Analisis Perancangan Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 Pada Pt Xyz Pada Objektif Apo13 Dan Dss05

1st Aisyah Wulan Aydila
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
aisyahaydila@student.telkomuniversity.ac.id

2nd Widyatasya Agustika Nurtrisha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
widyatasyaelkomuniversity.ac.id

3rd Dhata Praditya
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
dhatap@telkomuniversity.ac.id

***Abstrak*— Di era digital yang terus berkembang, teknologi informasi (TI) menjadi krusial bagi kelangsungan operasional perusahaan di berbagai sektor. Penelitian ini bertujuan untuk menganalisis penerapan tata kelola TI di PT XYZ, terutama dalam aspek keamanan informasi, menggunakan kerangka kerja COBIT 2019. Fokus penelitian ini adalah pada objektif APO13 (Managed Security) dan DSS05 (Managed Security Services). Evaluasi menunjukkan bahwa PT XYZ telah mencapai tingkat kapabilitas yang memadai di beberapa area, namun terdapat kekurangan dalam pengelolaan keamanan jaringan, titik akhir, dan akses informasi. Rekomendasi yang diberikan mencakup aspek people, process, dan technology, dengan saran untuk perbaikan kebijakan, prosedur, dan penerapan teknologi guna meningkatkan keamanan informasi. Hasil penelitian ini diharapkan dapat membantu PT XYZ dalam mencapai standar tata kelola TI yang lebih baik dan meningkatkan daya saing perusahaan di pasar.**

***Kata kunci*— APO13, COBIT 2019, DSS05, Tata Kelola Teknologi Informasi**

I. PENDAHULUAN

Pada era digital yang terus berkembang, keberadaan teknologi informasi (TI) telah menjadi fokus utama bagi kelangsungan operasional perusahaan di berbagai sektor industri. TI tidak hanya memungkinkan perusahaan untuk meningkatkan efisiensi dan efektivitas operasional, tetapi juga untuk mempermudah pengguna dalam melakukan pekerjaan, dapat memecah masalah yang dihadapi pengguna, membuka kreativitas, efektivitas dan efisiensi dalam melakukan pekerjaan. Dalam konteks ini, IT *Governance* (Tata Kelola TI) dalam ITGID (2019) menjadi semakin krusial. Tata Kelola TI merupakan serangkaian proses yang bertujuan untuk memantau dan mengendalikan kemampuan pengambilan keputusan teknologi informasi, dengan tujuan memastikan bahwa teknologi informasi memberikan nilai yang optimal kepada pemangku kepentingan utama dalam suatu organisasi. Konsep ini diperkuat dengan penjelasan Weill dan Ross (2004) tentang tata kelola teknologi informasi sebagai penentuan hak keputusan dan akuntabilitas dalam kerangka kerja yang mendukung penggunaan teknologi informasi sesuai dengan yang diinginkan.[1]

PT XYZ sebagai salah satu perusahaan terkemuka di Indonesia, terutama dalam industri pertahanan yang sangat strategis, tidak dapat mengabaikan peran vital TI dalam menjaga posisinya di pasar. Untuk mempertahankan dan meningkatkan daya saingnya, PT XYZ, telah mengambil langkah-langkah strategis dengan mengadopsi dan mengelola berbagai sistem TI yang mendukung berbagai aspek bisnisnya. Menurut laporan tahunan PT XYZ tahun 2023, PT XYZ telah melakukan peningkatan kapasitas dan kapabilitas melalui pengembangan dan atau peningkatan infrastruktur, solusi, layanan teknologi informasi, serta manajemen keamanan informasi. Selain itu, PT XYZ juga meningkatkan manajemen layanan TI melalui penerapan IT Service *Management*. Program-program Teknologi Informasi yang telah dilakukan senantiasa dievaluasi secara berkala, salah satunya melalui *assessment* Tata Kelola TI dengan perolehan skor 3,4 (*Defined*) yang menandakan bahwa proses yang diterapkan telah mencapai tujuan yang dengan didukung oleh payung regulasi yang jelas.[2]

Dalam konteks ini, penting untuk memperbarui analisis implementasi tata kelola TI di PT XYZ dengan menggunakan kerangka kerja terbaru. Salah satu kerangka kerja yang dianggap relevan dan terkemuka dalam analisis tata kelola TI adalah *Control Objectives for Information and Related Technologies* (COBIT) 2019. COBIT 2019 memberikan pedoman dan panduan yang komprehensif untuk pengelolaan TI yang efektif, memastikan bahwa perusahaan mematuhi standar industri dan praktik terbaik. Objektif APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*) dalam COBIT 2019 menjadi fokus utama dalam penelitian ini. Keamanan informasi merupakan prioritas utama bagi PT XYZ, terutama dalam menghadapi tantangan serius terkait keamanan data sensitif dan kritis di industri pertahanan.

Penelitian ini bertujuan untuk menganalisis implementasi tata kelola TI, khususnya dalam pengelolaan keamanan informasi, dengan menggunakan kerangka kerja COBIT 2019 di PT XYZ. Dari hasil analisis kondisi saat ini dan target yang ditetapkan, penelitian ini akan memberikan

rekomendasi untuk meningkatkan kapabilitas PT XYZ agar sesuai dengan target yang ditetapkan. Pemilihan kerangka kerja COBIT 2019 dilakukan karena kesesuaian perkembangan teknologi informasi, serta kemampuannya untuk menyesuaikan diri dengan kerangka kerja manajemen TI lain yang diterapkan oleh perusahaan, sehingga memungkinkan adaptasi yang lebih baik untuk meningkatkan implementasi yang efektif.

Oleh karena itu, peneliti melakukan penelitian tata kelola teknologi informasi pada PT XYZ dengan judul "Analisis Implementasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 pada PT XYZ pada Objektif APO13 dan DSS05". Hasil dari penelitian ini diharapkan dapat membantu perusahaan untuk menjadikan tata kelola TI PT XYZ mencapai standar terkini sesuai dengan tujuan perusahaan.

II. KAJIAN TEORI

A. Tata Kelola TI

Menurut Weill dan Ross (2004), tata kelola TI adalah hak keputusan dan kerangka akuntabilitas untuk mendorong perilaku yang diinginkan dalam penggunaan TI. Tata kelola TI mencerminkan prinsip tata kelola perusahaan yang lebih luas dengan fokus pada pengelolaan dan penggunaan TI untuk mencapai tujuan kinerja perusahaan.[1]

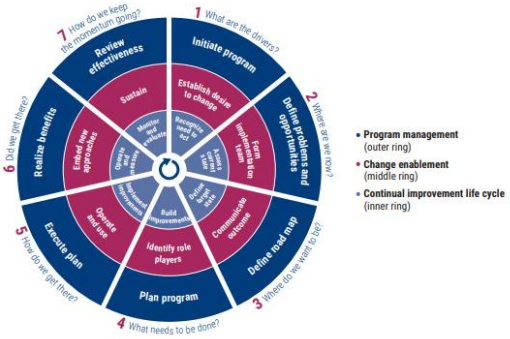
Mengingat pentingnya hal ini bagi manajemen risiko perusahaan dan penciptaan nilai, tata kelola informasi dan teknologi perusahaan (EGIT) telah menjadi fokus penting untuk manajemen risiko dan penciptaan nilai. EGIT, sebagai bagian dari tata kelola perusahaan, diterapkan oleh dewan direksi untuk memastikan proses, struktur, dan hubungan organisasi yang efektif. Hal ini membantu pemangku kepentingan bisnis dan TI memenuhi tanggung jawab mereka dalam menyelaraskan bisnis dengan TI dan menciptakan nilai melalui investasi IT.

B. COBIT 2019

COBIT (*Control Objectives for Information and Related Technology*) merupakan kerangka kerja untuk tata kelola dan pengelolaan informasi dan teknologi yang ditujukan untuk seluruh perusahaan. IT perusahaan mencakup semua teknologi dan pemrosesan informasi yang diterapkan perusahaan untuk mencapai tujuannya. Kerangka kerja COBIT dengan jelas membedakan antara tata kelola dan pengelolaan. Kedua prinsip ini mencakup aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda, dan memenuhi tujuan yang berbeda.[3]

C. COBIT 2019 *Implementation Guide*

COBIT 2019 *Implementation Guide* menekankan pandangan seluruh perusahaan mengenai tata kelola IT, karena IT sendiri sudah menyebar luas ke perusahaan-perusahaan dan merupakan praktik yang baik untuk membedakan bisnis dan aktivitas terkait IT. Tata kelola dan manajemen IT harus menjadi bagian integral dari tata kelola perusahaan, mencakup semua tanggung jawab bisnis dan fungsi IT secara menyeluruh.[3]



GAMBAR I
COBIT 2019 *Implementation Guide*

Phase 1 – What Are the Drivers
Mengidentifikasi pendorong perubahan dari kondisi eksternal dan internal untuk mendorong perubahan di tingkat manajemen eksekutif dengan COBIT 2019.
Phase 2 - Where Are We Now?
Menyelaraskan tujuan IT dengan strategi perusahaan dan memprioritaskan proses untuk mencapai tujuan tata kelola optimal.
Phase 3 - Where Do We Want to Be?
Menetapkan target perbaikan dan menganalisis kesenjangan untuk menemukan solusi potensial.
Phase 4 - What Needs to Be Done?
Merencanakan solusi yang praktis dan mendefinisikan proyek yang didukung oleh kasus bisnis.
Phase 5 - How Do We Get There?
Mengimplementasikan solusi dan menetapkan sistem pemantauan untuk memastikan keselarasan bisnis.
Phase 6 - Did We Get There?
Memastikan transisi ke operasi normal dan memantau perbaikan dengan metrik kinerja.
Phase 7 - How Do We Keep the Momentum Going?
Meninjau kesuksesan inisiatif dan mendorong perbaikan berkelanjutan.

D. *Managed Security*

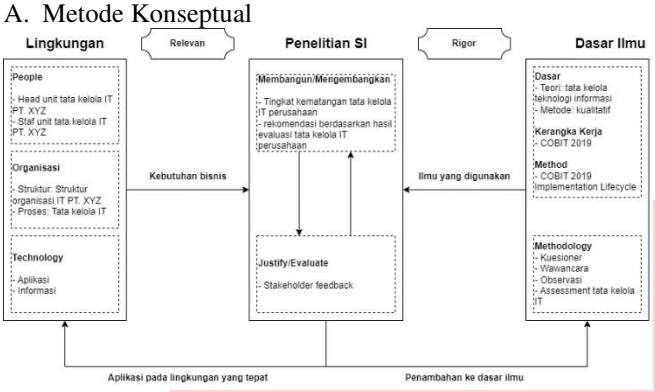
Managed Security dalam COBIT merujuk pada tindakan-tindakan seperti mendefinisikan, mengoperasikan dan memantau sistem manajemen keamanan informasi. Proses ini bertujuan untuk meminimalkan risiko insiden keamanan informasi dan memastikan bahwa dampak dari insiden tersebut sesuai dengan toleransi risiko yang ditetapkan oleh perusahaan.[4]

E. *Managed Security Services*

Managed Security Services dalam COBIT melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Menetapkan dan memelihara keamanan informasi dan hak akses, serta melakukan pemantauan keamanan. Tujuannya adalah untuk meminimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.[4]

III. METODE

A. Metode Konseptual



GAMBAR II
Metode Konseptual

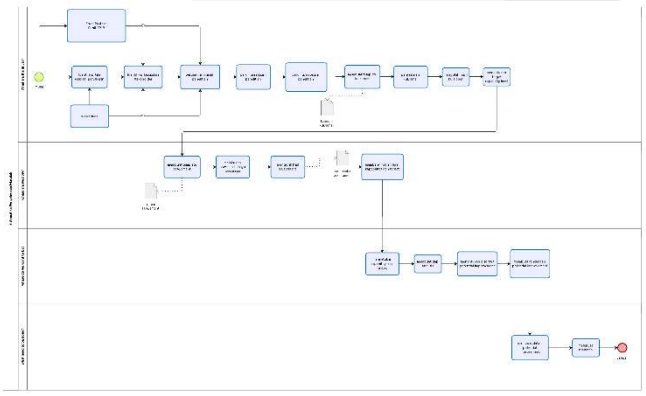
Penelitian ini dimulai dengan tiga aspek utama: *people, organization,* dan *technology*. Pertama, aspek lingkungan (*environment*) berfokus pada kebutuhan bisnis PT XYZ, dengan responden utama berupa kepala dan staf unit tata kelola TI. Kedua, aspek organisasi (*organization*) meneliti PT XYZ sebagai objek penelitian, sementara aspek teknologi (*technology*) menggunakan aplikasi dan informasi perusahaan.

Aspek dasar ilmu didasarkan pada teori tata kelola TI dan menggunakan metode kualitatif. Siklus implementasi COBIT 2019 menjadi landasan teoritis, dengan fokus pada empat tahap: *What are the drivers, Where are we now, Where do we want to be,* dan *What needs to be done*. Metode penelitian mencakup kuesioner dan wawancara dengan pemangku kepentingan di PT XYZ.

Setelah ketiga aspek ini terpenuhi, langkah berikutnya adalah menganalisis tingkat kematangan tata kelola TI dan menyusun rekomendasi berdasarkan hasil evaluasi, dengan masukan dari stakeholder pada tahap *justify/evaluate.*

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah dalam penelitian ini menggunakan framework COBIT 2019 dan mencakup tujuh fase. Namun, penelitian ini hanya fokus pada fase 1 hingga 4, karena ruang lingkupnya hanya mencakup tahap perancangan. Fase 5 dan seterusnya, yang berhubungan dengan implementasi, tidak menjadi fokus penelitian ini.



GAMBAR III
Sistematika Penyelesaian Masalah

C. Pengumpulan Data

Penelitian ini mengumpulkan data melalui dua metode: data primer dan sekunder. Data primer didapat dari wawancara dengan kepala unit tata kelola TI PT XYZ selama 1 minggu di bulan Mei, serta kuesioner berbasis framework COBIT 2019 yang disebarkan kepada kepala unit dan staf selama bulan April. Responden dipilih berdasarkan jabatan dan peran mereka. Data sekunder diperoleh dari literatur seperti buku, jurnal, dan artikel untuk memvalidasi informasi dari data primer.

D. Pengolahan Data

Setelah mengumpulkan data, peneliti akan mengelola informasi dari stakeholder PT XYZ dengan menggunakan daftar pertanyaan wawancara dan template *assessment* berbasis COBIT 2019. Data akan dianalisis secara kualitatif, dan hasil kuesioner akan diolah dengan Excel sesuai standar ISACA COBIT 2019 untuk menentukan *design factor* dan *target capability level*. Peneliti akan melakukan analisis kesenjangan (*Gap Analysis*) untuk mengidentifikasi perbedaan antara kondisi eksisting dan target, dan memberikan saran untuk perbaikan. Proses ini bertujuan menghasilkan analisis yang akurat sesuai kondisi lapangan.

E. Metode Evaluasi

Setelah data dikumpulkan dan diolah, peneliti akan mengevaluasi hasil dengan umpan balik dari stakeholder PT XYZ. Umpan balik ini memastikan bahwa hasil penelitian sesuai dengan tujuan dan kebutuhan perusahaan.

IV. HASIL DAN PEMBAHASAN

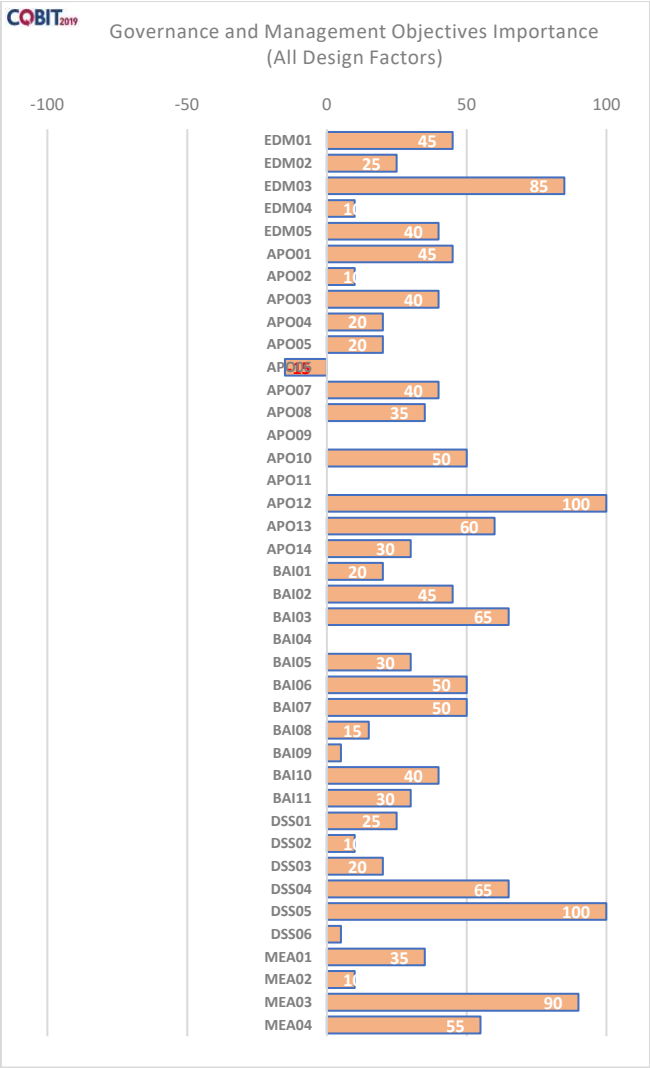
Proses analisis data dalam penelitian ini merujuk pada langkah yang dilakukan setelah pengumpulan data selesai. Tahapan ini menjadi dasar bagi penyusunan rekomendasi dalam penelitian, sehingga analisis data bukan hanya merupakan tahap penting dalam proses penelitian, tetapi juga menjadi fondasi yang kokoh untuk pengambilan keputusan yang informatif dan relevan.

A. *Phase 1 – Recognized Need to Act*

Dalam tugas akhir ini, peneliti mengacu pada sumber utama COBIT 2019, yaitu *Implementing and Optimizing an Information and Technology Governance Solution*. Proses implementasi dimulai dengan menjawab pertanyaan "*What are the drivers*?" pada fase 1 untuk mengidentifikasi faktor pendorong penerapan COBIT 2019 dan memastikan fokus pada manfaat dan realisasi program. Analisis dilakukan terhadap *design factor*, yaitu faktor-faktor yang mempengaruhi desain sistem tata kelola dan keberhasilan penggunaan IT. [5]

1. Pemilihan Domain

Penilaian ini menetapkan obektif inti di PT XYZ dengan 40 proses yang diberi nilai. Nilai tinggi menunjukkan pentingnya proses, sementara nilai negatif menandakan prioritas yang lebih rendah. Gambar dibawah menunjukkan hasil penilaian 10 faktor desain, visualisasi nilai setiap obektif, dan fokus utama perusahaan untuk mencapai tujuan strategis.



GAMBAR IV
Hasil *Design Factor* Tata Kelola TI

Penelitian ini membatasi fokus pada objektif proses dari *Governance and Management Objectives*, dengan menilai domain *Information Security:* APO13 *Managed Security* dan DSS05 *Managed Security Service* menggunakan COBIT 2019. Kedua domain ini dipilih berdasarkan penilaian *design factor* yang menunjukkan kepentingannya bagi PT XYZ untuk mencapai target.

TABEL I
Pemilihan Domain dan Proses

Score	*Objektif*	*Governance/Management Objective Priority*	*Target Capability Level*
60	APO13	*Managed Security*	3
100	DSS05	*Managed Security Service*	4

B. *Phase 2 – Assess Curent State*

Pada tahap ini, dilakukan analisis kondisi eksisting tata kelola TI di PT XYZ dengan mengevaluasi proses objektif APO13 dan DSS05. Penilaian dilakukan melalui wawancara dengan stakeholder dari Divisi Teknologi Informasi, khususnya Manajemen Keamanan TI dan *Cyber*. Hasil *assessment capability level* yang telah didapatkan adalah sebagai berikut:

TABEL II
Hasil *Assessment Capability Level* APO13

APO13 – *Manage Security*				
No	**Aktivitas**	**Pencapaian**	**Level Kapabilitas**	**Target**
1	APO13.01 Pembangunan dan Pengelolaan Sistem Manajemen Keamanan Informasi (Information Security Management System atau ISMS).	100% (*fully*)	2	2
2	APO13.02 Penentuan dan Pengelolaan Rencana Perlakuan terhadap Risiko Keamanan dan Privasi Informasi.	100% (*fully*)	3	3
		100% (*fully*)	4	
3	APO13.03 Pemantauan dan Peninjauan ISMS.	100% (*fully*)	4	3
		100% (*fully*)	5	

TABEL III
Hasil Assessment Capability Level DSS05

DSS05 – *Manage Security Service*				
No	**Aktivitas**	**Pencapaian**	**Level Kapabilitas**	**Target**
1	DSS05.01 Melindungi dari perangkat lunak berbahaya.	100% (*fully*)	2	4
		100% (*fully*)	3	
		100% (*fully*)	4	
2	DSS05.02 Kelola keamanan jaringan dan konektivitas.	50% (*partially*)	2	4
		83% (*largelly*)	3	
		100% (*fully*)	4	
3	DSS05.03 Kelola keamanan titik akhir.	89% (*largelly*)	2	4
		0% (*not*)	3	

DSS05 – *Manage Security Service*				
No	**Aktivitas**	**Pencapaian**	**Level Kapabilitas**	**Target**
4	DSS05.04 Kelola identitas pengguna dan akses logis.	100% (*fully*)	2	4
		40% (*partially*)	3	
		75% (*largelly*)	4	
5	DSS05.05 Mengelola akses fisik ke aset I&T.	75% (*largelly*)	2	4
		67% (*largelly*)	3	
6	DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.	75% (*largelly*)	2	4
		33% (*partially*)	3	
7	DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan.	63% (*largelly*)	2	4
		100% (*fully*)	3	

C. *Phase 3 - Define Target State*

Pada *Phase 3 Define Target State* menetapkan target untuk perbaikan yang dilanjutkan dengan *gap analysis* untuk mengidentifikasi solusi potensial. Beberapa domain yang akan dianalisis yaitu APO13 *Manage Security* dan DSS05 *Manage Security Service.* Berikut adalah tabel hasil dari penjabaran *Gap* (kesenjangan) dapat dilihat pada tabel dibawah ini:

TABEL IV
Gap Analysis APO13 *(Manage Security)*

APO13 (*Manage Security*)			
Managed Security	***Existing***	***Target***	***Gap***
APO13.01 Pembangunan dan Pengelolaan Sistem Manajemen Keamanan Informasi (Information Security Management System atau ISMS).	2	2	Tidak ada kesenjangan
APO13.02 Penentuan dan Pengelolaan Rencana Perlakuan terhadap Risiko Keamanan dan Privasi Informasi.	4	3	Tidak ada kesenjangan
APO13.03 Pemantauan dan Peninjauan ISMS.	5	3	Tidak ada kesenjangan

Tabel V *Gap Analysis* DSS05 *(Manage Security Service)*

DSS05 (*Manage Security Service*)			
Managed Security Service	***Existing***	***Target***	***Gap***
DSS05.01 Melindungi dari perangkat lunak berbahaya.	4	4	Tidak ada kesenjangan
DSS05.02 Kelola keamanan jaringan dan konektivitas.	1	4	Perusahaan belum memiliki kebijakan dan teknologi untuk perangkat resmi yang mengakses informasi dan jaringan perusahaan, serta kurangnya dokumentasi tentang penerapan keamanan jaringan dan penggunaan SSH untuk mengkonfigurasi jaringan.
DSS05.03 Kelola keamanan titik akhir.	2	4	Belum adanya pencatatan laporan terkait penggunaan fitur autolock dan penggunaan protokol dan koneksi aman untuk pengelolaan konfigurasi jaringan. Serta baru adanya inisiasi dan belum menerapkan enkripsi informasi dalam penyimpanan
DSS05.04 Kelola identitas pengguna dan akses logis.	2	4	Perusahaan belum memantau dan mengelola akun pengguna istimewa secara

DSS05 (*Manage Security Service*)			
Managed Security Service	***Existing***	***Target***	***Gap***
			aktif, belum melaksanakan pemrosesan informasi berdasarkan fungsional, dan belum mengidentifikasi semua pengguna.
DSS05.05 Mengelola akses fisik ke aset I&T.	1	4	Belum adanya pencatatan laporan terkait penggunaan IT card dan pengawasan secara ketat di sekitar situs TI sesitif.
DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.	1	4	Perusahaan belum menerapkan kontrol kriptografi, meskipun telah mengambil langkah alternatif seperti kontrol backup data dan database.
DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan.	1	4	Perusahaan memahami skenario risiko, namun belum melaksanakan atau melaporkannya. Identifikasi potensi insiden dipantau, tetapi tidak secara real-time dan tanpa personel khusus.

D. *Phase 4 – Build Improvement*

Pada fase 4, peneliti merancang solusi praktis dengan menentukan proyek-proyek spesifik untuk mengatasi kesenjangan yang ditemukan dalam analisis. Perbaikan potensial disusun untuk mencapai level target yang diinginkan, dengan fokus pada aspek *people, process,* dan *technology.* Langkah-langkah berikut diuraikan untuk menyusun rencana perbaikan.

1. *Perancangan People Aspect*

aspek people dilakukan dengan merujuk pada rekomendasi yang telah dipertimbangkan sebelumnya. Rekomendasi aspek people yang diberikan untuk PT XYZ diantaranya adalah rekomendasi *responsibility* dan *communication*. Tujuan aspek people ini untuk meningkatkan kinerja karyawan di PT XYZ.

TABEL VI
Potential Improvement People Aspect Responsibility

No	***Practice-Activity***	Peran	Tanggung Jawab
1	DSS05.04 Kelola identitas pengguna dan akses logis	*IT and Cyber Security Manager*	1. Mengelola dan memantau akun pengguna istimewa sesuai kebijakan keamanan. 2. Mengembangkan proses pemrosesan informasi sesuai tanggung jawab pengguna. 3. Menerapkan sistem identifikasi unik untuk semua pengguna. 4. Memantau aktivitas pengguna secara individual.
2	DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.		1. Mengembangkan kebijakan kriptografi. 2. Memastikan penerapan kontrol kriptografi yang tepat. 3. Melakukan audit dan evaluasi berkala untuk mengatasi kelemahan kriptografi.
3	DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan	Manajemen infrastruktur TI	1. Menilai risiko keamanan. 2. Mengembangkan dan menerapkan rencana tanggap insiden. 3. Memantau dan merespons insiden keamanan secara real-time.

Rekomendasi *skill and awareness* merupakan saran atau panduan mengenai keterampilan dan kesadaran yang perlu dikembangkan oleh individu atau organisasi. Rekomendasi yang diberikan peneliti untuk DSS05.03 terkait penerapan enkripsi informasi dalam penyimpanan yaitu membuat pelatihan kesadaran terkait pentingnya keamanan informasi dalam penyimpanan. Perusahaan dapat menyelenggarakan *Program Security Awareness* dan memberikan sertifikasi *Certified Information Systems Security Professional* (CISSP) untuk meningkatkan kesadaran dan pengetahuan karyawan tentang pentingnya keamanan data, khususnya yang berkaitan dengan enkripsi.

Rekomendasi *communication* mencakup kemampuan untuk meningkatkan cara organisasi berkomunikasi baik secara internal maupun eksternal. Dalam penelitian ini, peneliti merekomendasikan agar perusahaan fokus pada DSS05.04 untuk meningkatkan koordinasi dan kolaborasi dengan unit bisnis untuk memastikan peran dan hak akses.

2. Perancangan *Process Aspect*

Aspek *process* dilakukan dengan merujuk pada rekomendasi yang telah dipertimbangkan sebelumnya. Rekomendasi aspek *process* yang diberikan untuk PT XYZ diantaranya adalah rekomendasi *policy, procedure,* dan *record.* Tujuan aspek *process* ini untuk meningkatkan kinerja karyawan di PT XYZ.

TABEL VII
Potential Improvement Process Aspect

No	*Practice-Activity*	Type	*Potential Improvement*
1	DSS05.02 Kelola keamanan jaringan dan konektivitas	*Policy*	Membuat kebijakan formal untuk mengatur penggunaan perangkat resmi yang mengakses informasi dan jaringan perusahaan. Kebijakan tersebut perlu mencakup persyaratan keamanan yang terperinci.
		Record	Membuat dokumentasi laporan terkait tentang penerapan keamanan jaringan, penggunaan SSH untuk mengkonfigurasi jaringan. Hal ini mencakup pencatatan rinci mengenai tindakan yang diambil, kebijakan yang diterapkan, serta hasil dari audit dan evaluasi keamanan yang dilakukan secara berkala.
2	DSS05.03 Kelola keamanan titik akhir.	*Policy*	Menetapkan kebijakan keamanan data yang komprehensif untuk penerapan enkripsi informasi
		Record	mencatat segala proses pelaporan terkait penggunaan fitur autolock dan penggunaan protokol dan koneksi aman untuk pengelolaan konfigurasi jaringan.
3	DSS05.04 Kelola identitas pengguna dan akses logis	*Policy*	Merancang kebijakan untuk pengelolaan akun pengguna istimewa dengan melakukan pemantauan aktif, membuat kebijakan pemroresan informasi berdasarkan fungsional, serta memverifikasi identifikasi unik pengguna dan aktivitas mereka di dalam sistem TI.
4	DSS05.05 Mengelola akses fisik ke aset I&T.	*Record*	mencatat dan membuat laporan terhadap segala aktivitas yang telah diimplementasikan sebagai dokumentasi laporan perusahaan yang terbaru dan melakukan evaluasi secara berkala.
5	DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.	*Policy*	membuat kebijakan terkait kontrol kriptografi untuk melindungi informasi sensitif yang disimpan secara elektronik.
6	DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan	*Procedure*	mengembangkan dan mengimplementasikan prosedur standar untuk menanggapi kerentanan dan insiden keamanan

3. Perancangan *Technology Aspect*

Aspek *technology* dilakukan dengan merujuk pada rekomendasi yang telah dipertimbangkan sebelumnya. Rekomendasi aspek *technology* yang diberikan untuk PT XYZ diantaranya adalah rekomendasi *tools* dan *features.* Tujuan aspek *technology* ini untuk meningkatkan keamanan perusahaan.

TABEL VIII
Potential Improvement Technology Aspect

Rekomendasi Kontrol *Technology*	Rekomendasi *Tools*	Deskripsi
DSS05.02 Kelola keamanan jaringan dan konektivitas		
mempertimbangkan adanya *tools* yang dapat membantu peninjauan perangkat dan koneksi keamanan	Mobile Device Management (MDM) and Endpoint (microsoft intune)	Perangkat yang dapat memberikan alat atau aplikasi produktivitas seluler untuk menjaga

untuk mengurangi risiko perusahaan		keamanan data perusahaan, serta dapat digunakan untuk berbagai platform (Windows, IOS, Android).
DSS05.06 Kelola dokumen sensitif dan perangkat keluaran.		
mempertimbangkan adanya teknologi untuk kriptografi dalam elektronik perusahaan sebagai perlindungn informasi sensitif	GPG (GNU *Privacy Guard*) OpenSSL	GnuPG menggunakan sistem kriptografi kunci publik, di mana setiap pengguna memiliki dua kunci: satu privat dan satu publik. OpenSSL adalah pustaka kriptografi sumber terbuka yang mendukung protokol TLS dan memungkinkan pembuatan CSR, kunci privat, serta pemasangan sertifikat SSL.
DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian terkait keamanan		
mempertimbangkan adanya teknologi yang membantu perusahaan dalam pemantauan secara real-time, seperti SIEM (Security Information and Event Management)	*Security Information and Event Management* (SIEM)	Sistem keamanan yang mampu merespons potensi serangan *cyber* dengan cepat serta memantau aktivitas jaringan secara berkelanjutan untuk mendeteksi ancaman secara *real-time*.

V. KESIMPULAN

Kesimpulan dari penelitian ini adalah sebagai berikut:

1. Penilaian *design factor* di PT XYZ menunjukkan bahwa objektif APO13 *Managed Security* (nilai 60) dan DSS05 *Managed Security Service* (nilai 100) adalah prioritas utama. Penelitian ini difokuskan pada penerapan target kapabilitas untuk kedua objektif tersebut guna meningkatkan efektivitas dan efisiensi tata kelola TI.
2. Analisis kesenjangan berdasarkan COBIT 2019 mengidentifikasi kekurangan dalam pengelolaan keamanan informasi. Tidak ada kesenjangan pada APO13, tetapi beberapa kesenjangan ditemukan pada DSS05, khususnya di DSS05.02 hingga DSS05.07. Ini menunjukkan perlunya peningkatan manajemen keamanan informasi.
3. Rekomendasi peneliti mencakup aspek *people, process,* dan *technology*, serta penyusunan *roadmap* implementasi untuk mengatasi kesenjangan dan meningkatkan tata kelola TI di PT XYZ.

REFERENSI

[1] S. School of Management, P. Weill, and J. W. Ross, "CENTER FOR INFORMATION SYSTEMS RESEARCH IT Governance on One Page Massachusetts Institute of Technology Cambridge Massachusetts," 2004. [Online]. Available: http://web.mit.edu/cisr/www

[2] PT Pindad, "Laporan Tahunan 2023 Annual Report." [Online]. Available: www.pindad.com.

[3] Information Systems Audit and Control Association, *COBIT® 2019 Framework: introduction and methodology*.

[4] Information Systems Audit and Control Association., *COBIT 2019 Framework Governance and Management Objectives*.

[5] *Implementing and Optimizing an Information and Technology Governance Solution*. 2018. [Online]. Available: http://linkd.in/ISACAOfficial