

## **BAB IV**

### **HASIL DAN PEMBAHASAN**

#### **4.1 Hasil Pengumpulan Data**

Penulis melakukan observasi di Kantor PT.Telekomunikasi Indonesia Unit *Wholesale Access Network* Palembang selama  $\pm$  6 minggu mengamati dan mengumpulkan data lainnya seperti SOP (Standar Operasional Prosedur), dokumentasi penelitian, *screenshots* aplikasi, kuisisioner dan simulasi perhitungan yang dapat dilihat pada lampiran, kemudian untuk mendukung data lainnya maka dilakukan wawancara, hasil wawancara terlampir. Selanjutnya studi pustaka mencari beberapa sumber untuk mendukung penelitian, sumber dapat dilihat pada penyusunan daftar pustaka.

#### **4.2 Menetapkan Proses Berdasarkan COBIT 5 *For Information Security***

COBIT 5 memiliki 5 domain diantaranya EDM, APO, BAI, DSS, dan MEA. Setiap domain memiliki proses, detailnya pada Gambar 3.2 bab sebelumnya. EDM memiliki 5 proses, APO memiliki 13, BAI memiliki 10 proses dan DSS memiliki 6 proses. Proses yang akan diteliti oleh penulis berjumlah 5 proses diantaranya EDM03, APO12, APO13, BAI06 dan DSS05 yang kelima proses ini termasuk dalam fokus COBIT 5 pada keamanan yang disebut *COBIT 5 for Information Security*.

Pada Tabel 4.1 menjelaskan deskripsi, tujuan dan keluaran dari masing-masing proses, sehingga pengukuran lebih terarah serta sistematis. Hal ini akan berpengaruh pada kuisisioner.

**Tabel 4.1** Deskripsi Proses pada COBIT 5 *for Information Security*

Kode Domain	Nama Proses COBIT 5	Deskripsi
EDM03	Memastikan Optimasi Risiko	<ol style="list-style-type: none"> <li>1. Deskripsi Memastikan bahwa selera risiko organisasi dan toleransi dipahami, diartikulasikan dan dikomunikasikan, dan risiko terhadap nilai organisasi yang terkait dengan penggunaan TI diidentifikasi dan dikelola.</li> <li>2. Tujuan Memastikan bahwa risiko organisasi terkait TI tidak melebihi selera risiko dan toleransi risiko, dampak risiko TI untuk nilai organisasi diidentifikasi dan dikelola, dan potensi kegagalan terhadap kepatuhan dapat diminimalkan.</li> <li>3. <i>Outcomes</i> (keluaran) <ol style="list-style-type: none"> <li>a. EDM03-O1 Manajemen risiko informasi sebagai bagian dari keseluruhan manajemen risiko perusahaan.</li> </ol> </li> </ol>
APO12	Mengelola Risiko	<ol style="list-style-type: none"> <li>1. Deskripsi Mengidentifikasi, menilai dan mengurangi risiko terkait TI secara terus-menerus dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.</li> <li>2. Tujuan Mengintegrasikan manajemen risiko perusahaan terkait TI dengan ERM secara keseluruhan, menyeimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait TI.</li> <li>3. <i>Outcomes</i> (keluaran) <ol style="list-style-type: none"> <li>a. APO12-O1 Profil risiko informasi lengkap yang ada saat ini pada teknologi, aplikasi dan infrastruktur dalam perusahaan.</li> <li>b. APO12-O2 Respons insiden keamanan informasi terintegrasi dengan proses manajemen risiko secara keseluruhan untuk memberikan kemampuan dalam rangka memperbarui portofolio manajemen risiko.</li> </ol> </li> </ol>

APO13	Mengelola Keamanan	<ol style="list-style-type: none"> <li>1. Deskripsi Mendefinisikan, mengoperasikan dan mengawasi sistem manajemen keamanan informasi.</li> <li>2. Tujuan Mengatasi dampak dan kejadian suatu insiden keamanan informasi dalam tingkatan selera risiko perusahaan.</li> <li>3. <i>Outcomes</i> (keluaran) <ol style="list-style-type: none"> <li>a. APO13-O1 Sistem yang mempertimbangkan persyaratan keamanan informasi perusahaan secara efektif.</li> <li>b. APO13-O2 Rencana keamanan telah dibangun, diterima dan dikomunikasikan ke seluruh bagian perusahaan.</li> <li>c. APO13-O3 Solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten ke seluruh bagian perusahaan.</li> </ol> </li> </ol>
BAI06	Mengelola Perubahan	<ol style="list-style-type: none"> <li>1. Deskripsi Mengelola semua perubahan dalam cara yang terkontrol, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur. Hal ini termasuk standar perubahan dan prosedur, penilaian dampak, prioritas dan otorisasi, perubahan darurat,</li> <li>2. Tujuan Memberikan perubahan secara cepat dan handal pada bisnis dan mitigasi risiko yang berdampak negatif pada stabilitas atau integritas lingkungan yang berubah.</li> <li>3. <i>Outcomes</i> (keluaran) <ol style="list-style-type: none"> <li>a. BAI06-O1 Persyaratan keamanan informasi dimasukkan ke dalam penilaian dampak proses, aplikasi dan infrastruktur.</li> <li>b. BAI06-O2 Perubahan yang darurat dimasukkan ke dalam persyaratan keamanan informasi yang penting.</li> </ol> </li> </ol>
DSS05	Mengelola Layanan Keamanan	<ol style="list-style-type: none"> <li>1. Deskripsi Melindungi informasi enterprise untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh enterprise sesuai dengan kebijakan keamanan. Membangun dan memelihara peran keamanan informasi dan hak akses serta melakukan pemantauan keamanan.</li> </ol>

		<p>2. Tujuan Meminimalkan dampak operasional bisnis ketika terdapat kelemahan dan insiden keamanan informasi.</p> <p>3. <i>Outcomes</i> (keluaran)</p> <p>a. DSS05-O1 Keamanan jaringan dan komunikasi sesuai dengan kebutuhan bisnis.</p> <p>b. DSS05-O2 Terlindunginya informasi yang diproses, disimpan dan ditransmisikan oleh perangkat <i>endpoint</i>.</p> <p>c. DSS05-O3 Semua pengguna secara unik dapat diidentifikasi dan memiliki hak akses yang sesuai dengan perannya dalam bisnis.</p> <p>d. DSS05-O4 Langkah secara fisik telah diimplementasikan untuk melindungi informasi dari akses ilegal, kerusakan dan intervensi ketika sedang diproses, disimpan atau ditransmisikan.</p> <p>e. DSS05-O5 Informasi elektronik diamankan secara tepat ketika disimpan, ditransmisikan atau dihancurkan.</p>
--	--	---

#### 4.3 Menentukan Responden Berdasarkan RACI (*Responsibility, Accountability, Consult, and Inform*) Chart

Setelah bab 3 yang sebelumnya telah membahas mengenai definisi RACI *Chart* yang berfungsi untuk memetakan responden berdasarkan peran dan tanggung jawabnya. Maka pada bab hasil dan pembahasan ini kita mulai menuliskan *actual respondent* (responden sebenarnya) yang mengelola langsung sistem pada struktur PT. Telkom Unit *Wholesale Access Network* (WAN).

Dengan melakukan pendekatan identifikasi responden yang mengacu pada diagram RACI tersebut, maka *sampling* responden diarahkan pada peran – peran yang terkait langsung. Sehingga jawaban atas kuesioner mempunyai validitas yang memadai dan dapat mewakili keadaan.

### 4.3.1 Identifikasi Responden Berdasarkan RACI Chart EDM03

Mengidentifikasi responden diawali dengan melihat struktur organisasi unit WAN, terdapat pada Gambar 2.2 dan mengetahui tugas serta tanggung jawab masing-masing pegawai, hal tersebut bisa didapat dari wawancara. Kemudian tugas serta tanggung jawab pegawai tersebut dibandingkan persamaan tugasnya dengan peran dalam struktur organisasi yang didefinisikan oleh ISACA dapat dilihat pada Tabel 3.3. Setelah mengetahui peran responden maka dipetakan dengan RACI Chart EDM03.

EDM03 RACI Chart																											
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer	
EDM03.01 Evaluate risk management.	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C								C
EDM03.02 Direct risk management.	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I	I
EDM03.03 Monitor risk management.	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	I	C

**Gambar 4.1** RACI Chart EDM03 (ISACA, 2012)

Sebenarnya responden *Board* sampai *Privacy Officer* berjumlah 26 namun setelah dipetakan berdasarkan tugas dan tanggung jawabnya serta jumlah pegawai unit WAN tidak sebanyak itu, serta yang memenuhi kualifikasi peran dalam struktur organisasi yang didefinisikan oleh ISACA hanya beberapa.

*Actual responden* (responden sebenarnya) yang telah dipetakan melalui Gambar 4.1 RACI Chart EDM03 (Memastikan Optimasi Resiko) berjumlah 13 responden. Terlihat pada Tabel 4.2.

**Tabel 4.2** Identifikasi Responden Berdasarkan RACI *Chart* EDM03

<i>RACI Respondent</i>	<i>Actual Respondent</i>	<b>Jumlah</b>
<i>Business Executive</i>	<i>Manager Wholesale Access Network (WAN)</i>	1
<i>Business Process Owners</i>	<i>Assistant Manager TGroup 1</i>	1
<i>Strategy (IT Executive) Committee</i>	<i>Assistant Manager Tgroup 2</i>	1
<i>Steering (Project and Programme) Committees</i>	<i>Assistant Manager Tgroup 3</i>	1
<i>Enterprise Risk Committee</i>	<i>Assistant Manager OLO (Other License Operator)</i>	1
<i>Head of IT Operations</i>	<i>Team Leader Tsel Service</i>	1
<i>Head IT Administration</i>	<i>Help Desk (HD) Tsel</i>	2
<i>Service Manager</i>	<i>Teknisi Tsel Service</i>	5
<b>Jumlah</b>		<b>13</b>

Responden pertama *Manager WAN* sebagai *Business Executive*, *Assistant Manager Tgroup 1* sebagai *Business Process Owners*, *Assistant Manager Tgroup 2* memiliki peran dan tanggung jawab sebagai *Strategy (IT Executive) Committee*.

*Steering (Project and Programme) Committees*, responden sebenarnya adalah *Assistant Manager Tgroup 3*. *Enterprise Risk Committee* responden sebenarnya adalah *Assistant Manager OLO (Other License Operator)*.

*Team Leader Tsel Service (Irham)* sebagai *Head of IT Operations*, *Help Desk (HD) Tsel* sebagai *Head IT Administration* dan *Teknisi Tsel Service* sebagai *Service Manager*, kedua responden ini memiliki peran dan tanggung jawab sebagai *Informed* dari seluruh proses pada EDM03.

#### **4.3.2 Identifikasi Responden Berdasarkan RACI *Chart* APO12**

Mengidentifikasi responden diawali dengan melihat struktur organisasi unit WAN, terdapat pada Gambar 2.2 dan mengetahui tugas serta tanggung jawab masing-masing pegawai, hal tersebut bisa didapat dari wawancara. Kemudian tugas

serta tanggung jawab pegawai tersebut dibandingkan persamaan tugasnya dengan peran dalam struktur organisasi yang telah didefinisikan oleh ISACA dapat dilihat pada Tabel 3.3. Setelah mengetahui peran responden maka dipetakan dengan RACI Chart APO12.

APO12 RACI Chart																											
Key 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	
AP012.01 Collect data.		I				R		R		R	R	R		I		C	C	A	R	R	R	R	R	R	R	R	R
AP012.02 Analyse risk.		I				R		C		R	C			I		R	R	A	C	C	C	C	C	C	C	C	C
AP012.03 Maintain a risk profile.		I				R		C		A	C			I		R	R	R	C	C	C	C	C	C	C	C	C
AP012.04 Articulate risk.		I				R		C		R	C			I		C	C	A	C	C	C	C	C	C	C	C	C
AP012.05 Define a risk management action portfolio.		I				R		C		A	C			I		C	C	R	C	C	C	C	C	C	C	C	C
AP012.06 Respond to risk.		I				R		R		R	R			I		C	C	A	R	R	R	R	R	R	R	R	R

**Gambar 4.2** RACI Chart APO12 (ISACA, 2012)

Sebenarnya responden dari RACI Chart APO12 dimulai dari CEO, *Business Process Owners, Project Management Office, Chief Risk Officer, Chief Information Security Officer, Enterprise Risk Committee, Compliance* sampai *Privacy Officer* berjumlah 17 namun setelah dipetakan berdasarkan tugas dan tanggung jawabnya serta jumlah pegawai unit WAN, yang memenuhi kualifikasi peran dalam struktur organisasi yang telah didefinisikan oleh ISACA hanya beberapa.

*Actual responden* (responden sebenarnya) yang telah dipetakan melalui Gambar 4.2 RACI Chart APO12 (Mengelola Resiko) berjumlah 13 responden. Terlihat pada Tabel 4.3.

**Tabel 4.3** Identifikasi Responden berdasarkan RACI Chart APO12

<i>RACI Respondent</i>	<i>Actual Respondent</i>	<b>Jumlah</b>
<i>Chief Executive Officer</i>	<i>Manager Wholesale Access Network (WAN)</i>	1
<i>Business Process Owners</i>	<i>Assistant Manager Tgroup 1</i>	1
<i>Project Management Office</i>	<i>Assistant Manager Tgroup 2</i>	1
<i>Chief Information Officer</i>	<i>Assistant Manager Tgroup 3</i>	1
<i>Enterprise Risk Committee</i>	<i>Assistant Manager OLO (Other License Operator)</i>	1
<i>Head of IT Operations</i>	<i>Team Leader Tsel Service</i>	1
<i>Head IT Administration</i>	<i>Help Desk (HD) Tsel</i>	2
<i>Service Manager</i>	<i>Teknisi Tsel Service</i>	5
Jumlah		13

Responden pertama *Manager WAN* sebagai *Chief Executive Officer*, *Assistant Manager Tgroup 1* sebagai *Business Process Owners*, *Assistant Manager Tgroup 2* memiliki peran dan tanggung jawab sebagai *Project Management Office*, *Assistant Manager Tgroup 3* merupakan responden sebenarnya dari *Chief Information Officer*.

*Enterprise Risk Committee* responden sebenarnya adalah *Assistant Manager OLO (Other License Operator)*, *Team Leader Tsel Service* sebagai *Head of IT Operations*, *Help Desk (HD) Tsel* sebagai *Head IT Administration* dan *Teknisi Tsel Service* sebagai *Service Manager*.

#### **4.3.3 Identifikasi Responden Berdasarkan RACI Chart APO13**

Mengidentifikasi responden diawali dengan melihat struktur organisasi unit WAN, terdapat pada Gambar 2.2 dan mengetahui tugas serta tanggung jawab masing-masing pegawai, hal tersebut bisa didapat dari wawancara. Kemudian tugas



serta tanggung jawab pegawai tersebut dibandingkan persamaan tugasnya dengan peran dalam struktur organisasi yang telah didefinisikan oleh ISACA dapat dilihat pada Tabel 3.3. Setelah mengetahui peran responden maka dipetakan dengan RACI Chart APO13.

APO13 RACI Chart																										
Key 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
APO13.01 Establish and maintain an ISMS.	C	C	C	C	I	C	I	I		C	A	C	C	C	C	C	R	I	I	I	R	I	R	C	C	
APO13.02 Define and manage an information security risk treatment plan.	C	C	C	C	C	C	I	I		C	A	C	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 4.3** RACI Chart APO13 (ISACA, 2012)

Sebenarnya responden dari RACI Chart APO13 dimulai dari CEO, *Chief Operating Officer* sampai *Project Management Office*, *Chief Risk Officer* sampai *Enterprise Risk Committee* dan *Compliance* sampai *Privacy Officer* berjumlah 22 namun setelah dipetakan berdasarkan tugas dan tanggung jawabnya serta jumlah pegawai unit WAN tidak sebanyak itu, yang memenuhi kualifikasi peran dalam struktur organisasi yang telah didefinisikan oleh ISACA hanya beberapa.

*Actual responden* (responden sebenarnya) yang telah dipetakan melalui Gambar 4.4 RACI Chart APO13 (Mengelola Resiko) berjumlah 13 responden. Terlihat pada Tabel 4.4.

**Tabel 4.4** Identifikasi Responden berdasarkan RACI Chart APO13

<i><b>RACI Respondent</b></i>	<i><b>Actual Respondent</b></i>	<b>Jumlah</b>
<i>Business Executive</i>	<i>Manager Wholesale Access Network (WAN)</i>	1
<i>Business Process Owners</i>	<i>Assistant Manager Tgroup 1</i>	1
<i>Strategy Executive Committee</i>	<i>Assistant Manager Tgroup 2</i>	1
<i>Steering (Project and Programme) Committees</i>	<i>Assistant Manager Tgroup 3</i>	1
<i>Enterprise Risk Committee</i>	<i>Assistant Manager OLO (Other License Operator)</i>	1
<i>Head of IT Operations</i>	<i>Team Leader Tsel Service</i>	1
<i>Head IT Administration</i>	<i>Help Desk (HD) Tsel</i>	2
<i>Service Manager</i>	<i>Teknisi Tsel Service</i>	5
<b>Jumlah</b>		<b>13</b>

Responden pertama *Manager WAN* sebagai *Business Executive*, *Assistant Manager Tgroup 1* sebagai *Business Process Owners*, *Assistant Manager Tgroup 2* memiliki peran dan tanggung jawab sebagai *Strategy Executive Committee*. *Steering (Project and Programme) Committees*, responden sebenarnya adalah *Assistant Manager Tgroup 3*. *Enterprise Risk Committee* responden sebenarnya adalah *Assistant Manager OLO (Other License Operator)*.

*Team Leader Tsel Service* sebagai *Head of IT Operations*, *Help Desk (HD) Tsel* sebagai *Head IT Administration* dan *Teknisi Tsel Service* sebagai *Service Manager*.

#### **4.3.4 Identifikasi Responden Berdasarkan RACI Chart BAI06**

Mengidentifikasi responden diawali dengan melihat struktur organisasi unit WAN, terdapat pada Gambar 2.2 dan mengetahui tugas serta tanggung jawab masing-masing pegawai, hal tersebut bisa didapat dari wawancara. Kemudian tugas

serta tanggung jawab pegawai tersebut dibandingkan persamaan tugasnya dengan peran dalam struktur organisasi yang telah didefinisikan oleh ISACA dapat dilihat pada Tabel 3.3. Setelah mengetahui peran responden maka dipetakan dengan RACI Chart BAI06.

BAI06 RACI Chart																										
Key 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
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C	C						C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I				C						C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R	C						C	C	R	C	R	R	I	I			

**Gambar 4.4** RACI Chart BAI06 (ISACA, 2012)

Sebenarnya responden dari RACI Chart BAI06 dimulai dari *Business Executive, Business Process Owners, Project Management Office, Chief Risk Officer, Compliance* sampai *Information Security Manager* berjumlah 13 namun setelah dipetakan berdasarkan tugas dan tanggung jawabnya serta jumlah pegawai unit WAN, yang memenuhi kualifikasi peran dalam struktur organisasi yang telah didefinisikan oleh ISACA hanya beberapa.

*Actual responden* (responden sebenarnya) yang telah dipetakan melalui Gambar 4.4 RACI Chart domain BAI06 (Mengelola Perubahan) berjumlah 12 responden. Terlihat pada Tabel 4.5.

**Tabel 4.5** Identifikasi Responden berdasarkan RACI Chart BAI06

<i>RACI Respondent</i>	<i>Actual Respondent</i>	<b>Jumlah</b>
<i>Business Executive</i>	<i>Manager Wholesale Access Network (WAN)</i>	1
<i>Business Process Owners</i>	<i>Assistant Manager Tgroup 1</i>	1
<i>Project Management Office</i>	<i>Assistant Manager Tgroup 2</i>	1
<i>Chief Information Officer</i>	<i>Assistant Manager Tgroup 3</i>	1
<i>Head of IT Operations</i>	<i>Team Leader Tsel Service</i>	1
<i>Head IT Administration</i>	<i>Help Desk (HD) Tsel</i>	2
<i>Service Manager</i>	<i>Teknisi Tsel Service</i>	5
Jumlah		12

Responden pertama *Manager WAN* sebagai *Business Executive*, *Assistant Manager Tgroup 1* sebagai *Business Process Owners*, *Assistant Manager Tgroup 2* memiliki peran dan tanggung jawab sebagai *Project Management Office*. *Chief Information Officer*, responden sebenarnya adalah *Assistant Manager Tgroup 3*.

*Team Leader Tsel Service* sebagai *Head of IT Operations*, *Help Desk (HD) Tsel* sebagai *Head IT Administration* dan *Teknisi Tsel Service* sebagai *Service Manager*.

#### **4.3.5 Identifikasi Responden Berdasarkan RACI Chart DSS05**

Mengidentifikasi responden diawali dengan melihat struktur organisasi unit WAN, terdapat pada Gambar 2.2 dan mengetahui tugas serta tanggung jawab masing-masing pegawai, hal tersebut bisa didapat dari wawancara. Kemudian tugas serta tanggung jawab pegawai tersebut dibandingkan persamaan tugasnya dengan

peran dalam struktur organisasi yang telah didefinisikan oleh ISACA dapat dilihat pada Tabel 3.3. Setelah mengetahui peran responden maka dipetakan dengan RACI *Chart* DSS05.

DSS05 RACI Chart																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programme/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 4.5 RACI Chart DSS05 (ISACA, 2012)

Sebenarnya responden dari RACI *Chart* DSS05 dimulai dari CEO, *Business Process Owners*, *Strategy Executive Committee*, *Chief Risk Officer*, *Chief Information Security Officer*, *Head Human Resources* sampai *Privacy Officer* berjumlah 16 namun setelah dipetakan berdasarkan tugas dan tanggung jawabnya serta jumlah pegawai unit WAN, yang memenuhi kualifikasi peran dalam struktur organisasi yang telah didefinisikan oleh ISACA hanya beberapa.

*Actual responden* (responden sebenarnya) yang telah dipetakan melalui Gambar 4.5 RACI *Chart* DSS05 (Mengelola Layanan Keamanan) berjumlah 12 responden. Terlihat pada Tabel 4.6.

**Tabel 4.6** Identifikasi Responden berdasarkan RACI *Chart* DSS05

<b><i>RACI Respondent</i></b>	<b><i>Actual Respondent</i></b>	<b>Jumlah</b>
<i>Chief Operating Officer</i>	<i>Manager Wholesale Access Network (WAN)</i>	1
<i>Business Process Owners</i>	<i>Assistant Manager Tgroup 1</i>	1
<i>Strategy Executive Committee</i>	<i>Assistant Manager Tgroup 2</i>	1
<i>Chief Information Officer</i>	<i>Assistant Manager Tgroup 3</i>	1
<i>Head of IT Operations</i>	<i>Team Leader Tsel Service</i>	1
<i>Head IT Administration</i>	<i>Help Desk (HD) Tsel</i>	2
<i>Service Manager</i>	<i>Teknisi Tsel Service</i>	5
Jumlah		12

Responden pertama *Manager WAN* sebagai *Chief Operating Officer*. *Assistant Manager Tgroup 1* sebagai *Business Process Owners*, *Assistant Manager Tgroup 2* memiliki peran dan tanggung jawab sebagai *Strategy Executive Committee*. *Chief Information Officer*, responden sebenarnya adalah *Assistant Manager Tgroup 3*, *Team Leader Tsel Service* sebagai *Head of IT Operations*, *Help Desk (HD) Tsel* sebagai *Head IT Administration* dan *Teknisi Tsel Service* sebagai *Service Manager*.

#### **4.4 Kuisisioner**

Dari pelaksanaan kuisisioner, diperoleh jawaban atas kuisisioner tersebut sebanyak jumlah kuisisioner yang didistribusikan kepada para responden yang telah dipetakan menggunakan RACI *Chart*. Hasil jawaban responden tersebut selanjutnya dibuat rekapitulasi yang secara garis besar dapat memberikan gambaran kecenderungan suatu tingkat kapabilitas atas beberapa atribut. Kuisisioner dapat dilihat pada lampiran.

#### 4.5 Perhitungan Berdasarkan *Process Assessment Model (PAM)*

##### 4.5.1 Hasil Pencapaian Level Proses EDM03

Hasil pengukuran tingkat kapabilitas pada proses EDM03 (Memastikan Optimasi Risiko) dapat dilihat pada Tabel 4.7.

**Tabel 4.7** Hasil Pencapaian Level Proses EDM03

Kriteria Penilaian dari Responden	Penilaian Proses EDM03										
	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	
<i>Manager Wholesale Access Network</i>		100	100	100	100	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	100	75	100	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	83,3	75	80	83,3	83,3	80	0	0	
<i>Assistant Manager Tgroup</i>		100	100	100	80	100	83,3	80	0	0	
<i>Assistant Manager OLO</i>		100	100	100	100	100	83,3	80	0	0	
<i>Team Leader Tsel Service</i>		100	100	100	100	83,3	100	80	0	0	
<i>Help Desk (HD) Tsel</i>		100	83,3	75	100	83,3	100	100	0	0	
<i>Help Desk (HD) Tsel</i>		100	83,3	75	80	83,3	83,3	80	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	80	83,3	66	60	0	0	
<i>Teknisi Tsel Service</i>		100	66	75	80	83,3	66	60	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	80	100	66	80	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	100	100	100	100	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	80	83,3	66	60	0	0	
Rata-rata		100	93,5	90,3	89,2	91	84,4	81,5	0	0	
Nilai	False	F	F	F	F	F	L	L	N	N	

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai *false* jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses EDM03 berada pada level 4 (*Predictable*) yang artinya proses yang telah berjalan dioperasikan dan dapat diprediksi dampak dari penerapan sistem. Melihat level yang telah dicapai dapat dipastikan bahwa risiko perusahaan terkait TI tidak melebihi toleransi risiko.

Berdasarkan Tabel 4.7 hasil pencapaian PA 4.1 yaitu 84,4 (*Largely Achieved*) menunjukkan bahwa perusahaan telah mengenal seberapa jauh hasil pengukuran dapat digunakan untuk memastikan bahwa performa proses mendukung tujuan organisasi dan PA 4.2 yaitu 81,5 (*Largely Achieved*) yang artinya pengukuran tentang seberapa jauh suatu proses secara kuantitatif bisa menghasilkan proses yang stabil.



#### 4.5.2 Hasil Pencapaian Level Proses APO12

Hasil pengukuran tingkat kapabilitas pada proses APO12 (Mengelola Risiko)

dapat dilihat pada Tabel 4.8.

**Tabel 4.8** Hasil Pencapaian Level Proses APO12

Kriteria Penilaian dari Responden	Penilaian Proses APO12									
	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
<i>Manager Wholesale Access Network</i>		100	100	100	100	100	0	0	0	0
<i>Assistant Manager TGroup</i>		100	100	75	100	100	0	0	0	0
<i>Assistant Manager TGroup</i>		100	100	75	100	83,3	0	0	0	0
<i>Assistant Manager TGroup</i>		100	83,3	100	80	83,3	0	0	0	0
<i>Assistant Manager OLO</i>		100	100	100	100	100	0	0	0	0
<i>Team Leader Tsel Service</i>		100	100	75	100	83,3	0	0	0	0
<i>Help Desk (HD) Tsel</i>		100	83,3	100	100	83,3	0	0	0	0
<i>Help Desk (HD) Tsel</i>		100	100	100	80	83,3	0	0	0	0
<i>Teknisi Tsel Service</i>		100	50	75	60	50	0	0	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	0	0	0	0
<i>Teknisi Tsel Service</i>		100	83,3	75	60	50	0	0	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	0	0	0	0
<i>Teknisi Tsel Service</i>		100	83,3	50	60	50	0	0	0	0
Rata-rata		100	91	86,5	87,6	82	0	0	0	0
Nilai	False	F	F	F	F	L	N	N	N	N

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai *false* jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses APO12 berada pada level 3 (*Established*) yang artinya sistem telah dibangun dan diimplementasikan, menggunakan proses yang telah didefinisikan untuk mencapai hasil yang diharapkan.

Dengan cara mengintegrasikan manajemen risiko perusahaan terkait bidang TI dengan pengelolaan sumber daya perusahaan secara keseluruhan, dan menyeimbangkan biaya dan manfaat dari pengelolaan risiko perusahaan yang berkaitan dengan TI hanya saja belum mencapai nilai maksimal karena sumber daya manusia yang mengerti dalam mengelola resiko secara keseluruhan masih belum cukup.

Berdasarkan Tabel 4.8 hasil pencapaian PA 3.1 yaitu 87,6 (*Fully Achieved*) menunjukkan bahwa perusahaan telah mampu mengukur proses mengukur sejauh mana proses standar dikelola untuk mendukung pengerjaan dari proses yang telah didefinisikan.

PA 3.2 yaitu 82 (*Largely Achieved*) yang artinya bahwa perusahaan telah mampu mengukur sejauh mana proses standar secara efektif telah dijalankan seperti yang telah didefinisikan untuk mencapai hasil dari proses.

### 4.5.3 Hasil Pencapaian Level Proses APO13

Hasil pengukuran tingkat kapabilitas pada proses APO13 (Mengelola Keamanan) dapat dilihat pada Tabel 4.9.

**Tabel 4.9** Hasil Pencapaian Level Proses APO13

Kriteria Penilaian dari Responden	Penilaian Proses APO13										
	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	
<i>Manager Wholesale Access Network</i>		100	100	100	100	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	100	100	100	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	100	75	100	83,3	100	80	0	0	
<i>Assistant Manager Tgroup</i>		100	83,3	100	80	100	83,3	100	0	0	
<i>Assistant Manager OLO</i>		100	100	100	100	100	100	100	0	0	
<i>Team Leader Tsel Service</i>		100	100	100	100	100	100	80	0	0	
<i>Help Desk (HD) Tsel</i>		100	100	100	100	83,3	83,3	80	0	0	
<i>Help Desk (HD) Tsel</i>		100	83,3	75	100	83,3	83,3	80	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	100	83,3	66	60	0	0	
<i>Teknisi Tsel Service</i>		100	83,3	75	80	83,3	66	60	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	80	100	83,3	80	0	0	
<i>Teknisi Tsel Service</i>		100	83,3	75	100	100	83,3	100	0	0	
<i>Teknisi Tsel Service</i>		100	100	100	80	83,3	66	60	0	0	
Rata-rata		100	94,8	92,3	93,8	92,2	85,7	83	0	0	
Nilai	False	F	F	F	F	F	F	L	N	N	

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai *false* jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses APO13 berada pada level 4 (*Predictable*) yang artinya proses yang telah berjalan dioperasikan dan dapat diprediksi dampak dari penerapan sistem.

Dengan cara menjalankankan dan mengawasi sistem manajemen keamanan informasi. Menetapkan serangkaian kontrol dan pedoman untuk memastikan bahwa prosedur keamanan yang mengatur penggunaan aset dan sumber daya keamanan TI pada perusahaan ditegakkan dengan benar dan diterapkan sesuai dengan tujuan.

Berdasarkan Tabel 4.9 hasil pencapaian PA 4.1 yaitu 85,7 (*Fully Achieved*) menunjukkan bahwa perusahaan telah mengenal seberapa jauh hasil pengukuran dapat digunakan untuk memastikan bahwa performa proses mendukung tujuan organisasi.

PA 4.2 yaitu 83 (*Largely Achieved*) yang artinya ada pencapaian pada proses yang dinilai menghasilkan proses yang stabil, mampu dan bisa diprediksi dalam batasan yang telah ditentukan.

#### 4.5.4 Hasil Pencapaian Level Proses BAI06

Hasil pengukuran tingkat kapabilitas pada proses BAI06 (Mengelola Perubahan) dapat dilihat pada Tabel 4.10.

**Tabel 4.10** Hasil Pencapaian Level Proses BAI06

Kriteria Penilaian dari Responden	Penilaian Proses BAI06									
	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
<i>Manager Wholesale Access Network</i>		100	100	100	100	100	0	0	0	0
<i>Assistant Manager Tgroup</i>		100	100	100	100	100	0	0	0	0
<i>Assistant Manager Tgroup</i>		100	83,3	75	100	83,3	0	0	0	0
<i>Assistant Manager Tgroup</i>		100	100	75	100	83,3	0	0	0	0
<i>Team Leader Tsel Service</i>		100	83,3	75	100	83,3	0	0	0	0
<i>Help Desk (HD) Tsel</i>		100	83,3	100	80	83,3	0	0	0	0
<i>Help Desk (HD) Tsel</i>		100	83,3	100	80	83,3	0	0	0	0
<i>Teknisi Tsel Service</i>		100	50	75	60	50	0	0	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	0	0	0	0
<i>Teknisi Tsel Service</i>		100	83,3	75	80	50	0	0	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	0	0	0	0
<i>Teknisi Tsel Service</i>		100	83,3	100	60	83,3	0	0	0	0
Rata-rata		100	87,4	89,5	88,3	83,3	0	0	0	0
Nilai	False	F	F	F	F	L	N	N	N	N

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai *false* jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses BAI06 berada pada level 3 (*Established*) yang artinya proses yang telah dibangun kemudian diimplementasikan menggunakan proses yang telah didefinisikan, yang mampu untuk mencapai hasil yang diharapkan.

Dengan cara melakukan inovasi dalam pelayanan yang handal dari perubahan bisnis dan mitigasi risiko yang berdampak negatif untuk menjaga stabilitas atau integritasi lingkungan berubah.

Berdasarkan Tabel 4.10 hasil pencapaian PA 3.1 yaitu 88,3 (*Fully Achieved*) menunjukkan bahwa perusahaan telah mampu mengukur sejauh mana proses standar dikelola untuk mendukung pengerjaan dari proses yang telah didefinisikan.

PA 3.2 yaitu 83,3 (*Largely Achieved*) yang artinya bahwa perusahaan telah mampu mengukur sejauh mana proses standar secara efektif telah dijalankan seperti yang telah didefinisikan untuk mencapai hasil dari proses.

#### 4.5.5 Hasil Pencapaian Level Proses DSS05

Hasil pengukuran tingkat kapabilitas pada proses DSS05 (Mengelola Layanan Keamanan) dapat dilihat pada Tabel 4.11.

**Tabel 4.11** Hasil Pencapaian Level Proses DSS05

Kriteria Penilaian dari Responden	Penilaian Proses DSS05									
	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
<i>Manager Wholesale Access Network</i>		100	100	100	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	100	75	100	100	100	100	0	0
<i>Assistant Manager Tgroup</i>		100	83,3	75	100	83,3	66	80	0	0
<i>Assistant Manager Tgroup</i>		100	100	100	100	100	100	80	0	0
<i>Team Leader Tsel Service</i>		100	100	75	100	83,3	66	80	0	0
<i>Help Desk (HD) Tsel</i>		100	83,3	100	100	83,3	100	100	0	0
<i>Help Desk (HD) Tsel</i>		100	83,3	100	100	83,3	83,3	60	0	0
<i>Teknisi Tsel Service</i>		80	33,3	75	60	50	66	60	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	100	100	0	0
<i>Teknisi Tsel Service</i>		80	83,3	75	100	100	83,3	60	0	0
<i>Teknisi Tsel Service</i>		100	100	100	100	100	100	80	0	0
<i>Teknisi Tsel Service</i>		100	83,3	100	80	83,3	66	60	0	0
Rata-rata	False	96	87	89,5	95	88,8	85,8	80	0	0
Nilai	False	F	F	F	F	F	F	L	N	N

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai *false* jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses DSS05 berada pada level 4 (*Predictable*) artinya proses telah berjalan kemudian dioperasikan dengan batasan yang ditentukan untuk mencapai hasil yang diharapkan dari proses pengelolaan layanan keamanan.

Berdasarkan Tabel 4.11 hasil pencapaian PA 4.1 yaitu 85,8 (*Fully Achieved*) menunjukkan bahwa perusahaan telah mengenal seberapa jauh hasil pengukuran dapat digunakan untuk memastikan bahwa performa proses mendukung tujuan perusahaan dan PA 4.2 yaitu 80 (*Largely Achieved*) yang artinya pencapaian dari atribut proses dapat menghasilkan proses yang stabil, mampu diprediksi dalam batasan yang telah ditentukan, memberikan pelayanan aplikasi di dalam proses TI, pengelolaan keamanan dan dukungan pelaksanaan proses TI yang lebih efektif dan efisien.

#### 4.5.6 Hasil Pencapaian Kapabilitas Keamanan Sistem

Hasil tingkat kapabilitas keamanan sistem informasi monitoring jaringan dari seluruh proses dirangkum pada Tabel 4.12.

**Tabel 4.12** Hasil Tingkat Kapabilitas Keamanan Sistem

<b>ID Proses</b>	<b>Nama Proses</b>	<b>Level</b>	<b>Tingkat Kapabilitas</b>
EDM03	<i>Ensure risk optimisation</i> (Memastikan Optimasi Risiko)	4	<i>Predictable</i> (Dapat Diprediksi)
APO12	<i>Manage risk</i> (Mengelola Risiko)	3	<i>Established</i> (Proses yang tetap)
APO13	<i>Manage security</i> (Mengelola keamanan)	4	<i>Predictable</i> (Dapat Diprediksi)
BAI06	<i>Manage changes</i> (Mengelola Perubahan)	3	<i>Established</i> (Proses yang tetap)
DSS05	<i>Manage security services</i> (Mengelola Layanan Keamanan)	4	<i>Predictable</i> (Dapat Diprediksi)



#### **4.6 Hasil Rekomendasi Perbaikan**

Hasil rekomendasi diharapkan dapat memberikan solusi tata kelola yang terbaik untuk perusahaan. Rekomendasi dibuat naik 1 level dari level yang telah dicapai, seperti proses EDM03 yang berada pada level 4, maka dibuatlah rekomendasi untuk mengoptimalkan sistem ke level 5. Proses APO12 yang berada pada level 3, maka dibuatlah rekomendasi untuk mencapai level 4, begitu juga dengan proses lainnya. Langkah penerapan tata kelola keamanan informasi yang direkomendasikan merujuk kepada pendekatan manajemen perubahan yang dikembangkan oleh John Kotter. Pendekatan ini diadopsi oleh COBIT 5 diantaranya, mendapatkan pemahaman tentang latar belakang program, tujuan dan pendekatan tata kelola saat ini.

##### **4.6.1 Rekomendasi Perbaikan Proses EDM03**

Berikut beberapa rekomendasi untuk meningkatkan level pada proses EDM03 (Memastikan Optimasi Risiko) :

1. Memeriksa dan membuat penilaian secara kontinu 3 bulan 1 kali tentang pengaruh risiko pada penggunaan TI saat ini dan masa depan di perusahaan.
2. Perusahaan membentuk tim sendiri untuk manajemen risiko dan pembagian tugas dan tanggung jawab sesuai dengan deskripsi ISACA.
3. Selalu memantau profil risiko informasi perusahaan agar antara risiko bisnis dan peluang berjalan seimbang.
4. Tidak menerima laporan gangguan melalui *chat* atau menerima laporan diluar aplikasi karena akan berdampak pada integritas data.

#### 4.6.2 Rekomendasi Perbaikan Proses APO12

Berikut beberapa rekomendasi untuk meningkatkan level pada proses APO12 (Mengelola Risiko) :

1. Mengidentifikasi dan mengumpulkan data yang relevan untuk mengidentifikasi, mengukur, menganalisis dan melaporkan risiko terkait TI secara efektif.
2. Mengembangkan informasi yang bermanfaat untuk mendukung keputusan risiko yang terdapat dalam faktor risiko bisnis yang relevan.
3. Memelihara inventaris risiko yang diketahui dan atributnya (termasuk frekuensi yang diharapkan, dampak yang potensial dan respons) serta sumber daya terkait, kemampuan dan kegiatan pengendalian.

#### 4.6.3 Rekomendasi Perbaikan Proses APO13

Berikut beberapa rekomendasi untuk meningkatkan level pada proses APO13 (Mengelola Keamanan) :

1. Melakukan tinjauan atau pengkajian terhadap efektivitas SMKI (Sistem Manajemen Keamanan Informasi) secara teratur 3 bulan 1 kali untuk memastikan bahwa pengamanan tetap berada pada ruang lingkup yang ditetapkan dan merekam tindakan atau peristiwa yang dapat berdampak pada efektivitas kinerja pada sitem monitoring jaringan.
2. Menggunakan *Application-Proxy Firewall* untuk memfilter informasi yang lewat dari *proxy sever*. *Proxy server* dapat memilih informasi yang akan diteruskan atau tidak berdasarkan *setting* atau *logic* dari *proxy server* tersebut.

3. Tidak menggunakan *floppy drive* pada *server* untuk menghindari penyusup dapat mengubah *password root* dengan menggunakan disket *boot*.
4. Menyediakan UPS (*Uninterruptible Power Supply*) untuk server aplikasi ataupun basis data untuk mencegah kerusakan fisik pada *server*.

#### **4.6.4 Rekomendasi Perbaikan Proses BAI06**

Berikut beberapa rekomendasi untuk meningkatkan level pada proses BAI06 (Mengelola Perubahan) :

1. Memperbarui dokumen dan prosedur kapanpun perubahan diimplementasikan agar pengguna yang terpengaruh oleh perubahan dapat beradaptasi lebih mudah.
2. Mengelola perubahan darurat dengan hari-hati untuk meminimalkan insiden lebih lanjut dan pastikan perubahan tersebut dikendalikan dan berlangsung aman. Memastikan bahwa perubahan darurat diukur dan disahkan secara tepat setelah perubahan.
3. Memelihara sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan yang ditolak, mengkomunikasikan status perubahan yang disetujui, dalam proses dan lengkap.

#### 4.6.5 Rekomendasi Perbaikan Proses DSS05

Berikut beberapa rekomendasi untuk meningkatkan level pada proses DSS05 (Mengelola Layanan Keamanan) :

1. Melakukan *penetration test* secara periodik, yaitu 3 bulan 1 kali.
2. Menentukan otorisasi terhadap devices yang boleh mengakses informasi institusi dan jaringan insitusi, artinya *screening* terhadap kode *device* (pencatatan kodefikasi dan pembuatan sistem *screening*).
3. Menerapkan enkripsi informasi (proses mengamankan informasi dengan cara membuat informasi tersebut tidak bisa dibaca tanpa bantuan pengetahuan khusus) dan pada saat pengiriman dibuat klasifikasinya agar informasi tersebut aman.