan tidak cukup hanya dengan membangun dari sisi teknis, tetapi juga perlu dilakukan penanganan keamanan informasi dari sisi manajerial dan penanganan risiko. Secara umum, manajemen keamanan informasi disesuaikan dengan kebutuhan dan tujuan dari perusahaan atau organisasi. Keamanan informasi diperlukan untuk menjaga aset-aset informasi yang dimiliki oleh perusahaan atau organisasi.

Meningkatnya penggunaan pada sistem berbasis komputer, manajemen keamanan informasi diperlukan bagi organisasi untuk melindungi organisasi untuk mengurangi dampak dari insiden keamanan informasi yang tidak diinginkan (Choobineh, et al., 2007). Sehingga diperlukan pengelolaan keamanan informasi untuk menjaga kesinambungan bisnis, mengurangi risiko yang terjadi serta mengembalikan investasi yang telah dilakukan (Basyarahil, et al., 2017).

Untuk dapat menerapkan manajemen keamanan informasi, terdapat 12 tahapan yang perlu dilakukan oleh perusahaan berdasarkan ISO/IEC 27001:2009.

1. Memastikan pimpinan menyetujui penerapan manajemen keamanan organisasi.
2. Menetapkan tugas dari setiap personalia organisasi sebagai bentuk komitmen untuk penerapan manajemen keamanan informasi.
3. Mendefinisikan ruang lingkup penerapan manajemen keamanan informasi.
4. Membandingkan antara kondisi saat ini (*as-is*) dan kondisi yang diharapkan (*to-be*) menggunakan *gap analysis*.
5. Melakukan *risk assessment* untuk mengetahui penerapan manajemen risiko dan melakukan *risk treatment plan* untuk mengetahui rencana mitigasi yang terdapat pada perusahaan/organisasi.
6. Menetapkan pengontrolan yang didasarkan identifikasi risiko pada langkah sebelumnya.
7. Menetapkan kebijakan dan prosedur manajemen keamanan informasi berdasarkan kontrol pada perusahaan.
8. Sosialisasi dan pelatihan terhadap prosedur yang telah dibuat untuk seluruh pegawai berdasarkan persetujuan pimpinan.
9. Penerapan kebijakan manajemen keamanan informasi.
10. Pengukuran terhadap efektivitas kebijakan, prosedur atau standar yang telah ditentukan sebelumnya.
11. Melakukan audit internal pada manajemen keamanan informasi sesuai prosedur dan kebijakan untuk menjamin kualitas penerapan.
12. Evaluasi, peninjauan dan penyempurnaan pada penerapan kebijakan, standar atau prosedur keamanan informasi yang telah ditetapkan.

Berdasarkan penjelasan tersebut diketahui penerapan manajemen keamanan informasi adalah sebuah kegiatan yang mengidentifikasi ancaman serangan pada sumber daya informasi yang mungkin terjadi pada perusahaan. Kemudian kegiatan untuk menjelaskan risiko keamanan yang ada. Berikutnya adalah kegiatan kontrol dan evaluasi dari sebuah risiko keamanan informasi untuk memberikan perlindungan dan mengurangi risiko agar sedapat mungkin tidak memberikan dampak bagi perusahaan.

2.7 Pengelolaan Keamanan

Pengelolaan keamanan adalah aktivitas terkait pendefinisian, pengoperasian, dan pengawasan dari penerapan sistem manajemen keamanan informasi. Pengelolaan keamanan merupakan proses pendekatan sistematis untuk memantau, mengimplementasikan, menetapkan, memelihara dan meningkatkan keamanan informasi dalam rangka mencapai tujuan dari organisasi (ISACA, 2012b). Proses pengelolaan keamanan menekankan bahwa proses keamanan tidak hanya berfokus dari perbaikan infrastruktur yang berkaitan dengan keamanan informasi, tetapi lebih memfokuskan pada bagaimana sumber daya manusia, organisasi, dan aset pada organisasi yang memiliki kaitan dengan proses keamanan informasi dapat dikelola untuk mendukung penggunaan infrastruktur. Berdasarkan penjelasan di atas dapat disimpulkan bahwa pengelolaan keamanan merupakan sebuah pendekatan manajerial yang dilakukan pada kegiatan pemantauan, implementasi, penetapan dan pemeliharaan proses keamanan informasi yang berjalan pada organisasi.

2.8 Pengelolaan Layanan Keamanan

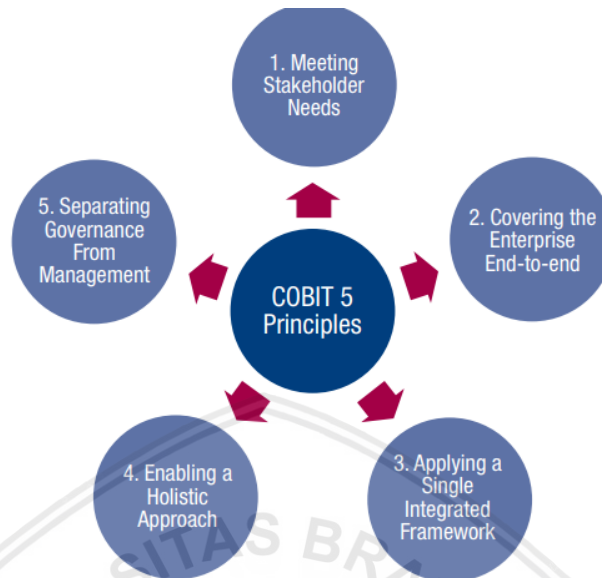
Pengelolaan layanan keamanan dapat didefinisikan sebagai aktivitas yang dilakukan untuk melindungi aset informasi organisasi agar sesuai dengan tingkatan keamanan informasi yang dapat diterima sesuai kebijakan organisasi. Pengelolaan layanan keamanan dengan kata lain juga dapat diartikan sebagai aktivitas untuk mengelola aset-aset penting terkait teknologi informasi dalam organisasi untuk memastikan layanan informasi yang dijalankan tetap aman. Pengelolaan layanan keamanan yang baik pada organisasi akan melindungi nilai dari investasi pada bidang keamanan informasi dan mengurangi biaya operasional keamanan organisasi (IBM, 2015). IBM (2015) mendefinisikan pengaturan pada pengelolaan layanan keamanan dapat memenuhi kebutuhan organisasi atas ketersediaan perangkat, *response time* dan *Service Level Agreement* (SLA). Berdasarkan penjelasan di atas dapat disimpulkan jika pengelolaan layanan keamanan merupakan sebuah aktivitas melindungi aset informasi dan memastikan layanan informasi yang dijalankan tetap aman sehingga dapat memenuhi kebutuhan keamanan informasi yang telah ditetapkan oleh organisasi.

2.9 COBIT 5

COBIT 5 adalah *framework* (kerangka kerja) tata kelola TI versi kelima yang dikeluarkan oleh ISACA. COBIT 5 membantu organisasi dengan menyediakan kerangka kerja untuk membantu penerapan tata kelola teknologi informasi dalam organisasi. Dalam hal ini, COBIT 5 membantu perusahaan menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan risiko serta penggunaan sumber daya (ISACA, 2012a).

COBIT 5 membantu pengelolaan TI dalam perusahaan tertata secara baik dengan berperan secara penuh dalam fungsional area TI. COBIT 5 dapat

digunakan dengan baik dalam berbagai jenis dan skala organisasi. Secara umum, COBIT 5 memiliki 5 prinsip seperti yang dijelaskan dalam gambar di bawah ini :



Gambar 2.3 Prinsip COBIT 5

Sumber : ISACA (2012)

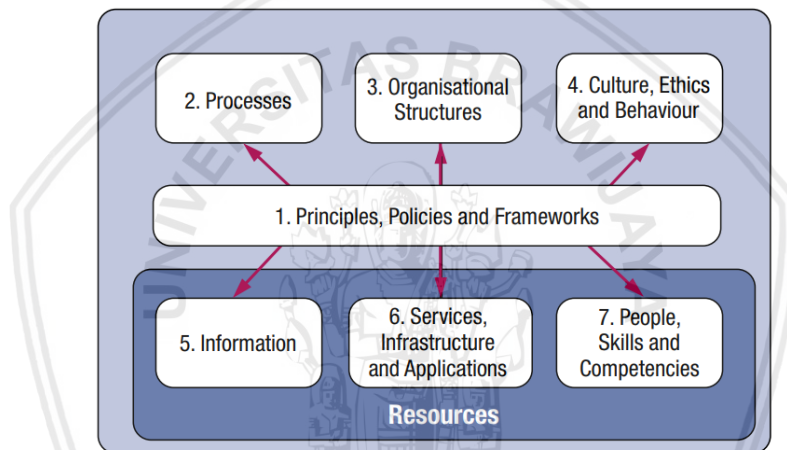
- 1. Meeting Stakeholder Needs**
Keseimbangan optimalisasi risiko, keuntungan serta penggunaan sumberdaya dipelihara oleh organisasi agar *stakeholder* mendapatkan nilai. Dalam hal ini, proses penciptaan nilai bisnis dan penerapan teknologi informasi yang dibutuhkan disediakan oleh COBIT 5.
- 2. Covering the Enterprise End-to-end**
Tata kelola organisasi diintegrasikan dengan tata kelola teknologi informasi organisasi dengan cakupan pada keseluruhan fungsi dan proses. COBIT 5 memperlakukan teknologi informasi sebagai aset lain dalam organisasi selain berfokus pada fungsional teknologi.
- 3. Applying a Single Integrated Framework**
COBIT 5 dapat bertindak secara menyeluruh sebagai sebuah kerangka kerja tata kelola TI yang digunakan perusahaan dengan menyelaraskan standar lain yang relevan dengan proses.
- 4. Enabling a Holistic Approach**
Memberikan dukungan pendekatan implementasi secara holistik pada tata kelola dan manajemen sistem dengan menyediakan *enabler*.
- 5. Separating Governance From Management**
Batasan dari tata kelola dan manajemen diberikan secara jelas oleh COBIT 5. Hal tersebut karena adanya perbedaan aktivitas, struktur organisasi dan kebutuhan yang berbeda. Pada COBIT 5, kelola

dibedakan dengan manajemen secara jelas terdapat pada Tabel 2.1 ini.

Tabel 2.1 Perbedaan Tata Kelola dan Manajemen

Tata Kelola	Manajemen
Kebutuhan <i>stakeholder</i> seimbang dengan tujuan organisasi	Perencanaan dalam hal membangun dan memantau kegiatan berdasarkan tujuan organisasi

Selain prinsip utama, COBIT 5 juga memiliki faktor-faktor yang memiliki pengaruh pekerjaan dalam organisasi yang disebut *enablers*. *Enablers* dalam COBIT 5 terbagi menjadi 7 kategori sebagai berikut menurut ISACA (2012a) :



Gambar 2.4 Enabler pada COBIT 5

Sumber : ISACA (2012a)

1. Prinsip, Kebijakan, dan Kerangka Kerja (*Principles, Policies and Frameworks*), merupakan sarana untuk menterjemahkan proses untuk membantu kegiatan manajemen dalam bentuk petunjuk.
2. Proses (*Process*), menjelaskan berbagai aktivitas terorganisir yang menghasilkan keluaran (*output*) tertentu yaitu berupa tujuan TI yang diinginkan.
3. Struktur Organisasi (*Organisational Structures*), adalah kunci utama dalam pengambilan keputusan.
4. Budaya, Etika dan Perilaku (*Culture, Ethics and Behavior*), adalah kebiasaan organisasi dan individu yang memiliki pengaruh dalam keberhasilan dan kegagalan dalam organisasi.
5. Informasi (*Information*) disini diartikan sebagai informasi yang digunakan untuk membantu berjalannya organisasi. Informasi juga digunakan sebagai hasil dari proses dalam tingkat operasional.

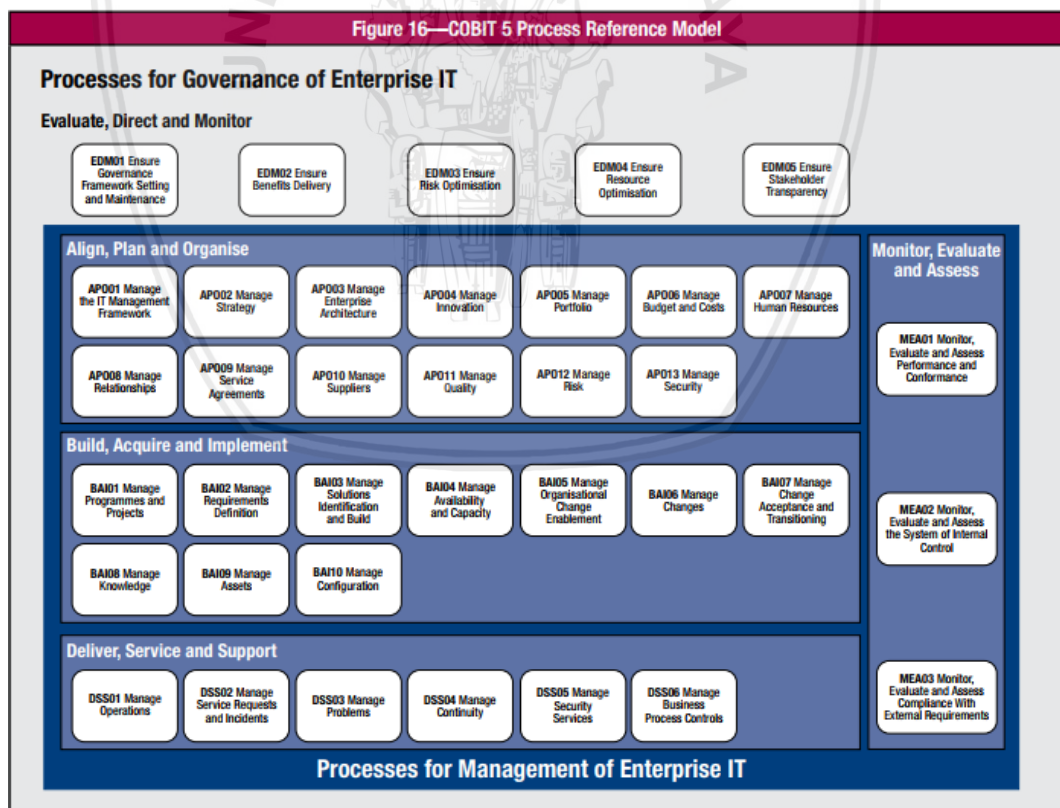
6. Layanan, Infrastruktur dan Aplikasi (*Services, Infrastructure and Applications*), adalah penggunaan layanan infrastruktur yang dapat mendukung proses organisasi melaksanakan teknologi informasi.
7. Manusia, Kemampuan dan Kompetensi (*People, Skills and Competencies*), berkaitan dengan individu dan perannya dalam memajukan organisasi sesuai kemampuannya.

2.10 Model Proses dan Domain dalam COBIT 5

COBIT 5 membagi proses tata kelola dan manajemen TI perusahaan menjadi 2 hal, yaitu :

1. Tata Kelola, terdiri dari 5 proses yang dapat ditemukan pada setiap proses dari domain *Evaluate, Direct and Monitor* (EDM).
2. Manajemen, terdiri dari 4 domain pada area *Plan, Build, Run and Monitor* (PBRM) dan. Proses ini terdiri dari 4 domain yaitu *Align, Plan and Organize* (APO); *Build, Acquire and Implement* (BAI), *Deliver, Service and Support* (DSS), dan *Monitor, Evaluate and Assess* (MEA).

Keseluruhan model proses dan domain dalam COBIT 5 dijelaskan pada gambar yang terdapat di bawah ini.



Gambar 2.5 Model Proses pada COBIT 5

Sumber : ISACA (2012a)

2.10.1 Evaluate, Direct and Monitor (EDM)

Proses pada EDM berkaitan dengan tujuan *stakeholder* dalam melakukan penilaian, optimasi risiko dan sumber daya (ISACA, 2012a). Berikutnya, perusahaan akan menetapkan arah TI yang diambil berdasarkan prioritas. Pada domain ini terdiri dari 5 proses.

Tabel 2.2 Domain EDM

Proses	Definisi
EDM01 (<i>Ensure Governance Framework Setting and Maintenance</i>),	yaitu proses untuk memastikan telah melakukan aktivitas pemeliharaan dan pengaturan kerangka kerja dalam aktivitas tata kelola.
EDM02 (<i>Ensure Benefit Delivery</i>),	yaitu proses untuk memastikan adanya manfaat yang diperoleh.
EDM03 (<i>Ensure Risk Optimisation</i>)	memastikan optimalisasi resiko yang ada.
EDM04 (<i>Ensure Resource Optimisation</i>)	Memastikan perusahaan telah mengoptimalkan penggunaan sumber dayanya.
EDM05 (<i>Ensure Stakeholder Transparency</i>)	Memastikan transparansi terhadap <i>stakeholder</i> organisasi.

2.10.2 Align, Plan and Organize (APO)

Domain APO mengarahkan untuk penyampaian solusi dan mendukung penyediaan layanan (ISACA, 2012a). Dalam hal ini, Domain APO berkaitan dengan Domain BAI dalam hal penyampaian solusi dan Domain DSS dalam hal penyediaan dukungan layanan. Domain ini terdiri dari 13 proses.

Tabel 2.3 Domain APO

Proses	Definisi
APO01 (<i>Manage the IT Management Framework</i>)	memastikan pengelolaan manajemen kerangka kerja TI.
APO02 (<i>Manage Strategy</i>)	memastikan adanya pengelolaan strategi.
APO03 (<i>Manage Enterprise Architecture</i>)	memastikan adanya pengelolaan arsitektur perusahaan.
APO04 (<i>Manage Innovation</i>)	memastikan adanya pengelolaan inovasi.

Tabel 2.3 Domain APO

Proses	Definisi
APO05 (<i>Manage Portfolio</i>)	memastikan adanya pengelolaan portfolio.
APO06 (<i>Manage Budget and Cost</i>)	memastikan adanya pengelolaan anggaran dan biaya dalam proses implementasi teknologi informasi.
APO07 (<i>Manage Human Resource</i>)	memastikan adanya pengelolaan sumber daya manusia.
APO08 (<i>Manage Relationships</i>)	memastikan adanya pengelolaan hubungan.
APO09 (<i>Manage Service and Agreements</i>)	memastikan adanya pengelolaan perjanjian layanan.
APO10 (<i>Manage Suppliers</i>)	untuk memastikan adanya pengelolaan pemasok.
APO11 (<i>Manage Quality</i>)	memastikan adanya pengelolaan kualitas.
APO12 (<i>Manage Risk</i>)	memastikan adanya pengelolaan risiko.
APO13 (<i>Manage Security</i>)	memastikan adanya pengelolaan keamanan.

2.10.3 Build, Acquire and Implement (BAI)

Domain BAI berguna dalam memberikan dan mengimplementasikan sebuah solusi dalam layanan. Domain ini terdiri dari 10 proses yaitu :

Tabel 2.4 Domain BAI

Proses	Definisi
BAI01 (<i>Manage Programmes and Projects</i>)	memastikan adanya pengelolaan program dan proyek.
BAI02 (<i>Manage Requirements Definitions</i>)	Untuk memastikan permintaan kebutuhan telah dikelola.
BAI03 (<i>Manage Solutions Identification and Build</i>)	Untuk memastikan telah dibangunnya identifikasi dan solusi.
BAI04 (<i>Manage Availability and Capacity</i>)	memastikan ketersediaan dan kapasitas telah dikelola.
BAI05 (<i>Manage Organisation Change Enablement</i>)	untuk memastikan adanya pengelolaan perubahan organisasi dan pemberdayaan.
BAI06 (<i>Manage Changes</i>)	memastikan adanya pengelolaan perubahan.
BAI07 (<i>Manage Change and Acceptance</i>)	memastikan adanya pengelolaan pada perubahan dan transisi.

<i>Transitioning</i>)	
BAI08 (<i>Manage Knowledge</i>)	memastikan adanya pengelolaan pengetahuan.
BAI09 (<i>Manage Assets</i>)	memastikan adanya pengelolaan asset.
BAI10 (<i>Manage Configuration</i>)	memastikan adanya pengelolaan konfigurasi.

2.10.4 Deliver, Service and Support (DSS)

Domain DSS menyediakan solusi layanan yang dibutuhkan pada pengguna akhir. Pada domain ini terdapat 6 proses, yaitu

Tabel 2.5 Domain DSS

Proses	Definisi
DSS01 (<i>Manage Operation</i>)	memastikan adanya pengelolaan operasi.
DSS02 (<i>Manage Service Request and Incident</i>) memastikan adanya pengelolaan layanan insiden dan permintaan	memastikan adanya pengelolaan layanan insiden dan permintaan.
DSS03 (<i>Manage Problems</i>)	memastikan adanya pengelolaan pada permasalahan.
DSS04 (<i>Manage Continuity</i>)	memastikan adanya pengelolaan layanan berkelanjutan.
DSS05 (<i>Manage Security Service</i>)	memastikan adanya pengelolaan layanan keamanan.
DSS06 (<i>Manage Business Process</i>)	mengelola proses bisnis.

2.10.5 Monitor, Evaluate and Assess

Domain MEA memberikan pengarah dan monitor pada semua proses dalam domain. Pada domain ini terdapat 3 proses yaitu :

Tabel 2.6 Domain MEA

Proses	Definisi
MEA01 (<i>Monitor Evaluate and Assess Performance and Conformance</i>)	memastikan adanya pemantauan, evaluasi dan penilaian terhadap kinerja.
MEA02 (<i>Monitor Evaluate and Assess</i>)	memastikan adanya pemantauan dan penilaian sistem pengendalian



<i>The System of Internal Control)</i>	internal.
MEA03 (<i>Monitor Evaluate and Assess Compliance with External Requirements</i>)	memastikan adanya pemantauan dan penilaian terhadap kepatuhan persyaratan eksternal.

2.11 COBIT 5 *Process Capability Model*

Process Capability Model (Model kapabilitas proses) pada COBIT 5 merupakan penilaian berdasarkan tingkat kapabilitas proses yang telah dipenuhi oleh organisasi saat ini. COBIT 5 memiliki 6 level kapabilitas yang harus dicapai dalam sebuah organisasi untuk mencapai penilaian tertinggi pada COBIT 5. Keenam level kapabilitas proses tersebut dijelaskan dalam gambar dibawah ini

Tingkatan pertama dalam penilaian model kapabilitas adalah level 0, yaitu kondisi dimana perusahaan belum melaksanakan proses TI atau belum mampu mencapai tujuan dari pelaksanaan proses teknologi informasi berdasarkan kerangka kerja COBIT 5. Pelaksanaan teknologi informasi yang dimaksud yaitu aktivitas teknologi informasi berdasarkan *Base Practices* (BP) dan *Work Product* (WP) yang menjadi dasar penilaian pada level 1 (ISACA, 2013a). Pada level 1, penilaian dilakukan berdasarkan BP dan WP dari setiap proses pada COBIT 5 yang dipilih untuk dinilai kapabilitasnya.

Berikutnya, pada penilaian kapabilitas level 2 (*Managed Process*) yaitu sebuah kondisi organisasi telah mencapai tujuan pelaksanaan proses TI. Pada level ini dan seterusnya, barang bukti yang digali tidak lagi berdasarkan pada BP/WP dari setiap proses pada COBIT 5, tetapi sudah menggunakan *Generic Practices* (GP) dan *Generic Work Product* (GWP) sebagai kegiatan dasar dan dokumen/kebijakan pendukung pelaksanaan proses. Pada level 2 ini penggalian data dan barang bukti difokuskan pada 2 atribut dengan masing-masing GP/GWP seperti dijelaskan dalam tabel. Atribut proses yang pertama adalah PA 2.1 *Performance Management* yaitu penilaian untuk mengukur sejauh mana pengelolaan dari sebuah proses. Atribut proses yang kedua adalah PA 2.2 *Work Product Management* yang mengukur sejauh mana hasil kerja proses COBIT 5 telah tercapai. Pemetaan GP dan GWP dari penilaian proses pada level 2 dijabarkan dalam tabel berikut.

Tabel 2.7 Penilaian Level 2 pada COBIT 5

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
PA 2.1 <i>Performance Management</i>	1	Tujuan dari kinerja proses telah teridentifikasi.	Mengidentifikasi tujuan dari dilaksanakannya kinerja proses.	Dokumentasi ruang lingkup proses.
				Perencanaan



Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
				proses yang menyertakan tujuan.
	2	Kinerja proses telah terencana dan terpantau.	Merencanakan dan memantau proses untuk memenuhi tujuan dari pelaksanaan proses.	Perencanaan proses Performa proses.
	3	Menyesuaikan kinerja proses yang teridentifikasi untuk memenuhi rencana.	Menyediakan alur jika proses tidak mampu tercapai	Menyediakan detail tindakan jika proses tidak tercapai.
	4	Tanggung jawab untuk melaksanakan proses telah didefinisikan, dijelaskan dan dikomunikasikan.	Penjelasan tanggung jawab untuk melaksanakan proses.	Dokumentasi proses yang menyediakan tanggung jawab detail. perencanaan komunikasi proses
	5	Informasi dan sumber daya yang dibutuhkan untuk melaksanakan proses telah diidentifikasi dan dialokasikan.	Identifikasi sumber daya yang diperlukan sesuai dengan perencanaan proses	Perencanaan proses yang menyediakan pelatihan dan pengalokasian sumber daya
	6	Pengelolaan antarmuka pada pihak-pihak yang terlibat.	Pengelolaan terkait mekanisme komunikasi antarpihak yang terlibat dan bertanggung	Dokumentasi proses yang menyediakan detail pihak yang terlibat

Tabel 2.7 (lanjutan)

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
			Jawab terkait proses	Rencana proses yang memuat detail perencanaan komunikasi
PA 2.2 (<i>Work Product Management</i>)	1	<i>Work product</i> yang telah didefinisikan	Menjelaskan kriteria struktur dan kualitas hasil	Perencanaan kualitas yang telah menjelaskan kriteria hasil
	2	Persyaratan pengendalian dokumentasi pada <i>work product</i> telah terpenuhi.	Menjelaskan kebutuhan dokumentasi dan kontrol proses	Menyediakan dokumentasi dan kontrol proses Detail hasil kerja yang telah menjelaskan perubahan kontrol
	3	<i>Work product</i> teridentifikasi, terdokumentasi dan terkontrol dengan tepat.	Identifikasi dokumen dan kontrol	Detail hasil kerja yang telah menjelaskan perubahan control
	4	<i>Work product</i> telah ditinjau ulang sesuai dengan perencanaan untuk memenuhi kebutuhan	Peninjauan hasil kerja terhadap kebutuhan yang telah didefinisikan di awal	Menyediakan jejak audit pada peninjauan ulang

Sumber : diadaptasi dari ISACA (2013a)

Penilaian berikutnya dilakukan pada level 3 atau *Established Process* yaitu sebuah kondisi dimana organisasi telah memiliki standar untuk menjalankan proses TI yang telah dilakukan. Dalam hal ini, standar untuk menjalankan proses TI telah berlaku dalam ruang lingkup organisasi. Level 3 memiliki 2 atribut proses yang diperlukan untuk menilai kapabilitas proses pada level 3. Atribut proses

yang pertama adalah PA 3.1 *Process Definition* yaitu pengukuran sejauh mana standar telah dijaga untuk mendukung pelaksanaan dari sebuah proses. Atribut proses yang kedua adalah PA 3.2 *Process Deployment* yang mengukur sejauh mana penerapan dari sebuah proses telah efektif untuk mencapai tujuan pelaksanaannya. Keseluruhan *Generic Practices* dan *Generic Work Product* dari penilaian pada level 3 dapat dilihat pada Tabel 2.8.

Tabel 2.8 Penilaian Level 3 COBIT 5

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
PA 3.1 <i>Process Definition</i>	1	Panduan untuk mengidentifikasi dasar proses yang telah didefinisikan.	Menjelaskan standar proses yang mendukung pelaksanaan proses.	Standar dan kebijakan yang menyediakan tujuan dan pencapaian minimum proses.
	2	Identifikasi urutan proses.	Menjelaskan interaksi antara proses satu dan lainnya.	Standar dan kebijakan yang menyediakan alur dan interaksi proses.
	3	Identifikasi komponen dan peranan untuk menjalankan proses.	Identifikasi peran dan tanggung jawab untuk melaksanakan proses.	Standar dan kebijakan yang menyediakan peranan dan tanggung jawab proses.
	4	Identifikasi infrastruktur dan lingkungan untuk menjalankan proses.	Kebutuhan infrastruktur dan lingkungan kerja untuk menjalankan proses	Telah terdapat infrastruktur minimum yang diperlukan untuk menjalankan proses

T



Tabel 2.8 (lanjutan)

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
	5	Telah terdapat pemantauan proses dengan metode yang sesuai.	Identifikasi metode yang sesuai untuk memantau efektivitas berjalannya proses.	Kebijakan terkait tujuan dan standar minimum proses telah dilaksanakan di organisasi.
PA 3.2 <i>Process Deployment</i>	1	Standar proses telah dilaksanakan pada proses yang berjalan.	Proses dilaksanakan pada area yang berbeda pada organisasi.	Standar dan kebijakan yang diikuti oleh keseluruhan organisasi.
	2	Identifikasi tanggung jawab yang diperlukan untuk menjalankan proses.	Menjelaskan peranan dan tanggung jawab untuk menjalankan proses.	Menyediakan detail tanggung jawab dan wewenang untuk menjalankan proses.
	3	Personil yang melaksanakan proses didasarkan pada pendidikan dan pelatihan tertentu.	Pelaksanaan proses dilakukan oleh personil kompeten dan terlatih.	Menjelaskan kompetensi dan pelatihan yang dibutuhkan.
				Menjelaskan rencana pelatihan terkait proses.
	4	Adanya alokasi informasi dan sumber daya untuk menjalankan proses.	Tersedianya sumber daya untuk mendukung pelaksanaan proses.	Menyediakan detail perencanaan sumber daya pada proses.
5	Identifikasi infrastruktur dan lingkungan untuk	Tersedianya infrastruktur yang sesuai	Menjelaskan infrastruktur dan lingkungan	



Tabel 2.8 (lanjutan)

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
	5	menjalankan proses.	untuk mendukung proses.	yang sesuai untuk menjalankan proses.
	6	Kinerja dan evaluasi proses dilakukan analisis untuk perbaikan berikutnya.	Analisis data telah dilakukan untuk mengukur efektivitas dari proses.	Barang bukti terkait peninjauan ulang pada setiap proses.

Sumber : Diadaptasi dari ISACA (2013a)

Penilaian berikutnya dilakukan pada level 4 atau *Predictable Process* yang pada tahapan ini organisasi telah menjalankan proses TI pada batasan yang sudah pasti dan memiliki hasil dari proses yang dijalankan. Batasan tersebut didapatkan dari pelaksanaan proses TI sebelumnya. Terdapat 2 atribut pengukuran proses yang terdiri dari PA 4.1 *Process Measurement* yang mengukur sejauh mana hasil pengukuran dapat mendukung tercapainya tujuan. Berikutnya terdapat atribut proses PA 4.2 *Predictable Process* yang mengukur secara kuantitatif sejauh mana batasan yang telah ditentukan. Pencapaian dari masing-masing atribut dijelaskan dalam Tabel 2.9.

Tabel 2.9 Penilaian Level 4 COBIT 5

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
PA 4.1 <i>Process Measurement</i>	1	Informasi yang dibutuhkan didefinisikan agar mencapai tujuan tertentu.	Pengukuran informasi proses terhadap tujuan bisnis	Menyediakan rencana peningkatan proses
	2	Tujuan proses terdefinisi berdasarkan informasi.	Mengukur proses berdasarkan tujuannya	Rencana tujuan pengukuran proses
	3	Kinerja proses yang relevan dengan tujuan	Mengukur secara kuantitatif tujuan dari bisnis	Rencana pengukuran



Tabel 2.9 (lanjutan)

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
	3	terdefiniskan secara kuantitatif		dan indikator pengukuran
	4	Melakukan pengukuran kuantitatif dari kinerja proses.	Pengukuran kuantitatif pada tujuan proses	Menyediakan prosedur pengumpulan data
	5	Melaporkan hasil analisis berdasarkan hasil pengukuran.	Hasil dari pengukuran yang dilaporkan dan dianalisis.	Adanya prosedur analisis data
				Adanya pengukuran dan analisis data
6	Karakterisasi kinerja proses berdasarkan hasil pengukuran.	Menggunakan hasil pengukuran untuk mengukur pencapaian proses	Adanya pengukuran dan analisis data	
PA 4.2 <i>Process Control</i>	1	Menentukan teknik analisis dan pengendalian proses.	Menggunakan teknik analisis yang sesuai untuk mengukur proses	Terdapat detail matriks kontrol
				kontrol pengukuran proses
	2	Batasan kontrol yang terdefinisi dari setiap kinerja proses.	Terdapat parameter pengukuran performa proses	Adanya rencana kontrol pada setiap batasan
	3	Pengukuran data digunakan untuk mengatasi penyebab perubahan.	Hasil pengukuran yang dianalisis untuk mengatasi masalah	Adanya detail pengukuran pada pengumpulan dan analisis
	4	Mengatasi masalah perubahan menggunakan tindakan korektif	Tindakan korektif yang diawasi dan dievaluasi	

Tabel 2.9 (lanjutan)

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
	5	Tindakan korektif yang telah didefinisikan dan adanya batas kontrol yang tetap	Adanya perubahan setelah tindakan korektif diambil	Adanya penspesifikan batas kontrol untuk setiap performa proses

Sumber : ISACA (2013a)

Penilaian berikutnya dilakukan pada level 5 atau *Optimizing Process* yaitu sebuah kondisi dimana organisasi telah meningkatkan kemampuan dengan melakukan perbaikan berkelanjutan dan inovasi. Level 5 memiliki 2 atribut proses yang diperlukan untuk menilai kapabilitas proses pada level 5. Atribut proses yang pertama adalah PA 5.1 *Process Innovation* Ukuran sejauh mana identifikasi perubahan proses. Atribut proses yang kedua adalah PA 5.2 *Process Optimisation* yang mengukur sejauh mana perubahan yang dituju menggunakan erforma proses. Penilaian pada level 5 merupakan penilaian terakhir dari 6 level penilaian kapabilitas pada proses COBIT 5 yang berjalan di organisasi. Dengan kata lain, jika sebuah proses dapat dikatakan berjalan dalam kategori penilaian paling tinggi jika telah berhasil mencapai penilaian level 5. Keseluruhan kriteria dan barang bukti yang digali dalam penilaian level 5 pada kedua atribut dapat dilihat pada tabel 2.10 berikut ini.

Tabel 2.10 Penilaian Level 5 COBIT 5

Process Attribute (PA)	No	Pencapaian Atribut	Generic Practices	Generic Work Product
PA 5.1 <i>Process Innovation</i>	1	Mendukung tujuan organisasi dengan menjelaskan maksud perbaikan proses.	Perbaikan proses untuk mendukung tujuan bisnis yang sesuai	Tujuan peningkatan proses dan rencana tindakannya
	2	Menganalisis dan mengidentifikasi penyebab perubahan menggunakan data yang tepat.	Analisis pengukuran data untuk mengidentifikasi potensi pada performa proses	Menyediakan detail pengukuran data yang diambil dan dianalisis
	3	Peluang perbaikan proses yang	Identifikasi kesempatan	Menyediakan <i>best practice</i>



Tabel 2.10 (lanjutan)

<i>Process Attribute (PA)</i>	No	Pencapaian Atribut	<i>Generic Practices</i>	<i>Generic Work Product</i>
		teridentifikasi.	peningkatan proses berdasarkan praktik industri	untuk melakukan peningkatan proses
	4	Mendefinisikan pencapaian proses.	Peningkatan proses berdasarkan <i>review</i> dan analisis konsep inovasi proses	Analisis kesempatan peningkatan teknologi
	5	Tersedianya strategi implementasi untuk mencapai peningkatan proses	Strategi implementasi proses berdasarkan visi dan tujuan jangka panjang	Detail strategi implementasi untuk peningkatan proses
PA 5.2 <i>Process Optimization</i>	1	Menilai perubahan yang terjadi pada kinerja proses dan dampaknya	Menilai dampak perubahan pada proses terhadap performa dari proses yang berjalan	Detail pendekatan kebutuhan untuk meningkatkan kualitas proses
	2	Kesepakatan mengenai perubahan diimplementasikan.	Mengelola kesepakatan perubahan proses sesuai strategi implementasi	Detail implementasi perubahan untuk meningkatkan proses pada dokumentasi, rencana kualitas, dan standar
	3	Syarat yang ditetapkan telah dievaluasi.	Evaluasi efektivitas perubahan berdasarkan performa proses	Kebutuhan pendekatan peningkatan kualitas proyek

Sumber : ISACA (2013a)



2.12 COBIT 5 Self Assessment

Self Assessment adalah panduan untuk mengukur kapabilitas dari proses teknologi informasi yang digunakan dalam perusahaan. *Self Assessment* dapat digunakan untuk mengukur penilaian secara tidak mendetail. Kombinasi dari *Process Assessment Model* perlu dilakukan dalam melakukan *self assessment* untuk mendapatkan hasil optimal dengan mengumpulkan bukti-bukti yang dapat digunakan sebagai penilaian. Penilaian jenis ini dapat dilakukan oleh tim penilai (*assessor*) yang tidak memiliki sertifikat resmi. Tujuan dari penilaian ini adalah untuk mengetahui tingkat kapabilitas proses yang telah dicapai (ISACA, 2013).

Proses *self assessment* terdiri dari lima tahapan, tahapan pertama dilakukan dengan mendefinisikan ruang lingkup proses yang akan dinilai. Pada tahapan ini penilai memilih proses yang ingin dinilai dalam kerangka kerja COBIT 5. Pada tahapan ini juga perusahaan akan menentukan *targeted level* yang ingin dicapai dari setiap proses yang sudah dipilih. Tahapan kedua menilai proses yang dilakukan pada level 1 untuk mengukur pencapaian. Tujuannya adalah untuk memastikan seluruh proses telah mencapai kapabilitas pada level 1. Pada level ini, penilaian akan difokuskan pada *Base Practices* dan *Work Product* yang terdapat pada setiap proses COBIT 5. Hasil dari penilaian pada level 1 dapat dilanjutkan ke tahapan berikutnya jika mencapai kriteria *fully achieved* atau *largely achieved*

Tahapan ketiga adalah menilai proses mulai dari level 2-5. Penilaian dilakukan berurutan dari level 2 hingga level 5 dengan memperhatikan indikator pencapaian dari setiap levelnya. Pada tahapan ini, indikator pencapaian yang digali berupa *Generic Practices* dan *Generic Work Product* yang ada pada setiap levelnya. Tahapan keempat adalah mencatat dan merangkum level kapabilitas yang telah dicapai. Penentuan level kapabilitas dilakukan berdasarkan indikator pencapaian dari setiap levelnya. Untuk mencapai peningkatan level berikutnya, dari setiap proses setidaknya harus memiliki nilai *largely achieved* atau *fully achieved*. Penentuan penilaian dilakukan dengan mempertimbangkan pencapaian *Base Practices/Generic Practices* dan *Work Product/Generic Work Product* terhadap *outcome* dari setiap proses yang dinilai. p.

Tabel 2.11 Kategori Penilaian Kapabilitas

Singkatan	Penjelasan	Pencapaian
N	<i>Not Achieved</i>	0 % sampai 15 % pencapaian
P	<i>Partially Achieved</i>	>15 % sampai 50% pencapaian
L	<i>Largely Achieved</i>	>50 % sampai 85 % pencapaian
F	<i>Fully Achieved</i>	>85 % pencapaian

Sumber : Diadaptasi dari ISACA (2013a)

Berdasarkan Tabel 2.11, diketahui jika sebuah proses akan mencapai kriteria *fully achieved* jika penilaian yang dilakukan pada proses dapat mencapai angka diatas 85%. Sedangkan sebuah proses jika hanya mampu berada pada rentang angka diatas 50% sampai dengan 85% maka proses tersebut dapat dikategorikan sebagai *Largely Achieved*. Sedangkan jika proses hanya mampu mencapai rentang angka 15% sampai dengan 50%, proses tersebut dikategorikan masuk kriteria *Partially Achieved*. Terakhir, jika proses yang dinilai hanya mencapai maksimal 15% dari pencapaian, maka proses dapat dikategorikan sebagai *Not Achieved*. Berdasarkan penjelasan dari kriteria penilaian yang dijabarkan pada Tabel 2.11, dapat diketahui bahwa sebuah proses dapat dinaikkan level kapabilitasnya jika setidaknya telah mencapai diatas 50% pencapaian dari setiap atribut proses pada atribut prosesnya.

Langkah terakhir dari penilaian *self assessment* adalah dengan merencanakan peningkatan level dari proses yang tercapai saat ini menuju level yang ingin dicapai dari setiap proses. Perencanaan peningkatan level yang dilakukan oleh organisasi dilakukan dengan mempertimbangkan analisis kesenjangan (*gap analysis*) yaitu dengan membandingkan level yang dicapai oleh organisasi dengan level yang ingin dicapai dari setiap proses yang dinilai pada COBIT 5. Setelah seluruh tahapan penilaian telah dilewati, maka langkah berikutnya adalah memberikan rekomendasi berdasarkan kebutuhan perusahaan agar mampu mencapai level yang ingin dicapai dari setiap prosesnya (ISACA, 2012). Selain itu, rekomedasi juga dapat diberikan untuk memenuhi kebutuhan yang masih belum mampu dicapai secara maksimal oleh perusahaan dan dapat digunakan sebagai dasar pembuatan *roadmap* penerapan proses TI pada organisasi.

2.13 Keamanan Informasi Pada COBIT 5

COBIT 5 memiliki dua proses utama yang dapat digunakan untuk melakukan pengukuran tingkat keamanan informasi. Kedua proses itu adalah APO13 (*Manage Security*) dan DSS05 (*Manage Security Services*) (ISACA, 2013b). Kedua proses tersebut dapat digunakan untuk mengukur tingkat keamanan informasi terutama pada bagian pengelolaan layanan dan pengelolaan layanan keamanan pada organisasi.

2.13.1 *Manage Security* (APO13)

APO13 adalah domain proses dari COBIT 5 terkait pengawasan, operasi dan definisi dari sistem manajemen keamanan informasi dan memiliki fungsi pada pengamanan dan menjaga risiko dari kejadian pada keamanan informasi agar berada pada level yang dapat diterima oleh perusahaan. Domain proses ini memiliki 3 *Outcomes* atau pencapaian utama yang menjadi tujuan pelaksanaan proses yang dijelaskan seperti pada Tabel 2.12.

Tabel 2.12 Penjelasan *Outcome* Proses APO13

<i>Outcome</i>	Definisi
APO13-01	Mempertimbangkan kebutuhan keamanan informasi sistem

Tabel 2.12 (lanjutan)

Outcome	Definisi
APO13-02	Perencanaan keamanan yang telah ada, diterima dan dikomunikasikan pada perusahaan
APO13-03	Solusi keamanan informasi yang telah diimplementasikan dan dioperasikan pada perusahaan

Sumber : Diadaptasi dari ISACA (2013a)

Dari ketiga *Outcome* tersebut kemudian diturunkan menjadi *Base Practices* (BP), yaitu praktik kegiatan dasar proses pada COBIT 5 yang dilakukan pada perusahaan. Pada APO13, terdapat 3 praktik dasar yang harus dilakukan oleh perusahaan untuk mencapai pencapaian. Selain *Base Practices*, terdapat juga *Work Product*, yaitu dokumen atau kebijakan terkait proses COBIT 5 yang berjalan pada organisasi.

1. APO13-BP1 *Estabilish and maintain an information security management system* adalah langkah untuk membangun dan memelihara sistem manajemen keamanan informasi dengan menyediakan standar dan prosedur berkelanjutan untuk menjamin keamanan informasi. *Base Practices* ini dilaksanakan untuk memenuhi *outcome* APO13-01. Pada *Base Practices* ini terdapat 3 *Work Product* (WP) atau dokumen kebijakan pendukung proses, yaitu :
 - a. Pendekatan Keamanan Informasi sebagai WP *output* dari APO13-BP1.
 - b. Kebijakan manajemen keamanan informasi sebagai WP *input* dari APO13-BP1.
 - c. Pernyataan ruang lingkup sistem manajemen keamanan informasi sebagai WP *output* dari APO13-BP1
2. APO13-BP2 *Define and manage an information security risk treatment plan* menggambarkan rencana untuk menjaga risiko keamanan informasi terkelola dan memastikannya agar selaras dengan strategi dan arsitektur perusahaan. Kegiatan yang dilakukan pada *base practices* ini dilakukan untuk memenuhi *outcome* proses APO13-01. *Base Practices* ini terdiri dari 5 *Work Product* (WP) atau dokumen kebijakan pendukung yang terdiri dari 3 WP *input* dan 2 WP *output*, yaitu :
 - a. Perubahan dan kesenjangan yang dibutuhkan untuk mencapai kapabilitas sebagai WP *input* dari APO13-BP2
 - b. Definisi arsitektur dan domain dasar sebagai WP *input* dari APO13-BP2

- c. Proposal untuk mengurangi keamanan risiko sebagai WP *input* dari APO13-BP2
 - d. Rencana penanganan risiko keamanan informasi sebagai WP *output* dari APO13-BP2
 - e. Studi kasus bisnis keamanan informasi sebagai WP *output* dari APO13-BP2
3. APO13-BP3 *Monitor and review information security management system* menjaga keamanan informasi secara teratur dari sisi manfaat dan kebutuhan. Kegiatan yang dilakukan pada *base practices* ini dilakukan untuk memenuhi outcome APO13-01 dan APO13-03. *Base Practices* ini terdiri dari 5 *Work Product* (WP) atau dokumen kebijakan pendukung yang terdiri dari 1 WP *input* dan 2 WP *output*, yaitu :
- a. Klasifikasi dan prioritas insiden permintaan layanan sebagai WP *input*
 - b. Laporan audit sistem manajemen keamanan informasi sebagai WP *output*
 - c. Rekomendasi untuk meningkatkan sistem manajemen keamanan informasi sebagai WP *output*

2.13.2 Manage Security Services (DSS05)

DSS05 adalah domain proses dari COBIT 5 yang berfokus dalam hal melindungi aset informasi serta mempertahankan risiko keamanan informasi pada tingkat yang dapat diterima oleh organisasi sesuai kebijakan keamanan. Domain proses ini memiliki 5 *outcome* atau pencapaian utama dari proses COBIT 5 yang berjalan pada organisasi

Tabel 2.13 Penjelasan Outcome Proses DSS05

Outcome	Definisi
DSS05-01	Pemenuhan atas kebutuhan keamanan komunikasi dan jaringan
DSS05-02	Informasi yang disimpan, diproses dan ditransmisikan pada perangkat akhir telah terlindungi
DSS05-03	Setiap pengguna memiliki identitas hak akses yang sesuai dengan kebutuhan bisnisnya
DSS05-04	Pengukuran yang dilakukan untuk melindungi informasi dari akses yang tidak diinginkan, kerusakan dan gangguan
DSS05-05	Pengamanan pada informasi elektronik ketika disimpan, ditransmisikan atau dimusnahkan

Sumber : Diadaptasi dari ISACA (2013a)

Kelima *outcome* atau pencapaian tersebut kemudian diturunkan menjadi *Base Practices* (BP) atau praktik dasar kegiatan proses berdasarkan COBIT 5 yang



dilakukan pada perusahaan untuk mencapai tujuan dari pelaksanaan proses COBIT 5. Selain itu, terdapat juga *Work Product* atau dokumen/kebijakan pendukung terkait pelaksanaan proses COBIT 5 pada organisasi.

1. DSS05-BP1 *Protect Against Malware* adalah sebuah praktek tata kelola dalam rangka memberikan perlindungan dari serangan *malware* seperti virus, worm, spyware, spam dan sejenisnya. Tata kelola perlindungan dilakukan dengan penerapan dan pemeliharaan dalam rangka melindungi aset TI dari serangan *malware*. *Base Practices* ini terdiri dari 2 *Work Product* (WP) *output* atau dokumen kebijakan pendukung, yaitu :
 - a. Kebijakan perlindungan dari *software* berbahaya
 - b. Evaluasi ancaman potensial keamanan informasi
2. DSS05-BP2 *Manage network and connectivity security* berkaitan dengan pengelolaan keamanan jaringan dan konektivitas. Praktek tata kelola dilakukan dengan adanya prosedur perlindungan keamanan pada konektivitas sehingga tetap aman bagi informasi. *Base Practices* ini terdiri dari 3 *Work Product* (WP) atau dokumen kebijakan pendukung yang terdiri dari 1 WP *input* dan 2 WP *output*, yaitu :
 - a. Dokumen perjanjian tingkat layanan sebagai WP *input*
 - b. Dokumen kebijakan keamanan informasi sebagai WP *output*
 - c. Dokumen hasil pengujian keamanan informasi sebagai WP *output*
3. DSS05-BP3 *Manage endpoint security* berkaitan dengan perangkat *endpoint* seperti laptop, *desktop*, server dan sejenisnya dengan menggunakan prosedur pengamanan agar tetap terjamin keamanannya. *Base Practices* ini terdiri dari 5 *Work Product* (WP) atau dokumen kebijakan pendukung yang terdiri dari 4 WP *input* dan 1 WP *output*, yaitu :
 - a. Dokumen model arsitektur sebagai WP *input*
 - b. Dokumen perjanjian tingkat operasional sebagai WP *input*
 - c. Dokumen pemeriksaan inventori fisik sebagai WP *input*
 - d. Dokumen pencatatan transaksi sebagai WP *input*
 - e. Kebijakan keamanan pada *endpoint* sebagai WP *output*
4. DSS05-BP4 *Manage user identity and logical access* berkaitan dengan pengelolaan hak akses dan identitas pengguna untuk memastikan hak akses semua pengguna sesuai dengan kebutuhannya. *Base Practices* ini terdiri dari 3 *Work Product* (WP) atau dokumen kebijakan pendukung yang terdiri dari 1 WP *input* dan 2 WP *output*, yaitu :

- a. Penjelasan peran dan tanggung jawab terkait TI sebagai *WP input*
 - b. Persetujuan hak akses sebagai *WP output*
 - c. Hasil peninjauan hak akses sebagai *WP output*
5. DSS05-BP5 *Manage Physical Security* berkaitan dengan prosedur untuk mencabut akses ketika keadaan darurat. Mengelola akses informasi pada tempat yang berwenang. Memantau tempat sumber informasi pada siapapun yang memasukinya. *Base Practices* ini terdiri dari 2 *Work Product (WP)* atau dokumen kebijakan pendukung yang terdiri dari 2 *WP output*, yaitu :
- a. Persetujuan permintaan hak akses
 - b. *Log* akses informasi
6. DSS05-BP6 *Manage Sensitive documents and output devices* berkaitan dengan praktik manajemen pengamanan dokumen dengan mengamankan fisik dokumen dan menginventarisasikan aset dan dokumen penting TI. *Base Practices* ini terdiri dari 1 *Work Product (WP) input* dan 2 *WP output* sebagai dokumen atau kebijakan pendukung yang dilaksanakan pada perusahaan
- a. Model arsitektur informasi sebagai *Work Product input*
 - b. Penyimpanan informasi dan perangkat sensitive sebagai *Work Product output*
 - c. Dokumen/kebijakan hak akses sebagai *work product output*
7. DSS05-BP7 *Monitor the infrastructure for security-related event* berkaitan dengan praktik pendefinisian menggunakan alat pendeteksi untuk memonitor infrastruktur dari akses yang tidak sah serta memastikan setiap peristiwa termonitor dan termanajemen dengan baik. *Base Practices* ini memiliki 3 *Work Product (WP) output* sebagai dokumen atau kebijakan pendukung pelaksanaan proses.
- a. Karakteristik insiden keamanan
 - b. *Log* kejadian keamanan
 - c. Insiden terkait keamanan

2.14 RACI Chart

RACI (*Responsible, Accountable, Consulted dan Informed*) Chart adalah sebuah matrik untuk menentukan peran dan tanggung jawab dalam sebuah aktivitas atau proses kinerja, dan proses organisasi dalam mengambil keputusan. Penggunaan RACI Chart bertujuan untuk memetakan proses atau aktivitas ke dalam struktur organisasi (Indrajit, 2016). Dalam COBIT 5, RACI Chart bertujuan untuk menggambarkan tanggung jawab dari setiap proses untuk membedakan

peran dan strukturnya (ISACA, 2012a). RACI Chart membagi tanggung jawab pada organisasi menjadi empat peran sebagai berikut :

1. *Responsible* (Pelaksana) adalah orang yang memiliki tanggung jawab secara langsung dalam sebuah kegiatan atau pekerjaan.
2. *Accountable* (Penanggung jawab) memiliki kewenangan atau tanggung jawab dalam mengambil sebuah keputusan atau tindakan.
3. *Consulted* (penasehat) adalah orang yang perlu diberikan pendapat atau saran dan memiliki kontribusi dari sebuah kegiatan atau pekerjaan.
4. *Informed* (terinformasi) adalah orang yang perlu diberitahukan terkait hasil dari sebuah keputusan atau tindakan.

RACI Chart pada COBIT 5 memiliki 26 *management practices* yang dipetakan ke dalam empat peranan yang ada dari setiap domain proses COBIT 5 dan subproses yang dimilikinya. Setiap subproses dalam domain proses COBIT 5 dapat memiliki peranan yang berbeda jika dipetakan ke dalam bentuk COBIT 5. Dalam hal ini, penentuan pihak mana saja yang terlibat untuk melaksanakan proses berdasarkan *management practices* yang ada dilakukan berdasarkan jumlah kewenangan yang dapat mewakili keseluruhan atau sebagian besar subproses pada proses COBIT 5. Keseluruhan pemetaan *management practices* terhadap proses dan aktivitasnya pada setiap domain proses APO13 dan DSS05 digambarkan dalam Gambar 2.7 dan Gambar 2.8.

APO13 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programs/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
APO13.01 Establish and maintain an ISMS.	C	C	C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C	
APO13.02 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	R	C	C	
APO13.03 Monitor and review the ISMS.					C	R	C		R		A				C	C	R	R	R	R	R	R	R	R	R	

Gambar 2.6 RACI Chart APO13

Sumber : ISACA (2012b)

DSS05 RACI Chart																										
Management 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
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Gambar 2.7 RACI Chart DSS05

Sumber : ISACA (2012b)

1. *Board*, adalah eksekutif tertinggi yang bertanggung jawab dalam hal tata kelola seluruh sumber daya organisasi.
2. *Chief Executive Officer* (CEO), adalah pimpinan dari perusahaan yang bertanggung jawab dalam hal manajemen perusahaan keseluruhan dan bertanggungjawab dalam setiap kegagalan maupun kesuksesan perusahaan.
3. *Chief Financial Officer* (CFO) bertanggung jawab pada keseluruhan pengelolaan dan perencanaan keuangan serta pengelolaan risiko keuangan perusahaan.
4. *Chief Operating Officer* (COO) adalah pemimpin perusahaan yang memiliki tanggung jawab dalam hal operasional internal perusahaan seperti operasional kantor, karyawan dan bisnis.
5. *Business Executive* bertanggung jawab dalam hal operasional di perusahaan maupun anak perusahaan.
6. *Business Process Owner* bertanggung jawab dalam mencapai tujuan proses dengan meningkatkan dan menyetujui performa proses jika diperlukan.
7. *Strategy Executive Committee* merupakan eksekutif perusahaan yang ditugaskan untuk menyusun dan mengatur strategi dan memastikan



dewan terlibat dan diinformasikan terkait keputusan TI. Bagian ini juga bertanggung jawab dalam hal pengelolaan portofolio investasi TI, layanan dan asset TI serta mengelola risiko. Pimpinan komite ini adalah anggota *Board*.

8. *Steering Programme/Projects* adalah seseorang yang memiliki tanggung jawab untuk mengarahkan proyek atau program serta mengendalikan proyek atau program tersebut dari awal hingga akhir.
9. *Project Management Office* berfungsi untuk menentukan, menjaga dan mengelola manajemen proyek sesuai standar sehingga organisasi dapat memperoleh keuntungan dari pelaksanaan proyek tersebut.
10. *Value Management Office* bertindak sebagai sekretariat dalam hal pengelolaan pembiayaan pada layanan dan investasi.
11. *Chief Risk Officer* adalah seseorang yang bertanggung jawab dalam hal pemantauan, pengawasan dan pengembangan keseluruhan manajemen risiko perusahaan yang berhubungan dengan TI.
12. *Chief Information Security Officer* memiliki tanggung jawab dalam hal keamanan informasi pada perusahaan dan memastikan keseluruhan aset informasi terlindungi dengan baik.
13. *Architecture Board* bertanggung jawab sebagai penasihat teknis dalam penetapan kebijakan standar arsitektur.
14. *Enterprise Risk Committee* memiliki tanggung jawab dalam memantau kebijakan pengelolaan risiko beserta rencana mitigasi risiko yang diambil oleh perusahaan.
15. *Head Human Resources* bertanggung jawab pada keseluruhan sumber daya manusia dan berperan sebagai pemberi kebijakan sumber daya manusia pada perusahaan.
16. *Compliance* berfungsi untuk memastikan pedoman hukum dan kontrak dipatuhi oleh perusahaan yang diberikan dengan memberikan bimbingan terkait pedoman dan kepatuhan.
17. *Auditor* bertanggung jawab melakukan audit internal dan eksternal pada perusahaan.
18. *Chief Information Officer (CIO)* bertanggung jawab mengarahkan penggunaan teknologi informasi yang mendukung tujuan perusahaan.
19. *Head of Architecture* adalah seseorang yang merancang arsitektur TI yang diterapkan pada perusahaan.
20. *Head Of Development* memiliki tanggung jawab untuk mengembangkan sistem atau aplikasi TI untuk menyelesaikan sebuah solusi bisnis pada perusahaan.
21. *Head of IT Operation* memiliki tanggung jawab untuk memelihara infrastruktur TI yang digunakan pada perusahaan

22. *Head of IT Administration* memiliki tanggung jawab dalam keseluruhan hal yang berkaitan dengan administrasi TI.
23. *Service Manager* memiliki tanggung jawab mengembangkan, mengimplementasikan dan mengelola layanan produk dengan baik kepada pelanggan.
24. *Information Security Manager* memiliki tanggung jawab dalam penilaian dan pengawasan keamanan informasi sehingga dipastikan informasi pada perusahaan terlindungi dengan baik.
25. *Business Continuity Manager* bertanggung jawab mengelola dan mengkaji keberlangsungan bisnis perusahaan.
26. *Privacy Officer* memiliki tanggung jawab menjaga keseluruhan privasi data perusahaan dan memantau risiko terkait hal tersebut.



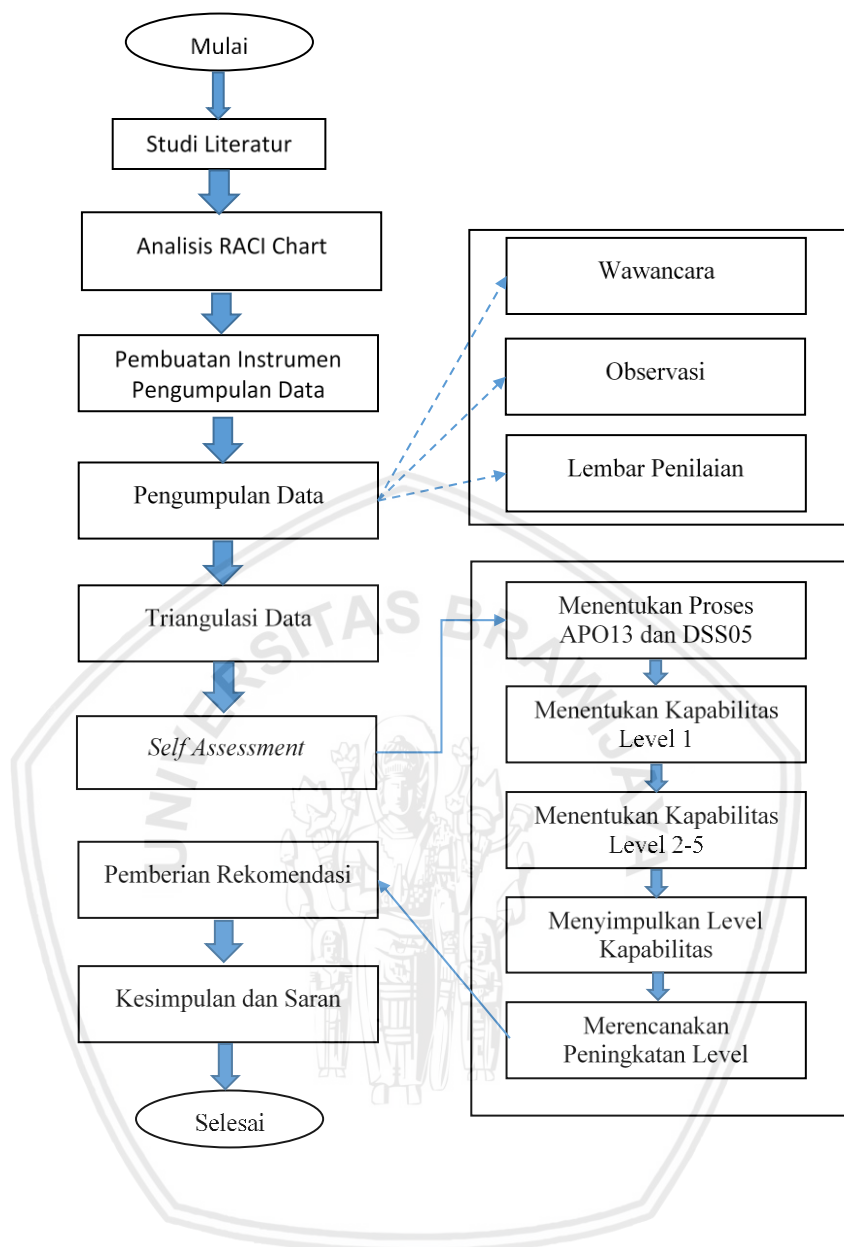
BAB 3 METODOLOGI

3.1 Metodologi Penelitian

Penelitian dilakukan berdasarkan metode kualitatif, yaitu metode penelitian yang dilakukan dengan melakukan pendekatan studi kasus berdasarkan bukti fisik seperti wawancara dan analisis laporan yang diperoleh dari pengamatan pada objek penelitian (Sugiyono, 2017). Metode kualitatif berfokus pada penyelidikan terhadap fenomena dalam konteks kehidupan nyata (Recker, 2013). Penelitian ini akan berfokus pada interpretasi hasil observasi, wawancara dan lembar penilaian sebagai sumber data.

Metodologi penelitian berisi tahapan penelitian yang dilakukan. Metodologi dibuat untuk menjelaskan arah penelitian yang dilakukan untuk menyelesaikan penelitian yang dilakukan. Berikut adalah alur yang digunakan dalam melakukan penelitian berdasarkan kerangka kerja COBIT 5 :





Gambar 3.1 Alur Penelitian

3.2 Studi Literatur

Studi literatur bertujuan untuk menelusuri teori terkait permasalahan dengan objek penelitian. Tujuannya adalah untuk memberikan gambaran bagaimana penelitian ini akan dijalankan. Studi literatur dimulai dengan menyusun gambaran materi yang terkait penelitian yang sedang dilakukan. Tujuannya untuk mempermudah mencari literatur yang memiliki keterkaitan dengan penelitian. Dalam penelitian ini, permasalahan pada objek penelitian adalah terkait evaluasi tata kelola keamanan pada perusahaan.

Dalam tahapan studi literatur ini, sumber yang dijadikan acuan adalah buku terkait tata kelola TI dan jurnal penelitian yang dilakukan sebelumnya. Sumber



jurnal dipilih karena memiliki permasalahan penelitian yang lebih spesifik dibandingkan dengan sumber lain seperti buku. Selain itu, pada jurnal terdapat berbagai indikator penelitian yang lebih mengarah pada masalah, sehingga dari beberapa jurnal acuan, salah satu atau sebagian jurnal penelitian dapat dijadikan acuan dalam melakukan penelitian pada objek yang akan diteliti.

Hasil dari studi literatur yang dilakukan adalah model penelitian yang digunakan dalam penelitian berdasarkan buku dan jurnal penelitian. Berdasarkan hasil studi literatur, metode penelitian yang digunakan adalah COBIT 5 dengan Domain APO13 dan DSS05 seperti yang telah dijelaskan pada latar belakang penelitian ini.

3.3 RACI Chart

RACI (*Responsible, Accountable, Consulted dan Informed*) adalah salah satu alat untuk membantu mengetahui peranan pada personel dalam organisasi. RACI Chart membantu identifikasi tanggung jawab dengan membedakan peran dan strukturnya. RACI Chart terdiri dari empat parameter, yaitu *Responsible* (Pelaksana Tugas), yaitu seseorang yang bekerja untuk menyelesaikan tugasnya. *Accountable* (Memberikan tugas), yaitu seseorang yang memberikan dan memeriksa pekerjaan. *Consulted* (Pemberi masukan atau saran). Dan *Informed* (pihak yang mengetahui informasi).

Analisis RACI Chart dilakukan untuk menentukan responden yang terlibat di setiap proses pada COBIT 5. Dalam penelitian ini, maka akan dilakukan analisis RACI Chart pada proses APO13 dan DSS05. Hasil analisis yang dilakukan akan digunakan untuk memetakan responden sesuai dengan struktur organisasi PT Gagas Energi Indonesia.

3.4 Pengumpulan Data

Pengumpulan data dilakukan dengan menggunakan kuesioner dengan tujuan untuk mengukur *capability level*. Kuesioner disusun berdasarkan pedoman yang diterbitkan oleh ISACA tahun 2013 dalam buku *Process Assessment Model : Using COBIT 5* dengan mengambil proses APO13 dan DSS05 sebagai proses terpilih. Lembar penilaian digunakan untuk mengukur kapabilitas keamanan informasi berdasarkan proses yang dipilih, yaitu APO13 dan DSS05.

Selain menggunakan kuesioner, data juga dikumpulkan melalui proses wawancara dan observasi yang bertujuan untuk mendapatkan gambaran permasalahan terkait keamanan informasi. Wawancara dilakukan pada pihak yang berwenang yang didasarkan oleh RACI Chart. wawancara bertujuan sebagai tindakan verifikasi dan penjelasan hasil kuesioner yang telah diisikan.

Selain wawancara dan pengisian lembar penilaian, penelitian ini juga menggunakan observasi. Observasi dilakukan dengan mengamati bagaimana berjalannya proses keamanan informasi pada PT Gagas Energi Indonesia. Tujuannya adalah untuk melihat sejauh mana berjalannya proses tata kelola keamanan informasi pada PT Gagas Energi Indonesia.

3.5 Triangulasi Data

Triangulasi data adalah pengumpulan dari beberapa jenis data dan barang bukti dalam satu penelitian (Reckers, 2013). Triangulasi data dilakukan untuk memperoleh situasi penelitian yang lebih bernuansa dan meningkatkan validitas dari temuan peneliti (Reckers, 2013). Dalam penelitian ini, triangulasi data dilakukan pada objek penelitian dari berbagai metode pengumpulan data yang berbeda.

3.6 Self Assessment

Self Assessment merupakan pengukuran terhadap tingkat kapabilitas dari setiap proses yang akan dinilai. Tahap ini terdiri dari 5 langkah untuk mengetahui kapabilitas dari proses. Tahapan pertama adalah menentukan proses yang akan dinilai. Kemudian menentukan level yang ingin dicapai dari perusahaan. Langkah berikutnya adalah melakukan penilaian dari setiap proses dengan kapabilitas pada level 1.

Setelah dilakukan penilaian kapabilitas dengan level 1, kemudian dilanjutkan dengan menilai kapabilitas proses pada level 2 hingga level 5. Tahapan ini menggunakan *Process Assessment Model* (PAM) untuk menilai level kapabilitas yang mampu diraih dari setiap proses. Lembar PAM terdiri dari empat kategori utama penilaian yaitu N (*Not Achieved*) dengan nilai 0-15%, P (*Partially Achieved*) dengan nilai >15%-50%, L (*Largely Achieved*) dengan nilai >50%-85% dan F (*Fully Achieved*) dengan nilai >85%-100%. Penilaian dalam lembar PAM dilakukan berdasarkan *Base Practices* (BP) dari setiap proses yang dipilih.

Kemudian, pada tahap terakhir adalah menimbang level yang dicapai oleh perusahaan dengan level yang ditargetkan perusahaan menggunakan analisis *gap* (*gap analysis*). Diskusi dan wawancara pada pihak terkait yang mewakili masing-masing proses dilakukan untuk mengetahui level target perusahaan. Sementara analisis kesenjangan didapatkan dari kuesioner penilaian yang telah dilakukan dengan membandingkan antara pencapaian saat ini dan target dari perusahaan. Analisis ini berguna sebagai langkah dalam pemberian rekomendasi untuk pengembangan keamanan informasi kedepannya.

3.7 Pemberian Rekomendasi

Rekomendasi yang diberikan didasarkan dari hasil *self assessment* yang telah dilakukan sebelumnya. Rekomendasi diberikan dengan menentukan level target yang ingin dicapai dari setiap proses berdasarkan hasil *capability level* dan analisis *gap*. Berikutnya, dilakukan analisis tata kelola TI pada domain yang dipilih dalam COBIT 5 untuk menentukan rekomendasi. Sedangkan pada analisis *gap*, penyusunan rekomendasi akan dilakukan dengan membandingkan kondisi pencapaian perusahaan dan peningkatan yang diinginkan oleh perusahaan. Pemberian rekomendasi akan disesuaikan dengan kemampuan perusahaan dan strategi bisnis yang akan dilakukan kedepannya. Pemberian rekomendasi

diharapkan mampu membantu meningkatkan tata kelola keamanan TI pada PT Gas Energi Indonesia.

3.8 Kesimpulan dan Saran

Kesimpulan didapatkan dari hasil kuesioner yang telah dianalisis sebelumnya. Kesimpulan berisi rekomendasi perbaikan secara umum. Selain berisi rekomendasi perbaikan, kesimpulan menjawab rumusan masalah dari penelitian ini. Sedangkan saran berisi pengembangan penelitian untuk meningkatkan kualitas penelitian ini kedepannya.



BAB 4 HASIL EVALUASI

4.1 Manage Security (APO13)

APO13 adalah proses pada COBIT 5 terkait dengan hal mendefinisikan, mengoperasikan dan mengawasi keamanan informasi serta menjaga risiko keamanan informasi agar tetap berada pada level yang dapat diterima oleh perusahaan (ISACA, 2012). Untuk melakukan penilaian pada proses APO13, maka terlebih dahulu dilakukan analisis RACI Chart pada APO13. Tujuannya agar menentukan siapa yang paling berhak untuk terlibat dalam penelitian pada proses APO13 sehingga mendapatkan data yang valid. Berikut adalah tabel analisis RACI Chart pada proses APO13 COBIT 5.

Tabel 4.1 Analisis RACI Chart APO13

No	Management Practice	RACI Chart			
		R	A	C	I
1	Board				
2	Chief Executive Officer			2	
3	Chief Financial Officer				
4	Chief Operating Officer			2	
6	Business Process Owners	1		1	1
7	Strategy Executive Committee			3	
8	Steering (Programmes/Project) Committee				2
9	Project Management Office	1			2
10	Value Management Office				
11	Chief Risk Officer			2	
12	Chief Information Security Officer		3		
13	Architecture Board			2	
14	Enterprise Risk Committee			2	
15	Head Human Resources				
16	Compliance			3	
17	Audit			3	
18	Chief Information Officer	3			
19	Head Architect	1		1	1

Tabel 4.1 Analisis RACI Chart APO13 (Lanjutan)

No	Management Practice	RACI Chart			
		R	A	C	I
20	Head Development	1		1	1
21	Head IT Operations	1		1	1
22	Head IT Administration	3			
23	Service Manager	1		1	1
24	Information Security Manager	3			
25	Business Continuity Manager	1		2	
26	Privacy Officer	1		2	

Tabel 4.1 menunjukkan jika nilai angka menggambarkan jumlah *base practices* pada proses COBIT 5 yang terlibat untuk menjalankan proses jika merujuk pada Gambar 2.8 yang terdapat pada bab 2. Dalam hal ini, *Chief Information Officer*, *Head IT Administration*, dan *Information Security Manager* adalah pihak *Responsible* pada proses APO13 dengan nilai tertinggi yaitu bernilai 3 pada masing-masing *management practice* yang berarti ketiga pihak tersebut terlibat sebagai pihak *Responsible* keseluruhan *base practices* dari proses APO13. Sedangkan *Chief Information Security Officer* merupakan pihak *Accountable* satu-satunya yang mampu memenuhi keseluruhan *base practices* dari proses APO13 sehingga dalam hal ini pihak *Chief Information Security Officer* dipilih menjadi pihak *accountable* berdasarkan hasil pemetaan *RACI Chart*. Pihak *Consulted* dalam proses ini adalah *Business Executives*, *Strategy Executive Committee*, *Compliance*, dan *Audit* dengan nilai 3 di masing-masing peran. Pihak *Informed* dalam proses ini adalah *Steering (Program/Project)* dan *Project Management Office* dengan nilai tertinggi 2 pada setiap perannya. Namun, pihak *consulted* dan *informed* dalam hal ini tidak terlalu berperan dalam menjalankan proses. Berdasarkan Hasil dari pemetaan pada *RACI Chart*, berikut adalah penjelasan yang ditampilkan pada Tabel 4.2 sebagai berikut.

Tabel 4.2 Pemetaan RACI Chart Terhadap Proses APO13

No	Komponen	Peran	Jabatan Organisasi
1	<i>Responsible</i>	<i>Chief Information Officer</i>	<i>Information and System Development Senior Staff</i>
2		<i>Head IT Administration</i>	-
3		<i>Information</i>	-



Tabel 4.2 (lanjutan)

No	Komponen	Peran	Jabatan Organisasi
3		<i>Security Manager</i>	-
4	<i>Accountable</i>	<i>Chief Information Security Officer</i>	<i>HR & IT Department Head</i>

Berdasarkan Tabel 4.2, pihak *Chief Information Officer* dalam jabatan organisasi disebut *Information and System Development Senior Staff* sebagai pihak *Responsible* yang berhak untuk mengisi lembar penilaian dokumen pada proses APO13. Hal tersebut dikarenakan berdasarkan berdasarkan struktur organisasi yang ada, pihak *Information and System Development Staff* memiliki tanggung jawab yang mirip dengan definisi dari *Chief Information Officer*, yaitu bertanggung jawab untuk mengarahkan penggunaan teknologi informasi untuk mencapai tujuan perusahaan. Sedangkan *Chief Information Security Officer* dalam jabatan organisasi disebut sebagai *HR & IT Department Head* sebagai pihak *Accountable* karena memiliki kemiripan tanggung jawab pada komponen dan peranan pada *RACI Chart* yaitu sebagai pihak yang memiliki kewenangan dalam hal penerapan TI di lingkungan perusahaan dan memiliki tanggung jawab dalam hal keamanan informasi pada perusahaan. Sedangkan pada peran lainnya jabatan tidak dapat ditemukan pada struktur organisasi. *Information and System Development Senior Staff* memiliki peran yang sama dengan *Chief Information Officer* dalam *RACI Chart* yaitu orang yang bertanggung jawab dalam hal penanganan masalah TI pada perusahaan. Sedangkan *Chief Information Security Officer* memiliki kesamaan peran dengan *HR & IT Department Head*, yaitu sebagai orang yang tanggung jawabnya dalam organisasi untuk menjaga keamanan informasi.

Pada APO13 terdapat 3 *Base Practices* (BP) yang dapat digunakan untuk mengukur penilaian pada proses APO13. BP pertama pada APO13 adalah menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (SMKI) yang menyediakan pendekatan standar secara terus menerus untuk manajemen keamanan informasi. BP kedua adalah menentukan dan merencanakan penanganan risiko keamanan informasi yang bertujuan untuk mempertahankan rencana keamanan informasi dan menyelaraskannya dengan arsitektur bisnis perusahaan. BP ketiga atau terkait pengawasan dan peninjauan ulang (*review*) dari sistem manajemen keamanan informasi. Tujuannya adalah untuk mempertahankan manfaat dari adanya perbaikan terus menerus pada sistem manajemen keamanan informasi.

Dari ketiga *Base Practices*, kemudian pada BP tersebut diturunkan menjadi beberapa *Work Product* (WP) yang nantinya digunakan untuk melakukan penilaian pada proses APO13. Tujuannya adalah untuk mempermudah responden dalam melakukan pengisian lembar penilaian. BP dan WP dari proses APO13 digunakan untuk mengukur tingkat kapabilitas pada level 1. Pada APO13-

BP1, *Work Product* yang dihasilkan adalah dokumen tentang pendekatan keamanan informasi perusahaan dan pendekatan kebijakan manajemen keamanan informasi. Dalam hal ini, PT Gagas Energi Indonesia telah menerapkan kedua WP tersebut dalam bentuk dokumen Pedoman Tata Kelola TI pada bagian Prosedur Pengamanan IT dan keseluruhan Dokumen Prosedur Operasi yang dimiliki oleh PT Gagas Energi Indonesia.

Pada APO13-BP2, *Work Product* yang dihasilkan tertulis dalam bentuk Dokumen Rencana *Grand Design IT* PT Gagas Energi Indonesia. Pada dokumen tersebut memuat beberapa WP yang menjadi bagian dari APO13-BP2. Diantaranya adalah dokumen tentang kesenjangan dan perubahan untuk mencapai kapabilitas yang terdapat pada bagian *ICT Strategic Roadmap* dan Transformasi. Pada bagian tersebut dijelaskan rencana TI yang dilakukan oleh PT Gagas Energi Indonesia dan kondisi TI yang diterapkan saat ini. Kemudian dokumen tentang definisi arsitektur dan domain dasar yang terdapat pada bagian *ICT Architecture*. Pada bagian ini dijelaskan model dan kerangka kerja arsitektur TI yang diterapkan oleh PT Gagas Energi Indonesia. Berikutnya adalah dokumen tentang rencana penanganan risiko keamanan informasi. Penanganan resiko keamanan informasi didefinisikan dalam dokumen *Grand Design IT* pada bagian Pengelolaan Manajemen Resiko.

Sedangkan pada APO13-BP3, *Work Product* pertama yang dihasilkan adalah dokumen tentang klasifikasi dan insiden perubahan layanan. Dokumen mengenai hal tersebut dijelaskan di Dokumen Prosedur Operasi Pengelolaan Permasalahan TI PT Gagas Energi Indonesia bagian prosedur. Pada bagian tersebut dijelaskan bagaimana klasifikasi dan prioritas yang dibutuhkan jika ingin melakukan perubahan TI pada Satuan kerja PT Gagas Energi Indonesia. Berikutnya adalah dokumen kebijakan manajemen keamanan informasi yang dijelaskan juga pada Dokumen Prosedur Operasi TI. Berikutnya adalah dokumen audit manajemen keamanan informasi yang dijelaskan juga pada Dokumen Prosedur Operasi TI. Keseluruhan *Base Practices* dan *Work Product* yang dihasilkan dari penilaian level 1 dijelaskan pada Tabel 4.3 berikut.

Tabel 4.3 Hasil Pemetaan Dokumen/Kebijakan Proses APO13

<i>Base Practices</i>	<i>Work Product</i>	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
Menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (SMKI)	Dokumen pendekatan keamanan informasi	Ya	Pedoman Tata Kelola TI pada Bagian Prosedur Pengamanan IT	Lampiran Prosedur Pengamanan IT dan Dokumen Terkait Prosedur Operasi

Tabel 4.3 (lanjutan)

<i>Base Practices</i>	<i>Work Product</i>	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
	Dokumen kebijakan manajemen keamanan informasi	Ya	Lampiran Prosedur Pengamanan IT dan Dokumen Prosedur Operasi	Lampiran Prosedur Pengamanan IT dan Dokumen Terkait Prosedur Operasi
Menentukan dan merencanakan penanganan risiko keamanan informasi	Dokumen tentang kesenjangan dan perubahan yang dibutuhkan untuk mencapai target kapabilitas	Ya	Dokumen Rencana <i>Grand Design IT</i> pada bagian <i>ICT Strategic Roadmap</i> dan Transformasi	Lampiran <i>Grand Design IT</i> dan <i>ICT Strategic Roadmap</i> dan Transformasi
	Dokumen tentang definisi arsitektur dan domain dasar	Ya	Dokumen Rencana <i>Grand Design IT</i> pada bagian <i>ICT Architecture</i>	Lampiran <i>ICT Architecture</i>
Menentukan dan merencanakan penanganan risiko keamanan informasi	Dokumen tentang proposal untuk mengurangi risiko keamanan informasi	Ya	Dokumen Rencana <i>Grand Design IT</i> pada bagian Pengelolaan Manajemen Risiko	Lampiran Pengelolaan Manajemen Risiko

Tabel 4.3 (Lanjutan)

<i>Base Practices</i>	<i>Work Product</i>	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
	Dokumen rencana penanganan risiko keamanan informasi	Ya	Dokumen Rencana <i>Grand Design IT</i> pada bagian <i>ICT Strategic Roadmap</i>	Lampiran <i>Grand Design IT</i> dan <i>ICT Strategic Roadmap</i>
	Dokumen tentang studi kasus dari keamanan informasi	Tidak	-	-
Mengawasi dan meninjau ulang (<i>review</i>) Sistem Manajemen Keamanan Informasi (SMKI)	Dokumen tentang audit manajemen keamanan informasi	Ya	Dokumen Prosedur Operasi TI	Lampiran terkait Dokumen Prosedur Operasi TI
	Dokumen rekomendasi peningkatan manajemen keamanan informasi	Tidak	-	-

Berdasarkan Tabel 4.3, diketahui jika hampir keseluruhan *Base Practices* dan *Work Product* yang telah dilakukan oleh PT Gagas Energi Indonesia dibagi menjadi tiga dokumen utama yaitu Dokumen Pedoman dan Tata Kelola TI, Dokumen *Grand Design IT* PT Gagas Energi Indonesia dan Dokumen Prosedur Operasi terkait penerapan TI pada PT Gagas Energi Indonesia. Sehingga dalam hal ini, penilaian kapabilitas pada level 1 telah memenuhi kriteria pencapaian dan dapat dilanjutkan ke penilaian kapabilitas level berikutnya. Dalam hal ini, penilaian pada proses APO13 telah mencapai *Largely Achieved* karena pada *Base Practices* dan *Work Product* berada pada rentang 50% sampai 85% yaitu pada angka 81%. Hasil penilaian pada level 1 dapat dilihat pada Tabel 4.4 berikut.

Tabel 4.4 Penilaian Level 1 Proses APO13

<i>Base Practices</i>	<i>Work Product</i> Terpenuhi	<i>Work Product</i> Total	Persentase
APO13-BP1	2	2	100%
APO13-BP2	4	5	80%
APO13-BP3	3	4	75%
Total	9	11	81%

Langkah berikutnya adalah melakukan penilaian yang dimulai dari level 2 sampai level 5. Pada level 2, terdapat atribut proses yaitu *Process Attribute 2.1 (Performance Management)* yang memiliki enam kriteria, dan *Process Attribute 2.2 (Work Product Management)* yang memiliki empat kriteria. Pada penilaian PA 2.1, beberapa *Generic Practices (GP)* dan *Generic Work Product (GWP)* yang telah diterapkan pada level ini yang pertama adalah identifikasi tujuan dan pelaksanaan proses. Setiap proses yang terdapat pada Dokumen Prosedur Operasi telah memiliki tujuan dilaksanakannya proses dan terdokumentasi dengan cukup baik. Kedua adalah kinerja proses yang telah disesuaikan dengan kebutuhan rencana. Dalam hal ini, pengelolaan proses telah disesuaikan dengan rencana yang diharapkan oleh perusahaan dan alternatif solusi jika proses tidak dapat terpenuhi. Ketiga adalah tanggung jawab dan wewenang untuk melakukan proses. Dari setiap dokumen yang ada, terutama dokumen prosedur operasi telah terdapat tanggung jawab dan wewenang terkait siapa yang memiliki hak untuk melaksanakan proses tertentu. Keempat adalah mengelola antarmuka dari setiap pihak yang terlibat. Dalam hal ini, keseluruhan dokumen terutama dokumen prosedur operasi telah menjelaskan pihak mana saja yang terlibat untuk melaksanakan sebuah proses dan komunikasi yang dibutuhkan untuk melaksanakan proses.

Berikutnya adalah melanjutkan penilaian pada level 2 atribut PA 2.2. Pada atribut ini, PT Gagah Energi Indonesia telah menerapkan 3 dari 4 *Generic Practices (GP)*. GP yang telah diterapkan dalam proses ini antara lain adalah penjelasan persyaratan hasil kerja, termasuk tujuan, struktur dan kriteria keberhasilan hasil kerja. Dalam hal ini, perusahaan telah menjelaskan persyaratan hasil kerja yang dibutuhkan untuk mencapai setiap proses yang dijalankan dalam perusahaan. Kedua adalah kebijakan untuk dokumentasi dan pengendalian hasil kerja yang tertuang dalam bentuk instruksi atau kebijakan untuk mendokumentasikan hasil kerja dari setiap proses pada Dokumen Prosedur Operasi. Ketiga adalah peninjauan ulang hasil kerja dengan perencanaan dan persyaratan hasil kerja. Dalam hal ini, dari setiap prosedur operasi yang menjadi bagian dari proses APO13 dan dijalankan dalam perusahaan telah terdapat permintaan untuk meninjau ulang proses yang telah dilakukan dengan perencanaan di awal. Sehingga, proses APO13 pada PA 2.2 mencapai kategori *Largely Achieved (L)*. Karena kedua atribut pada penilaian

level 2 telah mencapai kategori *Largely Achieved*, maka proses penilaian dapat dilanjutkan ke level berikutnya atau level 3.

Kemudian pada penilaian level 3 PA 3.1, PT Gagas Energi Indonesia telah menetapkan standar proses untuk mendukung pendefinisian proses dalam bentuk prosedur TI. Kedua adalah menentukan interaksi antarproses dalam bentuk diagram alir (*flowchart*) dari sebuah proses dalam setiap dokumen prosedur TI. Ketiga adalah identifikasi kompetensi dan peran proses sebagai bagian dari standar proses dalam bentuk pembagian peran berdasarkan kompetensi dari masing-masing bagian pada proses. Sedangkan pada dua proses lainnya tidak ditemukan bukti yang cukup kuat pada dokumen sehingga pada PA 3.1 hanya mampu mencapai tiga dari lima kriteria *Generic Practices* atau mencapai kriteria *Largely Achieved* (L). Langkah berikutnya adalah melakukan penilaian pada PA 3.2. Pada penilaian ini, tercapai dua dari enam kriteria GP yaitu pada komunikasi dan penjelasan peran, tanggung jawab dan wewenang dari setiap proses dan data yang sesuai telah dikumpulkan dan dianalisis untuk memahami proses. Pada PA 3.2, pencapaian GP hanya mampu mencapai kriteria *Partially Achieved* (P) sehingga proses penilaian berhenti pada level 3. Dalam hal ini, penilaian dapat disimpulkan berada pada level 2 namun dengan catatan pada level 3 atribut proses 3.1 mencapai *largely achieved* dan pada atribut proses 3.2 mencapai *partially achieved*. Hasil penilaian keseluruhan pada proses APO13 dapat dilihat pada Tabel 4.5 berikut ini.

Tabel 4.5 Perhitungan Kapabilitas Proses APO13

Level	Atribut Proses	BP/GP Terpenuhi	BP/GP Target	WP/GWP Terpenuhi	WP/GWP Target	Persentase	Skala
Level 1	PA 1.1	3	3	9	11	81%	L
Level 2	PA 2.1	4	6	7	10	70%	L
	PA 2.2	3	4	4	5	75%	L
Level 3	PA 3.1	3	5	4	6	67%	L
	PA 3.2	2	6	2	7	28%	P
Level 4	PA 4.1	0	6	0	7	0%	N
	PA 4.2	0	5	0	6	0%	N
Level 5	PA 5.1	0	5	0	5	0%	N
	PA 5.2	0	3	0	3	0%	N

Berdasarkan analisis yang dilakukan berdasarkan *Base Practices* (BP)/*Generic Practices* (GP) dan *Work Product* (WP)/*Generic Work Product* (GWP), diketahui jika proses APO13 mencapai tingkat kapabilitas pada level 2 (*Managed Process*) dengan pencapaian pada level 2 mencapai *largely achieved* pada kedua atribut

dan salah satu atribut pada level 3 (*Established Process*) mencapai level *partially achieved*. Proses penilaian dihentikan pada level 3 karena salah satu atribut dari level tersebut belum mencapai *largely achieved* sebagai syarat untuk menaikkan ke level berikutnya. Sehingga, penilaian pada level berikutnya tidak dapat dilakukan dan level penilaian diturunkan satu level dari pencapaian maksimal yang dicapai pada penilaian proses APO13. Keseluruhan hasil konversi nilai angka terhadap penilaian kriteria pada COBIT 5 dengan fokus proses APO13 digambarkan dalam Tabel 4.6. Tabel 4.6 juga menggambarkan kapabilitas yang telah dicapai oleh setiap proses pada COBIT 5 proses APO13.

Tabel 4.6 Penilaian Pada Proses 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		
KRITERIA		L	L	L	L	P						
KAPABILITAS				2								
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%)												

Hasil wawancara yang dilakukan menginginkan *targeted level* pada proses ini berada pada level 3 (*Established Process*). Untuk dapat mencapai level 3, setidaknya pada level 3 harus mencapai *Largely Achieved* pada kedua atribut yang terdapat di dalamnya (ISACA, 2013). Sedangkan pada hasil penelitian menunjukkan bahwa proses APO13 yang telah dicapai berada pada level 2 (*Managed Process*). Berdasarkan hal tersebut diketahui bahwa kesenjangan antara proses yang telah diraih dan yang ingin dicapai adalah sebesar 1 tingkat seperti yang dijelaskan pada Tabel 4.7 di bawah ini.

Tabel 4.7 Analisis Kesenjangan Proses APO13

Nama Proses	Level yang Dituju	Level yang Dicapai	Kesenjangan
APO13	3	2	1

4.2 Manage Security Services (DSS05)

DSS05 adalah sebuah proses pada COBIT 5 dengan fokus mengelola layanan keamanan pada organisasi untuk mempertahankan risiko keamanan informasi berada pada batas aman yang telah ditentukan (ISACA, 2012a). Untuk melakukan penilaian pada proses DSS05, maka terlebih dahulu dilakukan analisis RACI *Chart*

pada DSS05. Tujuannya agar menentukan siapa yang paling berhak untuk terlibat dalam penelitian pada proses DSS05 sehingga mendapatkan data yang valid. Berikut adalah tabel analisis *RACI Chart* pada proses DSS05 COBIT 5.

Tabel 4.8 Analisis RACI Chart DSS05

No	Management Practice	RACI Chart			
		R	A	C	I
1	Board				
2	Chief Executive Officer				
3	Chief Financial Officer				
4	Chief Operating Officer				1
6	Business Process Owners	2		1	3
7	Strategy Executive Committee				1
	Steering (Programmes/Project)				
8	Committee				
9	Project Management Office				
10	Value Management Office				
11	Chief Risk Officer			5	2
12	Chief Information Security Officer		6		
13	Architecture Board				
14	Enterprise Risk Committee				
15	Head Human Resources	1			1
16	Compliance			7	
17	Audit			7	
18	Chief Information Officer		6		
19	Head Architect				6
20	Head Development	3		3	
21	Head IT Operations	7			
22	Head IT Administration				
23	Service Manager				6
24	Information Security Manager	6			
25	Business Continuity Manager				2

Tabel 4.8 Analisis RACI Chart DSS05 (Lanjutan)

No	Management Practice	RACI Chart			
		R	A	C	I
26	Privacy Officer			1	1

Nilai angka yang dijabarkan pada Tabel 4.3 didapatkan dari jumlah keterlibatan pihak manajemen pada *base practices* yang terdapat pada proses DSS05. Berdasarkan hal tersebut, nilai tertinggi pada pihak *Responsible* didapatkan pada pihak *Head IT Operations* dengan nilai 7, dan *Information Security Manager* dengan nilai 6 yang berarti pihak *Head IT Operations* dan *Information Security Manager* masing-masing menjalankan 7 dan 6 kegiatan atau *base practices* pada proses DSS05. Sedangkan *Chief Information Security Officer* menjadi pihak *Accountable* dalam DSS05 dengan nilai tertinggi yaitu 7. Artinya adalah pihak *Chief Information Security Officer* bertanggung jawab untuk menjalankan 7 kegiatan atau *base practices* pada proses DSS05. Pihak *Consulted* dalam proses ini adalah *Compliance*, dan *Audit* dengan nilai 7 di masing-masing peran. Pihak *Informed* dalam proses ini adalah *Service Manager* dengan nilai tertinggi 7. Berdasarkan hasil analisis RACI Chart, maka berikut adalah pemetaan terhadap responden pada proses DSS05 yang dijabarkan dalam Tabel 4.4.

Tabel 4.9 Pemetaan RACI Chart Terhadap Proses DSS05

No	Komponen	Peran	Jabatan Organisasi
1	<i>Responsible</i>	<i>Head IT Operations</i>	<i>Infrastructure and Network Senior Staff</i>
3		<i>Information Security Manager</i>	-
4	<i>Accountable</i>	<i>Chief Information Security Officer</i>	<i>HR & IT Department Head</i>

Berdasarkan Tabel 4.4, pihak *Head IT Operations* dalam jabatan organisasi disebut *Infrastructure and Network Senior Staff* sebagai pihak *Responsible* yang berhak untuk mengisi lembar penilaian dokumen pada proses DSS05 karena memiliki kemiripan tanggung jawab dengan peranan yang terdapat pada pihak *Responsible* pada peranan *Head IT Operations* yaitu sebagai pihak yang melaksanakan pekerjaan dalam hal pemeliharaan infrastruktur TI pada perusahaan. Sedangkan *Chief Information Security Officer* dalam jabatan organisasi disebut sebagai *HR & IT Department Head* sebagai pihak *Accountable*. Sedangkan pada peran lainnya tidak ditemukan jabatan yang sesuai dengan struktur organisasi. *Infrastructure and Network Senior Staff* memiliki peran yang sama dengan *Head IT Operations* dalam RACI Chart yaitu sebagai pihak yang bertanggung jawab untuk menangani masalah infrastruktur TI pada perusahaan.

Sedangkan *Chief Information Security Officer* memiliki kesamaan peran dengan *HR & IT Department Head*, yaitu sebagai orang yang memiliki tanggung jawab untuk menjaga keamanan informasi di dalam organisasi secara umum.

Proses DSS05 memiliki tujuh *Base Practices* (BP) atau kegiatan dasar yang terdapat pada proses DSS05. *Base Practices* pertama adalah perlindungan dari *malware*. Pada BP ini, terdapat dua *Work Product* atau dokumen pendukung dari sebuah kebijakan. Yaitu dokumen pencegahan perangkat lunak berbahaya dan dokumen evaluasi ancaman potensial keamanan. PT Gagas Energi Indonesia telah menerapkan dokumen pencegahan perangkat lunak berbahaya dalam bentuk Prosedur Operasi dan *Monitoring Software* yang menjelaskan jika instalasi sebuah *software* atau perangkat lunak dapat ditolak jika dinilai memiliki ancaman bahaya untuk perusahaan. Sedangkan pada dokumen evaluasi ancaman potensial keamanan tidak ditemukan dokumen yang sesuai dengan WP tersebut.

Base Practices kedua yaitu pengelolaan jaringan dan konektivitas. BP ini terdiri dari tiga *Work Product* (WP) yaitu klasifikasi data, pengujian keamanan dan kebijakan keamanan pada konektivitas. Pada BP ini, PT Gagas Energi Indonesia telah menerapkan keseluruhan BP/WP dalam bentuk implementasi secara langsung, data *log* dan dokumen prosedur operasi. Implementasi secara langsung dilakukan pada klasifikasi data dengan mengklasifikasikan data berdasarkan sumber dan jenisnya, namun pada bagian ini belum ditemukan dokumentasi yang jelas terkait klasifikasi data. Sedangkan pada hasil pengujian keamanan bukti yang ditemukan adalah *log firewall* dan antivirus. Dokumentasi tertulis dalam bentuk prosedur operasi ditemukan pada kebijakan keamanan pada konektivitas dalam bentuk Dokumen Prosedur Operasi Hak Akses yang menjelaskan bagaimana mekanisme perusahaan untuk mengamankan akses terhadap sumber informasi yang bersifat sensitif dalam lingkup perusahaan.

Base Practices ketiga yaitu mengelola keamanan pada titik akhir (*endpoint*) perangkat seperti laptop, PC, printer dan sebagainya. Pada BP ini, PT Gagas Energi Indonesia telah menerapkan keseluruhan *Work Product* yang menjadi bagian dari proses ini. *Work Product* tersebut diantaranya adalah dokumen tentang model arsitektur informasi dalam bentuk Dokumen *Grand Design* ICT Gagas pada bagian *ICT Architecture*. Pada dokumen tersebut telah dijelaskan model arsitektur informasi yang digunakan oleh PT Gagas Energi Indonesia. Selanjutnya adalah dokumen perjanjian tingkat operasional (OLA) yang tertulis dalam Prosedur Operasi (PO) Permasalahan IT pada kebijakan pencatatan dan penyelesaian permasalahan IT. Selanjutnya terdapat dokumen pemeriksaan inventori fisik yang diatur dalam Dokumen Data IT Gagas. Dokumen berikutnya adalah tentang hasil dari transaksi dalam bentuk Dokumen Instalasi dan *Monitoring Software*. Pada dokumen tersebut dijelaskan mekanisme pengadaan dan instalasi *software* yang diperlukan dari satuan kerja PT Gagas Energi Indonesia. Dokumen terakhir pada BP ini adalah dokumen kebijakan pada perangkat *endpoint* seperti laptop, komputer, *server* dan perangkat lainnya yang terdapat pada PO Instalasi dan *Monitoring Software*. Pada dokumen tersebut

memuat kebijakan keamanan pada perangkat *endpoint* dengan mensyaratkan bahwa setiap *software* yang akan digunakan dalam lingkup perusahaan harus memenuhi kebutuhan keamanan informasi disamping memenuhi kebutuhan usaha perusahaan.

Base Practices keempat yaitu mengelola identitas pengguna dan hak akses. Pada BP ini, *Work Product* atau dokumen kebijakan yang dapat dipenuhi oleh PT Gagas Energi Indonesia adalah dokumen tentang dokumen antara peran dan tanggung jawab TI serta dokumen persetujuan hak akses pengguna dalam bentuk Prosedur Operasi Pengelolaan Hak Akses. Hubungan peran dan tanggung jawab TI serta persetujuan hak akses pengguna tertulis dalam dokumen ini dalam bentuk peranan TI dan tanggung jawab dari *HR and IT Department* dan satuan kerja atau pihak ketiga lainnya dalam bentuk pemberian hak akses ke fasilitas informasi kepada setiap satuan kerja/pihak ketiga hanya ketika hal tersebut sesuai dengan cakupan perjanjian kontrak antara pengguna internal dan *HR and IT Department Head* dan pengguna menyetujui pernyataan untuk menjaga keamanan informasi perusahaan dan informasi digunakan sesuai dengan kebutuhan pengguna tersebut.

Base Practices kelima adalah pengelolaan pada aset fisik TI. BP ini terdiri dari dua *Work Product* atau dokumen yang diperlukan yaitu dokumen persetujuan permintaan hak akses dan *access logs* pada sistem. Kedua persyaratan dokumen tersebut telah dipenuhi PT Gagas Energi Indonesia melalui Dokumen Prosedur Operasi (PO) Pengelolaan Hak Akses. Pada dokumen tersebut, telah terdapat persetujuan permintaan hak akses pada pengguna terhadap fasilitas informasi yang terdapat di PT Gagas Energi Indonesia. Persetujuan permintaan hak akses dilakukan oleh *HR and IT Department Head* apabila pengguna telah memenuhi persyaratan yang telah ditentukan oleh Satuan Kerja IT. Sedangkan dokumen *access logs* pada sistem dijabarkan pada bagian terakhir prosedur Dokumen Pengelolaan Hak Akses yaitu dilakukannya penjejakan pada saat penutupan akses pada pengguna terkait telah berakhir. Hal ini dilakukan untuk menjaga jejak audit informasi pada PT Gagas Energi Indonesia.

Base Practices keenam adalah mengelola dokumen penting dan perangkat *output* lainnya. Pada BP ini terdapat dua *Work Product* utama atau dokumen yang harus dipenuhi agar BP keenam dapat terpenuhi dengan maksimal. dokumen yang harus dipenuhi adalah dokumen tentang model arsitektur informasi dan dokumen tentang wewenang hak akses pada sistem. Namun, pada PT Gagas Energi Indonesia tidak ditemukan sama sekali dokumen yang terkait dengan kedua WP tersebut sehingga BP keenam secara keseluruhan tidak dapat terpenuhi dengan baik. *Base Practices* ketujuh adalah memantau infrastruktur untuk setiap hal yang berhubungan dengan keamanan. Terdapat tiga *Work Product* atau dokumen yang terkait BP ketujuh ini. WP pertama adalah dokumen karakteristik risiko keamanan, dokumen daftar peristiwa keamanan informasi dan dokumen risiko keamanan informasi. Ketiga dokumen tersebut tidak terdapat pada PT Gagas Energi Indonesia. Dalam hal ini BP ketujuh tidak dapat dicapai oleh PT Gagas Energi Indonesia. Keseluruhan *Base Practices* dan *Work*

Products pada Proses DSS05 beserta dokumen/kebijakan yang ada pada PT Gagas Energi Indonesia terdapat pada tabel berikut.

Tabel 4.10 Pemetaan Kebijakan/Dokumen Proses DSS05

Base Practices	Work Product	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
Perlindungan dari ancaman <i>malware</i>	Pencegahan perangkat lunak berbahaya	Ya	Dokumen PO Instalasi dan Monitoring <i>Software</i> pada bagian pencegahan perangkat lunak berbahaya	Lampiran Prosedur Instalasi dan Monitoring <i>Software</i>
	Dokumen evaluasi ancaman potensial keamanan	Tidak	-	-
Pengelolaan Jaringan dan Konektivitas	Dokumen klasifikasi data	Ya	Sudah dilaksanakan namun tidak didokumentasikan	Tidak ditemukan dokumen tertulis
	Dokumen hasil pengujian keamanan	Ya	Log <i>firewall</i> dan antivirus	Dokumen tidak dapat dilampirkan
	Dokumen kebijakan keamanan pada konektivitas	Ya	Dokumen PO Hak Akses pada bagian mekanisme mendapatkan hak akses terhadap data sensitif	Lampiran Prosedur Hak Akses
Mengelola Keamanan pada <i>Endpoint</i>	Dokumen model arsitektur informasi	Ya	Dokumentasi <i>Grand Design ICT</i> Gagas pada bagian <i>ICT Architecture</i>	Lampiran <i>ICT Architecture</i>
	Dokumen perjanjian tingkat	Ya	Dokumen PO Permasalahan IT	Lampiran Permasalahan IT

Tabel 4.10 Pemetaan Kebijakan/Dokumen Proses DSS05 (Lanjutan)

<i>Base Practices</i>	<i>Work Product</i>	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
	layanan (OLA)			
	Dokumen pemeriksaan inventori fisik	Ya	Dokumen Data IT Gagas	Dokumen tidak dapat dilampirkan
	Dokumen hasil dari transaksi	Ya	Dokumen Lisensi <i>Software</i> pada bagian pengadaan perangkat lunak	Lampiran Instalasi dan Monitoring <i>Software</i>
	Dokumen kebijakan keamanan pada perangkat <i>endpoint</i>	Ya	Dokumen PO Instalasi dan Monitoring <i>Software</i> pada prosedur pengamanan <i>software</i>	Lampiran Dokumen Instalasi dan Monitoring <i>Software</i>
Mengelola identitas pengguna dan hak akses	Dokumen hubungan peran dan tanggung jawab TI	Ya	Dokumen PO Pengelolaan Hak Akses	Lampiran Pengelolaan Hak Akses
	Dokumen Persetujuan hak akses pengguna	Ya	Dokumen PO Pengelolaan Hak Akses pada bagian permintaan hak akses	Lampiran Pengelolaan Hak Akses
	Dokumen hasil peninjauan ulang (<i>review</i>) hak akses pengguna	Tidak	-	-
Mengelola aset fisik TI	Dokumen persetujuan permintaan	Ya	Dokumen PO Pengelolaan Hak Akses pada	Lampiran Pengelolaan Hak Akses



Tabel 4.10 Pemetaan Kebijakan/Dokumen Proses DSS05 (Lanjutan)

<i>Base Practices</i>	<i>Work Product</i>	Terpenuhi (Ya/Tidak)	Dokumen / Kebijakan pada Perusahaan	Lampiran
	hak akses		kebijakan permintaan hak akses	
	Dokumen <i>access logs</i> pada sistem	Ya	Dokumen PO Pengelolaan Hak Akses pada bagian terakhir dari prosedur	Lampiran Pengelolaan Hak Akses
Mengelola dokumen penting dan perangkat keluaran (output) lainnya.	Dokumen tentang model arsitektur informasi	Tidak	-	-
	Dokumen tentang wewenang hak akses pada sistem	Tidak	-	-
Memantau infrastruktur untuk setiap kegiatan yang berhubungan dengan keamanan	Dokumen tentang karakteristik risiko keamanan	Tidak	-	-
	Dokumen tentang daftar peristiwa keamanan informasi	Tidak	-	-
	Dokumen tentang risiko keamanan informasi	Tidak	-	-



Berdasarkan penilaian yang telah dilakukan pada *Base Practices* dan *Work Products*, diketahui jika PT Gagas Energi Indonesia telah memenuhi 13 dari 20 *Work Product* atau sebesar 61% dari keseluruhan *Work Product* yang terdapat pada proses DSS05. Dalam hal ini, proses DSS05 yang dijalankan pada level satu termasuk pada kategori *Largely Achieved* (L) karena pada penilaian *Base Practices* dan *Work Product* berada pada nilai lebih dari 50% sampai 85%. Sehingga proses DSS05 telah memenuhi persyaratan penilaian pada level 1 yaitu lebih dari 50% BP/WP telah terpenuhi dan proses dapat diteruskan ke penilaian kapabilitas berikutnya. Hasil penilaian dapat dilihat pada tabel berikut.

Tabel 4.11 Penilaian Level 1 Proses DSS05

<i>Base Practices</i>	<i>Work Product</i> Terpenuhi	<i>Work Product</i> Total	Persentase
DSS05-BP1	1	2	50%
DSS05-BP2	3	3	100%
DSS05-BP3	5	5	100%
DSS05-BP4	2	3	67%
DSS05-BP5	2	2	100%
DSS05-BP6	0	2	0%
DSS05-BP7	0	3	0%
Total	13	20	61%

Langkah berikutnya adalah melakukan penilaian pada level 2 sampai dengan level 5. Pada PA 2.1, terdapat enam kriteria yang harus terpenuhi agar mencapai kriteria *fully achieved*. Dari enam kriteria yang harus dipenuhi pada PA2.1, proses DSS05 telah memenuhi empat dari enam kriteria yang disyaratkan untuk mencapai *fully achievement*. Keempat kriteria tersebut yang pertama adalah identifikasi tujuan dan pelaksanaan proses. Dalam hal ini, dari setiap Prosedur Operasi yang ada telah terdapat tujuan dari dilaksanakannya proses tersebut. Kedua adalah kinerja proses yang telah disesuaikan dengan kebutuhan rencana. Dalam hal ini, pengelolaan proses telah disesuaikan dengan rencana yang diharapkan oleh perusahaan. Ketiga adalah tanggung jawab dan wewenang untuk melakukan proses. Dari setiap dokumen yang ada, terutama dokumen prosedur operasi telah dijelaskan kewenangan dan tanggung jawab terkait hak untuk menjalankan proses tertentu. Keempat adalah mengelola antarmuka dari setiap pihak yang terlibat. Dalam hal ini, keseluruhan dokumen terutama dokumen prosedur operasi telah menggambarkan aktivitas antarmuka dari setiap pihak yang terlibat melalui prosedur komunikasi dan tanggung jawab dari setiap pihak terhadap sebuah proses tertentu. Berdasarkan penjelasan di atas,

proses DSS05 yang dijalankan oleh PT Gagas Energi Indonesia telah mencapai *largely achieved*.

Penilaian berikutnya dilakukan pada PA 2.2 yang memiliki empat kriteria pencapaian untuk mencapai *fully achieved*. Proses DSS05 yang dijalankan oleh PT Gagas Energi Indonesia telah memenuhi tiga dari empat proses yang disyaratkan. Ketiga proses tersebut adalah pendefinisian hasil proses kerja yang disebutkan di setiap Prosedur Operasi yang sesuai dengan proses DSS05. Kedua, adanya permintaan dokumentasi dan pengendalian hasil kerja dalam bentuk pelaporan hasil kerja yang dilakukan di setiap tahapan atau di akhir proses kerja. Ketiga, adanya peninjauan hasil kerja terhadap aturan dan persyaratan yang telah direncanakan sebelumnya. Hal ini dilakukan di akhir proses dari setiap Dokumen Prosedur Operasi terkait DSS05. Karena keseluruhan atribut proses pada penilaian level dua telah mencapai *largely achieved*, maka penilaian dapat dilanjutkan ke level berikutnya atau level 3.

Penilaian berikutnya dilakukan pada level 3 yang memiliki dua atribut penilaian. Atribut pertama adalah PA 3.1 yang memiliki lima kriteria. Pada PA 3.1 ini, proses DSS05 yang dijalankan oleh PT Gagas Energi Indonesia memenuhi tiga dari lima kriteria yang disyaratkan untuk mencapai *fully achievement*. Kriteria pertama yang terpenuhi adalah standar pedoman proses yang menggambarkan elemen-elemen fundamental pada proses. Dalam hal ini, PT Gagas Energi Indonesia telah memiliki prosedur yang dituangkan dalam Dokumen Prosedur Operasi yang memiliki kaitan dengan proses DSS05. Kriteria kedua adalah urutan dan interaksi standar proses dengan proses lainnya yang telah ditentukan dalam bentuk penjabaran secara kalimat dan secara diagram alir (*flowchart*) yang menjelaskan bagaimana alur jika proses dapat terpenuhi dan tidak dapat terpenuhi yang terdapat di setiap Dokumen Prosedur Operasi terkait proses DSS05. Kriteria ketiga yang telah terpenuhi adalah kompetensi dan peran yang diperlukan untuk melakukan proses. Dalam hal ini, dari setiap Dokumen Prosedur Operasi telah mensyaratkan peran dari unit tertentu yang dibutuhkan untuk menjalankan proses.

Selanjutnya adalah penilaian pada PA 3.2 yang memiliki enam kriteria penilaian. Proses DSS05 pada PA 3.2 yang dijalankan oleh PT Gagas Energi Indonesia memenuhi dua dari enam kriteria yang disyaratkan. Kriteria pertama yang dipenuhi adalah terdapat peran dan tanggung jawab yang telah dijelaskan dari setiap Prosedur Operasi yang dijalankan. Peran dan tanggung jawab mengenai siapa saja yang harus menjalankan proses telah dijelaskan secara tertulis di dalam Prosedur Operasi yang dijalankan di PT Gagas Energi Indonesia, khususnya terkait proses DSS05. Kriteria kedua yang telah terpenuhi adalah pelaksanaan proses oleh pihak yang berdasarkan pada kompetensi yang dimiliki. Dalam hal ini, pelaksanaan proses DSS05 yang dijalankan oleh PT Gagas Energi Indonesia dilakukan oleh pihak yang memiliki kompetensi dalam bidang tersebut yaitu pihak Satuan Kerja TI PT Gagas Energi Indonesia. Pada penilaian PA 3.2, proses DSS05 hanya mampu mencapai *partially achieved* (P) sehingga proses

penilaian berhenti pada level 3. Keseluruhan hasil penilaian pada proses DSS05 dapat dilihat pada Tabel 4.10 berikut.

Tabel 4.12 Penilaian Kapabilitas Proses DSS05

Level	Atribut Proses	BP/GP Terpenuhi	BP/GP Target	WP/GWP Terpenuhi	WP/GWP Target	Persentase	Skala
Level 1	PA 1.1	5	7	13	21	61%	L
Level 2	PA 2.1	4	6	7	10	68,33%	L
	PA 2.2	2	4	4	5	75%	L
Level 3	PA 3.1	3	5	4	6	67%	L
	PA 3.2	2	6	3	7	38,09%	P
Level 4	PA 4.1	0	6	0	7	0%	N
	PA 4.2	0	5	0	6	0%	N
Level 5	PA 5.1	0	5	0	5	0%	N
	PA 5.2	0	3	0	3	0%	N

Berdasarkan analisis yang dilakukan berdasarkan *Base Practices (BP)/Generic Practices (GP)* dan *Work Product (WP)/Generic Work Product (GWP)*, diketahui jika proses DSS05 mencapai tingkat kapabilitas pada level 2 (*Managed Process*) dengan pencapaian pada level 2 mencapai *largely achieved* pada kedua atribut dan salah satu atribut pada level 3 (*Established Process*) mencapai level *partially achieved*. Proses penilaian dihentikan pada level 3 karena salah satu atribut dari level tersebut belum mencapai *largely achieved* sebagai syarat untuk menaikkan ke level berikutnya. Tabel 4.11 berikut akan menggambarkan penilaian pada proses DSS05 COBIT 5.

Tabel 4.13 Penilaian Pada Proses 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		
DSS05												
KRITERIA		L	L	L	L	P						
KAPABILITAS				2								
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%)												

Berdasarkan hasil wawancara yang telah dilakukan, *targeted level* pada proses DSS05 berada pada level 3 (*Established Process*). Untuk dapat mencapai level 3, setidaknya pada level 3 harus mencapai *Largely Achieved* pada kedua atribut yang terdapat di dalamnya (ISACA, 2013). Berdasarkan hal tersebut diketahui bahwa kesenjangan antara proses yang telah diraih dan yang ingin dicapai adalah sebesar 1 tingkat seperti yang dijelaskan pada Tabel 4.9 di bawah ini.

Tabel 4.14 Analisis Kesenjangan Proses DSS05

Nama Proses	Level yang Dituju	Level yang Dicapai	Kesenjangan
DSS05	3	2	1



BAB 5 PEMBAHASAN

5.1 *Manage Security* (APO13)

Hasil analisis data menunjukkan jika proses APO13 (*Manage Security*) mencapai level 2 (*Managed Process*). PT Gagas Energi Indonesia memiliki target level pencapaian proses APO13 berada pada level 3 (*Established Process*). Dalam hal ini, PT Gagas Energi Indonesia menginginkan proses APO13 yang dilaksanakan telah terimplementasikan dengan standar proses yang telah didefinisikan dan telah mencapai tujuan utama dari proses tersebut (ISACA, 2013a).

Untuk meningkatkan level yang ingin dicapai pada proses APO13, rekomendasi pertama yang diberikan adalah dengan membuat dokumen tentang studi kasus bisnis (*business case*) terkait keamanan informasi. Dokumen studi kasus mengenai keamanan informasi akan membantu dalam memenuhi salah satu *outcome* dari proses APO 13 yaitu adanya keamanan informasi yang telah dibangun, diterima dan dikomunikasikan ke seluruh perusahaan (ISACA, 2013a). Penerapan keamanan informasi dapat dikomunikasikan dalam bentuk dokumen studi kasus bisnis untuk melindungi informasi penting (Sherizen, 2000). Selain itu, adanya dokumen studi kasus juga berguna untuk mengurangi potensi ketidaktahuan pada *stakeholder* terhadap keamanan informasi dan kebijakannya dalam organisasi (SkyFoundry, 2012). Diharapkan dengan adanya dokumen studi kasus bisnis terkait keamanan informasi, maka kebijakan keamanan informasi pada perusahaan akan lebih mudah untuk dipahami dan diterapkan oleh keseluruhan *stakeholder* PT Gagas Energi Indonesia.

Rekomendasi kedua yang diberikan adalah mendefinisikan kebijakan untuk meningkatkan manajemen keamanan informasi ke dalam bentuk dokumen. Berdasarkan observasi yang telah dilakukan, PT Gagas Energi Indonesia belum memiliki dokumen/kebijakan untuk meningkatkan keamanan informasi pada perusahaan. Dokumen mengenai peningkatan keamanan informasi yang dilakukan oleh PT Gagas Energi Indonesia dibuat dengan mempertimbangkan ruang lingkup risiko keamanan informasi. Untuk dapat meningkatkan sistem manajemen keamanan informasi yang telah diterapkan, perlu adanya pendekatan keamanan berdasarkan standar internasional seperti ISO/IEC 27001:2013 (Hohan, et al., 2015). Langkah yang dapat dilakukan untuk meningkatkan keamanan manajemen keamanan informasi adalah dengan mengidentifikasi potensi keamanan informasi yang dapat ditingkatkan (ISACA, 2013b). Dalam hal ini, peningkatan manajemen keamanan informasi akan dilakukan pada bagian keamanan yang berperan penting dalam perusahaan.

Kemudian rekomendasi ketiga yang diberikan adalah dengan melakukan audit keamanan informasi secara mendetail dan berkala menggunakan standar nasional/internasional yang berlaku. Rekomendasi ini diberikan berdasarkan Dokumen Pedoman Tata kelola Teknologi Informasi PT Gagas Energi Indonesia yang menyebutkan perlunya untuk melakukan *review* dan pengujian secara

berkala terhadap proses pengamanan informasi. Selama ini evaluasi dan audit keamanan informasi yang dilakukan di lingkup PT Gagas Energi Indonesia dilakukan oleh pihak internal dalam bentuk pelaporan dan pengarsipan yang dilakukan setiap bulannya. Namun, berdasarkan hasil observasi dan wawancara belum pernah dilakukan evaluasi dan audit secara mendetail dan menggunakan standar internasional. Berdasarkan hal tersebut maka hal yang harus dilakukan oleh PT Gagas Energi Indonesia adalah mengadakan evaluasi dan audit dalam hal pengelolaan manajemen keamanan informasi secara berkala dengan menggunakan standar internasional yang berlaku seperti ISO/IEC 27001 atau standar lainnya yang sejenis seperti ITIL *Security Management* atau standar lokal seperti Indeks KAMI. Penggunaan standar nasional/internasional yang berlaku bertujuan untuk memberikan kriteria yang tepat terkait aturan, petunjuk atau penjelasan dari karakteristik sebuah proses (NPES, 2005). Dengan menggunakan standar internasional yang berlaku, maka PT Gagas Energi Indonesia dapat mengetahui kriteria yang dibutuhkan untuk mencapai tingkat keamanan informasi serta petunjuk atau prosedur yang harus dijalankan untuk dapat mencapai standar tersebut.

Rekomendasi keempat yang diberikan untuk meningkatkan proses APO13 yang berjalan adalah dengan meningkatkan pengetahuan keamanan informasi pada seluruh satuan kerja. Rekomendasi ini diberikan berdasarkan hasil observasi yang menemukan adanya ketidakpahaman pengguna terhadap keamanan informasi khususnya keamanan data perusahaan sehingga pernah terjadi perpindahan informasi kepada pihak yang tidak berhak atas informasi tersebut. Perpindahan informasi ini terjadi secara internal melalui sistem *fileshare* yang terdapat pada perangkat setiap pekerja. Pengetahuan dari setiap individu memiliki peranan penting terhadap hasil akhir dari keputusan atas kebijakan keamanan informasi (*security policy*) organisasi oleh setiap pegawai (Mishra, et al., 2014). Sehingga pemahaman pengguna terhadap keamanan informasi perlu menjadi tanggung jawab seluruh satuan kerja PT Gagas Energi Indonesia tidak terbatas hanya pada satuan kerja TI. Sedangkan pada satuan kerja TI perlu ditingkatkan pengetahuannya agar dapat melaksanakan pekerjaan spesifik terkait keamanan informasi, terutama pekerjaan yang memerlukan keahlian dan sertifikasi khusus.

Rekomendasi kelima yang diberikan adalah melengkapi Dokumen Pedoman Tata Kelola TI dengan menambahkan infrastruktur dan lingkungan kerja yang dibutuhkan untuk menjalankan proses manajemen keamanan informasi. Sedangkan rekomendasi keenam yang diberikan adalah dengan mendefinisikan kebijakan untuk melakukan pemantauan dan pelaporan proses manajemen keamanan informasi berdasarkan kriteria yang telah ditentukan sebelumnya. Kedua rekomendasi ini diberikan untuk menyempurnakan keempat rekomendasi sebelumnya agar proses APO13 yang dijalankan dapat mencapai level 3 seperti yang diharapkan.

Tabel 5.1 Pemetaan Rekomendasi Proses APO13

No	Rekomendasi	Alasan	Outcome yang dipenuhi
1	Membuat dokumen tertulis tentang studi kasus bisnis terkait Sistem Manajemen Keamanan Informasi.	Dokumen terkait studi kasus SMKI pada perusahaan belum tersedia sehingga dapat menyebabkan kebijakan keamanan informasi yang diterapkan oleh perusahaan tidak dapat dipahami oleh <i>stakeholder</i>	APO13-02 (rencana keamanan informasi yang terkomunikasi dan ditetapkan di perusahaan)
2	Membuat dokumen tertulis tentang rekomendasi untuk meningkatkan Sistem Manajemen Keamanan Informasi.	Dokumen terkait belum tersedia pada perusahaan sehingga belum ada standar keamanan informasi yang secara jelas diterapkan dalam perusahaan dan cara untuk meningkatkan manajemen keamanan informasi	APO13-01 (pertimbangan kebutuhan keamanan informasi) , APO13-03 (implementasi keamanan informasi)
3	Melakukan audit manajemen keamanan informasi secara mendetail menggunakan standar internasional/nasional yang berlaku.	Audit manajemen keamanan informasi telah disebutkan dalam Dokumen Pedoman Tata Kelola TI tetapi belum dijelaskan prosedur detail dan standar yang digunakan untuk melakukan audit. Selain itu, rekomendasi ini diberikan untuk memenuhi pencapaian pada level 2 (<i>Managed Process</i>)	APO13-01 (pertimbangan kebutuhan keamanan informasi)
4	Meningkatkan pengetahuan terkait keamanan informasi.pada seluruh pihak dalam perusahaan.	Adanya pengguna yang belum memahami keamanan informasi sehingga pernah terjadi kebocoran data. Sedangkan pada satuan kerja TI belum ditemukan adanya kebijakan terkait kriteria keahlian yang	APO13-03 (implementasi keamanan informasi)

Tabel 5.1 (lanjutan)

No	Rekomendasi	Alasan	Outcome yang dipenuhi
4		dibutuhkan untuk menjalankan proses terkait keamanan informasi.	
5	Melengkapi Dokumen Tata Kelola TI dengan menambahkan infrastruktur dan lingkungan kerja minimal yang dibutuhkan untuk menjalankan proses manajemen keamanan informasi.	Pada dokumen belum dilengkapi infrastruktur minimal untuk menjalankan proses manajemen keamanan informasi	APO13-02 (rencana keamanan informasi yang terkomunikasi dan ditetapkan di perusahaan)
6	Melengkapi Dokumen Tata Kelola TI dengan menambahkan kebijakan untuk melakukan pemantauan dan pelaporan terkait proses manajemen keamanan informasi yang dijalankan.	Belum adanya kebijakan pemantauan dan pelaporan pada proses manajemen keamanan informasi	APO13-02 (rencana keamanan informasi yang terkomunikasi dan ditetapkan di perusahaan)

5.2 Manage Security Services (DSS05)

Berdasarkan analisis terhadap data yang telah dilakukan, diketahui bahwa proses DSS05 (*Manage Security Services*) berada pada level 2 (*Managed Process*). Sedangkan level pencapaian yang diinginkan oleh PT Gagas Energi Indonesia berada pada level 3 (*Established Process*) atau proses DSS05 yang dilaksanakan telah terimplementasikan dengan standar proses yang telah didefinisikan dan telah mencapai tujuan utama dari proses tersebut (ISACA, 2013a). Hal ini menunjukkan terjadi tingkat kesenjangan sebanyak 1 level berdasarkan analisis kesenjangan yang telah dilakukan. Sementara, dengan tercapainya level 2 pada proses DSS05, menunjukkan jika proses tersebut telah diimplementasikan, terkontrol dan termanajemen dengan baik (ISACA, 2013a).

Rekomendasi yang diperlukan untuk meningkatkan kualitas pada proses DSS05 yang pertama adalah dengan melengkapi dokumen mengenai evaluasi ancaman potensial keamanan informasi. Berdasarkan hasil evaluasi yang

dilakukan, PT Gagas Energi Indonesia belum memiliki dokumen evaluasi pada potensi ancaman keamanan informasi. Dokumen evaluasi ancaman potensial keamanan informasi berisikan daftar potensi ancaman terhadap keamanan informasi yang dapat terjadi pada perusahaan. Pembuatan kebijakan mengenai ancaman potensial bertujuan untuk meminimalisasi ancaman terkait keamanan dengan membuat sedetail mungkin hal-hal yang mungkin menjadi ancaman (Ibrahim dan Koswara, 2010). Dokumen ini diperlukan sebagai bagian dari penanggulangan terhadap risiko keamanan informasi yang mungkin dapat terjadi di lingkungan PT Gagas Energi Indonesia.

Rekomendasi kedua yang diberikan adalah melengkapi Dokumen Prosedur Operasi Pengelolaan Hak Akses dengan menambahkan hasil *review* (peninjauan ulang) terhadap pengguna dan hak aksesnya. Rekomendasi ini diambil berdasarkan penilaian pada level 1 yang menunjukkan belum adanya dokumen *review* terhadap pengguna dan hak aksesnya. Peninjauan ulang terhadap hak akses dilakukan untuk mengetahui kesesuaian hak akses yang diberikan pada pengguna serta untuk mencegah adanya kecurangan dan kesalahan (Xu, 2017). Peninjauan ulang terhadap hak akses dilakukan dengan mempertimbangkan peran pengguna pada perusahaan (Jaferian, et al., 2014). Proses ini perlu dilakukan setiap jangka waktu tertentu untuk memastikan setiap satuan kerja PT Gagas Energi Indonesia memiliki hak akses yang sesuai dengan kebutuhannya.

Rekomendasi ketiga yang diberikan adalah melakukan pengelolaan pada dokumen penting dan perangkat *output* (keluaran) seperti laptop, printer dan sejenisnya. Tujuannya adalah untuk menetapkan perlindungan fisik yang sesuai pada manajemen aset-aset TI yang bersifat sensitif (ISACA, 2013a). Berdasarkan hasil observasi dan penilaian yang dilakukan, pihak PT Gagas Energi Indonesia belum sama sekali menerapkan pengelolaan dokumen dan perangkat keluaran yang bersifat sensitif. Pengelolaan dokumen penting perlu dilakukan untuk mencegah terjadinya kebocoran data dalam dokumen pada pihak yang tidak diinginkan. Pengelolaan dokumen dan perangkat *output* akan membantu menanggulangi kebocoran data yang pernah terjadi sebelumnya dimana data dari departemen satu dapat berpindah tangan ke departemen lain melalui sistem *fileshare* yang tersedia pada perangkat *laptop* perusahaan. Perpindahan pada data tersebut dapat terjadi akibat belum adanya kontrol keamanan pada perangkat keluaran sehingga pengguna dapat melakukan *copy* pada data yang terdapat pada sistem *fileshare* perusahaan. Dalam hal ini diperlukan model arsitektur informasi untuk menghasilkan pemilihan teknologi yang ada, sistem operasi, jaringan, teknologi keamanan serta arsitektur internet yang mendukung aplikasi (Yunis & Surendro, 2009).

Rekomendasi keempat yang diberikan adalah melakukan dokumentasi klasifikasi data. Diketahui berdasarkan hasil observasi pada PT Gagas Energi Indonesia telah dilakukan klasifikasi data yang terdapat dalam sistem atau aplikasi yang ada, tetapi belum dilakukan pendokumentasian dalam bentuk dokumen tertulis. Klasifikasi data dilakukan berdasarkan tingkat sensitivitas, nilai, kekritisitas serta sumber data tersebut. Klasifikasi data yang dilakukan merupakan

sebuah elemen kunci dalam melakukan kebijakan keamanan informasi (Woodbury, 2007). Woodbury (2007) juga menjelaskan tanpa adanya klasifikasi data, maka kebijakan keamanan informasi akan sulit untuk diterapkan pada perusahaan karena tidak adanya kebijakan internal terkait pengaksesan data. Kebijakan pengklasifikasian data juga akan menentukan bagaimana organisasi akan melakukan pengendalian dan perlindungan dari data (Carnegie Mellon University, 2008). Dokumentasi klasifikasi data dalam bentuk tertulis disarankan untuk membantu menjelaskan mekanisme pengamanan data dalam bentuk pengendalian data yang digunakan oleh perusahaan.

Rekomendasi kelima yang diberikan adalah melakukan pemantauan infrastruktur secara detail pada setiap hal yang terkait keamanan informasi. Tidak adanya kegiatan pemantauan infrastruktur TI dapat meningkatkan berbagai kejadian kritis dalam infrastruktur TI yang dapat berpengaruh pada bisnis (Opsview, 2018). Sehingga untuk meningkatkan pengelolaan keamanan informasi khususnya pada aset informasi maka perlu dilakukan pemantauan pada infrastruktur TI. Secara umum, PT Gagas Energi Indonesia telah melakukan pemantauan infrastruktur yang memiliki kaitan dengan keamanan informasi. Pemantauan tersebut dilakukan dengan memantau aktivitas pengguna pada jaringan yang ada, termasuk melakukan pemantau pada CCTV yang ada pada setiap area penting yang dimiliki oleh perusahaan. Namun, dalam melakukan pengelolaan masih belum adanya pendefinisian karakteristik risiko keamanan informasi yang dilakukan untuk mencatat risiko-risiko yang dapat terjadi pada infrastruktur TI. Risiko yang mungkin terjadi dapat berasal dari internal seperti kegagalan jaringan, kerusakan pada *hardware* maupun *software*, kehilangan data, virus atau risiko yang berasal dari eksternal seperti bencana alam (Stoneburner, et.al dalam Megawati et.al, 2014).

Rekomendasi keenam yang diberikan adalah melakukan pengujian keamanan informasi pada sistem informasi yang diimplementasikan. Rekomendasi ini diambil berdasarkan hasil observasi yang menemukan jika pihak PT Gagas Energi Indonesia belum melakukan pengujian keamanan informasi pada sistem informasi yang diimplementasikan. Hal ini menyebabkan belum adanya jaminan keamanan dari sistem yang digunakan di lingkungan PT Gagas Energi Indonesia. Dalam hal ini, pengujian keamanan informasi dilakukan dengan cara *penetration test* serta *vulnerability assessment*. Sedangkan hasil temuan pada perusahaan menunjukkan pengujian keamanan informasi hanya dilakukan sebatas pada *log firewall* dan antivirus perusahaan. Hal tersebut belum dapat dikategorikan sebagai *penetration test* sebab belum adanya simulasi atau percobaan serangan untuk mengetahui celah keamanan pada aplikasi, sistem atau jaringan (Scarfone, et al., 2008). Sedangkan aktivitas *vulnerability assessment* dan *penetration test* merupakan bagian yang tidak terpisahkan sebab beberapa aktivitas *vulnerability assessment* terdapat juga pada *penetration test*. Salah satu contoh dari hal tersebut seperti pada pengujian jaringan, seorang asesor akan melakukan *network vulnerability scan* untuk identifikasi dan analisis target potensial untuk kemudian merencanakan serangan (ISACA, 2017). Sehingga dapat disimpulkan

jika *penetration test* digunakan untuk mengkonfirmasi hasil dari *vulnerability assessment* yang dilakukan (Doshi & Trivedi, 2015).

Tabel 5.2 Pemetaan Rekomendasi Proses DSS05

No	Rekomendasi	Alasan	Outcome yang dipenuhi
1	Membuat dokumen terkait evaluasi terhadap ancaman keamanan informasi.	Belum ditemukan dokumen evaluasi ancaman potensial keamanan informasi pada perusahaan sehingga penanganan risiko terkait keamanan informasi belum dapat dijalankan.	DSS05-01 (keamanan komunikasi memenuhi bisnis), DSS05-02 (keamanan informasi pada <i>endpoint</i>)
2	Melengkapi Dokumen Prosedur Operasi Hak Akses dengan kebijakan untuk <i>review</i> hak akses pengguna terhadap sumber daya informasi.	Mengetahui apakah hak akses yang diberikan pengguna telah sesuai dengan perannya dalam perusahaan yang bertujuan untuk mengurangi adanya penyalahgunaan hak akses dan kesalahan dalam hal pengaksesan data.	DSS05-03 (hak akses pengguna sesuai peranan bisnis)
3	Melakukan pengelolaan pada dokumen penting dan perangkat <i>output</i> atau keluaran seperti laptop, printer dan sebagainya.	Belum ditemukan kegiatan/kebijakan terkait pengelolaan dokumen penting dan perangkat keluaran yang menyebabkan rawan terjadi kebocoran data atau perpindahan data/dokumen penting dari perangkat keluaran yang tersedia.	DSS05-05 (informasi elektronik yang aman)
4	Mendokumentasikan klasifikasi data dalam bentuk dokumen atau panduan untuk membantu proses pengendalian data pada perusahaan.	Klasifikasi data sudah terlaksana tetapi belum didokumentasikan dalam bentuk dokumen tertulis yang dapat menyebabkan proses pengendalian data dalam perusahaan menjadi kurang optimal.	DSS05-01 (keamanan komunikasi memenuhi bisnis)

Tabel 5.2 (lanjutan)

No	Rekomendasi	Alasan	Outcome yang dipenuhi
5	Melakukan pemantauan infrastruktur yang memiliki kaitan dengan keamanan informasi.	Pemantauan infrastruktur telah terlaksana tetapi belum terlalu memperhatikan risiko keamanan yang dapat terjadi pada perusahaan.	DSS05-01 (keamanan komunikasi memenuhi bisnis)
6	Melakukan pengujian keamanan informasi dengan cara <i>penetration test</i> dan <i>vulnerability assessment</i>	Pengujian keamanan informasi hanya didasarkan pada <i>log keamanan</i> bukan berdasarkan <i>penetration test</i> dan <i>vulnerability assessment</i> . Selain itu, pengujian keamanan dilakukan untuk mengetahui kelemahan dari sistem yang diterapkan di lingkungan perusahaan sehingga dapat mengurangi dampak dari serangan keamanan informasi	DSS05-04 (pengukuran untuk melindungi dari akses pihak yang tidak berwenang)

Berdasarkan Tabel 5.2, rekomendasi pertama diberikan untuk memenuhi kriteria *fully achieved* pada level 1 dan memenuhi penilaian level 2 pada PA 2.1 bagian pengawasan pada kinerja proses dan identifikasi sumber informasi yang diperlukan. Rekomendasi kedua diberikan untuk melengkapi dokumen pada penilaian level satu dan memenuhi penilaian level 2 pada PA 2.2 bagian hasil kerja yang ditinjau sesuai dengan rencana dan disesuaikan untuk memenuhi persyaratan. Rekomendasi ketiga diberikan selain untuk melengkapi dokumen yang belum terpenuhi pada level 1, juga dapat digunakan untuk memenuhi penilaian pada level 3 PA 3.1 bagian metode yang relevan untuk memantau kesesuaian dan efektivitas proses. Sedangkan rekomendasi keempat dan kelima diberikan untuk memenuhi penilaian pada level 3 PA 3.1 bagian identifikasi lingkungan dan infrastruktur kerja sebagai bagian dari standar proses serta PA 3.2 pada bagian alokasi sumber daya yang diperlukan untuk menjalankan proses dan pengelolaan infrastruktur dan lingkungan kerja yang dibutuhkan. Selain itu, pada klasifikasi data juga dapat digunakan untuk memenuhi atribut proses PA 3.2

pada bagian pengumpulan dan analisis data untuk memahami dan menunjukkan perilaku proses serta untuk mengevaluasi perbaikan proses secara terus menerus.



BAB 6 PENUTUP

6.1 Kesimpulan

Kesimpulan yang didapatkan dari hasil evaluasi pada tata kelola keamanan informasi menggunakan kerangka kerja COBIT 5 pada APO13 dan DSS05 menunjukkan hasil berikut ini :

1. Berdasarkan hasil penilaian diketahui jika proses APO13 dan DSS05 yang dijalankan oleh PT Gagas Energi Indonesia berada pada level 2 (*Managed Process*) dengan rincian pada level 1 proses mencapai kriteria *Largely Achieved*, kemudian pada level 2 PA 2.1 dan PA 2.2 masing-masing mencapai kriteria *Largely Achieved*, serta pada level 3 PA 3.1 mencapai kriteria *Largely Achieved* dan pada PA 3.2 mencapai kriteria *Partially Achieved*.
2. Pihak PT Gagas Energi Indonesia menginginkan pada masing-masing proses (APO13 dan DSS05) dapat dijalankan pada level 3 (*Established Process*). Sedangkan hasil evaluasi yang dilakukan menunjukkan pada proses APO13 dan DSS05 yang dijalankan berada pada level 2 (*Managed Process*). Hal ini menunjukkan terjadi kesenjangan antara level yang dicapai dan level yang ingin dituju sebesar 1 level.
3. Rekomendasi yang diberikan untuk mencapai level yang diinginkan oleh perusahaan (*targeted level*), maka hal yang harus dilakukan oleh perusahaan adalah sebagai berikut :
 - a. Pada proses APO13, hal yang harus dilakukan yang pertama yaitu dengan mendefinisikan dokumen mengenai studi kasus bisnis terkait keamanan informasi. Berikutnya adalah membuat kebijakan untuk meningkatkan keamanan informasi yang telah diterapkan. Ketiga, melakukan audit keamanan informasi dengan menggunakan standar yang berlaku secara berkala. Keempat yaitu meningkatkan pengetahuan *stakeholder* mengenai manajemen keamanan informasi perusahaan. Rekomendasi kelima melengkapi Dokumen Pedoman Tata Kelola TI dengan infrastruktur dan lingkungan kerja minimal yang dibutuhkan untuk menjalankan proses keamanan informasi. Rekomendasi keenam yaitu dengan menambahkan kebijakan untuk melakukan pemantauan dan pelaporan terkait proses keamanan informasi.
 - b. Pada proses DSS05, hal yang harus dilakukan yaitu melengkapi dokumen mengenai ancaman keamanan informasi. Rekomendasi kedua adalah dengan membuat dokumen *user access review*. Rekomendasi ketiga adalah melakukan pengelolaan pada dokumen penting. Rekomendasi keempat yaitu melakukan

dokumentasi klasifikasi data yang telah dilakukan. Rekomendasi kelima yaitu melakukan pemantauan infrastruktur secara detail pada setiap hal yang terkait keamanan informasi. Rekomendasi keenam yaitu melakukan pengujian keamanan informasi dalam bentuk *penetration test* dan *vulnerability assessment*.

6.2 Saran

Saran yang diberikan oleh peneliti untuk pengembangan penelitian ini lebih lanjut adalah :

1. Penelitian selanjutnya dapat menggunakan proses lain dari COBIT 5 yang memiliki kaitan dengan keamanan informasi seperti EDM03 (*Ensure Risk Optimisation*), APO12 (*Manage Risk*), BAI06 (*Manage Changes*) atau proses lain dalam COBIT 5 yang berkaitan dengan keamanan informasi.

Penelitian ini dapat dikembangkan dengan melakukan penelitian menggunakan kerangka kerja atau standar lain yang berkaitan dengan keamanan informasi seperti ISO/IEC 27001, ITIL (*Information Technology Infrastructure Library*) For *Information Security*, ISO 31000 dan kerangka kerja lainnya serta melakukan integrasi dengan penelitian ini untuk mengetahui hubungan antara masing-masing standar keamanan informasi.

DAFTAR REFERENSI

- Andress, J., 2014. *The Basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd penyunt. Waltham: Syngress.
- Basyarahil, F. A., Astuti, H. M. & Hidayanto, B. C., 2017. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada DPTSI ITS Surabaya. *Jurnal Teknik ITS*, 6(1), pp. 122-128.
- Carnegie Mellon University, 2008. *Guidelines for Data Classification*. [Online] Available at: <https://www.cmu.edu/iso/governance/guidelines/dataclassification.html>
- Choobineh, J., Dhillon, G., Grimaila, M. R. & Rees, J., 2007. Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems*, 20(57).
- Ciptaningrum, D., Nugroho, E. & Adhipta, D., 2015. *Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5*. Yogyakarta, Seminar Nasional Teknologi Informasi dan Komunikasi 2015 (SENTIKA 2015).
- Doshi, J. & Trivedi, B., 2015. Comparison of Vulnerability Assessment and Penetration Testing. *International Journal of Applied Information Systems (IJ AIS)*, 8(6), pp. 51-53.
- Hohan, A. I., Olarub, M. & Pirnea, I. C., 2015. Assessment and continuous improvement of information security based on TQM and business excellence principles.. *Procedia Economics and Finance*, Volume 32, pp. 352-359.
- IBM, 2015. *IBM Managed Security Services*. Somers: IBM Global Services.
- Ibrahim, R. N. & Koswara, H., 2010. Kerangka Kerja Manajemen Keamanan Berdasarkan ISO 27000 Beserta Turunannya Untuk Sistem Pada E-Government. *Jurnal Computech & Bisnis*, 4(1), pp. 7-16.
- Indrajit, R. E., 2016. *Konsep Dasar Tata Kelola Teknologi Informasi*. s.l.:Preinexus.
- ISACA, 2012a. *COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows: ISACA.
- ISACA, 2012b. *COBIT 5 Enabling Process*. Rolling Meadows: ISACA.
- ISACA, 2013a. *Self-assessment Guide : Using COBIT 5*. Rolling Meadows: ISACA.
- ISACA, 2013b. *Transforming Cybersecurity Using COBIT 5*. Rolling Meadows: ISACA.
- ISACA, 2017. *Vulnerability Assessment*, s.l.: ISACA.

- Jaferian, P., Rashtian, H. & Beznosov, K., 2014. *To authorize or not authorize: helping users review access policies in organizations*. Menlo Park, Usenix Association.
- Jogiyanto, H. M., 2011. *Sistem Tata Kelola Teknologi Informasi*. Yogyakarta: Andi Offset.
- Kadir, A., 2014. *Pengenalan Sistem Informasi Edisi Revisi*. 2nd penyunt. Yogyakarta: Penerbit Andi.
- Matin, I. M. M., Arini & Wardhani, L. K., 2017. Analisis Keamanan Informasi Data Center Menggunakan COBIT 5. *Jurnal Teknik Informatika*, 10(2), pp. 119-128.
- Megawati, T. A., Astuti, H. M. & Herdiyanti, A., 2014. *PENGELOLAAN RISIKO ASET TEKNOLOGI INFORMASI PADA PERUSAHAAN PROPERTI PT XYZ, TANGERANG BERDASARKAN KERANGKA KERJA COBIT 4.1*. Surabaya, Seminar Nasional Sistem Informasi Indonesia.
- Mishra, S., Snehlata, S. & Srivastava, A., 2014. Information Security Behavioral Model: Towards Employees' Knowledge and Attitude. *Journal of Telematics and Informatics*, 2(1), pp. 22-28.
- NPES, 2005. *STANDARDS: WHAT ARE THEY AND WHY ARE THEY IMPORTANT?*. [Online] Available at: <http://www.npes.org/pdf/Standards-WhatAreThey.pdf> [Diakses 15 Mei 2019].
- Omari, L. A., 2016. *Adapting and Adopting The COBIT Framework for Public Sector Organisations*. s.l.:s.n.
- Opsview, 2018. *Why Monitoring IT Infrastructure Is So Important*. [Online] Available at: <https://www.opsview.com/resources/infrastructure/blog/why-monitoring-it-infrastructure-so-important> [Diakses 15 Mei 2019].
- Recker, J., 2013. *Scientific Research in Information Systems*. Berlin: s.n.
- Scarfone, K., Souppaya, M., Cody, A. & Orebaugh, A., 2008. *Technical Guide to Information Security Testing and Assessment*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf> [Diakses 20 Mei 2019].
- Sherizen, S., 2000. *The Business Case for Information Security: Selling Management on the Protection of Vital Secrets*. s.l.:Auerbach Publications.
- SkyFoundry, 2012. *The Business Case For Analytics : A White Paper*. s.l.:SkyFoundry.

- Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems*. Gaithersburg: NIST Special Publication 800-30.
- Sugiyono, 2017. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. 25 penyunt. Bandung: Penerbit Alfabeta.
- Suminar, S. & Fitroh, 2016. *Evaluation of Information Technology Governance Using COBIT 5 Framework Focus APO13 and DSS05 in PPIKSN-BATAN*. s.l., International Conference on Cyber and IT Service Management (CITSM).
- Wirawan, 2012. *Evaluasi: Teori, Model, Standar, Aplikasi dan Profesi*. Jakarta: PT. Raja Grafindo Persada.
- Wolden, M., Valverde, R. & Talla, M., 2015. The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. *IFAC-PaperOnLine*, 48(3), pp. 1846-1852.
- Woodbury, C., 2007. The Importance of Data Classification and Ownership. *SkyView Partner Inc*, pp. 1-4.
- Xu, L., 2017. *User Access Review and a UAR Supporting Tool for Improving Manual Access Review Process in Enterprise Environment*. [Online] Available at: <https://pdfs.semanticscholar.org/3cf5/5479a22c396c27265958114aa37be78c89ee.pdf> [Diakses 14 Mei 2019].
- Yunanda, M., 2009. *Evaluasi Pendidikan*. Jakarta: Balai Pustaka.
- Yunis, R. & Surendro, K., 2009. *Perancangan Model Enterprise Architecture Dengan TOGAF Architecture Development Method*. Yogyakarta, Seminar Nasional Aplikasi Teknologi Informasi 2009 (SNATI 2009) .

LAMPIRAN A PEMETAAN RESPONDEN

A.1 Pemetaan Responden APO13

LEMBAR PEMETAAN PERAN BERDASARKAN PERHITUNGAN RACI CHART COBIT 5

APO13 <i>Manage Security</i>				
<p>Responsible (R) adalah pihak yang menjalankan tugas. Dalam hal ini berkaitan dengan orang yang berada pada bagian operasional utama perusahaan untuk memenuhi hasil yang diharapkan</p>				
NO	PERAN	DESKRIPSI	JABATAN DALAM ORGANISASI	KETERANGAN
1	<i>Chief Information Officer</i>	Salah satu petinggi dari sebuah instansi yang bertanggung jawab dalam menangani masalah TI di dalam instansi tersebut	<i>Information and System Development Senior Staff</i>	
2	<i>Head IT Administration</i>	Pihak yang bertanggung jawab untuk meningkatkan proses dan kebijakan, mengelola staf administratif dan memimpin perencanaan jangka panjang TI pada organisasi	-	
3	<i>Information Security Manager</i>	Pihak yang bertanggung jawab dalam penerapan dan pengembangan keamanan TI.	-	
<p>Accountable (A) adalah pihak yang memiliki tanggung jawab dalam hal keberhasilan suatu tugas dan memiliki kewenangan untuk memutuskan suatu perkara</p>				
NO	PERAN	DESKRIPSI	JABATAN DALAM ORGANISASI	KETERANGAN
1.	<i>Chief Information Security Officer</i>	Salah satu petinggi perusahaan yang memiliki tanggung jawab atas keamanan informasi di dalam perusahaan	<i>HR & IT Department Head</i>	

Jakarta,



PT. GAGAS
Jl. Raya



A.2 Pemetaan Responden DSS05

LEMBAR PEMETAAN PERAN BERDASARKAN PERHITUNGAN RACI CHART COBIT 5

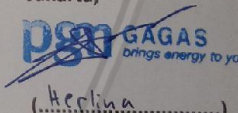
DSS05 Manage Security Services

Responsible (R) adalah pihak yang menjalankan tugas. Dalam hal ini berkaitan dengan orang yang berada pada bagian operasional utama perusahaan untuk memenuhi hasil yang diharapkan

NO	PERAN	DESKRIPSI	JABATAN DALAM ORGANISASI	KETERANGAN
1.	Head IT Operations	Salah satu petinggi dari sebuah instansi yang bertanggung jawab atas operasional dan infrastruktur TI	Infrastructure and Network Senior Staff	
2.	Information Security Manager	Pihak yang bertanggung jawab dalam penerapan dan pengembangan keamanan TI.	-	

Accountable (A) adalah pihak yang memiliki tanggung jawab dalam hal keberhasilan suatu tugas dan memiliki kewenangan untuk memutuskan suatu perkara

NO	PERAN	DESKRIPSI	JABATAN DALAM ORGANISASI	KETERANGAN
1.	Chief Information Security Officer	Salah satu petinggi perusahaan yang memiliki tanggung jawab atas keamanan informasi di dalam perusahaan	HR & IT Department Head	

Jakarta,

 (...Herlina.....)

A.3 Hasil Wawancara

LAMPIRAN TRANSKRIP WAWANCARA

Wawancara : Penggalan informasi terkait permasalahan teknologi informasi pada PT Gagas Energi Indonesia

Narasumber : Moch. Rashid Ridho

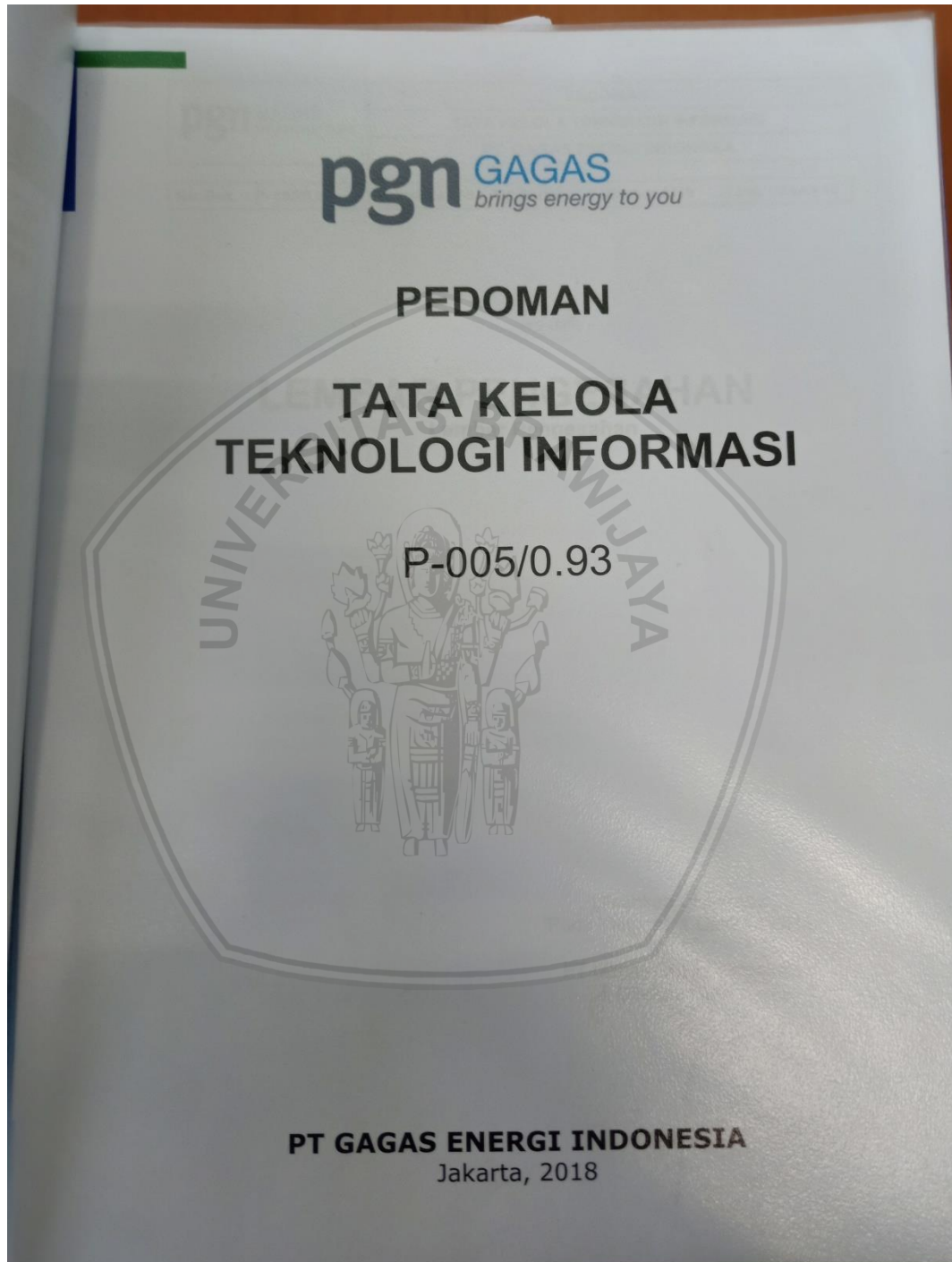
Jabatan : *Information System Development Senior Staff*

Waktu Pelaksanaan : 1 April 2019

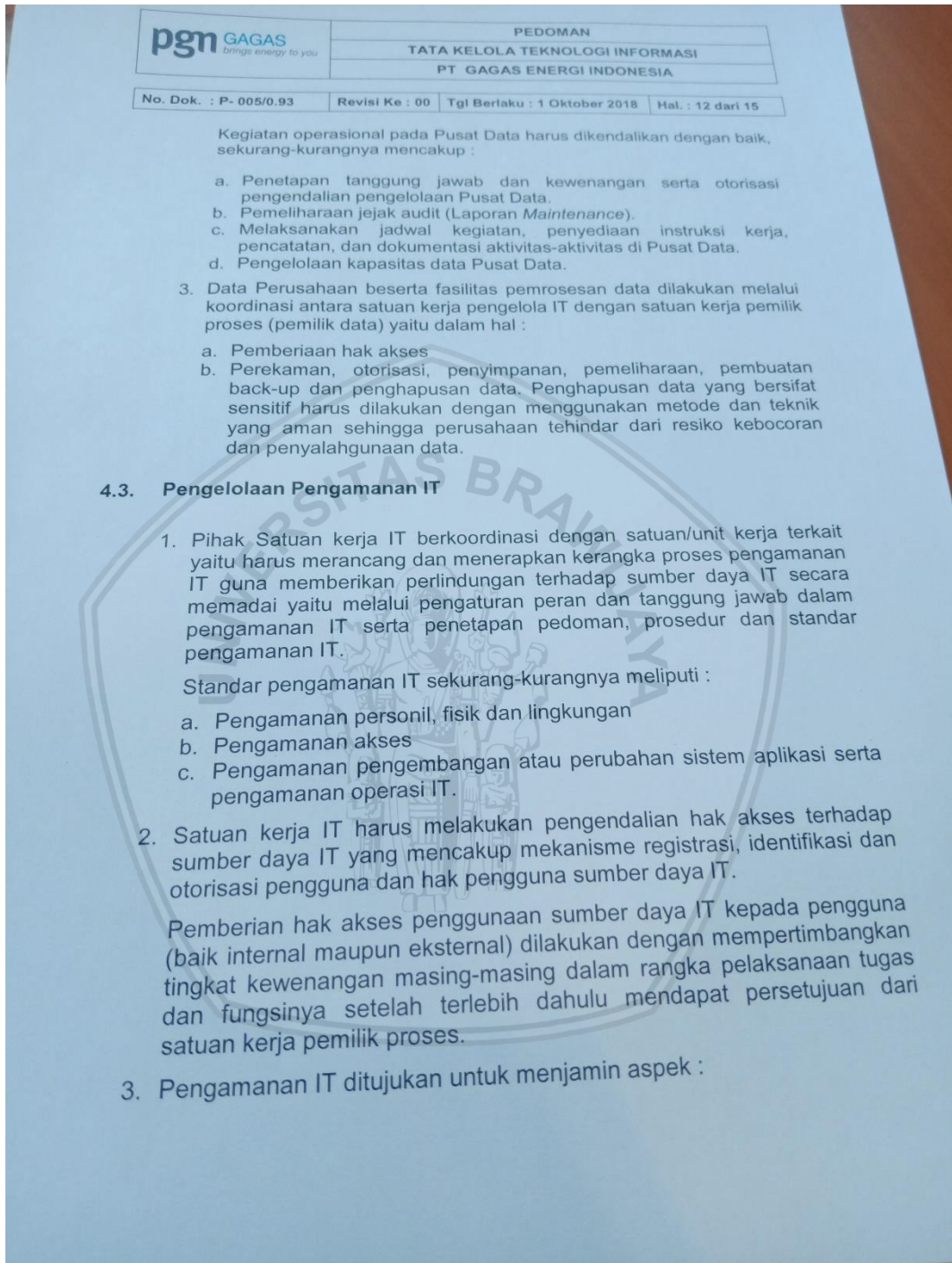
1. P : Bagaimana gambaran pelaksanaan teknologi informasi di PT Gagas Energi Indonesia?
J : Pelaksanaan teknologi informasi di PT Gagas Energi Indonesia dibagi menjadi dua bagian, yaitu bagian pengembangan sistem informasi, dan bagian infrastruktur dan jaringan. Kedua bagian tersebut berada dibawah naungan departemen HR & IT.
2. P : Apakah pernah terjadi masalah yang terkait dengan keamanan informasi
J : Ada, yang pertama adalah pernah terjadi perpindahan data dari departemen satu ke departemen lain melalui *fileshare* dari laptop pegawai. Sehingga data-data dari *fileshare* yang seharusnya hanya diakses oleh pegawai departemen tersebut, datanya bisa diakses oleh pegawai dari luar departemen tersebut. Kedua, ada beberapa kali percobaan serangan pada website utama PT Gagas Energi Indonesia.
3. P : Apakah ada dokumen atau prosedur terkait pengelolaan keamanan informasi pada PT Gagas Energi Indonesia?
J : Ada, dokumen pengelolaan keamanan terdapat pada dokumen Pedoman Tata Kelola dan Dokumen Prosedur Operasi TI PT Gagas Energi Indonesia.
4. P : Seberapa sering PT Gagas Energi Indonesia melakukan evaluasi terhadap keamanan informasi?
J : Untuk evaluasi biasanya dilakukan setiap bulan dalam bentuk laporan, tetapi untuk evaluasi secara lebih mendetail belum pernah dilakukan, terutama evaluasi melalui pihak ketiga dengan menggunakan standar internasional.
5. P : Adakah standar keamanan yang menjadi patokan khusus?
J : Untuk saat ini belum ada tetapi kita berusaha untuk mengacu pada standar internasional yang berlaku.

LAMPIRAN B HASIL OBSERVASI DOKUMEN

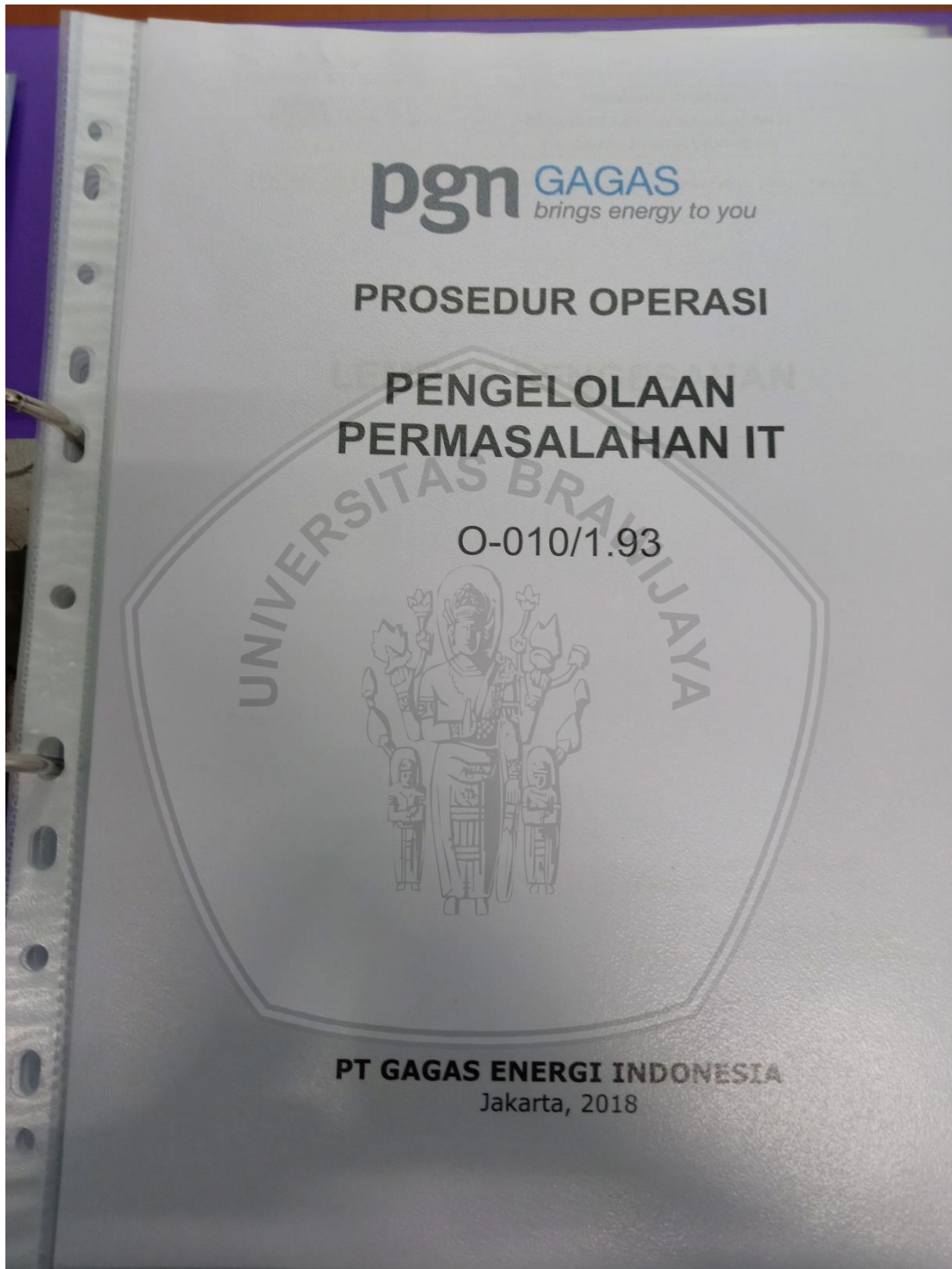
B.1 Dokumen Pedoman Tata Kelola Teknologi Informasi



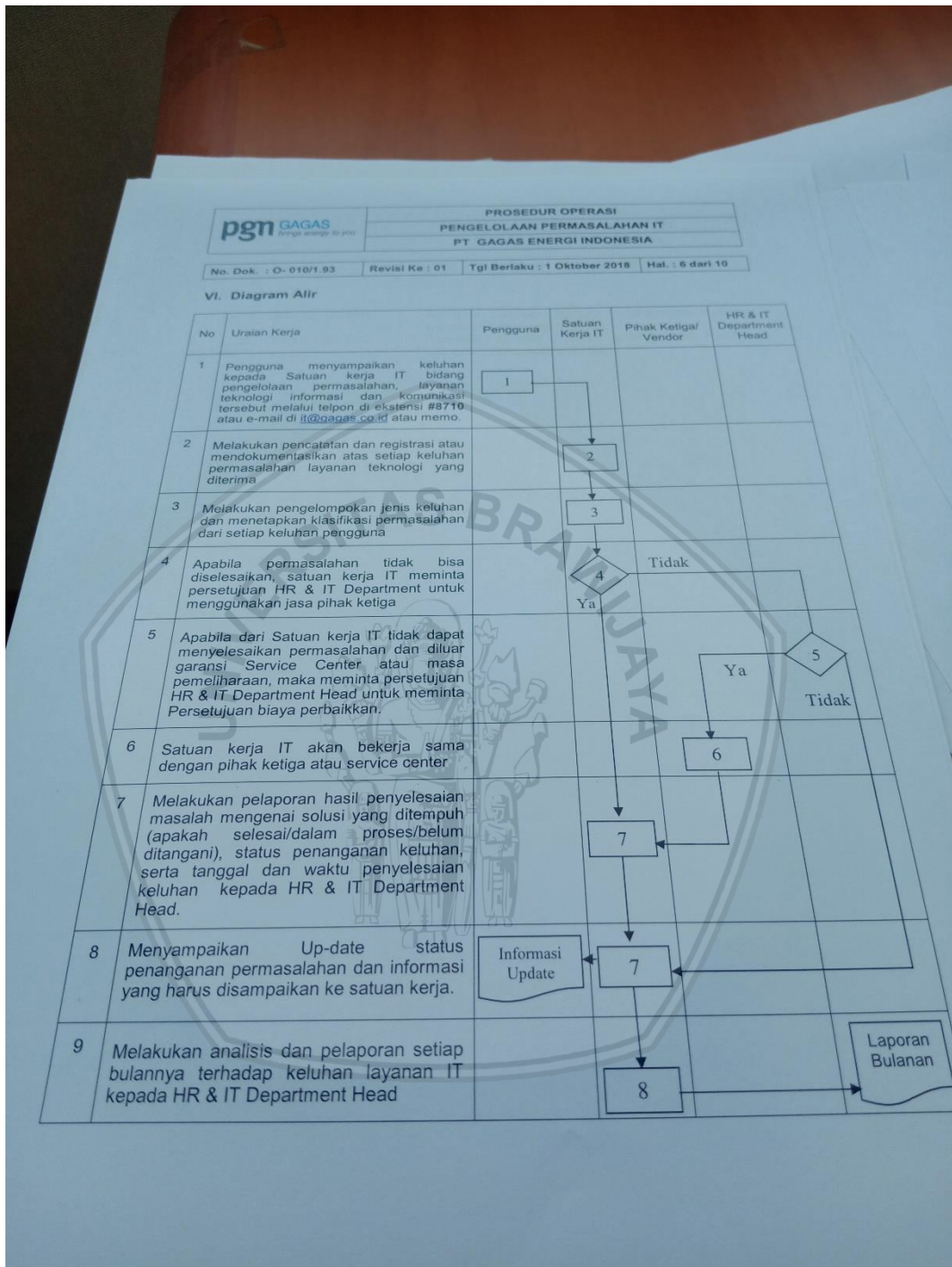
B.2 Prosedur Pengamanan IT



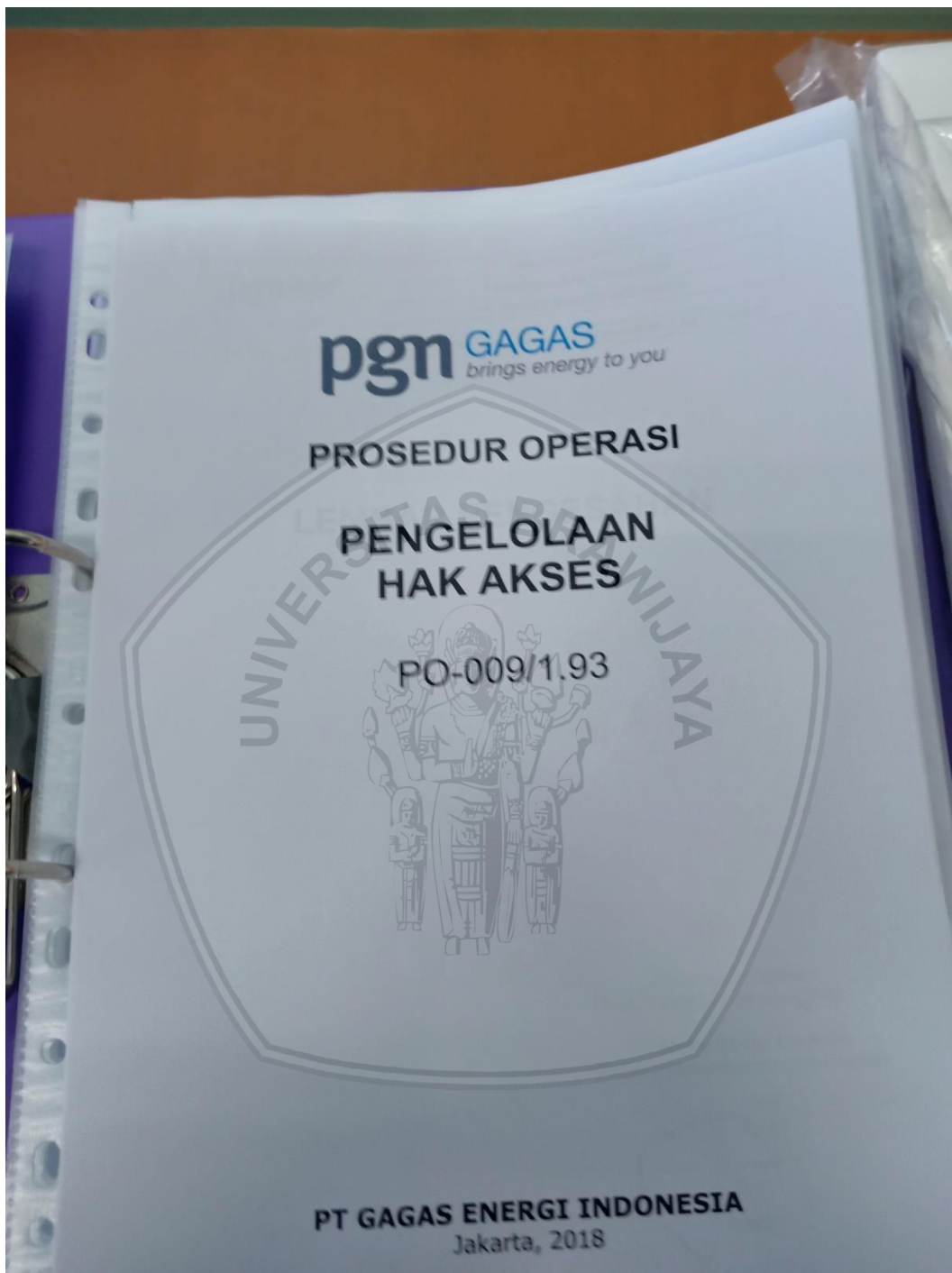
B.3 Tampilan Dokumen Prosedur Operasi Permasalahan IT

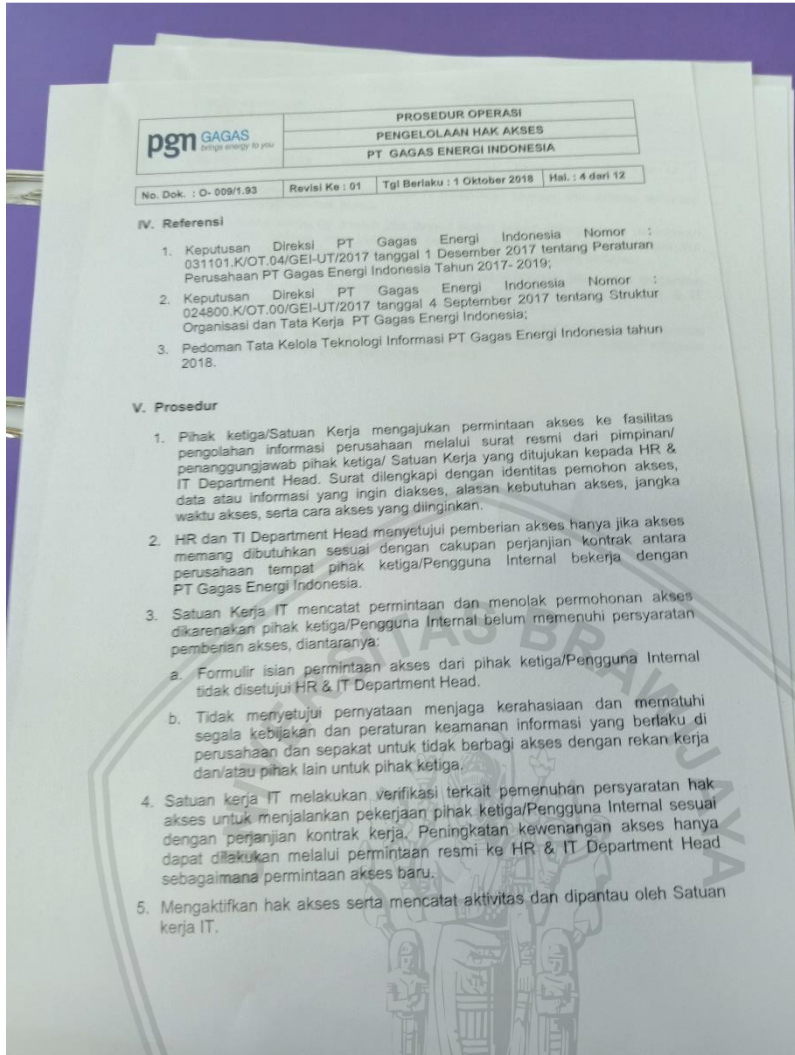


B.4 Tampilan Prosedur Pengelolaan Permasalahan IT



B.5 Tampilan Dokumen Prosedur Pengelolaan Hak Akses





PROSEDUR OPERASI			
PENGELOLAAN HAK AKSES			
PT GAGAS ENERGI INDONESIA			
No. Dok. : O-009/1.93	Revisi Ke : 01	Tgl Berlaku : 1 Oktober 2018	Hal. : 4 dari 12

IV. Referensi

1. Keputusan Direksi PT Gagas Energi Indonesia Nomor : 031101.K/OT.04/GEI-UT/2017 tanggal 1 Desember 2017 tentang Peraturan Perusahaan PT Gagas Energi Indonesia Tahun 2017- 2019;
2. Keputusan Direksi PT Gagas Energi Indonesia Nomor : 024800.K/OT.00/GEI-UT/2017 tanggal 4 September 2017 tentang Struktur Organisasi dan Tata Kerja PT Gagas Energi Indonesia;
3. Pedoman Tata Kelola Teknologi Informasi PT Gagas Energi Indonesia tahun 2018.

V. Prosedur

1. Pihak ketiga/Satuan Kerja mengajukan permintaan akses ke fasilitas pengolahan informasi perusahaan melalui surat resmi dari pimpinan/ penanggungjawab pihak ketiga/ Satuan Kerja yang ditujukan kepada HR & IT Department Head. Surat dilengkapi dengan identitas pemohon akses, data atau informasi yang ingin diakses, alasan kebutuhan akses, jangka waktu akses, serta cara akses yang diinginkan.
2. HR dan TI Department Head menyetujui pemberian akses hanya jika akses memang dibutuhkan sesuai dengan cakupan perjanjian kontrak antara perusahaan tempat pihak ketiga/Pengguna Internal bekerja dengan PT Gagas Energi Indonesia.
3. Satuan Kerja IT mencatat permintaan dan menolak permohonan akses dikarenakan pihak ketiga/Pengguna Internal belum memenuhi persyaratan pemberian akses, diantaranya:
 - a. Formulir isian permintaan akses dari pihak ketiga/Pengguna Internal tidak disetujui HR & IT Department Head.
 - b. Tidak menyetujui pernyataan menjaga kerahasiaan dan mematuhi segala kebijakan dan peraturan keamanan informasi yang berlaku di perusahaan dan sepakat untuk tidak berbagi akses dengan rekan kerja dan/atau pihak lain untuk pihak ketiga.
4. Satuan kerja IT melakukan verifikasi terkait pemenuhan persyaratan hak akses untuk menjalankan pekerjaan pihak ketiga/Pengguna Internal sesuai dengan perjanjian kontrak kerja. Peningkatan kewenangan akses hanya dapat dilakukan melalui permintaan resmi ke HR & IT Department Head sebagaimana permintaan akses baru.
5. Mengaktifkan hak akses serta mencatat aktivitas dan dipantau oleh Satuan kerja IT.



pgn GAGAS
brings energy to you

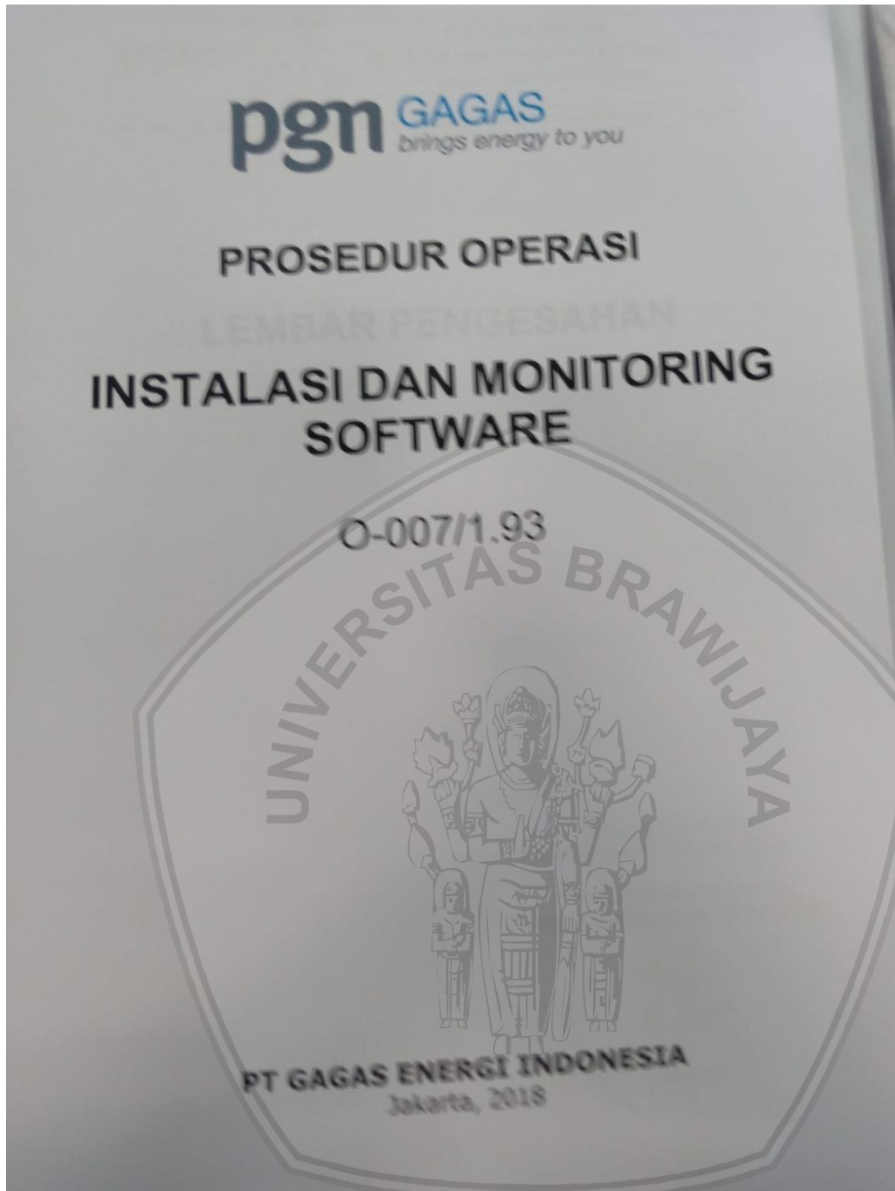
**PROSEDUR OPERASI
PENGELOLAAN HAK AKSES
PT GAGAS ENERGI INDONESIA**

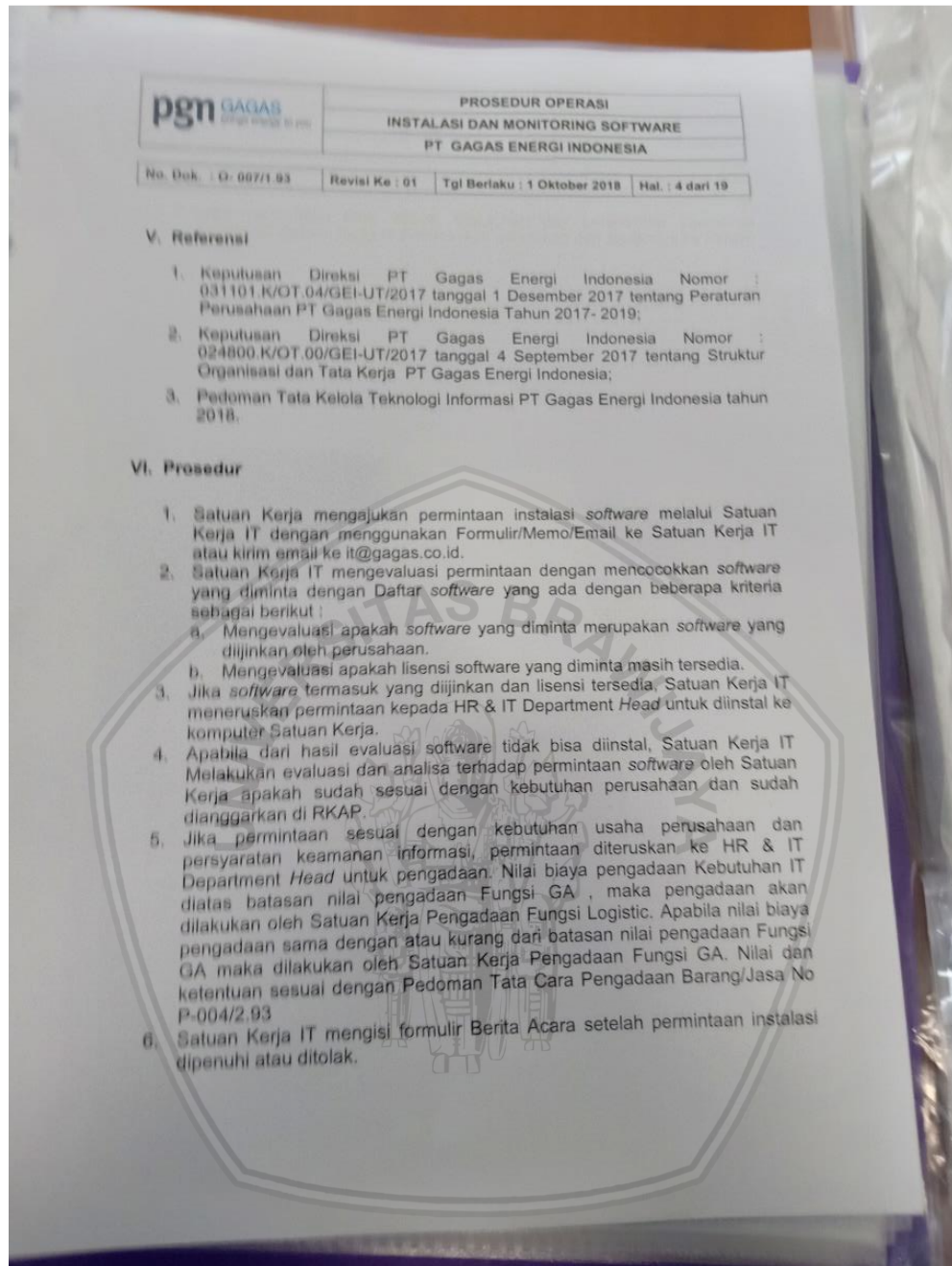
No. Dok. : O- 009/1.93 Revisi Ke : 01 Tgl Berlaku : 1 Oktober 2018 Hal. : 5 dari 12

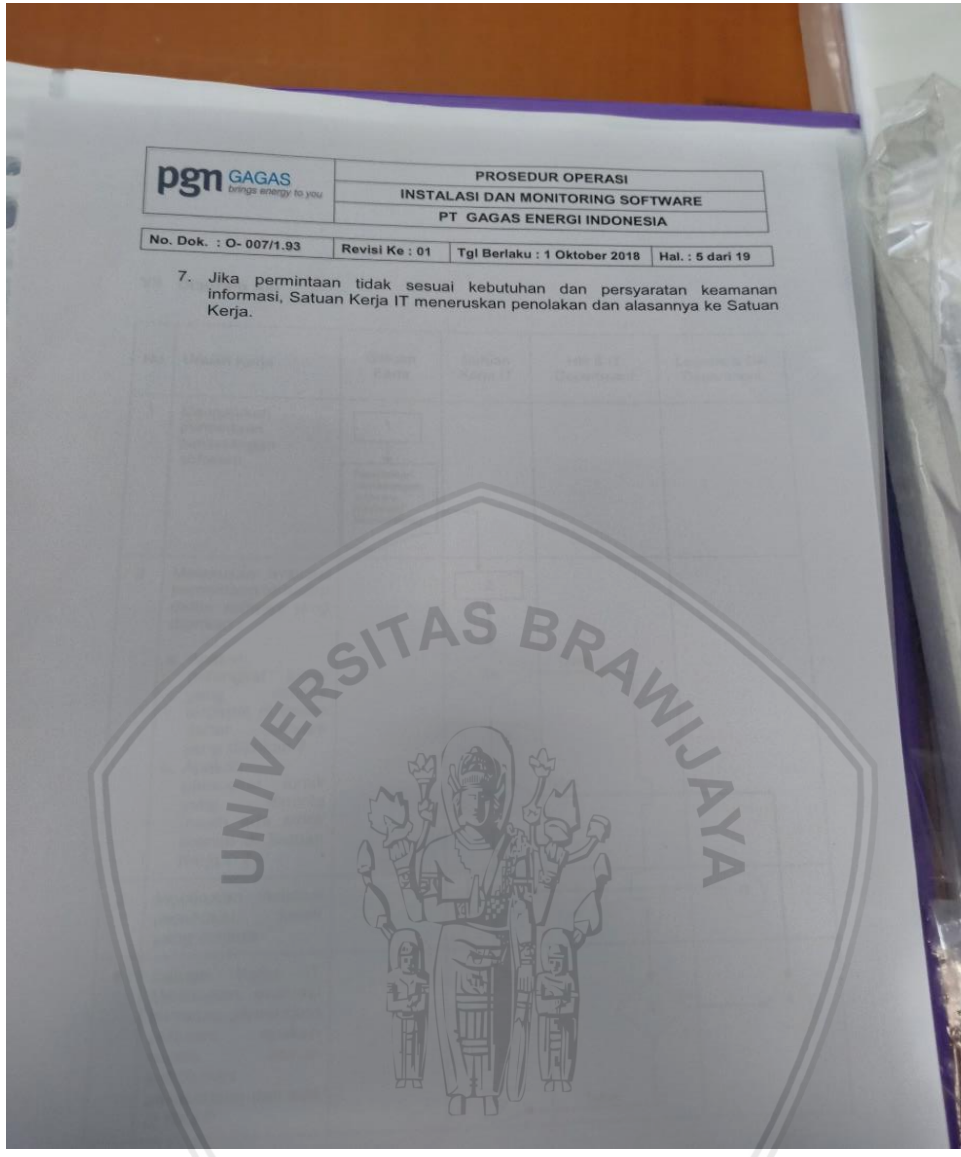
6. Secara berkala Satuan Kerja IT melakukan tinjauan dan analisa terhadap penggunaan hak akses.
7. Akses langsung ditutup jika jangka waktu akses sebagaimana dimintakan telah selesai, atau jika masa perjanjian kontrak telah berakhir, atau jika dicurigai terjadinya pelanggaran terhadap ketentuan yang berlaku.
Perpanjangan jangka waktu akses dapat dilakukan jika masa perjanjian kontrak masih berlangsung dan melalui permintaan resmi ke HR & IT Department Head sebagaimana permintaan akses baru.
8. Penutupan akses harus disertai dengan pengarsipan seluruh aset informasi (dokumen, *files*, *logs*, dll.) yang terkait dengan akses pihak ketiga/Pengguna Internal. Hal ini untuk menjaga jejak audit.



B.6 Tampilan Prosedur Operasi Instalasi Software



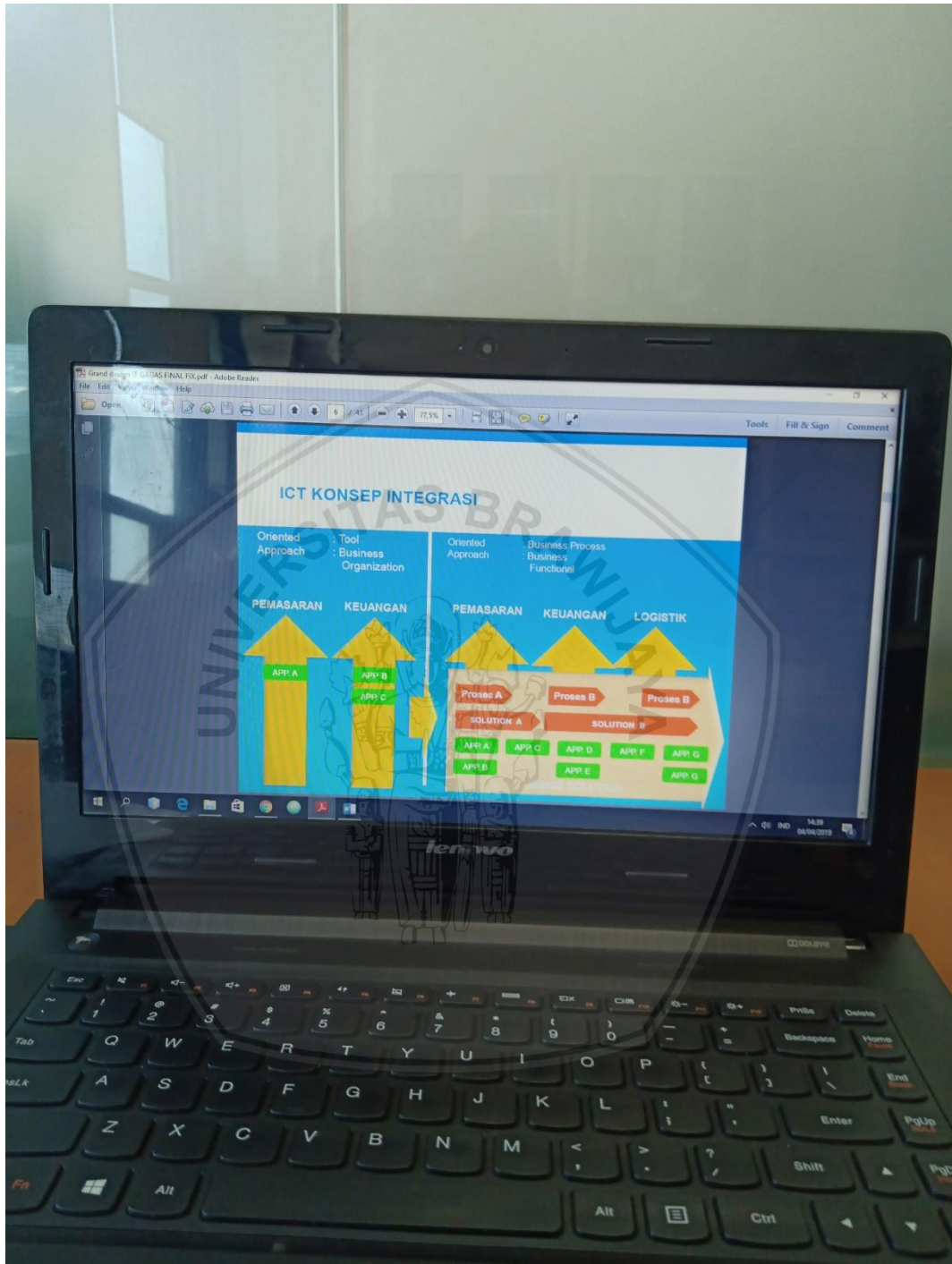




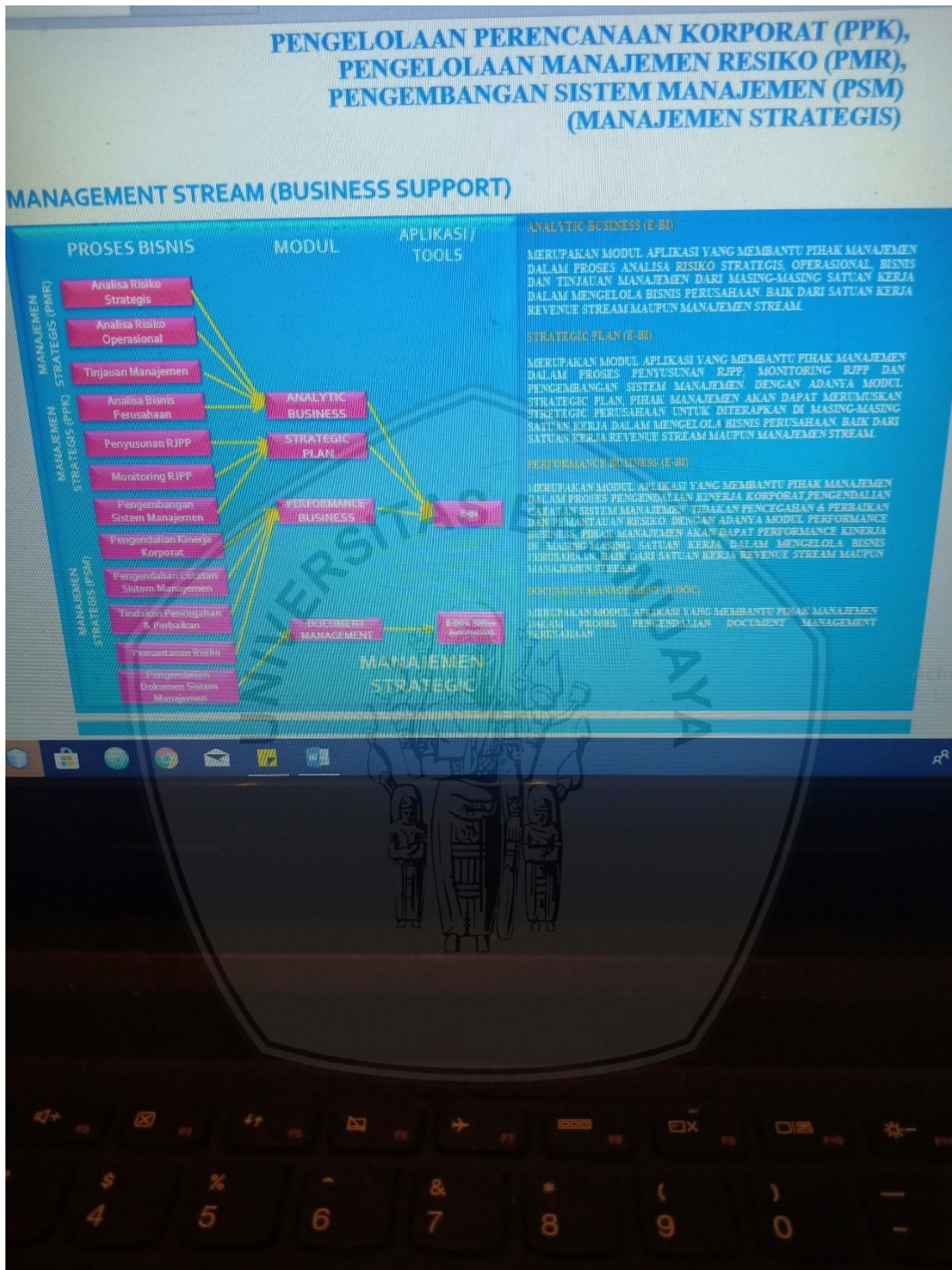
B.7 Tampilan Dokumen Grand Design (Roadmap) IT



B.8 Tampilan Konsep Integrasi ICT



B.9 Tampilan Pengelolaan Manajemen Resiko



LAMPIRAN C HASIL PENILAIAN

C.1 Hasil Penilaian Proses APO13



DATA RESPONDEN SESUAI DENGAN PROSES APO13

Nama Responden	Moch. RASHID RIDHO
Jabatan Responden	Senior Staff IT, Information Development System
APO13	Manage Security
Deskripsi Proses	Mendefinisikan suatu aktivitas pemantauan sistem keamanan informasi
Tujuan	Menjaga dampak dari terjadinya suatu risiko keamanan informasi dalam perusahaan sesuai dengan batas yang telah ditetapkan

KEGIATAN DASAR YANG DILAKUKAN

*Catatan : setiap dokumen yang dimiliki harus disertai keterangan berupa bukti untuk mendukung penelitian

APO13-BP1	STATUS		KETERANGAN
	YA	TIDAK	
Menetapkan dan memelihara Sistem Manajemen Keamanan informasi (SMKI)			
DOKUMEN			
Dokumen tentang pendekatan keamanan informasi perusahaan	✓		Ada didalam pedoman Tata Kelola IT dan Prosedur Operasi
Dokumen kebijakan manajemen keamanan informasi	✓		~ ~
APO13-BP2	STATUS		KETERANGAN
Menentukan dan mengelola rencana penanganan risiko keamanan informasi	YA	TIDAK	
DOKUMEN			
Dokumen tentang kesenjangan dan perubahan yang dibutuhkan untuk mencapai target kapabilitas	✓		Dokumen Rencana Grand Design IT yg termuat di dokumen Pre sentas
Dokumen tentang definisi arsitektur dan domain dasar	✓		~ ~
Dokumen tentang proposal untuk mengurangi risiko keamanan informasi	✓		~ ~



APO13-BP2	Menentukan dan mengelola rencana penanganan risiko keamanan informasi		
Dokumen rencana penanganan risiko keamanan informasi	✓		<i>[Signature]</i>
Dokumen tentang studi kasus dari keamanan informasi		✓	<i>[Signature]</i>

APO13-BP3	Mengawasi dan meninjau ulang (review) Sistem Manajemen Keamanan Informasi (SMKI)		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen tentang klasifikasi dan prioritas insiden perubahan layanan	✓		Ada didalam Prosedur Operasi IT
Dokumen kebijakan manajemen keamanan informasi	✓		<i>[Signature]</i>
Dokumen tentang audit manajemen keamanan informasi	✓		<i>[Signature]</i>
Dokumen tentang rekomendasi untuk meningkatkan manajemen keamanan informasi		✓	<i>[Signature]</i>

Jakarta,
 Nama Responden

[Signature]

 (Moch. Rashid Ridho)



LEMBAR PENILAIAN PADA PROSES APO13

NAMA RESPONDEN	MOCH. RASHID RIDHO
JABATAN RESPONDEN	Information and System Development, Senior Staff

APO13	Manage Security
Deskripsi Proses	Mendefinisikan aktivitas dan pemantauan pada manajemen sistem keamanan informasi
Tujuan	Menjaga dampak dari terjadinya risiko keamanan sistem informasi sesuai dengan batas yang ditetapkan perusahaan

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Ket
Level 0 Incomplete	Perusahaan tidak mengetahui atau hanya sedikit mengetahui proses teknologi informasi di perusahaannya							
Level 1 Performed	PA 1.1 (Process Performance) Proses tata kelola keamanan informasi telah	<ul style="list-style-type: none"> APO13.01 (Menetapkan dan memelihara Sistem Manajemen Keamanan Informasi). 	Y			L		- Men dari G dahun disya pada check



APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
	mencapai tujuan	<ul style="list-style-type: none"> • APO13.02 (Menentukan dan mengelola rencana penanganan risiko keamanan informasi). • APO13.03 (Mengawasi dan meninjau ulang (review) Sistem Manajemen Keamanan Informasi (SMKI)). 	Y Y				
Level 2 Managed Process	PA 2.1 (Performance Management) Mengukur sejauh mana proses keamanan informasi dikelola	<ul style="list-style-type: none"> a. Identifikasi tujuan pelaksanaan proses. b. Kinerja proses direncanakan dan diawasi. c. Kinerja proses disesuaikan untuk memenuhi rencana. d. Tanggung jawab dan wewenang 	Y Y Y			L	

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
		<p>untuk melakukan proses.</p> <p>e. Sumber dan informasi yang diperlukan untuk melakukan proses telah diidentifikasi, tersedia dan digunakan.</p> <p>f. Antarmuka pihak-pihak yang terlibat berhasil diwujudkan melalui komunikasi yang efektif dan tanggung jawab jelas .</p>	<p>T</p> <p>Y</p>			L	
	PA 2.2 <i>Work Product Management</i> – Sejauh mana hasil kinerja tata kelola keamanan	<p>a. Persyaratan hasil proses kerja didefinisikan.</p> <p>b. Permintaan untuk dokumentasi dan pengendalian</p>	<p>Y</p> <p>Y</p>				

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Ke
	informasi dapat dicapai dengan baik	<p>hasil kerja telah didefinisikan.</p> <p>c. Hasil kerja telah diidentifikasi, didokumentasi dan dikendalikan dengan tepat.</p> <p>d. Hasil kerja ditinjau sesuai dengan pengaturan yang direncanakan dan disesuaikan untuk memenuhi persyaratan .</p>	<p>Y</p> <p>Y</p>					<p>- Pe</p> <p>unt</p> <p>hai</p> <p>ter</p> <p>Dok</p> <p>Ope</p> <p>- P</p> <p>pro</p> <p>has</p> <p>debe</p> <p>pal</p> <p>ope</p>
Level 3 Established Process	PA 3.1 Process Definition – mengukur sejauh mana standar proses manajemen keamanan informasi	a. Standar proses, meliputi pedoman yang tepat yang menggambarkan elemen-elemen fundamental yang harus	Y					<p>-</p> <p>Ste</p> <p>dan</p> <p>pro</p> <p>dan</p> <p>pad</p> <p>Tat</p>

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
		e. Metode yang relevan telah ditentukan untuk memantau efektivitas dan kesesuaian proses.	T				
	PA 3.2 <i>Process Deployment</i> – Mengukur sejauh mana standar proses telah ditetapkan secara efektif sebagai proses yang ditetapkan untuk mencapai hasil prosesnya	<p>a. Proses yang telah didefinisikan berjalan berdasarkan standar proses yang dipilih dan/atau disesuaikan.</p> <p>b. Peran, tanggung jawab dan wewenang yang diperlukan untuk melakukan proses yang telah didefinisikan dan dikomunikasikan</p> <p>c. Pihak yang melaksanakan</p>	T				

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
		<p>proses didefinisikan berdasarkan kompetensi, pendidikan, pelatihan dan pengalaman.</p> <p>d. Sumber daya dan informasi yang diperlukan untuk melakukan proses harus tersedia, teralokasikan dan digunakan dengan baik.</p> <p>e. Infrastruktur dan lingkungan kerja yang dibutuhkan untuk melakukan proses harus tersedia, dikelola dan dievaluasi.</p> <p>f. Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk</p>	<p>Y</p> <p>T</p> <p>T</p>				



APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
		memahami perilaku proses, menunjukkan kesesuaian dan efektivitasnya serta untuk mengevaluasi perbaikan proses dapat dilakukan secara terus menerus					
Level 4 Predictable Process	PA 4.1 Process Measurement – mengukur sejauh mana hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung pencapaian tujuan kinerja proses yang relevan dengan	<ul style="list-style-type: none"> a. Kebutuhan dari proses mendukung tujuan bisnis yang telah ditetapkan b. Tujuan dari penilaian berasal dari kebutuhan proses informasi c. Tujuan kuantitatif dari proses kinerja untuk mendukung tujuan bisnis 	T				



APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
	tujuan bisnis yang ditetapkan.	<p>yang telah ditetapkan</p> <p>d. Frekuensi penilaian diidentifikasi dan didefinisikan sesuai dengan tujuan penelitian kuantitatif untuk proses kinerja</p> <p>e. Hasil penelitian dikumpulkan, dianalisis dan dilaporkan untuk mengawasi sejauh mana tujuan kuantitatif dari proses kinerja dapat terpenuhi</p> <p>f. Hasil penilaian digunakan untuk karakterisasi proses kinerja</p>	<p>T</p> <p>T</p> <p>T</p>				
	PA 4.2 Process Control –	a. Teknik analisis dan	T				

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
	Mengukur sejauh mana proses secara kuantitatif dikelola untuk menghasilkan proses yang stabil, mampu dan dapat diprediksi dalam batas yang ditentukan.	<p>pengendalian ditentukan dan diterapkan apabila.</p> <p>memungkinkan</p> <p>b. Batas variasi kontrol ditetapkan untuk proses kinerja normal.</p> <p>c. Data penilaian dianalisis untuk variasi penyebab khusus masalah.</p> <p>d. Tindakan korektif diambil untuk mengatasi penyebab khusus masalah.</p> <p>e. Batas control ditetapkan kembali jika perlu mengikuti tindakan korektif.</p>	<p>T</p> <p>T</p> <p>T</p> <p>F</p>				



APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
Level 5 <i>Optimising Process</i>	PA 5.1 <i>Process Innovation – Mengukur sejauh mana perubahan pada proses diidentifikasi dari analisis variasi penyebab umum masalah dalam kinerja dan dari investigasi pendekatan inovatif terhadap definisi dan penerapan proses.</i>	<p>a. Tujuan perbaikan proses didefinisikan dan mendukung tujuan bisnis yang relev</p> <p>b. Data yang tepat dianalisis untuk mengidentifikasi variasi penyebab umum dari masalah dalam proses kinerja</p> <p>c. Data yang tepat dianalisis untuk mengidentifikasi peluang praktik dan inovasi terbaik</p> <p>d. Peluang perbaikan yang berasal dari teknologi baru dan konsep proses yang telah diidentifikasi</p>	<p>T</p> <p>T</p> <p>T</p> <p>T</p>				


APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
		e. Strategi implementasi ditetapkan untuk mencapai tujuan perbaikan proses	T				
	PA 5.2 <i>Process Optimization</i> – Mengukur sejauh mana perubahan pada definisi, manajemen, dan kinerja proses menghasilkan dampak efektif yang mencapai tujuan dari perbaikan proses.	<p>a. Dampak dari semua perubahan yang diusulkan dinilai berdasarkan tujuan proses dan standar proses yang ditetapkan.</p> <p>b. Pelaksanaan semua perubahan yang telah disepakati, dikelola untuk memastikan bahwa gangguan terhadap proses kinerja dipahami dan ditindaklanjuti.</p>	T				

APO13	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Ac (>1)
		c. Berdasarkan kinerja aktual, efektivitas perubahan proses dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk menemukan apakah hasil tersebut disebabkan oleh penyebab umum atau khusus.	T				

Jakarta,

Responden 1

(Herluna)



ngn GAGAS
brings energy to you

(Moch)

C.2 Hasil Penilaian Proses DSS05

DATA RESPONDEN SESUAI DENGAN PROSES DSS05

Nama Responden	Andika Agustafin
Jabatan Responden	Network & Infrastructure

DSS05	Manage Security Services
Deskripsi Proses	Perlindungan aset informasi untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh organisasi sesuai kebijakan keamanan
Tujuan	Meminimalkan dampak risiko pada bisnis dari aktivitas keamanan informasi

KEGIATAN DASAR YANG DILAKUKAN

*Catatan : setiap dokumen yang dimiliki harus disertai keterangan berupa bukti untuk mendukung penelitian

DSS05-BP1	Perlindungan dari ancaman virus dan malware		KETERANGAN
	STATUS		
	YA	TIDAK	
Dokumen pencegahan perangkat lunak yang berbahaya	<input checked="" type="checkbox"/>	<input type="checkbox"/>	PO, Instalasi dan monitoring Software
Dokumen tentang evaluasi dari ancaman potensial keamanan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

DSS05-BP2	Pengelolaan jaringan dan konektivitas		KETERANGAN
	STATUS		
	YA	TIDAK	
Dokumen tentang klasifikasi data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sudah dilakukan & belum di dokumentasikan
Dokumen hasil pengujian keamanan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Log - Firewall & Antivirus
Dokumen kebijakan keamanan pada konektivitas	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PO, Hubs Access

DSS05-BP3	Mengelola keamanan pada titik akhir (<i>endpoint</i>)		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen tentang model arsitektur informasi	✓		Dokumentasi Grand Design ICT Gagas
Dokumen perjanjian tingkat operasional (OLA) yang mendukung perjanjian tingkat layanan	✓	✓	P.O. Pengelolaan permasalahan IT
Dokumen pemeriksaan inventori fisik	✓		Dokumen Data IT Gagas
Dokumen hasil dari transaksi	✓	✓	Dokumen lisensi software
Dokumen kebijakan keamanan pada perangkat <i>endpoint</i> seperti laptop, komputer, <i>server</i> dan perangkat lainnya	✓	✓	P.O. Instalasi & Monitoring Software

DSS05-BP4	Mengelola identitas pengguna dan hak akses		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen tentang hubungan antara peran dan tanggung jawab TI	✓		P.O. Pengelolaan Hak Akses
Dokumen persetujuan hak akses pengguna	✓		P.O. Pengelolaan Hak Akses
Dokumen hasil peninjauan ulang (<i>review</i>) pengguna dan hak aksesnya		✓	

DSS05-BP5	Pengelolaan pada aset fisik TI.		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen persetujuan permintaan hak akses	✓		P.O. Pengelolaan Hak Akses
Dokumen access logs pada sistem	✓		P.O. Pengelolaan Hak Akses

DSS05-BP6	Mengelola dokumen penting dan perangkat keluaran (output) lainnya.		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen tentang model arsitektur informasi		✓	
Dokumen tentang wewenang hak akses pada sistem		✓	

DSS05-BP7	Memantau infrastruktur untuk setiap kegiatan yang berhubungan dengan keamanan		
DOKUMEN	STATUS		KETERANGAN
	YA	TIDAK	
Dokumen tentang karakteristik risiko keamanan		✓	
Dokumen tentang daftar peristiwa keamanan informasi		✓	
Dokumen tentang risiko keamanan informasi		✓	

Jakarta, 4 April 2013

Nama Responden

pgn **PAGAS**
bring energy to you

(.....Andika Agustina.....)

LEMBAR PENILAIAN PADA PROSES DSS05

NAMA RESPONDEN	Andika AGUSTAFIA
JABATAN RESPONDEN	Infrastructure and Network Senior Staff

DSS05	<i>Manage Security Services</i>
Deskripsi Proses	Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Proses ini juga menetapkan peran dari keamanan informasi, pengelolaan wewenang hak akses, dan memantau keamanan.
Tujuan	Meminimalkan dampak bisnis dari tingkat kerentanan dan insiden dari proses operasional keamanan TI

s

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
Level 0 Incomplete	Perusahaan tidak mengetahui atau hanya sedikit mengetahui proses teknologi informasi di perusahaannya							
Level 1 Performed	PA 1.1 (Process Performance) Proses tata kelola keamanan informasi telah	<ul style="list-style-type: none"> DSS05.01 (Perlindungan terhadap risiko virus komputer). 	Y			L		Persepsi pada dokumen perusahaan Perangkat Lunak berbahaya

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
	mencapai tujuan	<ul style="list-style-type: none"> DSS05.02 Mengelola keamanan dari konektivitas dan jaringan DSS05.03 Mengelola keamanan keamanan endpoint DSS05.04 Mengelola identitas pengguna dan hak akses DSS05.05 (Mengelola akses fisik ke aset TI) DSS05.06 (Mengelola dokumen penting dan bentuk output yang lain) DSS05.07 (Memantau infrastruktur 	<p>Y</p> <p>Y</p> <p>Y</p> <p>Y</p> <p>T</p> <p>T</p>					<p>2. Keseluruhan dokumen telah terpenuhi</p> <p>3. Keseluruhan dokumen telah terpenuhi</p> <p>4. Telah terdapat pengelolaan identitas pengguna dan hak akses pada dokumen Po Hak Akses</p> <p>5. Akses Fisik ke aset TI diatur pada Po Hak Akses</p>

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		yang berhubungan dengan keamanan)						
Level 2 Managed Process	PA 2.1 (Performance Management) Mengukur sejauh mana proses keamanan informasi dikelola	a. Identifikasi tujuan pelaksanaan proses. b. Kinerja proses direncanakan dan diawasi. c. Kinerja proses disesuaikan untuk memenuhi rencana. d. Tanggung jawab dan wewenang untuk melakukan proses. e. Sumber dan informasi yang diperlukan untuk melakukan proses telah diidentifikasi, tersedia dan digunakan.	Y T Y Y T			L		- Terdapat tujuan pelaksanaan proses di dokumen Tata kelola serta prosedur operasi - Kinerja proses telah disesuaikan dengan tujuan pelaksanaan proses yang terdapat pada Dokumen Prosedur operasi serta memuat telah memuat alur alternatif proses. - Tanggung jawab secara umum telah dikelola dijelaskan dalam Dokumen P.O.

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		f. Antarmuka pihak-pihak yang terlibat berhasil diwujudkan melalui komunikasi yang efektif dan tanggung jawab jelas .	Y					- Pihak yang terlibat dalam proses disebutkan sangat jelas pada Dokumen Prosedur Operasi
	PA 2.2 Work Product Management – Sejauh mana hasil kinerja tata kelola keamanan informasi dapat dicapai dengan baik	<p>a. Persyaratan hasil proses kerja didefinisikan.</p> <p>b. Permintaan untuk dokumentasi dan pengendalian hasil kerja telah didefinisikan.</p> <p>c. Hasil kerja telah diidentifikasi, didokumentasi dan dikendalikan dengan tepat.</p> <p>d. Hasil kerja ditinjau sesuai dengan</p>	<p>Y</p> <p>Y</p> <p>Y</p> <p>T</p>			L		<p>- Persyaratan hasil kerja telah disebutkan pada dokumen P-a</p> <p>- Hasil kerja telah</p> <p>- Adanya dokumentasi hasil kerja pada setiap dokumen Prosedur Operasi</p>

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		pengaturan yang direncanakan dan disesuaikan untuk memenuhi persyaratan .						
Level 3 Established Process	PA 3.1 Process Definition – mengukur sejauh mana standar proses manajemen keamanan informasi dikelola untuk mendukung proses yang telah ditentukan	<p>a. Standar proses, meliputi pedoman yang tepat yang menggambarkan elemen-elemen fundamental yang harus dimasukkan ke dalam proses.</p> <p>b. Urutan dan interaksi dari standar proses dengan proses lainnya telah ditentukan.</p> <p>c. Kompetensi dan peran yang diperlukan untuk melakukan proses telah diidentifikasi</p>	Y			L		<p>- Terdapat standar proses yang terdapat pada Dokumen Prosedur Operasi TI</p> <p>- Alur pelaksanaan proses terdapat jelas dalam bentuk tulisan dan diagram alir pada Prosedur Operasi</p> <p>- Peran yang diperlukan untuk menjalankan proses dijelaskan pada Dokumen Prosedur Operasi ..</p>

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		<p>sebagai bagian dari standar proses.</p> <p>d. Infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan suatu proses diidentifikasi sebagai bagian dari standar proses.</p> <p>e. Metode yang relevan telah ditentukan untuk memantau efektivitas dan kesesuaian proses.</p>	T					
	PA 3.2 <i>Process Deployment</i> – Mengukur sejauh mana standar proses telah ditetapkan secara efektif sebagai proses	a. Proses yang telah didefinisikan berjalan berdasarkan standar proses yang dipilih	T		P			

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
	yang ditetapkan untuk mencapai hasil prosesnya	<p>dan/atau disesuaikan.</p> <p>b. Peran, tanggung jawab dan wewenang yang diperlukan untuk melakukan proses yang telah didefinisikan dan dikomunikasikan</p> <p>c. Pihak yang melaksanakan proses didefinisikan berdasarkan kompetensi, pendidikan, pelatihan dan pengalaman.</p> <p>d. Sumber daya dan informasi yang diperlukan untuk melakukan proses harus tersedia, teralokasikan</p>	<p>Y</p> <p>Y</p> <p>Y</p>		P			<p>- Peran dan tanggung jawab untuk menjalankan proses di sebutkan pada Dokumen Prosedur Operasi</p> <p>- Pihak yang melaksanakan proses didasarkan pada satuan kerja terkait proses tersebut yang dijelaskan pada Dokumen Prosedur Operasi</p>

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		<p>dan digunakan dengan baik.</p> <p>e. Infrastruktur dan lingkungan kerja yang dibutuhkan untuk melakukan proses harus tersedia, dikelola dan dievaluasi.</p> <p>f. Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami perilaku proses, menunjukkan kesesuaian dan efektivitasnya serta untuk mengevaluasi perbaikan proses dapat dilakukan secara terus menerus</p>	<p>T</p> <p>T</p>					
Level 4 Predictable Process	PA 4.1 Process Measurement – mengukur	a. Kebutuhan dari proses mendukung	T					

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
	sejauh mana hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung pencapaian tujuan kinerja proses yang relevan dengan tujuan bisnis yang ditetapkan.	tujuan bisnis yang telah ditetapkan b. Tujuan dari penilaian berasal dari kebutuhan proses informasi c. Tujuan kuantitatif dari proses kinerja untuk mendukung tujuan bisnis yang telah ditetapkan d. Frekuensi penilaian diidentifikasi dan didefinisikan sesuai dengan tujuan penelitian kuantitatif untuk proses kinerja e. Hasil penelitian dikumpulkan, dianalisis dan dilaporkan untuk	T T T					

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		<p>mengawasi sejauh mana tujuan kuantitatif dari proses kinerja dapat terpenuhi</p> <p>f. Hasil penilaian digunakan untuk karakterisasi proses kinerja</p>	T					
	<p>PA 4.2 Process Control – Mengukur sejauh mana proses secara kuantitatif dikelola untuk menghasilkan proses yang stabil, mampu dan dapat diprediksi dalam batas yang ditentukan.</p>	<p>a. Teknik analisis dan pengendalian ditentukan dan diterapkan apabila memungkinkan</p> <p>b. Batas variasi kontrol ditetapkan untuk proses kinerja normal.</p> <p>c. Data penilaian dianalisis untuk variasi penyebab khusus masalah.</p>	T					

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
		d. Tindakan korektif diambil untuk mengatasi penyebab khusus masalah. e. Batas control ditetapkan kembali jika perlu mengikuti tindakan korektif.	T T					
Level 5 Optimising Process	PA 5.1 <i>Process Innovation</i> – Mengukur sejauh mana perubahan pada proses diidentifikasi dari analisis variasi penyebab umum masalah dalam kinerja dan dari investigasi pendekatan inovatif terhadap	a. Tujuan perbaikan proses didefinisikan dan mendukung tujuan bisnis yang relev b. Data yang tepat dianalisis untuk mengidentifikasi variasi penyebab umum dari masalah dalam proses kinerja c. Data yang tepat dianalisis untuk mengidentifikasi	T T T					

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
	definisi dan penerapan proses.	<p>peluang praktik dan inovasi terbaik</p> <p>d. Peluang perbaikan yang berasal dari teknologi baru dan konsep proses yang telah diidentifikasi</p> <p>e. Strategi implementasi ditetapkan untuk mencapai tujuan perbaikan proses</p>	<p>T</p> <p>T</p>					
	PA 5.2 Process Optimization – Mengukur sejauh mana perubahan pada definisi, manajemen, dan kinerja proses menghasilkan dampak efektif	<p>a. Dampak dari semua perubahan yang diusulkan dinilai berdasarkan tujuan proses dan standar proses yang ditetapkan.</p> <p>b. Pelaksanaan semua</p>	<p>T</p> <p>T</p>					

DSS05	Atribut Proses	Kriteria	Sesuai Kriteria (Y/T)	Not Achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)	Keterangan
	yang mencapai tujuan dari perbaikan proses.	<p>perubahan yang telah disepakati, dikelola untuk memastikan bahwa gangguan terhadap proses kinerja dipahami dan ditindaklanjuti.</p> <p>c. Berdasarkan kinerja aktual, efektivitas perubahan proses dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk menemukan apakah hasil tersebut disebabkan oleh penyebab umum atau khusus.</p>	T					

Jakarta,

Responden 1

(Herlina.....)

pgm GAGAS
brings energy to you

Responden 2

(Ariska A.....)



