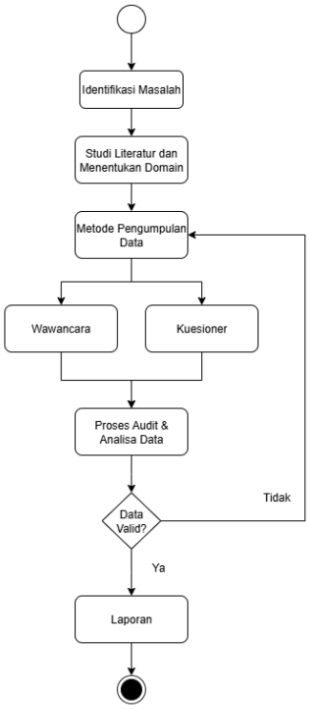
BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Proses *Audit* Sistem Informasi *Website* IlmuKomputer.Com (IKC) PT Brainnatics Indonesia Cendekia memiliki beberapa tahapan-tahapan yaitu :



Gambar II.2 Tahapan Penelitian

1. Identifikasi Masalah

Proses identifikasi permasalahan dilakukan secara langsung di PT Brainmatics Indonesia Cendekia guna memperoleh pemahaman yang komprehensif terhadap kondisi nyata yang terjadi di lingkungan perusahaan. Langkah ini bertujuan untuk mengumpulkan data dan informasi secara objektif melalui observasi dan interaksi langsung dengan pihak terkait.

Tahapan ini untuk mengumpulkan isu dan permasalahan yang tengah dihadapi oleh perusahaan, sehingga dapat menjadi landasan dalam merumuskan fokus penelitian.

2. Studi Literatur dan Menentukan Domain

Studi literatur menurut Putrihapsari & Fauziah, 2020 yaitu sebagai penelitian yang dilakukan dengan cara menelaah berbagai kajian kepustakaan yang diperlukan dalam penelitian [25].

Tujuan utama untuk memperoleh pemahaman yang menyeluruh mengenai pengetahuan yang telah tersedia terkait topik yang dibahas, mengidentifikasi kesenjangan dalam penelitian terdahulu, serta memberikan dasar teoritis yang kuat bagi pengembangan penelitian selanjutnya [26].

Studi literatur Evaluasi *Capability Level Website* IlmuKomputer.Com *(*IKC) PT Brainmatics Indonesia Cendekia dengan cara melakukan pengkajian berbagai sumber seperti jurnal ilmiah, buku referensi, dan penelitian terdahulu, serta mempelajari *Framework* COBIT sebagai landasan utama dalam mengevaluasi tata kelola dan manajemen teknologi informasi.

Berdasarkan hasil studi literatur tersebut, peneliti menetapkan domain penelitian yang difokuskan pada Evaluasi *Capability Level Website* IlmuKOmputer.Com Menggunakan *Framework* COBIT 5 dengan domain *Deliver, Service, and Support* (DSS) dan *Monitor,Evaluate,and Asesment* (MEA) Penentuan domain ini bertujuan untuk membatasi ruang lingkup kajian agar evaluasi dapat dilakukan secara sistematis dan terarah sesuai dengan prinsip, tujuan, dan proses yang terdapat dalam kerangka kerja COBIT 5.

3. Metode Pengumpulan Data

a. Wawancara

Metode pengumpulan data yang digunakan dalam proses *Audit* sistem informasi di PT Brainmatics Indonesia Cendekia adalah wawancara. Wawancara ini dilakukan bersama Direktur *Learning* dan *Manager Training* pada hari Rabu,19

Maret 2025 pukul 16.00 – Selesai. Bertujuan untuk menggali informasi mendalam terkait sejarah pembentukan IlmuKomputer.Com (IKC) serta mengetahui latar belakang dan alasan dibentuknya *website* tersebut sebagai bagian dari layanan perusahaan.

Wawancara ini juga bertujuan untuk mengidentifikasi berbagai kendala atau bottleneck yang sering dihadapi oleh perusahaan dalam pengelolaan sistem tata kelola Teknologi Informasi (TI), khususnya dalam operasional dan pengembangan *website* IlmuKomputer.Com (IKC). Informasi yang diperoleh dari wawancara ini akan menjadi dasar dalam menganalisis efektivitas sistem informasi yang ada serta memberikan rekomendasi perbaikan ke depannya

b. Kuesioner

Pengumpulan data dalam proses *Audit* sistem informasi dilakukan menggunakan metode kuesioner dengan skala likert, Menurut Sugiono [27] Skala Likert merupakan metode yang digunakan untuk menilai sikap, opini, dan persepsi seseorang atau kelompok terhadap suatu fenomena sosial. Adapun tabel skala likert disajikan sebagai berikut:

Tabel II.2 Skala Likert

Kriteria	Skala Penilaian
Sangat Setuju	5
Setuju	4
Cukup/Netral	3
Tidak Setuju	2
Sangat Tidak Setuju	1

Kuesioner tersebut melibatkan 5 (lima) responden dari berbagai posisi strategis di PT Brainmatics Indonesia Cendekia, yaitu Karno Nur Cahyo (Direktur *Training*), Fandika (*Manager Training*),Nayla Nur Fatma (Marketing Brainmatics), Muhadi (*Specialist)* dan Ernata Marbun (*Specialist).*

Responden dalam penelitian ini dilakukan secara purposive sampling, yaitu pemilihan responden yang dianggap memiliki pemahaman, keterlibatan, dan otoritas dalam pengelolaan *website* IlmuKomputer.Com (IKC).

Total lima orang responden dipilih karena mereka merupakan perwakilan dari unit yang terlibat langsung dalam operasional, pengembangan, dan pengelolaan teknologi informasi di lingkungan PT Brainmatics Indonesia Cendekia.

c. Proses *Audit* & Analisa Data

Evaluasi *Capability Level* sistem informasi dilaksanakan dengan menggunakan *google form* sebagai sarana pengumpulan data. Penggunaan *Google Form* dipilih karena kemudahan dalam penyebaran ke responden secara luas, serta efisiensi dalam waktu dan tempat pelaksanaan.

Selain itu, platform ini juga memfasilitasi proses rekapitulasi data secara otomatis, sehingga mempercepat tahap awal analisis. Pernyataan yang disusun mengacu pada kerangka kerja COBIT 5 dengan ruang lingkup 2 domain yaitu: DSS *(Deliver, Service and Support)* dan MEA *(Monitor, Evaluate and Assess)*.

Setelah pengumpulan data selesai, jawaban dari responden diunduh dalam format *Microsoft Excel* guna dianalisis lebih lanjut. Proses analisis meliputi beberapa langkah utama:

1) Menentukan Target *Level*

Penetapan target *level* ini dilakukan berdasarkan hasil diskusi dan kesepakatan antara peneliti dan pihak perusahaan, dengan mempertimbangkan kebutuhan bisnis, strategi organisasi, serta kondisi aktual proses yang sedang dinilai. Target *level* biasanya dinyatakan dalam skala *Level* 1 hingga *Level* 5,

yang mencerminkan tingkat kematangan dan pengendalian proses mulai dari yang paling dasar hingga proses yang terkelola secara optimal.

2) Perhitungan Nilai Kuesioner

Pengolahan jawaban responden terhadap pertanyaan yang termasuk dalam subdomain tersebut. Setiap jawaban diberi skor sesuai skala yang digunakan, kemudian skor dari semua pertanyaan dalam subdomain dijumlahkan untuk setiap responden. Selanjutnya, dihitung rata-rata skor seluruh responden sehingga diperoleh nilai representatif subdomain. Rumus mencari nilai kuesioner persubdomain merujuk pada [28].

$$Nilai\ SubDomain = \frac{\sum Skor\ Item\ dalam\ Subdomain}{Jumlah\ Item\ dalam\ Subdomain} \quad (1)$$

Sumber : Audit Sistem Informasi Absensi pada Kejaksaan Negeri Kota Bandung Menggunakan *Framework* Cobit 5

Keterangan :

$\sum Skor\ Item\ dalam\ Subdomain$: Total nilai per-subsub domain

$Jumlah\ Item\ dalam\ Subdomain$: Total Per-subsub domain

3) Perhitungan *Index* Kuesioner

Menghitung indeks kuesioner dengan memberi nilai pada setiap jawaban, menjumlahkan semua nilai jawaban tiap responden, lalu menghitung rata-rata dari semua responden yang ikut mengisi. Rumus mencari *index* kuesioner merujuk pada[28].

$$Index\ Kuesioner = \frac{\sum Nilai\ Subdomain}{Jumlah\ Subdomain} \quad (2)$$

Sumber : Audit Sistem Informasi Absensi pada Kejaksaan Negeri Kota Bandung Menggunakan *Framework* Cobit 5

Keterangan :

$\sum Nilai\ Subdomain$: Nilai Per-Subdomain

$Jumlah\ Subdomain$: Total Subdomain

4) Perhitungan *Capability Level*

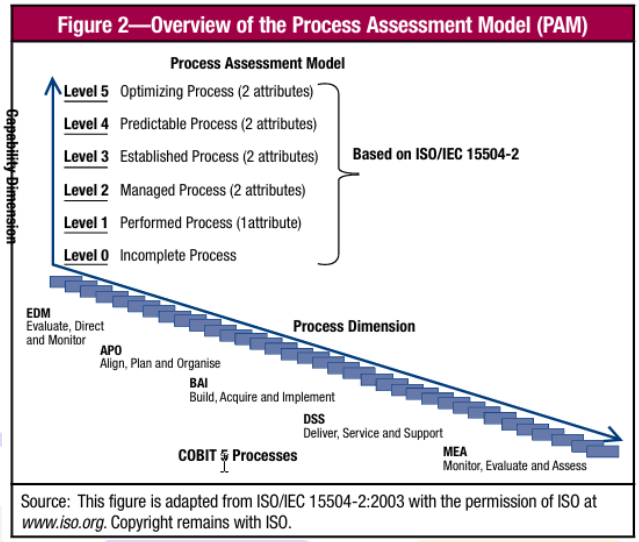
Menilai setiap atribut proses pada tiap *level*, mulai dari *level* 1 hingga *level* tertinggi. Masing-masing atribut dinilai berdasarkan tingkat pencapaiannya, lalu dikategorikan dalam empat tingkat: *Not achieved* (N), *Partially achieved* (P), *Largely achieved* (L), dan *Fully achieved* (F).Suatu *level* dianggap tercapai apabila seluruh atribut pada *level* tersebut mendapat nilai "Fully achieved" (F). Jika ada satu saja atribut yang belum F, maka *level* tersebut belum dianggap tercapai.

Tabel III.3 Skala Pencapaian

Kategori penilaian	Deskripsi	% Pencapaian
N	*Not achieved*	0% - 15%
P	*Partially achieved*	>15% - 50%
L	*Largely achieved*	>50% - 85%
F	*Fully achieved*	>85% - 100%

5) Perhitungan *Work Product* (WP)

Perhitungan nilai total dari sebuah produk dengan melihat beberapa aspek penting yang berbeda. Setiap aspek diberi nilai dan juga bobot sesuai seberapa penting aspek itu.Caranya, nilai setiap aspek dipangkatkan dengan bobotnya, lalu hasilnya dikalikan semua. Dari hasil perkalian ini, kita dapat melihat produk mana yang punya nilai terbaik berdasarkan aspek-aspek yang sudah dinilai. Contoh aspek yang ditentukan untuk *Work Product* (WP) yaitu SOP yang berjalan.



Gambar III.3 Sumber : COBIT 5 - *Process Asessment Method* (PAM)
Level Wp Product

6) Perhitungan *Maturity* Indeks

Tahapan ini melakukan analisis terhadap data kuesioner yang telah dikumpulkan, yang kemudian diolah untuk menghasilkan nilai indeks kematangan menggunakan pendekatan kuantitatif berdasarkan rumus yang relevan.[29]

Cara menghitungnya yaitu nilai *Work Product* (WP) yang diketahui dibagi Nilai *Work Product* (WP) Standar dari *Process Asesment Model* (PAM) di kali Indeks Kuesioner persubdomain, Rumus maturity indeks merujuk pada[30].

$$Maturity\ Index = \left(\frac{Nilai\ WP\ Aktual}{Nilai\ WP\ Standar}\right) x\ Indeks\ Kuesioner \quad (3)$$

Sumber : Kajian Ilmiah Informatika dan Komputer Audit Sistem Informasi Aplikasi Absensi Greatday Menggunakan *Framework* Cobit 5

Keterangan :

$Nilai\ WP\ Aktual$: Nilai tercapai dari Work Product berdasarkan dokumen

$Nilai\ WP\ Standar$: Nilai target Work Product sesuai COBIT 5 PAM

7) Perhitungan *Maturity Level*

Model Tingkat Kematangan (*Maturity* Model) kerangka yang digunakan untuk menghitung sejauh mana kematangan pengelolaan teknologi informasi di suatu organisasi.[31] Rumus *Maturity Level* merujuk pada [30].

$$Maturity\ Level = \frac{Total\ Maturity\ Indeks}{Jumlah\ Subdomain} \quad (4)$$

Sumber : Kajian Ilmiah Informatika dan Komputer Audit Sistem Informasi Aplikasi Absensi Greatday Menggunakan *Framework* Cobit 5

Keterangan :

$Total\ Maturity\ Indeks$: Merupakan rata-rata indeks kematangan dari seluruh subdomain dalam satu domain (misalnya DSS atau MEA)

$Jumlah\ Subdomain$: Total jumlah subdomain yang dievaluasi dalam satu domain

8) Perhitungan GAP

Perhitungan GAP digunakan untuk mengetahui selisih antara kondisi saat ini dengan kondisi yang diharapkan dalam suatu proses atau kinerja. Dengan kata lain, GAP menunjukkan berapa jauh proses atau hasil yang dicapai dibandingkan dengan target atau standar yang sudah ditentukan.

Cara menghitungnya yaitu dengan mengurangi nilai capaian saat ini dari nilai target yang diinginkan. Rumus mencari GAP merujuk pada[28]

$$GAP = Target\ Level - Capability\ Level \quad (5)$$

Sumber : Audit Sistem Informasi Absensi pada Kejaksaan Negeri Kota Bandung Menggunakan *Framework* Cobit 5

Keterangan :

$Target\ Level$: Nilai target yang ingin dicapai

$Capability\ Level$: Nilai yang dicapai

d. Pelaporan

Pelaporan *Audit* sistem informasi ini disusun sebagai bagian dari evaluasi terhadap tingkat kematangan tata kelola Teknologi Informasi (TI) yang diterapkan oleh PT Brainmatics Indonesia Cendekia. Laporan ini bertujuan untuk memberikan gambaran yang objektif mengenai sejauh mana proses-proses TI dalam organisasi telah memenuhi prinsip tata kelola yang baik sesuai dengan kerangka kerja COBIT 5, sekaligus menjadi bagian dari penyusunan skripsi. Melalui pendekatan berbasis COBIT 5, diharapkan hasil *Audit* ini dapat menjadi dasar dalam peningkatan kualitas pengelolaan Teknologi Informasi (TI) yang mendukung pencapaian tujuan strategis perusahaan.

3.2 *Framework*/Metode *Audit* Sistem Informasi

Pemetaan RACI bertujuan untuk menjelaskan peran dan tanggung jawab masing-masing individu atau tim dalam suatu proses atau proyek.Diagram RACI berasal dari *kata Responsible, Accountable, Consulted, dan Informed* yaitu sebuah matriks yang menunjukkan peran dan kekuasaan suatu organisasi atau perusahaan dalam proses pengambilan Keputusan.[32]

Tabel III.4 Penjelasan RACI

Simbol	Arti	Penjelasan
R	*Responsible*	Pihak yang melaksanakan tugas atau yang bertanggungjawab
A	*Accountable*	Pihak yang bertanggung jawab akhir terhadap hasil
C	*Consulted*	Pihak yang diberi konsultasi, biasanya memiliki keahlian atau informasi penting
I	*Informed*	Pihak yang diberi informasi tentang kemajuan atau hasil, tapi tidak ikut serta aktif

Diagram RACI dari setiap Subdomain PT Brainmatics Cendekia Indonesia, Keterangan diagram RACI yaitu :

Tabel III.5 RACI *Chart* COBIT 5 DSS01

DSS01 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
DSS01.01 Perform operational procedures.																					A		C	C	C	
DSS01.02 Manage outsourced IT services.											I							A			R					
DSS01.03 Monitor IT infrastructure.				I		C					I						C	I		C	A		C	C		
DSS01.04 Manage the environment.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS01.05 Manage facilities.						I					C	A				C	C	C	I	C	R		I	R	I	

Tabel III.6 RACI DSS01

DSS01
RACI *Chart*

Management Practice

	CEO	*Director of Learning*	*Deputy Director of Leaning*	*Deputy Director of Learning (Marketing)*	*Deputy Director of Development*	*Manager of Training*	*Manager of Development*	*Manager of Marketing*	*Specialist in Marketing*	*Specialist in Software*	*Specialist in Learning*	*Specialist in Training*
DSS01.01 *Perform Operational Procedure*	**I**	**C**				**C**	**A**			**R**	**R**	**R**
DSS01.02 *Manage Outsourced IT Service*	**I**	**I**			**A**		**R**		**C**	**C**		
DSS01.03 *Monitor IT Infrastructure*	**I**				**C**	**C**	**A**			**R**		**R**
DSS01.04 *Manage The Enviroment*	**I**		**C**		**C**	**A**	**A**	**A**	**R**	**R**	**R**	**R**
DSS01.05 *Manage Facilities*	**I**		**C**	**C**		**A**	**A**	**A**			**R**	**R**

Tabel 7 RACI *Chart* COBIT 5 DSS02

DSS02 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
DSS02.01 Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
DSS02.03 Verify, approve and fulfil service requests.						R												I		R	R		A			
DSS02.04 Investigate, diagnose and allocate incidents.						R					I	I				I	I	I		C	R		A	C		
DSS02.05 Resolve and recover from incidents.						I					I	I				C	C	I		R	R		A	R		C
DSS02.06 Close service requests and incidents.						I					I	I				I	I	I		I	A		I	R		I
DSS02.07 Track status and produce reports.						I					I	I				I	I	I		I	A		R	I		

Pembagian tanggung jawab dalam proses pengelolaan operasional teknologi informasi berdasarkan praktik manajemen COBIT 5 pada subdomain DSS01 menunjukkan adanya struktur kolaboratif yang terorganisasi dengan baik. Dalam aktivitas mulai dari pelaksanaan prosedur operasional (DSS01.01) hingga pengelolaan fasilitas Teknologi Informasi (TI) (DSS01.05), peran sebagai penanggung jawab *(Accountable/A)* secara konsisten diemban oleh *Manager of Training*, yang mencerminkan peran strategisnya dalam memastikan kelangsungan operasional serta penerapan standar layanan yang efektif.

Tugas pelaksanaan *(Responsible/R)* didistribusikan kepada beberapa pihak teknis seperti *Specialist in Software, Specialist in Learning, dan Specialist in Training*, yang bertanggung jawab langsung dalam eksekusi

operasional sehari-hari termasuk pengawasan infrastruktur, layanan *outsourcing*, dan manajemen lingkungan kerja TI.

Tabel III.8 RACI DSS02

DSS02
RACI *Chart*

Management Practice

	CEO	Director of Learning	Deputy Director of Leaning	Deputy Director of Learning (Marketing)	Deputy Director of Development	Manager of Training	Manager of Development	Manager of Marketing	Specialist in Marketing	Specialist in Software	Specialist in Learning	Specialist in Training
DSS01.02 *Define Incident And Service Request Classification Schemes*	I				A		R			C		C
DSS02.02 *Record, Classify And Prioritise Requests And Incident*					I	C	A			R		C
DSS02.03 *Verify, Approve And Fulfil Service Requests*		I	I		A	C	R					C
DSS02.04 *Investigate, diagnose and allocate incidents*		I	I			C	A			R		C
DSS02.05 *Resolve and recover from incidents*		I				C	A			R		C
DSS02.06 *Close service requests and incidents*	I	I	I		C	C	A			R		
DSS02.07 *Track status and produce reports*	I	I	I			C	A			R		C

Pembagian tanggung jawab dalam proses penanganan permintaan layanan dan insiden berdasarkan praktik manajemen COBIT 5 menunjukkan struktur pengelolaan yang jelas dan kolaboratif. Dalam aktivitas seperti pendefinisian skema klasifikasi permintaan dan insiden (DSS02.01) hingga verifikasi dan pemenuhan permintaan layanan (DSS02.03), peran utama

sebagai penanggung jawab *(Accountable/A)* secara konsisten dipegang oleh *Deputy Director of Learning*, yang menunjukkan kepemimpinan strategis dalam pengambilan keputusan terkait penanganan layanan TI.

Tugas pelaksanaan *(Responsible/R)* secara dominan dijalankan oleh *Manager of Training*, yang berperan penting dalam mengoordinasikan proses teknis serta memastikan respons yang cepat dan tepat terhadap insiden yang terjadi.

Tabel III.9 RACI *Chart* COBIT 5 DSS03

DSS03 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
DSS03.01 Identify and classify problems.					I	C					I	I				I	I	R	C	R	R		A	C		
DSS03.02 Investigate and diagnose problems.											I	I							C	C	A		R	R		
DSS03.03 Raise known errors.																					A		R	R		
DSS03.04 Resolve and close problems.					I	C					I	I				C	C	I	C	C	R		A			
DSS03.05 Perform proactive problem management.						C													C	C	R		A			

Tabel III.10 RACI DSS03

DSS03 **RACI *Chart***

Management Practice

	CEO	*Director of Learning*	*Deputy Director of Leaning*	*Deputy Director of Learning (Marketing)*	*Deputy Director of Development*	*Manager of Training*	*Manager of Development*	*Manager of Marketing*	*Specialist in Marketing*	*Specialist in Software*	*Specialist in Learning*	*Specialist in Training*
DSS03.01 *Identify and classify problems*	**I**	**I**				**C**	**A**			**R**		**C**
DSS03.02 *Investigate and diagnose problems*		**I**	**I**		**C**	**C**	**A**			**R**		
DSS03.03 *Raise known errors*		**I**	**I**			**C**	**A**			**R**		**C**
DSS03.04 *Resolve and close problems*	**I**	**I**			**C**	**C**	**A**			**R**		
DSS03.05 *Perform proactive problem management*		**I**			**A**	**C**	**R**			**C**		**C**

Pembagian tanggung jawab dalam proses manajemen masalah berdasarkan praktik manajemen COBIT 5. Dalam aktivitas seperti identifikasi masalah (DSS03.01) hingga manajemen proaktif atas masalah (DSS03.05), peran utama sebagai penanggung jawab *(Accountable/A)* secara konsisten dilakukan oleh *Manager of Development*, menegaskan otoritas manajerial dalam penyelesaian masalah operasional yang berdampak terhadap layanan TI.

Tugas *(Responsible/R)* mayoritas berada pada *Specialist in Software*, mencerminkan keterlibatan teknis langsung dalam proses identifikasi, investigasi, dan penyelesaian masalah. Beberapa peran lain *seperti Specialist in Learning* dan *Deputy Director of Development* juga ikut berkontribusi sebagai pihak yang dikonsultasikan *(Consulted/C)* atau diberi informasi *(Informed/I)* untuk memastikan transparansi dan kolaborasi lintas unit.

Tabel III.11 Tabel RACI *Chart* COBIT 5 DSS04

DSS04 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
DSS04.01 Define the business continuity policy, objectives and scope.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Maintain a continuity strategy.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Develop and implement a business continuity response.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Exercise, test and review the BCP.					I	R									I		R	R		C	R				A	
DSS04.05 Review, maintain and improve the continuity plan.				A	I	R					I							R		C	R				R	
DSS04.06 Conduct continuity plan training.					I	R												R		R	R	R			A	
DSS04.07 Manage backup arrangements.											I									C	A				R	
DSS04.08 Conduct post-resumption review.					C	R					I							R	C	C	R	R			A	

Tabel III.12 RACI DSS04

DSS04
RACI *Chart*

Management Practice

	CEO	***Director of Learning***	***Deputy Director of Leaning***	***Deputy Director of Learning (Marketing)***	***Deputy Director of Development***	***Manager of Training***	***Manager of Development***	***Manager of Marketing***	***Specialist in Marketing***	***Specialist in Software***	***Specialist in Learning***	***Specialist in Training***
DSS04.01 *Define the business continuity policy, objectives and scope*	**C**	**A**			**R**		**C**			**I**		**I**
DSS04.02 *Maintain a continuity strategy*	**I**	**I**			**A**	**C**	**R**			**A**		**C**
DSS04.03 *Develop and implement a business continuity response*					**I**	**C**	**A**			**R**		**C**

DSS04.04 *Exercise, test and Review the* BCP	**I**	**I**					**C**	**A**			**R**			**C**		
DSS04.05 *Review*, maintain and improve the continuity plan	**I**	**I**				**A**		**R**			**C**			**C**		
DSS04.06 *Conduct continuity plan Training*		**A**	**I**				**R**	**C**					**C**	**C**		
DSS04.07 *Manage backup arrangements*	**I**	**I**				**A**	**C**				**R**			**C**		
DSS04.08 *Conduct post-resumption Review*					**I**	**C**		**A**			**R**			**C**		

Pembagian tanggung jawab dalam pengelolaan keberlangsungan layanan Teknologi Informasi (TI) *(business continuity)* berdasarkan kerangka kerja COBIT 5. Aktivitas seperti penyusunan kebijakan dan ruang lingkup keberlanjutan layanan (DSS04.01) hingga tinjauan pasca-pemulihan (DSS04.08) menunjukkan bahwa tanggung jawab utama *(Accountable/A)* banyak diemban oleh *Manager of Development*, yang menjadi pihak sentral dalam menjamin keberlanjutan operasional organisasi.

Tugas pelaksana *(Responsible/R)* didistribusikan kepada beberapa peran, seperti *Deputy Director of Development*, *Specialist in Learning*, dan *Specialist in Training,* yang terlibat langsung dalam implementasi dan pelatihan rencana keberlangsungan bisnis *Business Continuity Plan* (BCP). Sementara itu, peran CEO dan beberapa manajer lainnya seperti *Manager of Marketing* serta *Director of Learning* lebih banyak ditempatkan sebagai pihak *Consulted (C) atau Informed (I)* dalam aktivitas yang berkaitan dengan kebijakan dan strategi berkelanjutan.

Tabel III.13 RACI *Chart* COBIT 5 DSS05

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

Tabel III.14 RACI DSS05

DSS05
RACI *Chart*

Management Practice

	CEO	***Director of Learning***	***Deputy Director of Leaning***	***Deputy Director of Learning (Marketing)***	***Deputy Director of Development***	***Manager of Training***	***Manager of Development***	***Manager of Marketing***	***Specialist in Marketing***	***Specialist in Software***	***Specialist in Learning***	***Specialist in Training***
DSS05.01 *Protect against Malware*	**I**	**I**					**A**			**R**		**C**
DSS05.02 *Manage network and connectivity security*	**I**	**I**			**C**		**A**			**R**	**C**	**C**
DSS05.03 *Manage endpoint security*	**I**	**I**			**C**		**A**			**C**	**C**	**R**
DSS05.04 *Manage user identity and logical access*	**I**	**A**	**C**	**C**	**R**				**C**	**C**	**C**	**C**

DSS05.05 *Manage physical access to IT assets*	**I**		**C**		**A**	**C**	**R**			**C**				
DSS05.06 *Manage sensitive documents and output devices*	**I**	**A**	**C**			**R**				**C**		**C**		
DSS05.7 *Monitor the infrastructure for security-related events*	**I**						**A**			**R**		**C**		

Pembagian peran dan tanggung jawab dalam pengelolaan layanan keamanan sistem informasi. Aktivitas manajemen seperti perlindungan terhadap *Malware* (DSS05.01), keamanan jaringan (DSS05.02), hingga pemantauan infrastruktur keamanan (DSS05.07) menunjukkan bahwa *Manager of Development* secara konsisten ditetapkan sebagai pihak yang paling bertanggung jawab *(Accountable/A)* dalam memastikan implementasi dan keberlangsungan kontrol keamanan.

Tugas pelaksana utama *(Responsible/R)* didominasi oleh Specialist in Software, yang menunjukkan keterlibatan teknis langsung dalam pelaksanaan pengamanan infrastruktur TI, seperti pengelolaan akses, perlindungan dokumen sensitif, serta mitigasi risiko keamanan digital lainnya. Peran lain seperti *Manager of Marketing, Deputy Director of Learning, dan Specialist in Training* juga berkontribusi sebagai pihak *Consulted (C)* maupun *Informed (I),* tergantung pada jenis aktivitas yang dilakukan.

Tabel III.15 *Chart* COBIT 5 DSS06

DSS06 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
DSS06.01 Align control activities embedded in business processes with enterprise objectives.		C	C	C	A	R					I	I				C	C	C			C		C	C		C
DSS06.02 Control the processing of information.		R	R	R	A	R					I	I				C	C	C			C		C	C		
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.			R		A	R						I			I	C	C	C			C		C	R		C
DSS06.04 Manage errors and exceptions.				I	I	A										C	C	I			C		R			
DSS06.05 Ensure traceability of information events and accountabilities.					C	A						I				C	C	C			C		C	C		
DSS06.06 Secure information assets.			C	C	C	A					I	I				C	C	C			C			C	C	C

Tabel III.16 RACI DSS06

DSS06
RACI *Chart*

Management Practice

	CEO	*Director of Learning*	*Deputy Director of Leaning*	*Deputy Director of Learning (Marketing)*	*Deputy Director of Development*	*Manager of Training*	*Manager of Development*	*Manager of Marketing*	*Specialist in Marketing*	*Specialist in Software*	*Specialist in Learning*	*Specialist in Training*
DSS06.01 *Align control activities embedded in business processes with enterprise objectives*	**I**	**I**			**A**		**R**			**C**		
DSS06.02 *Control the processing of information*			**I**			**C**	**A**			**R**		
DSS06.03 *Manage roles, responsibilities, access privileges and levels of authority*	**I**	**A**				**R**						**C**

DSS06.04 *Manage errors and exceptions*			**I**			**C**	**A**			**R**		**C**
DSS06.05 *Ensure traceability of information events and accountabilities*	**I**		**A**			**C**	**R**			**C**		
DSS06.06 *Secure information assets*		**C**			**I**		**A**			**R**		

Pembagian peran dalam pengelolaan aktivitas kontrol bisnis yang berhubungan dengan sistem informasi. Dalam praktik manajemen seperti pengendalian pemrosesan informasi (DSS06.02) hingga pengamanan aset informasi (DSS06.06), tanggung jawab utama *(Accountable/A)* umumnya berada di tangan *Manager of Development*, menandakan posisi strategis dalam memastikan kelangsungan kontrol operasional yang sejalan dengan tujuan bisnis.

Peran pelaksana utama *(Responsible/R)* banyak diemban oleh *Specialist in Software*, menunjukkan keterlibatan langsung dalam teknis pengelolaan kontrol dan keamanan sistem. Selain itu, *Manager of Marketing* dan *Specialist in Learning* juga turut terlibat sebagai pihak *Consulted (C)* atau *Informed (I),* yang mencerminkan adanya komunikasi serta koordinasi antarunit dalam mendukung implementasi kontrol yang efektif.

Tabel III.17 *Chart* COBIT 5 MEA01

MEA01 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
MEA01.01 Establish a monitoring approach.		A	R	R	R	I	C		I						C	C	C	R	I	C	C	I	C	I	I	I
MEA01.02 Set performance and conformance targets.		I	I	I	A	R			I						C			C	C	R	R	I	R	I	I	I
MEA01.03 Collect and process performance and conformance data.					C	R			I						C			A		R	R	I	R	I	I	I
MEA01.04 Analyse and report performance.					A	R			C						C	C	C	C	C	R	R	C	R	C	C	C
MEA01.05 Ensure the implementation of corrective actions.	I	I	I	I	C	R			C						C	C	C	A	C	R	R	C	R	C	C	C

Tabel III.18 RACI MEA01

MEA01
RACI *Chart*

Management Practice

	CEO	***Director of Learning***	***Deputy Director of Leaning***	***Deputy Director of Learning (Marketing)***	***Deputy Director of Development***	***Manager of Training***	***Manager of Development***	***Manager of Marketing***	***Specialist in Marketing***	***Specialist in Software***	***Specialist in Learning***	***Specialist in Training***
MEA01.01 *Monitor internal controls*	**I**	**I**			**A**		**R**			**C**		**C**
MEA01.02 *Review* business *Process Controls* effectiveness		**I**			**A**	**C**	**R**			**C**		
MEA01.03 *Perform control self-assessment*		**I**				**C**	**A**			**R**		**C**
MEA01.04 *Identify and report control deficiencies*			**C**		**I**		**A**			**R**		**C**
MEA01.05	**A**	**R**	**C**			**I**	**I**	**I**		**R**		

Ensure that assurance providers are independent and qualified

Pembagian tanggung jawab dalam kegiatan pemantauan dan penilaian sistem pengendalian *internal* di organisasi. Dalam aktivitas seperti *Monitoring* kontrol *internal* (MEA01.01) hingga memastikan independensi *assurance provider* (MEA01.05), terlihat bahwa peran *Accountable (A)* secara konsisten dipegang oleh *Manager of Training*, yang menandakan tanggung jawab utama pengambilan keputusan berada di *level* manajerial.

Pelaksanaan kegiatan teknis *(Responsible*) umumnya dilakukan oleh *Deputy Director of Learning (Marketing)* atau *Specialist in Software*. Pihak lain seperti CEO, *Director of Learning, dan Manager of Development* peran *Consulted (C) dan Informed (I)*, menunjukkan adanya komunikasi dua arah dan keterlibatan lintas fungsi.

Tabel III.19 *Chart* COBIT 5 MEA02

MEA02 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
MEA02.01 Monitor internal controls.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.02 Review business process controls effectiveness.	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
MEA02.03 Perform control self-assessments.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
MEA02.05 Ensure that assurance providers are independent and qualified.						R										A	A	R								
MEA02.06 Plan assurance initiatives.		A			C	R			C							C	C	R	C	C	C	C	C	C	C	C
MEA02.07 Scope assurance initiatives.				R	R	R			C							C	A	R	C	C	C	C	C	C	C	C
MEA02.08 Execute assurance initiatives.	I	I			C	R			C		I	I				C	A	R	C	C	C	C	C	C	C	C

Tabel III.20 RACI MEA02

MEA02
RACI *Chart*

Management Practice

	CEO	Director of *Learning*	Deputy Director of Leaning	Deputy Director of *Learning* (Marketing)	Deputy Director of Development	*Manager of Training*	*Manager* of Development	*Manager* of Marketing	Specialist in Marketing	Specialist in Software	Specialist in *Learning*	Specialist in *Training*
MEA02.01 *Monitor internal controls*	I	C				C	A			R		
MEA02.02 *Review* business *Process Controls* effectiveness		I			A		R				C	C
MEA02.03 *Perform control self-assessment*			I				A			R		C
MEA02.04 *Identify and report control deficiencies*					I		A			R	C	C
MEA02.05 *Ensure that assurance providers are independent and qualified*	A	R	C			I	I	I				
MEA02.06 *Plan assurance initiatives*	I	A			C		R			C		
MEA02.07 *Scope assurance initiatives*		C	C		I	I	A	I		R		
MEA02.08 *Execute assurance initiatives*		I					A			R	C	C

Pembagian tanggung jawab dalam aktivitas pengawasan dan penjaminan mutu *internal*. Aktivitas seperti *Monitoring* kontrol *internal* (MEA02.01) hingga pelaksanaan inisiatif assurance (MEA02.08) melibatkan kolaborasi antara jajaran manajemen dan tim spesialis.

Peran *Accountable* (A) umumnya dipegang oleh *Manager of Training*, sementara *Specialist in Learning* dan *Specialist in Software* berperan sebagai *Responsible (R)* untuk pelaksanaan teknis. Adapun D*irector of Learning dan Manager*

of Development berfungsi sebagai pihak yang *Consulted (*C*) atau Informed* (I) dalam mendukung efektivitas proses pengendalian dan assurance.

Tabel III.21 *Chart* COBIT 5 MEA03

MEA03 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
MEA03.01 Identify external compliance requirements.					A	R										R	R	R								R
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C

Tabel III.22 RACI MEA03

MEA03
RACI *Chart*

Management Practice

	CEO	***Director of Learning***	***Deputy Director of Leaning***	***Deputy Director of Learning (Marketing)***	***Deputy Director of Development***	***Manager of Training***	***Manager of Development***	***Manager of Marketing***	***Specialist in Marketing***	***Specialist in Software***	***Specialist in Learning***	***Specialist in Training***
MEA03.01 Identify external compliance requirement	**C**	**C**		**I**			**A**			**C**	**R**	**R**
MEA03.02 Optimise response to external requirement	**I**	**A**	**C**			**I**	**R**	**I**		**C**		
MEA03.03 Confirm external compliance	**C**	**C**			**C**		**A**		**I**	**I**	**I**	**R**

MEA03.04 Obtain assurance of external compliance	**A**		**C**			**R**	**I**		**I**		**I**		**C**

Pembagian peran berdasarkan RACI *Chart* pada Subdomain MEA03, yang mencakup aktivitas pemenuhan kepatuhan terhadap regulasi *Eksternal*. Dalam aktivitas MEA03.01 dan MEA03.03, peran utama *(Accountable)* dipegang oleh *Manager of Training*, dengan pelaksana teknis (*Responsible)* seperti *Specialist in Learning* dan *Specialist in Training*. Sedangkan pada MEA03.04, tanggung jawab utama dialihkan ke *Director of Learning* dengan dukungan dari beberapa pihak teknis dan manajemen.