# ANALISIS KAPABILITAS TATA KELOLA TI DI LEMBAGA XYZ PROVINSI JAWA BARAT MENGGUNAKAN FRAMEWORK COBIT 2019 PADA ASPEK KEAMANAN INFORMASI


1st Muhammad Reza Irfandi
Sistem Informasi
Telkom University
Bandung, Indonesia
mrezairfandi@student.telkomuniversity.ac.id

2nd Ir. Ari Fajar Santoso, M.T.
Sistem Informasi
Telkom University
Bandung, Indonesia
arifajar@telkomuniversity.ac.id

3rd Dr. Dhata Praditya, S.T., M.T.
Sistem Informasi
Telkom University
Bandung, Indonesia
dhatap@telkomuniversity.ac.id



***Abstrak* — Perkembangan teknologi informasi mendorong implementasi *e-government* di lembaga pemerintah, termasuk Lembaga XYZ, untuk meningkatkan layanan publik sesuai Inpres No. 3 Tahun 2003. Keamanan informasi menjadi aspek krusial yang perlu didukung oleh tata kelola TI yang baik. COBIT 2019 merupakan kerangka kerja tata kelola TI yang dapat dimanfaatkan Lembaga XYZ untuk memperkuat keamanan informasi dan mencapai tujuan *e-government*. Penelitian ini bertujuan untuk menganalisis kapabilitas dan kondisi tata kelola TI di Lembaga XYZ serta memberikan rekomendasi berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*). Metode penelitian menggunakan implementasi COBIT 2019 fase satu sampai empat, meliputi penentuan ruang lingkup, penentuan target, analisis kondisi eksisting, dan penyusunan rekomendasi. Hasil penelitian menunjukkan beberapa kelemahan dalam tata kelola TI Lembaga XYZ, terutama pada aspek keamanan informasi. Analisis gap mengidentifikasi perbedaan antara kondisi saat ini dengan target yang diharapkan. Rekomendasi yang disusun mencakup peningkatan proses manajemen keamanan berupa pembaruan kebijakan dan prosedur, pelatihan karyawan, serta penggunaan *tools* yang sesuai. Penerapan kerangka kerja COBIT 2019 dapat membantu Lembaga XYZ meningkatkan tata kelola TI dan keamanan informasi, dengan implikasi berupa peningkatan efektivitas dan efisiensi layanan publik serta perlindungan aset informasi yang lebih baik.**



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


## I. PENDAHULUAN

Perkembangan teknologi informasi (TI) di era globalisasi telah mengalami kemajuan pesat dan menjadi kebutuhan mendasar bagi masyarakat maupun organisasi. TI tidak hanya berfungsi sebagai alat komunikasi, tetapi juga sebagai sarana utama untuk mencari informasi dan menjalankan operasional organisasi guna meningkatkan efektivitas kinerja [1]. Pemanfaatan TI kini menjadi bagian penting bagi banyak organisasi, termasuk lembaga pemerintah. *E-government*, sebagai penerapan TI di pemerintahan, diharapkan mampu meningkatkan efisiensi, efektivitas, transparansi, dan akuntabilitas penyelenggaraan pemerintahan. Tujuan ini sejalan dengan Inpres No. 3 Tahun 2003 yang mendorong perbaikan penyelenggaraan pemerintahan melalui pengembangan *e-government*, guna meningkatkan efektivitas dan efisiensi layanan publik [2] [3].

Dalam pemanfaatan TI, keamanan informasi menjadi aspek yang sangat penting. Keamanan informasi tidak hanya melindungi aset teknologi, tetapi juga informasi yang menjadi pondasi operasi setiap organisasi. Fokus utama dari keamanan informasi adalah menjaga integritas, kerahasiaan, dan ketersediaan data, dengan tujuan mengurangi risiko dalam aktivitas bisnis, serta menjamin kelangsungan operasional organisasi [4]. Manajemen keamanan informasi bertujuan untuk melindungi data secara aman dan memastikan bahwa organisasi mematuhi peraturan, undang-undang, dan standar yang berlaku [5].

Untuk memastikan keamanan informasi yang optimal, organisasi perlu melakukan evaluasi terhadap implementasi TI yang terkait dengan infrastruktur TI. Evaluasi ini bertujuan menilai sejauh mana manajemen infrastruktur TI telah dilaksanakan secara efektif. Keselarasan antara tujuan organisasi dan penerapan TI menentukan keberhasilan tata kelola TI. Salah satu kerangka kerja yang digunakan untuk menyelaraskan tata kelola TI adalah COBIT 2019 [6].

COBIT 2019 adalah kerangka kerja yang mengutamakan prinsip-prinsip utama untuk sistem tata kelola TI dan bertujuan menyempurnakan efektivitas, efisiensi, keamanan, dan ketaatan dalam pengelolaan TI. Kerangka kerja ini sangat relevan dalam praktik pengelolaan TI, khususnya dalam hal keamanan informasi. Lembaga XYZ, sebagai salah satu lembaga pemerintah non kementerian yang bertanggung jawab langsung kepada Presiden, dapat memanfaatkan COBIT 2019 untuk meningkatkan tata kelola TI, khususnya dalam keamanan informasi. Panduan komprehensif dari COBIT 2019 memungkinkan Lembaga XYZ untuk mengidentifikasi ancaman terhadap keamanan informasi, membuat kebijakan yang tepat, dan memastikan penerapan praktik terbaik [7].

Lembaga XYZ menghadapi kompleksitas keamanan informasi dalam implementasi *e-government*, termasuk integrasi sistem, kurangnya pedoman kebijakan, ancaman siber, dan kepatuhan regulasi. Untuk mengatasi komplesitas tersebut Lembaga XYZ bisa menerapkan kerangka kerja COBIT 2019, khususnya domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*). APO13 fokus pada pengelolaan keamanan menyeluruh, sementara DSS05 menangani layanan keamanan operasional. Implementasi ini akan membantu Lembaga XYZ mengatasi tantangan keamanan informasi, meningkatkan tata kelola TI, dan mendukung tujuan e-government sesuai Inpres No. 3 Tahun 2003, sehingga meningkatkan efisiensi dan keamanan layanan publik.

Penelitian ini bertujuan untuk menganalisis kapabilitas tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*). Analisis ini meliputi penilaian kondisi tata kelola TI saat ini dan penyusunan rekomendasi untuk meningkatkan tata kelola TI di Lembaga XYZ. Penelitian ini akan fokus pada penilaian kapabilitas dan kesenjangan tata kelola TI, serta penyusunan rekomendasi solusi hingga tahap *build improvement*.

## II. KAJIAN TEORI

### A. Tata Kelola TI

Konsep IT (*Information Technology*) *Governance* adalah cara sebuah organisasi menggunakan teknologi informasi. *IT Governance* mencakup perencanaan dan pengorganisasian, pembangunan dan pengimplementasian, penyediaan dan dukungan, dan pemantauan kinerja sistem informasi untuk memastikan bahwa kalau informasi dan teknologi yang terkait mendukung tujuan dan misi organisasi. Proses audit sistem adalah salah satu cara untuk mengetahui hal tersebut [8].

Tata kelola TI (Teknologi Informasi) memberikan dasar struktur yang mengaitkan dan menyelaraskan proses-proses TI, sumber daya TI, dan informasi yang dibutuhkan perusahaan untuk menerapkan strateginya untuk mencapai tujuan yang telah ditetapkan. Tata kelola TI mencakup integrasi dan optimalisasi metode untuk merencanakan, mengorganisir, melaksanakan akuisisi dan implementasi, menyediakan dukungan, serta memonitor dan mengevaluasi kinerja TI. Hal ini penting untuk mencapai tujuan yang telah ditetapkan [9].

### B. Kerangka Kerja Tata Kelola TI

Dalam era TI yang dinamis, tata kelola yang efektif sangat penting untuk kesuksesan. Supaya tata kelola berjalan dengan baik tentunya memerlukan sebuah kerangka kerja seperti COBIT 2019, ITIL, dan ISO 27001. COBIT 2019 merupakan kerangka kerja untuk mengevaluasi dan meningkatkan tata kelola serta manajemen TI dalam organisasi. Tujuannya adalah mengoptimalkan nilai dari informasi dan teknologi, membantu organisasi mengelola risiko, mengidentifikasi keuntungan, dan memaksimalkan pemanfaatan sumber daya [10]. ITIL adalah kerangka kerja sistematis untuk mengelola layanan TI, dengan fokus utama pada kebutuhan bisnis dan kepuasan pelanggan. ITIL menyediakan praktik dan proses terbaik yang dapat diterapkan dalam lingkungan TI untuk meningkatkan kualitas layanan [11]. ISO 27001 adalah standar yang menetapkan sistem manajemen keamanan informasi dengan menyediakan kerangka kerja untuk mengembangkan, mengimplementasikan, menjalankan, memantau, mengevaluasi, dan meningkatkan sistem manajemen keamanan informasi [12]. Oleh karena itu, setiap kerangka kerja memiliki fokus yang berbeda-beda, memberikan organisasi berbagai pilihan untuk mengelola dan mengoptimalkan penggunaan TI sesuai dengan tujuan dan prinsip yang ditetapkan.

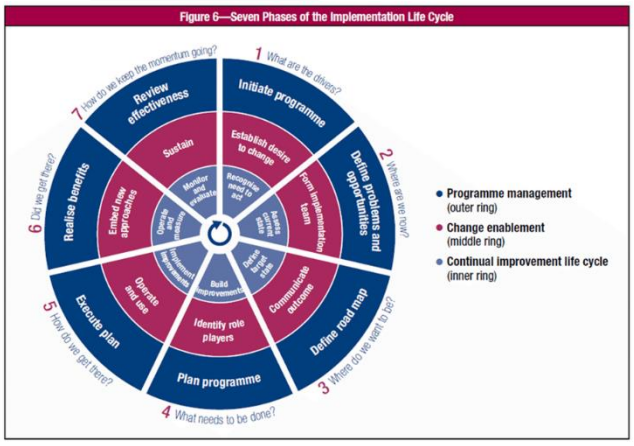
### C. COBIT 2019

ISACA (*Information System Audit and Control Association*) memperkenalkan COBIT untuk pertama kalinya pada 1996 sebagai alat bantu dalam melaksanakan audit teknologi informasi. Kerangka kerja ini dirancang untuk membantu organisasi dalam mengelola dan mengawasi proses TI mereka secara lebih efektif. COBIT 2019 mengalami modifikasi pada prinsip-prinsipnya, memperbarui goals cascade, memperkenalkan tiga proses baru, serta menambahkan fokus area untuk memberikan perhatian khusus pada penyelesaian masalah tertentu. Pengenalan design factor juga dilakukan dengan tujuan memfasilitasi implementasi EGIT yang lebih sesuai dengan kebutuhan [13].

COBIT adalah kerangka kerja yang dirancang untuk mengelola dan mengatur teknologi dan informasi di seluruh bagian perusahaan. *Enterprise I&T* (Informasi dan Teknologi Perusahaan) mengacu pada semua teknologi dan proses pengolahan informasi yang diterapkan oleh perusahaan untuk mencapai tujuan bisnisnya, tanpa memandang lokasi penerapan tersebut dalam perusahaan. Dengan demikian, *Enterprise I&T* tidak hanya terdiri dari seluruh bagian perusahaan. ISACA telah merilis beberapa versi COBIT sebagai tanggapan atas kemajuan teknologi. COBIT 2019, penerus dari COBIT 5, dirilis dengan menambahkan perkembangan terbaru yang dapat mempengaruhi organisasi dalam hal informasi dan teknologi. Dalam COBIT 2019, beberapa elemen desain yang telah disediakan akan membantu perusahaan merancang sistem tata kelola [13].

### D. COBIT 2019 *Implementation Guide*

Panduan implementasi COBIT 2019 menjelaskan prinsip-prinsip yang menekankan pandangan perusahaan tentang tata kelola teknologi informasi. Panduan ini juga menjelaskan bagaimana melaksanakan EGIT (*Enterprise Governance of Information and Technology*). Gambar 1 berikut adalah implementasi *roadmap* COBIT, yang terdiri dari tujuh tahap.




Gambar 1 COBIT 2019 *Implementation Guide* [14]

1. *What are the driver?*

   Fase pertama implementasi adalah menemukan pendorong perubahan. Pendorong perubahan dapat berupa peristiwa internal atau eksternal, tren, kinerja yang buruk, atau tujuan perusahaan. Risiko implementasi dijelaskan dan dikelola dalam kerangka kasus bisnis, yang berfungsi sebagai dasar untuk membenarkan, mendukung, dan memastikan kesuksesan inisiatif, termasuk perbaikan sistem tata kelola. Monitoring kerangka kasus bisnis memastikan

fokus tetap pada keuntungan program dan pencapaian hasil.

2. *Where are we now?*

   Fase 2 mengidentifikasi kemampuan saat ini dan kekurangan. Ini dapat dicapai dengan membandingkan kemampuan proses terkini dengan status proses tertentu. Panduan Desain COBIT 2019 menawarkan beberapa faktor desain untuk membantu dalam membuat keputusan ini. Faktor-faktor ini didasarkan pada tujuan perusahaan dan TI yang telah dipilih, serta faktor desain lainnya. Perusahaan harus menentukan tujuan penting dalam manajemen dan tata kelola, serta proses-proses dasar yang diperlukan untuk memastikan keberhasilan.

3. *Where do we want to be?*

   Fase 3 memulai dengan menetapkan target peningkatan dan kemudian melakukan analisis kesenjangan untuk menemukan solusi potensial. Solusi tertentu memungkinkan hasil cepat, sementara solusi lain membutuhkan lebih banyak upaya dalam jangka panjang. Proyek yang lebih mudah dicapai dan berpotensi menghasilkan hasil terbaik harus diprioritaskan.

4. *What needs to be done?*

   Fase 4 menjelaskan bagaimana merencanakan solusi yang dapat diwujudkan dan praktis dengan mendefinisikan proyek yang didukung oleh business case yang dapat dibenarkan dan rencana perubahan untuk implementasinya. Business case yang baik dapat membantu memastikan bahwa manfaat proyek diidentifikasi dan terus dipantau.

5. *How do we get there?*

   Fase 5 menjelaskan bagaimana menerapkan solusi yang diusulkan melalui praktik sehari-hari, serta bagaimana membuat ukuran dan sistem pemantauan untuk memastikan pencapaian keselarasan bisnis dan pengukuran kinerja. Keterlibatan, kesadaran, komunikasi, pemahaman, dan komitmen dari manajemen puncak serta kepemilikan dan kepemilikan proses TI yang terkena dampak diperlukan untuk mencapai keberhasilan.

6. *Did we get there?*

   Fase 6 berkonsentrasi pada pemantauan pencapaian perbaikan melalui penggunaan metrik kinerja dan keuntungan yang diharapkan. Ini juga membahas transisi dari praktik pengelolaan dan tata kelola yang ditingkatkan ke dalam operasi bisnis yang biasa.

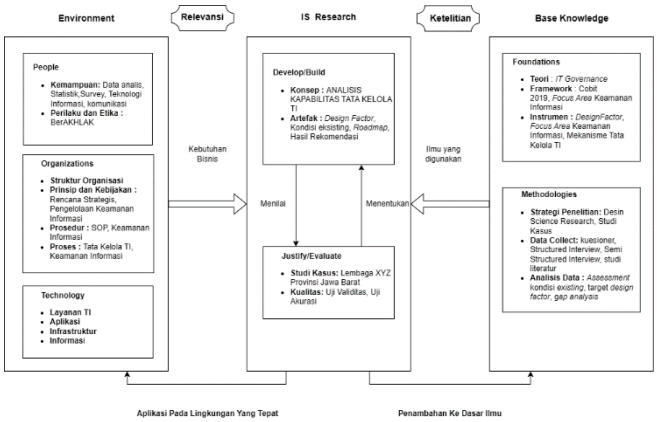
7. *How do we keep the momentum going?*

   Fase 7 mengevaluasi keberhasilan inisiatif, menentukan apakah ada kebutuhan tambahan untuk tata kelola atau manajemen, dan meningkatkan keinginan untuk perbaikan yang berkelanjutan. Ini juga memprioritaskan peluang untuk meningkatkan sistem tata kelola. Manajemen program dan proyek berdasarkan praktik terbaik dengan checkpoint di setiap fase untuk memastikan kinerja program yang optimal [13].

## III. METODE

### A. Model Konseptual

Model konseptual merupakan suatu kerangka berpikir yang menjelaskan hubungan antara beberapa elemen, mulai dari individu dan kelompok hingga peristiwa, dalam suatu ilmu dan pengembangannya. Model konseptual memiliki peran penting dalam penelitian karena membantu mengorganisir masalah, mengidentifikasi berbagai faktor yang relevan, memetakan hubungan antara faktor-faktor tersebut, dan memudahkan dalam mengidentifikasi inti masalah. Penelitian ini berfokus untuk mencari solusi terhadap tantangan yang dihadapi oleh suatu lembaga pemerintahan. Oleh karena itu, studi kasus digunakan untuk memberikan gambaran kondisi aktual objek penelitian. Penelitian ini mengadopsi kerangka DSR (*Design Science Research*), sebuah metode yang memiliki keunggulan dalam menghasilkan kontribusi ilmiah yang kuat dan artefak desain yang inovatif, serta mendorong kolaborasi antara industri dan akademisi. Kerangka DSR memberikan gambaran singkat tentang pelaksanaan penelitian yang memanfaatkan ilmu desain dalam sistem informasi, serta menyajikan pedoman yang jelas untuk memahami, melaksanakan, dan mengevaluasi penelitian melalui suatu kerangka konseptual [15].




Gambar 2 Model Konseptual

Gambar 2 merupakan kerangka model untuk mendukung alur dalam penelitian ini agar menjadi terstruktur serta dapat mencapai hasil yang diharapkan. Berdasarkan kerangka model Gambar 2 dapat diketahui bahwa:

1. *Environment*

   Bagian ini memberikan penjelasan tentang peran yang dimainkan oleh setiap unit TI dalam organisasi yang berdampak pada proses transformasi, serta bagaimana kontribusi mereka mendukung pencapaian tujuan organisasi. Bagian ini terbagi ke dalam tiga aspek: *people*, *organization*, dan *technology*. Setiap aspek dipetakan berdasarkan kondisi terkini organisasi. Dalam aspek manusia, poin-poin dibagi menjadi dua aspek: kemampuan serta perilaku dan etika. Dalam aspek kemampuan sumber daya yang tersedia dimanfaatkan untuk menyelesaikan tugas-tugas yang praktis dalam bidang terkait. Selanjutnya terdapat empat bagian terdiri dari poin-poin dalam aspek organisasi, meliputi struktur organisasi, prinsip dan kebijakan, prosedur, dan proses organisasi. Setiap poin memiliki tanggung jawab dan

tugasnya sendiri, dan mereka bekerja bersama-sama untuk mencapai tujuan organisasi. Sementara itu, dalam aspek teknologi, terdapat beberapa elemen seperti informasi, infrastruktur, layanan TI, dan aplikasi. Dalam hal ini, poin-poin tersebut berfungsi sebagai sarana untuk membantu organisasi mencapai tujuannya.

2. *Base Knowledge*

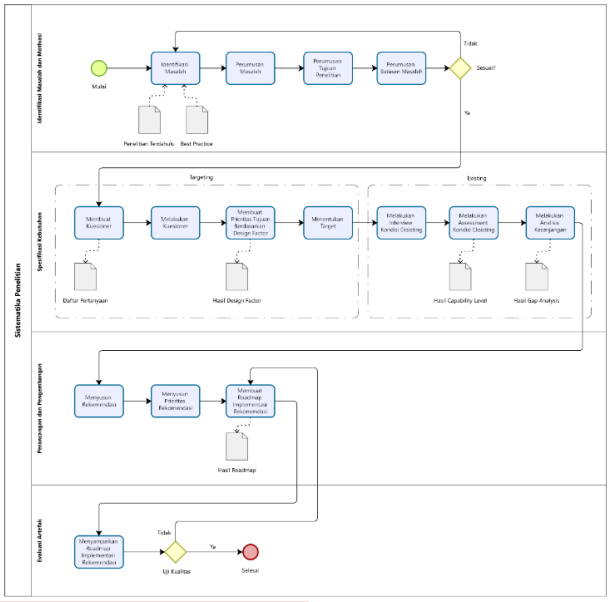
   Dalam bagian ini, terdapat dua aspek utama yaitu pondasi dan metodologi. Pada aspek pondasi, membahas teori, *framework*, dan instrumen yang digunakan dalam penyusunan penelitian ini. Komponen konsep berperan sebagai landasan untuk memahami dan menginterpretasikan data, konstruksi berfungsi sebagai proses untuk membangun dan mengembangkan sistem serta alat penelitian, dan instrumen digunakan sebagai alat untuk mengumpulkan data. Kerangka kerja bertindak sebagai struktur dan organisasi data yang dikumpulkan. Kemudian, dalam aspek metodologi, terdapat berbagai aspek, termasuk pengumpulan data, strategi penelitian, dan analisis data. Strategi penelitian membentuk metode dan pendekatan penelitian, sementara analisis data melibatkan proses pengolahan dan penyajian data yang telah diteliti.

3. *IS Research*

   Bagian ini terdiri dari dua aspek utama, yaitu pengembangan dan justifikasi/evaluasi. Pengembangan/pembangunan dibagi menjadi dua bagian, yaitu konsep dan artefak. Konsep merujuk pada ide atau gagasan yang akan diimplementasikan, mencakup visi, tujuan, dan target yang ingin dicapai. Sebagai contoh, penerapan konsep pengembangan keamanan informasi. Artefak mengacu pada hasil pengembangan sistem informasi, yang didasarkan pada faktor perancangan, tingkat kematangan saat ini dan yang diharapkan, serta rekomendasi optimalisasi tujuan berdasarkan tingkat kematangan. Artefak juga mencakup rancangan optimalisasi prioritas esensial. Dengan memperhatikan konsep dan artefak dalam pengembangan sistem informasi, organisasi dapat memastikan bahwa sistem yang dibangun sesuai dengan kebutuhan dan tujuan, serta dapat beroperasi dengan efektif dan efisien. Aspek kedua, justifikasi/evaluasi, terdiri dari dua bagian yaitu studi kasus dan kualitas. Pada aspek ini berisi studi kasus yang digunakan pada Lembaga XYZ, serta evaluasi kualitas melalui uji validitas dan uji akurasi

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah pada penelitian ini menggunakan panduan *implementation guide* dari COBIT 2019. Tahapan implementasi yang digunakan terdiri empat fase yang mencakup fase satu hingga empat, masing-masing fase dilakukan untuk mencapai tujuan yang telah ditetapkan. Gambar 3 dibawah ini merupakan sistematika penyelesaian masalah yang akan digunakan pada penelitian ini.




Gambar 3 Sistematika Penyelesaian Masalah

Gambar 3 Sistematika Penelitian diadopsi dari [16]

Berikut ini merupakan penjelasan dari Gambar 3.

1. Identifikasi Masalah

   Tahap ini membahas penjelasan mengenai permasalahan yang akan diatasi serta bertujuan untuk membentuk dasar pengembangan manajemen keamanan informasi. Proses ini dimulai dengan identifikasi masalah melalui penelitian literatur guna menyajikan latar belakang yang mendalam. Terdapat beberapa peraturan, baik tingkat nasional maupun internasional, yang mendukung penjelasan latar belakang permasalahan ini. Di antaranya adalah Inpres No. 3 Tahun 2003 dan BSSN N0. 4 Tahun 2021. Selain itu, penelitian sebelumnya, standar internasional, dan pedoman kerangka kerja COBIT 2019 turut dimasukkan. Setelah permasalahan teridentifikasi, langkah selanjutnya adalah merumuskan dan membatasi permasalahan sesuai dengan kerangka penelitian yang telah ditetapkan. Pembuatan perumusan dan pembatasan ini menjadi pedoman agar penelitian dapat difokuskan pada tujuan atau sasaran penelitian.

2. Spesifikasi Kebutuhan

   Pada tahap ini, peneliti merumuskan pertanyaan yang diperlukan untuk penelitian dan mengevaluasi kondisi tata kelola teknologi informasi di perusahaan dengan menggunakan kerangka kerja COBIT 2019. Pertanyaan kemudian disesuaikan dan diperinci untuk mencapai ketepatan. Setelah pertanyaan terbentuk, dilakukan wawancara semi-terstruktur dengan pihak terkait. Hasil wawancara digunakan untuk menentukan prioritas dengan mempertimbangkan faktor desain yang akan menjadi dasar penentuan prioritas. Setelah mendapatkan hasil penilaian, dilakukan analisis kesenjangan untuk mengidentifikasi perbedaan antara kondisi sekarang dan kondisi yang diinginkan. Analisis kesenjangan ini menjadi dasar untuk menyusun rekomendasi perbaikan potensial.

3. Perancangan dan Pengembangan
   Pada tahap ini dilakukan penyusunan rekomendasi hasil analisis kesenjangan yang ada pada kondisi eksisting Lembaga XYZ. Setelah dilakukan penyusunan kemudian menentukan prioritas rekomendasi sesuai dengan kebutuhan. Pada tahap ini juga melakukan pembuatan *roadmap* implementasi rekomendasi.
4. Evaluasi
   Pada tahap melakukan penyampaian hasil *roadmap* implementasi rekomendasi dan mengevaluasi artefak. Evaluasi artefak menggunakan uji validitas dan uji akurasi. Uji validitas dilakukan untuk mengevaluasi sejauh mana instrumen atau metode yang digunakan dapat mengukur apa yang seharusnya diukur, serta seberapa baik hasil tersebut mencerminkan fenomena yang sedang diteliti. Sementara itu, uji akurasi dilakukan untuk memastikan bahwa hasil rekomendasi atau temuan yang diperoleh dari penelitian akurat.

## IV. HASIL DAN PEMBAHASAN

### A. Fase 1 - *Recognize Need to Act*

Fase ini berfokus pada identifikasi pendorong perubahan dan membangun keinginan untuk berubah di tingkat manajemen eksekutif. Pendorong perubahan bisa berasal dari internal atau eksternal, seperti tren industri, kinerja yang kurang baik, atau implementasi teknologi baru. Manajemen kemudian menyusun kasus bisnis yang menjelaskan kebutuhan perubahan, manfaat yang diharapkan, dan risiko yang mungkin timbul. Kasus bisnis ini akan menjadi panduan sepanjang proses perubahan [13].

Tabel 1 Hasil *Design Factor*

| *Score* | Domain | *Governance / Management Objective Priority* | Target *Capability Level* |
|---|---|---|---|
| 100 | DSS05 | *Managed Security Service* | 4 |
| 55 | APO13 | *Managed Security* | 3 |

Setelah melakukan design factor, hasil akhir dari perancangan sistem tata kelola ditentukan berdasarkan penilaian 10 faktor desain. Penilaian ini akan menentukan objektif inti di Lembaga XYZ, yang terdiri dari 40 proses dengan beragam nilai. Semakin tinggi nilai dari objektif inti, semakin penting proses tersebut bagi Lembaga XYZ. Pada Tabel 1 merupakan hasil *design factor* yang cukup tinggi.

Hasil *design factor* yang menunjukkan referensi target *capability level* dimana objektif terkait ditentukan dengan menggunakan acuan COBIT 2019 *Design Guide* yang menerapkan kriteria sebagai berikut:

1. *Governance/Management Objective Priority Managed Security Service* (DSS05) dengan skor 100 mempunyai *target capability level* 4.
2. *Governance/Management Objective Priority Managed Security* (APO13) dengan skor 55 mempunyai *target capability level* 3.

### B. Fase 2 – *Assess to Current*

Fase ini melibatkan penyelarasan tujuan TI dengan strategi perusahaan. Menggunakan panduan dari COBIT 2019, perusahaan mengidentifikasi tujuan penting untuk manajemen dan tata kelola, serta proses-proses kunci yang diperlukan [13].

Setelah penilaian aktivitas proses dilakukan pada domain APO13 dan DSS05, didapatkan hasil tingkat kapabilitas dari setiap aktivitas proses tersebut. Tabel 2 menunjukkan hasil penilaian APO13 untuk *Managed Security*, sedangkan tabel 3 menunjukkan hasil penilaian DSS05 untuk *Managed Security Service*. Tabel 2 dibawah merupakan hasil *capabiltiy assessment* APO13.

Tabel 2 Hasil *Capability Assessment* APO13

| **APO13 – *Manage Security*** | | | |
|---|---|---|---|
| **No** | **Aktivitas** | **Pencapaian** | **Level Kapabilitas** |
| 1. | APO13.01 Menetapkan dan memelihara sistem manajemen keamanan informasi | 100%(*Fully*) | 2 |
| 2. | APO13.02 Menetapkan dan mengelola rencana penanganan risiko keamanan informasi dan privasi. | 42% (*Partially*) | 3 |
| | | 0% (*None*) | 4 |
| 3. | APO13.03 Memantau dan meninjau sistem manajemen keamanan informasi | 38% (*Partially*) | 4 |
| | | 0% (*None*) | 5 |

Tabel 3 *Hasil Capability Assessment* DSS05

| **DSS05 – Manage Security Services** | | | |
|---|---|---|---|
| **No** | **Aktivitas** | **Pencapaian** | **Level Kapabilitas** |
| 1. | DSS05.01 Melindungi dari perangkat lunak berbahaya. | 75% (*Largely*) | 2 |
| | | 0% (*None*) | 3 |
| | | 0% (*None*) | 4 |
| 2. | DSS05.02 Mengelola keamanan jaringan dan konektivitas | 75% (*Largely*) | 2 |
| | | 0% (*None*) | 3 |
| | | 0% (*None*) | 4 |
| 3. | DSS05.03 Mengelola keamanan pada endpoint | 56% (*Largely*) | 2 |
| | | 0% (*None*) | 3 |
| 4. | DSS05.04 Mengelola identitas pengguna dan akses logis | 100% (*Fully*) | 2 |
| | | 30% (*Partially*) | 3 |
| | | 0% (*None*) | 4 |
| 5. | DSS05.05 Mengelola akses fisik ke aset TI. | 100% (*Fully*) | 2 |
| | | 50% (*Largely*) | 3 |
| 6. | DSS05.06 Mengelola dokumen sensitif dan perangkat *output*. | 25% (*Partially*) | 2 |
| | | 0% (*None*) | 3 |
| 7. | DSS05.07 Mengelola kerentanan dan memantau infrastruktur untuk kejadian yang berhubungan dengan keamanan. | 13% (*None*) | 2 |
| | | 0% (*None*) | 3 |

### C. Fase 3 – *Define to Target*

Pada fase ini, perusahaan mengidentifikasi solusi potensial dan menetapkan target perbaikan. Prioritas diberikan pada proyek yang mudah dilaksanakan dan berpotensi memberikan manfaat besar. Tugas-tugas yang

lebih kompleks dipecah menjadi bagian-bagian yang lebih kecil dan lebih mudah dikelola [13].

Berdasarkan hasil penilaian kapabilitas yang telah dilakukan, terdapat gap pada proses domain APO13 (*Managed Security*) *dan* DSS05 (*Managed Security Service*). Kesenjangan yang ditemukan di atas berasal dari perbandingan antara kondisi eksisting dan target. Kondisi eksisting diperoleh dari penilaian kapabilitas untuk mengetahui berada di level berapa Lembaga XYZ. Sementara itu, nilai target didapatkan dari hasil *assessment design factor* pada target *capability level*. Pada Tabel 4 dibawah ini merupakan hasil *gap analysis* pada domain APO13 dan DSS05.

Tabel 4 Tabel 4 Hasil *Gap Analysis* APO13

| Management Practice | Kesenjangan |
|---|---|
| APO13.01 | Tidak ada kesenjangan |
| APO13.02.1<br>APO13.02.2<br>APO13.02.3 | Lembaga XYZ tidak memiliki peodman untuk menghadapi manajemen risiko keamanan informasi, termasuk kurangnya rencana terdokumentasi yang selaras dengan tujuan strategis, inventarisasi komponen keamanan yang tidak lengkap, dan tidak adanya proposal terdokumentasi untuk mengimplementasikan rencana manajemen risiko. |
| APO13.02.4<br>APO13.02.7 | Lembaga XYZ belum memberikan masukan yang memadai untuk desain dan pengembangan praktik manajemen risiko, serta belum adanya metode yang ditetapkan untuk mengukur efektivitas praktik manajemen yang dipilih. |
| APO13.02.5<br>APO13.02.6 | Tidak ada kesenjangan |
| APO13.03.1<br>APO13.03.2<br>APO13.03.3<br>APO13.03.5 | Lembaga XYZ tidak melakukan *review* dan audit ISMS secara berkala dan terdokumentasi, serta kurangnya masukan untuk pemeliharaan rencana keamanan berdasarkan temuan dari aktivitas pemantauan dan *review* karena hanya melakukan perbaikan saat terjadi insiden |
| APO13.03.4 | Tidak ada kesenjangan |

Tabel 5 Hasil *Gap Analysis* DSS05

| Management Practice | Kesenjangan |
|---|---|
| DSS05.01.1<br>DSS05.01.4 | Lembaga XYZ hanya menginstal dan mengaktifkan alat perlindungan perangkat lunak berbahaya pada sebagian peralatan, serta tidak mendistribusikan perangkat lunak perlindungan secara terpusat. |
| DSS05.01.3<br>DSS05.01.5 | Lembaga XYZ tidak mengkomunikasikan kesadaran tentang perangkat lunak berbahaya dan tidak menegakkan prosedur pencegahan, serta tidak melakukan *review* dan evaluasi informasi tentang ancaman baru secara teratur. |
| DSS05.02.1<br>DSS05.02.3 | Tidak ada kesenjangan |
| DSS05.02.2<br>DSS05.02.4<br>DSS05.02.5<br>DSS05.02.7 | Lembaga XYZ tidak mewajibkan semua lalu lintas dikantor melalui VPN, hanya sebagian peralatan jaringan yang dikonfigurasi dengan cara yang aman, tidak mengenkripsi data sesuai dengan klasifikasinya, dan tidak ada mekanisme yang didukung untuk memastikan penerimaan informasi yang aman. |
| DSS05.02.6<br>DSS05.02.8<br>DSS05.02.9 | Lembaga XYZ tidak memiliki kebijakan yang ditetapkan dan diterapkan berdasarkan penilaian risiko dan persyaratan bisnis, serta tidak melakukan pengujian penetrasi dan pengujian keamanan sistem secara berkala. |
| DSS05.03.1<br>DSS05.03.2<br>DSS05.03.7 | Tidak ada kesenjangan |
| DSS05.03.3<br>DSS05.03.9 | Lembaga XYZ tidak mengelola akses dan kontrol jarak jauh dengan baik, dan manajemen akses sedang off. |
| DSS05.03.4<br>DSS05.03.5<br>DSS05.03.6 | Lembaga XYZ tidak mengonfigurasi semua jaringan dengan metode yang aman, pemfilteran lalu lintas jaringan endpoint hanya diterapkan saat menggunakan VPN, dan tidak semua sistem integrasi terlindungi dengan aman, termasuk penggunaan perangkat pribadi. |
| DSS05.03.8<br>DSS05.03.10 | Lembaga XYZ sudah melakukan pembuangan dan penghapusan data dengan aman tetapi tidak memiliki dokumen prosedur penghapusan data, serta tidak mengenkripsi informasi yang disimpan sesuai dengan klasifikasinya. |
| DSS05.04.1 | Tidak ada kesenjangan |
| DSS05.04.2<br>DSS05.04.8 | Perubahan hak akses belum dikelola dengan maksimal secara tepat waktu dan belum terdokumentasi, serta tidak ada tinjauan rutin oleh manajemen atas semua akun dan hak terkait. |
| DSS05.04.3<br>DSS05.04.7 | Belum dilakukan pemantauan secara berkala mengenai akun pengguna dengan hak istimewa yang tidak dipisahkan, diminimalkan, dan diawasi, serta tidak ada jejak audit yang dipelihara untuk akses informasi. |
| DSS05.04.4<br>DSS05.04.6 | Lembaga XYZ tidak memiliki identifikasi unik untuk semua aktivitas pemrosesan informasi berdasarkan peran fungsional, dan hanya sebagian aktivitas pada sistem TI yang dapat diidentifikasi. |
| DSS05.04.5 | Autentikasi tidak dilakukan berdasarkan peran individu. |
| DSS05.05.1<br>DSS05.05.2<br>DSS05.05.3<br>DSS05.05.4<br>DSS05.05.6 | Tidak ada kesenjangan |
| DSS05.05.5<br>DSS05.05.7 | Sebagian besar izin akses sudah diotorisasi tapi belum dikelola dengan baik, serta tidak ada pelatihan kesadaran keamanan informasi fisik yang dilakukan secara teratur. |
| DSS05.06.1<br>DSS05.06.4<br>DSS05.06.5 | Aktivitas penerimaan, penggunaan, penghapusan, dan pembuangan dokumen sensitif serta perangkat output sudah dilakukan akan tetapi belum ada prosedurnya, inventarisasi dokumen sensitif dan *output devi*ces tidak dilakukan, dan tidak ada pengamanan fisik yang memadai untuk dokumen sensitif. |
| DSS05.06.2<br>DSS05.06.3 | Kontrol kriptografi tidak diterapkan untuk melindungi informasi elektronik sensitif, dan lembaga XYZ tidak melakukan pelatihan berkala tentang malware dan penggunaan *email* serta Internet. |
| DSS05.07.1<br>DSS05.07.3 | Tidak menggunakan teknologi yang didukung untuk mengidentifikasi kerentanan keamanan informasi seperti menerapkan teknologi pemindai kerentanan, serta tidak secara teratur meninjau log peristiwa untuk potensi insiden. |
| DSS05.07.2 | Tidak mengomunikasikan skenario risiko dengan menyeluruh hanya sebatas dokumen penaganan risiko terkait data saja. |
| DSS05.07.4<br>DSS05.07.5 | Tidak membuat tiket insiden terkait keamanan secara tepat waktu dan tidak mencatat serta menyimpan catatan peristiwa terkait keamanan untuk periode yang ditentukan. |

## D. Fase 4 – *Build Improvement*

Pada tahap peningkatan (*build improvement*), langkah pertama adalah menyusun rencana perubahan berdasarkan kondisi eksisting yang teridentifikasi dari tahap penilaian kapabilitas dan analisis kesenjangan (*gap analysis*). Setelah mengetahui kesenjangan yang ada, langkah perbaikan konkret akan diambil untuk mengatasi masalah tersebut. Fokus utama adalah meningkatkan kualitas tata kelola TI di Lembaga XYZ, dengan penekanan khusus pada aspek

keamanan informasi. Rekomendasi yang akan dirumuskan pada tahap ini akan berfungsi sebagai panduan bagi Lembaga XYZ dalam memperbaiki dan meningkatkan tata kelola TI mereka. Rekomendasi ini akan mencakup tiga aspek utama: *people*, *process*, dan *technology*, sehingga memastikan bahwa perbaikan yang diusulkan mencakup berbagai elemen yang relevan dan penting bagi keseluruhan sistem.

Tabel 6 Rekomendasi Perbaikan APO13

| Aktivitas | Aspek | Tipe | Improvement |
|---|---|---|---|
| APO13.02.1<br>APO13.02.2<br>APO13.02.3 | *Process* | *Policy* | Membuat kebijakan untuk pedoman manajemen risiko keamanan informasi yang komprehensif. |
| | | *Procedure* | Membuat prosedur untuk mengidentifikasi, menganalisis dan mengelola risiko keamanan informasi. |
| | | *Record* | Membuat dokumentasi hasil manajemen risiko. |
| APO13.02.4<br>APO13.02.7 | *Process* | *Policy* | Kembangkan kebijakan untuk praktik manajemen risiko dan pengukuran efektivitas praktik manajemen risiko. |
| APO13.03.1<br>APO13.03.2<br>APO13.03.3<br>APO13.03.5 | *Process* | *Policy* | Membuat kebijakan untuk pemeliharaan rencana keamanan berdasarkan temuan dari aktivitas pemantauan dan *review*. |
| | | *Procedure* | Membuat prosedur untuk *review* dan audit ISMS secara berkala dan terdokumentasi. |
| | | *Record* | Menyimpan hasil *review* dan audit. |
| | *People* | *Roles* | Menetapkan peran auditor internal |

Tabel 7 Rekomendasi Perbaikan DSS05

| Aktivitas | Aspek | Tipe | Improvement |
|---|---|---|---|
| DSS05.01.1<br>DSS05.01.4 | *Process* | *Policy* | Membuat kebijakan pengaktifan alat perlindungan perangkat lunak secara terpusat |
| | | *Procedure* | Membuat prosedur standar instalasi dan aktivasi perangkat lunak perlindungan *malware* secara terpusat. |
| | | *Record* | Membuat dokumentasi seluruh kegiatan |
| DSS05.01.3<br>DSS05.01.5 | *People* | *Skill & Awareness* | Mengadakan pelatihan rutin untuk meningkatkan kesadaran karyawan tentang ancaman perangkat lunak berbahaya dan cara mencegahnya. |
| DSS05.02.2<br>DSS05.02.4<br>DSS05.02.5<br>DSS05.02.7 | *Process* | *Policy* | Membuat kebijakan keamanan jaringan yang mencakup penggunaan VPN dan enkripsi data. |
| DSS05.02.6<br>DSS05.02.8<br>DSS05.02.9 | *Process* | *Policy* | Membuat kebijakan keamanan jaringan dan pengujian penetrasi |
| | | *Procedure* | Membuat prosedur untuk melakukan pengujian penetrasi dan pengujian keamanan sistem secara berkala. |
| | | *Record* | Membuat dokumentasi hasil pengujian keamanan |
| | *People* | *Roles* | Menetapkan peran pentester |
| DSS05.03.3<br>DSS05.03.9 | *People* | *Responsibility* | Menetapkan penanggung jawab dalam tim IT untuk mengelola akses dan kontrol jarak jauh |
| DSS05.03.4<br>DSS05.03.5<br>DSS05.03.6 | *Process* | *Policy* | Membuat kebijakan untuk memastikan semua jaringan dan sistem integrasi terlindungi dengan metode yang aman. |
| DSS05.03.8<br>DSS05.03.10 | *Process* | *Policy* | Membuat kebijakan untuk enkripsi informasi yang disimpan sesuai dengan klasifikasinya |
| | | *Procedure* | Membuat prosedur penghapusan data yang aman |
| | | *Record* | Membuat dokumentasi proses dan hasil penghapusan data |
| DSS05.04.2<br>DSS05.04.8 | *Process* | *Policy* | Membuat kebijakan tentang identitas pengguna dan hak akses. |
| | | *Procedure* | Membuat prosedur untuk dokumentasi dan tinjauan rutin atas semua akun dan hak terkait. |
| DSS05.04.3<br>DSS05.04.7 | *Process* | *Record* | Menyimpan jejak aktivitas akses informasi. |
| DSS05.04.4<br>DSS05.04.6 | *Technology* | *Tools* | Menggunakan alat manajemen identitas dan akses (IAM) yang mendukung pemantauan dan pelacakan aktivitas pengguna. |
| | | *Features* | Alat IAM tersebut memiliki fitur pelacakan dan pelaporan aktivitas akses pengguna. |
| DSS05.04.5 | *Technology* | *Tools* | Menggunakan alat manajemen identitas dan akses yang mendukung autentikasi berbasis peran. |
| | | *Features* | Alat memiliki fitur autentikasi yang fleksibel dan dapat disesuaikan dengan peran individu. |
| DSS05.05.5<br>DSS05.05.7 | *Process* | *Policy* | Membuat kebijakan tentang akses fisik ke aset I&T. |
| DSS05.06.1<br>DSS05.06.4<br>DSS05.06.5 | *Process* | *Policy* | Membuat kebijakan untuk mengelola dokumen sensitif dan perangkat *output* |
| | | *Procedure* | Membuat prosedur untuk penerimaan, penggunaan, penghapusan, dan pembuangan dokumen sensitif serta perangkat *output*. |
| | | *Record* | Menyimpan catatan inventarisasi dokumen sensitif dan perangkat *output*. |
| DSS05.06.2<br>DSS05.06.3 | *Process* | *Policy* | Membuat kebijakan kontrol kriptografi untuk melindungi informasi elektronik sensitif |
| DSS05.07.1<br>DSS05.07.3 | *Process* | *Policy* | Membuat kebijakan identifikasi kerentanan keamanan informasi |
| | *Technology* | *Tools* | Menggunakan alat pemindai kerentanan yang mendukung identifikasi kerentanan keamanan informasi |
| | | *Features* | Memastikan alat tersebut memiliki fitur peninjauan log peristiwa secara otomatis dan teratur |
| DSS05.07.2 | *People* | *Communications* | Mengadakan sesi pertemuan secara berkala antara manajemen dan karyawan, di mana skenario risiko dibahas secara mendalam. |
| DSS05.07.4<br>DSS05.07.5 | *Process* | *Policy* | Membuat kebijakan yang mengatur tentang kerentanan |

| Aktivitas | Aspek | Tipe | Improvement |
|---|---|---|---|
| | | | dan pemantauan infrastruktur untuk kejadian terkait keamanan. |
| | *Techno logy* | *Tools* | Menggunakan sistem manajemen insiden yang mendukung pembuatan tiket otomatis dan penyimpanan catatan peristiwa keamanan |
| | | *Features* | Memastikan sistem tersebut memiliki fitur pelacakan insiden dan pelaporan yang komprehensif. |

## V. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan dalam analisis kapabilitas tata kelola TI di Lembaga XYZ Provinsi Jawa Barat menggunakan *framework* COBIT 2019 pada aspek keamanan informasi dapat ditarik kesimpulan sebagai berikut:

Penelitian ini menggunakan *framework* COBIT 2019 untuk mengukur tingkat kapabilitas tata kelola TI di Lembaga XYZ, dengan fokus pada aspek keamanan informasi. Berdasarkan analisis yang dilakukan, diperoleh hasil sebagai berikut: proses APO13 (*Managed Security*) mencapai nilai 2.3 dari target 3, sedangkan proses DSS05 (*Managed Security Services*) memperoleh nilai 1.2 dari target 4. Hasil ini menunjukkan adanya kesenjangan antara kondisi eksisting dengan kondisi target yang diharapkan dalam tata kelola TI pada aspek keamanan informasi di Lembaga XYZ.

Kondisi tata kelola TI di Lembaga XYZ pada domain APO13 dan DSS05 menunjukkan bahwa lembaga ini belum memiliki pedoman kebijakan manajemen keamanan informasi yang komprehensif, serta kurangnya prosedur terdokumentasi untuk pemeliharaan layanan keamanan informasi. Selain itu, praktik manajemen keamanan informasi belum diterapkan secara konsisten dan merata. Hal ini menunjukkan adanya kekurangan yang signifikan dalam manajemen keamanan informasi di Lembaga XYZ.

Untuk meningkatkan tata kelola TI di Lembaga XYZ berdasarkan COBIT 2019 pada domain APO13 dan DSS05, perlu dilakukan beberapa perbaikan. Perbaikan tersebut meliputi penerapan kebijakan dan prosedur yang komprehensif, pelaksanaan sosialisasi, penyelenggaraan pelatihan rutin, serta penerapan *tools* terkait manajemen keamanan informasi dan keamanan layanan TI. Implementasi perbaikan ini dapat meningkatkan efektivitas pengelolaan keamanan informasi dan memperkuat kontrol keamanan informasi di Lembaga XYZ.

## REFERENSI


[1] A. D. Purba, I. K. A. Purnawan, and I. Pratama, "Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 Dengan COBIT 5," *Jurnal Ilmiah Merpati*, 2018, [Online]. Available: https://www.researchgate.net/profile/I-Putu-Agus-Eka-Pratama/publication/337522009_Audit_Keamanan_TI_Menggunakan_Standar_ISOIEC_27002_dengan_COBIT_5/links/5ea2ae01299bf1438943fb8a/Audit-Keamanan-TI-Menggunakan-Standar-ISO-IEC-27002-dengan-COBIT-5.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail&_rtd=e30%3D

[2] "Instruksi Presiden Republik Indonesia," 2003.

[3] H. Setiawan and K. Mustofa, "Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia," *JURNAL IPTEKKOM* , 2013, [Online]. Available: https://jurnal.kominfo.go.id/index.php/iptekkom/article/view/506

[4] A. Nisri, "Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019," *Jurnal Tata Kelola dan Kerangka Kerja Teknologi*, 2023, [Online]. Available: https://ojs.unikom.ac.id/index.php/jtk3ti/article/view/9672

[5] M. E. Whitman and H. J. Mattord, "Principles of Information Security Fourth Edition," *Learning*, 2011.

[6] M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," *JEPIN (Jurnal Edukasi dan Penelitian*, 2021, [Online]. Available: https://jurnal.untan.ac.id/index.php/jepin/article/view/48228

[7] B. Panjaitan and L. Abdurrahman, "Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001: 2013 Menggunakan Kontrol Annex: Studi Kasus: Data Center PT. XYZ," *eProceedings*, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/viewFile/14682/14459

[8] A. Muliani, *Tata Kelola Teknologi Informasi*. Deli Serdang: PT Cahaya Rahmat Rahmani, 2023.

[9] H. Kusbandono, D. Ariyadi, and T. Lestariningsih, *Tata Kelola Teknologi Informasi*. CV. Nata Karya, 2019.

[10] S. F. Bayastura and S. Krisdina, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," *JIKO (Jurnal Informatika)*, 2021, [Online]. Available: http://ejournal.unkhair.ac.id/index.php/jiko/article/view/2977

[11] D. Krismayanti and T. Sutabri, "Analisis IT Service Management (ITSM) Pada Layanan Administrasi Mahasiswa STIPER Sriwigama Menggunakan Framewok ITIL V3," 2023, [Online]. Available: http://journal.ilmudata.co.id/index.php/ijmst/article/view/149

[12] S. R. Musyarofah and R. Bisma, "Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001: 2013 dan ISO/IEC 27002: 2013 pada Dinas Komunikasi Informatika," 2020, [Online]. Available: https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/36860

[13] ISACA, *COBIT® 2019 Framework : introduction and methodology*. 2018.
[14] ISACA, *COBIT 2019 Design guide designing an information and technology governance solution*. 2018.
[15] A. Hevner, S. March, J. Park, and S. Ram, "Design Science in information system research.[viitattu 10.9. 2012]," 2004.
[16] K. Peffers, T. Tuunanen, and M. A. Rothenberger, "A design science research methodology for information systems research," 2007, [Online]. Available: https://www.jstor.org/stable/40398896