Audit Keamanan Sistem Informasi PERJADIN BKKBN Provinsi Riau Menggunakan COBIT 19: APO12 dan APO13

Akmal Andri Yantama[1], Afifah Mesha Putri*[2], Sekar Arum Wulandari[3], Almuhadi[4], Megawati[5]
[1,2,3,4,5]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim
Riau, Indonesia
Email: [1]12050312486@students.uin-suska.ac.id, [2]12050322534@students.uin-suska.ac.id, [3]12050322463@students.uin-suska.ac.id, [4]12050312101@students.uin-suska.ac.id, [5]megawati@uin-suska.ac.id

Abstract

The process of digitalization has occurred in various aspects of life around us. BKKBN is one of the state agencies, namely BKKBN. BKKBN (National Population and Family Planning Agency) is a government agency in Indonesia that is responsible for planning and controlling population and implementing family planning programs. In the governance of business processes in it, the PERJADIN (Service Travel) system is used which regulates activities related to official travel information for workers there. The purpose of this research is to audit the PERJADIN system at the agency. The audit is carried out in order to improve the quality of the system used, besides that it also aims to find out how maximum the system is used. The audit was conducted using COBIT 2019 in the APO12 and APO13 domains. The APO12 and APO13 domains were chosen considering the importance of the letters in the system, therefore system security is the most important thing. This audit aims to evaluate the implementation of relevant security controls in the PERJADIN system and determine the agency's level of compliance with the security standards set out in COBIT 2019. It is expected that this research can contribute to strengthening the security of the PERJADIN system. The audit results and improvement recommendations provided can be a reference for agencies in improving security controls in the management of the PERJADIN system, as well as improving compliance with the security standards set out in COBIT 2019 in domains APO12 and APO13.

***Keyword** : Audit, PERJADIN System, BKKBN, COBIT 2019, APO12, APO13*

Abstraksi

Proses digitalisasi telah terjadi di berbagai aspek kehidupan di sekitar kita. BKKBN pada salah satu badan instansi milik negara yaitu BKKBN. BKKBN (Badan Kependudukan dan Keluarga Berencana Nasional) adalah lembaga pemerintah di Indonesia yang bertanggung jawab dalam perencanaan dan pengendalian kependudukan serta pelaksanaan program Keluarga Berencana (KB). Dalam tata kelola proses bisnis yang ada di dalamnya digunakan sistem PERJADIN (Perjalanan Dinas) yang mengatur aktivitas terkait informasi perjalanan dinas bagi pekerja di sana. Tujuan penelitian ini adalah untuk melakukan audit terhadap sistem PERJADIN di Instansi tersebut. Audit

dilakukan guna meningkatkan kualitas sistem yang digunakan selain itu juga bertujuan mencari tahu seberapa maksimal sistem IT yang digunakan. Audit dilakukan menggunakan COBIT 2019 pada domain APO12 dan APO13. Domain yang APO12 dan APO13 dipilih mengingat begitu pentingnya surat-surat yang ada pada sistem oleh sebab itu keamanan sistem menjadi hal yang terpenting. Audit ini bertujuan untuk mengevaluasi implementasi kontrol keamanan yang relevan dalam sistem PERJADIN dan menentukan tingkat kepatuhan instansi terhadap standar keamanan yang ditetapkan dalam COBIT 2019. Diharapkan penelitian ini dapat memberikan kontribusi dalam memperkuat keamanan sistem PERJADIN. Hasil audit dan rekomendasi perbaikan yang diberikan dapat menjadi acuan bagi instansi dalam meningkatkan kontrol keamanan dalam pengelolaan sistem PERJADIN, serta meningkatkan kepatuhan terhadap standar keamanan yang ditetapkan dalam COBIT 2019 pada domain APO12 dan APO13.

Kata Kunci : *Audit, Sistem PERJADIN, BKKBN, COBIT 2019, APO12, APO13*

1. PENDAHULUAN

BKKBN atau Badan Kependudukan dan Keluarga Berencana Nasional merupakan suatu lembaga pemerintah di Indonesia yang didirikan dengan tujuan untuk mengendalikan pertumbuhan penduduk serta melaksanakan program Keluarga Berencana (KB). Pertumbuhan penduduk yang cepat dan tidak terkendali dapat memiliki dampak negatif terhadap pembangunan dan kesejahteraan masyarakat. Sebelum didirikannya BKKBN, Indonesia menghadapi masalah serius dalam hal pertumbuhan penduduk yang tinggi dan kurangnya akses dan pengetahuan mengenai pengaturan keluarga. Dalam dekade 1960-an, pertumbuhan penduduk Indonesia mencapai tingkat yang sangat tinggi, yang berpotensi memberikan tekanan pada sumber daya alam, infrastruktur, dan pembangunan nasional secara umum.

Dalam proses operasionalnya telah diterapkan berbagai teknologi informasi sebagai penunjang efisiensi kerja di instansi. Salah satunya adalah dengan penerapan PERJADIN. Sistem PERJADIN di BKKBN Riau merupakan sistem yang digunakan untuk mengelola perjalanan dinas yang dilakukan oleh pegawai BKKBN Riau. Sistem ini bertujuan untuk memudahkan proses perencanaan, pengendalian, dan pelaporan perjalanan dinas serta memastikan transparansi dan akuntabilitas dalam pengelolaan perjalanan dinas di lingkungan BKKBN Riau. Sistem ini telah memberikan manfaat yang signifikan, antara lain meningkatkan efisiensi proses perjalanan dinas, mengurangi potensi kesalahan dan penyalahgunaan anggaran, serta meningkatkan transparansi dan akuntabilitas dalam pengelolaan perjalanan dinas[1].

Dalam rangka memastikan keamanan, integritas, dan ketersediaan sistem PERJADIN, serta mendukung pencapaian tujuan organisasi secara efektif, penting untuk melakukan audit yang terstruktur dan menyeluruh[2]. Salah satu kerangka audit yang umum digunakan adalah COBIT (Control Objectives for Information and Related Technologies)[3], yaitu sebuah kerangka kerja yang terkenal serta diakui secara internasional untuk pengelolaan dan pengendalian teknologi informasi[4]. Versi terbaru dari COBIT adalah COBIT 2019, yang memberikan panduan yang komprehensif dalam

merancang, mengimplementasikan, dan mengelola tata kelola teknologi informasi yang efektif[5]. Melalui audit menggunakan metode COBIT 2019 domain APO12 dan APO13, dapat dievaluasi implementasi kontrol keamanan yang relevan dalam sistem PERJADIN di instansi Perwakilan BKKBN Provinsi Riau[6]. Audit ini akan memberikan pemahaman yang lebih baik tentang kepatuhan instansi Perwakilan BKKBN Provinsi Riau terhadap standar keamanan yang ditetapkan dalam COBIT 2019[7].

Domain yang dipilih ialah APO12 dan APO13, domain ini di pilih karena pada studi kasus kali ini berfokus kepada keamanan sistem mengingat sistem yang digunakan berisi surat-surat penting. Pemangku kepentingan utama harus selalu mendapat informasi melalui artikulasi status risiko, termasuk skenario terburuk dan skenario yang paling mungkin terjadi.

Penelitian ini akan memberikan kontribusi penting dalam meningkatkan keamanan sistem PERJADIN di instansi. Hasil audit akan mengidentifikasi kelemahan dan celah dalam implementasi keamanan saat ini serta memberikan rekomendasi perbaikan yang dapat membantu instansi untuk meningkatkan pengendalian keamanan dan meminimalkan risiko yang mungkin timbul[8]. Dengan adanya audit menggunakan metode COBIT 2019 pada domain APO12 dan APO13, diharapkan instansi dapat memperkuat tata kelola dan keamanan sistem PERJADIN, menjaga keutuhan data, melindungi informasi sensitif, dan meningkatkan kinerja operasional serta reputasi instansi secara keseluruhan[9].

1.1. Penelitian Terdahulu

Berdasarkan penelitian yang berjudul "Rencana Audit Teknologi Informasi Menggunakan COBIT 2019 Pada Unit ISTI Universitas Telkom" (Fadhilah et al., 2021), didapatkanlah hasil dari analisis penelitian berupa rekomendasi rencana audit teknologi informasi berdasarkan COBIT 2019, yang dimana di dalamnya terdapat lingkup audit, metode audit, sumber daya yang dibutuhkan, jadwal pemeriksaan, yang dapat diterapkan pada unit Infrastruktur TI Direktorat Pusat Teknologi Informasi (PuTI) Universitas Telkom dengan menyesuaikan dari kebutuhan bisnis maupun kebutuhan TI organisasi.

Selain itu berdasarkan penelitian yang berjudul "Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan *Framework* COBIT 2019 pada PT XYZ Balikpapan"[10], didapatkan Hasil dari perancangan manajemen TI menggunakan *framework* COBIT 2019 diperoleh *core* model yang penting bagi PT XYZ Balikpapan dengan masing-masing *core* model memiliki nilai lebih dari 75 dengan masing-masing tingkat kapabilitas pada level 4. Adapun *core* model diantaranya yaitu APO09 *Managed Service Agreements*, APO12 *Managed Risk*, APO13 *Managed Security*, dan DSS02 *Managed Service Requests & Incidents*.

1.2. COBIT 2019

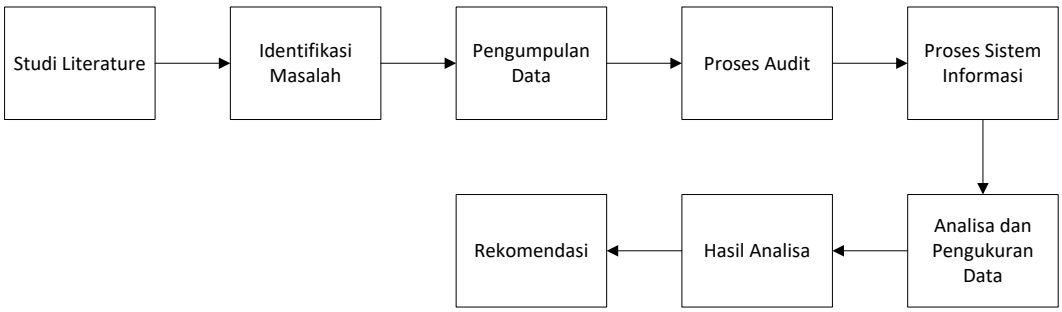
COBIT 2019 adalah kerangka kerja yang menyediakan prinsip, praktik, alat, dan model yang diterima secara global untuk meningkatkan kepercayaan dan nilai dari IT

perusahaan. Tata kelola yang efektif atas informasi dan teknologi sangat penting untuk kesuksesan bisnis, tentunya harus dikelola secara holistik menggunakan model proses yang terintegrasi, bersifat *end-to-end*, melingkupi pembagian peran dan tanggung jawab serta implementasi praktik terbaik. Di sinilah peranan penting dari COBIT 2019 untuk melakukan kontrol dan memaksimalkan nilai dari informasi dan teknologi. Sehingga, organisasi mencapai optimalisasi risiko, tata kelola dan manajemen IT. COBIT 2019 adalah evolusi dari versi sebelumnya, COBIT 5[11].

Pada dasarnya kerangka COBIT merupakan standar terhadap kendali- kendali yang umum berlaku di dunia teknologi informasi di mana kerangka kerja ini dapat diterima dan diterapkan secara global. Pada COBIT 2019, ada 7 komponen tata kelola yang perlu diperhatikan agar dapat mencapai objektif tata kelola yaitu penciptaan nilai (*value creation*), yaitu: proses, struktur organisasi, prinsip-prinsip, kebijakan dan kerangka kerja, informasi, kultur, etik, kebiasaan, SDM, keterampilan dan kompetensi, layanan, infrastruktur dan aplikasi.

2. METODE PENELITIAN

Metodologi penelitian merujuk pada langkah-langkah sistematis yang diikuti oleh seorang peneliti. Metodologi ini menyediakan kerangka kerja untuk merancang suatu penelitian yang valid, reliabel, dan dapat dipertanggungjawabkan. Berikut adalah beberapa komponen utama dalam metodologi penelitian dapat dilihat pada gambar 1:



Gambar 1. Metodologi Penelitian

Pada gambar di atas dapat dilihat pendalaman artikel ini dimulai dari studi literatur yaitu mencari artikel-artikel terkait sebagai referensi penulis setelah itu dilakukan analisis dan identifikasi masalah sehingga pada akan menghasilkan rekomendasi kepada instansi terkait. Berikut penjabaran tentang setiap tahapan[12].

2.1. Studi Literatur

Studi literatur sebuah kegiatan yang berguna dalam mempelajari penelitian yang telah ada sebelumnya termasuk literatur yang berhubungan dengan topik pengelolaan investasi teknologi informasi. Kegiatan ini dapat dilakukan melalui beberapa sumber seperti buku, *paper*, maupun internet *sources* yang masih relevan dengan penelitian mengenai topik audit sistem informasi sistem kepegawaian dengan *framework* COBIT 2019[13].

2.2. Identifikasi Masalah

Identifikasi masalah dilakukan guna menentukan rumusan masalah yang bersifat umum hingga ke bagian yang lebih spesifik termasuk mencoba melihat ruang lingkup dari objek yang diaudit, analisa visi, misi, tujuan dari objek tersebut, dan cara atau upaya menyelesaikan masalah.

2.3. Pengumpulan Data

Metode yang digunakan untuk mengumpulkan data adalah kuesioner, wawancara, dan observasi. Kuesioner terdiri dari serangkaian pertanyaan dengan kemungkinan jawaban yang disiapkan agar responden dapat memilih jawaban yang paling sesuai. Untuk membantu dalam menentukan tingkat kapasitas yang sesuai dengan pertanyaan yang dapat diakses dalam kerangka kerja COBIT 2019, peneliti menggunakan pendekatan skala Likert dalam kuesioner ini[14].

2.4. Proses Audit

Proses audit yang dilakukan pertama ialah menentukan ruang lingkup audit yang mencakup objek, orang yang akan di audit, dan observasi data lapangan. Lingkup audit perlu didefinisikan dengan baik agar audit dapat difokuskan dan efisien. Berkomunikasi dengan pihak terkait, termasuk manajemen, untuk memberi tahu mengenai audit yang akan dilakukan, tujuannya, serta aspek-aspek lain yang relevan. Ini juga mencakup penentuan pemangku kepentingan yang akan diwawancara atau terlibat dalam proses audit.

2.5. Proses Sistem Informasi

Pada proses sistem informasi ini peneliti melakukan analisis terhadap sistem yang digunakan, untuk melihat siapa saja yang terlibat pada sistem hingga mencari tahu siapa yang bertanggung jawab terhadap sistem. Dimana hal ini menjadi sangat penting untuk mengetahui kepada siapa peneliti harus melakukan audit.

2.6. Analisa dan Pengumpulan Data

Pada tahapan ini dilakukanlah pengumpulan data sesuai dengan desain penelitian. Ini dapat mencakup wawancara, survei, observasi, atau pengambilan data dari instansi terkait. Memastikan bahwa data yang dikumpulkan valid dan akurat. Proses ini melibatkan pengecekan dan konfirmasi keabsahan data. Melakukan analisis data sesuai dengan pertanyaan penelitian.

2.7. Hasil Analisa

Setelah dilakukan pengumpulan data tahap selanjutnya ialah melakukan perhitungan terhadap data yang telah didapat menggunakan rumus yang telah ditetapkan.

2.8. Rekomendasi

Tahap ini merupakan analisa *capability* level terhadap domain COBIT 2019 yang dipilih serta dari hasil *capability* level yang diperoleh BKKBN Provinsi Riau Formula rekomendasi. Tahapan ini berupa penyusunan rekomendasi, peneliti akan merekomendasikan sesuai dengan hasil domain COBIT 2019 yang digunakan berdasarkan *maturity* level dan *expected* level oleh pihak BKKBN Provinsi Riau.

3. HASIL DAN PEMBAHASAN

3.1. Identifikasi Masalah Sistem

Berikut daftar pertanyaan yang kami gunakan untuk mendeteksi permasalahan yang terdapat di sistem informasi PERJADIN Perwakilan BKKBN Provinsi Riau sebagai berikut.

Tabel 1. *List* Pertanyaan Indetifikasi Masalah

Pertanyaan	Jawaban	
	YA	TIDAK
Apakah pernah dilakukan evaluasi terhadap sistem PERJADIN ?	√	
Apakah pernah terjadi kendala terhadap pada website PERJADIN ?	√	
Apakah ada kemungkinan risiko keamanan terhadap sistem PERJADIN ?		√
Apakah ada dilakukan pemeriksaan berkala terhadap sistem PERJADIN ?		√
Apakah pernah terjadi kebocoran data pada sistem PERJADIN ?		√

Berdasarkan hasil wawancara pada tabel 1 yang telah dilakukan kepada Perencana Ahli Muda, ditemukan bahwa permasalahan sistem pada bagian keamanan sistem informasi PERJADIN Perwakilan BKKBN Provinsi Riau. Maka dari itu kami memilih domain APO13 untuk proses audit terhadap sistem informasi PERJADIN Perwakilan BKKBN Provinsi Riau karena sesuai dengan permasalahan yang terjadi terhadap sistem. Setelah dilakukannya audit sistem informasi kami dapat mengetahui tingkatan keamanan sistem PERJADIN perwakilan BKKBN Provinsi Riau menurut standar COBIT 2019. Selain itu kami juga menggunakan domain APO12 untuk mengukur manajemen risiko terhadap sistem karena ini berkaitan dengan keamanan sistem informasi.

3.2. Kuesioner

3.2.1. Pertanyaan *Capability* APO12

Daftar pertanyaan *capability* APO12 Level 2 pada tabel 2, daftar pertanyaan *capability* APO12 Level 3 pada tabel 3, daftar pertanyaan *capability* APO12 Level 4 pada tabel 4, daftar pertanyaan *capability* APO12 Level 5 pada tabel 5 berikut.

Tabel 2. Pertanyaan *Capability* APO12 Level 2

No	Pertanyaan Capability Level 2	Jawaban	
		Yes	No
1	Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI		
2	Mencatat data terkait risiko TI yang relevan dan signifikan di lingkungan operasi internal dan eksternal perusahaan.		
3	Menginventarisir proses bisnis dan mendokumentasikan ketergantungannya pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Perusahaan telah identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen outsourcing.		
4	Menentukan & menyetujui layanan TI dan sumber daya infrastruktur TI yang penting untuk menopang pengoperasian proses bisnis. Perusahaan telah menganalisis ketergantungan dan mengidentifikasi tautan TI yang lemah.		
5	Mengumpulkan skenario risiko TI saat ini menurut kategori, lini bisnis, dan area fungsional		
6	Menjaga inventaris aktivitas pengendalian yang ada untuk memitigasi risiko, dan yang memungkinkan risiko diambil sejalan dengan selera risiko dan toleransi. Perusahaan telah mengklasifikasikan dan memetakan aktivitas pengendalian ke skenario risiko TI yang spesifik dan agregasi skenario risiko TI.		

Tabel 3. Pertanyaan *Capability* APO12 Level 3

No	Pertanyaan Capability Level 3	Jawaban	
		Yes	No
1	Mengadopsi atau mendefinisikan taksonomi risiko untuk definisi yang konsisten dari skenario risiko dan kategori dampak & kemungkinan.		
2	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai dengan kategori dampak yang ditentukan dalam taksonomi risiko. Perusahaan telah menangkap data yang relevan dari masalah, insiden, dan investigasi terkait TI.		
3	Menentukan ruang lingkup yang tepat dari upaya analisis risiko, dengan mempertimbangkan semua faktor risiko dan kekritisan bisnis aset.		
4	Membangun dan memperbarui skenario risiko TI secara teratur; Perusahaan mengeksposur kerugian terkait TI; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang mengalir atau kebetulan. Perusahaan telah mengembangkan ekspektasi untuk aktivitas pengendalian khusus dan kemampuan untuk mendeteksi risiko TI.		
5	Memperkirakan frekuensi (kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.		
6	Membandingkan risiko saat ini (mengeksposur kerugian terkait TI) dengan selera risiko dan toleransi risiko yang diterima.		
7	Mengusulkan tanggapan risiko untuk risiko yang melebihi selera risiko dan tingkat toleransi.		
8	Menentukan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Perusahaan telah identifikasi persyaratan dan ekspektasi untuk pengendalian kunci (ahli) yang tepat untuk respons mitigasi risiko.		
9	Menangkap semua informasi profil risiko secara teratur dan menggabungkan ke dalam profil risiko gabungan.		
10	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko TI perusahaan.		
11	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam istilah & format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, perusahaan menyertakan probabilitas dan kisaran kerugian atau keuntungan bersama dengan tingkat kepercayaan, untuk memungkinkan manajemen menyeimbangkan pengembalian risiko.		
12	Memberi para pembuat keputusan pemahaman tentang skenario kasus terburuk dan yang paling memungkinkan, mengeksposur kerugian terkait TI dan reputasi yang signifikan, mempertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.		
13	Melaporkan profil risiko saat ini kepada semua pemangku kepentingan. Termasuk informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, gap, inkonsistensi, redundansi, status remediasi dan dampaknya terhadap profil risiko.		
14	Mengidentifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar serta peningkatan pertumbuhan dan pengembalian secara berkala untuk area dengan risiko relatif dan kesamaan kapasitas risiko.		
15	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.		
16	Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan.		
17	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.		

Tabel 4. Pertanyaan *Capability* APO12 Level 4

No	Pertanyaan Capability Level 4	Jawaban	
		Yes	No
1	Adanya Survei dan analisis data risiko TI yang historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, database, dan perjanjian industri untuk pengungkapan peristiwa umum.		
2	Untuk kelas acara serupa, atur data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Perusahaan menentukan faktor- faktor yang berkontribusi umum di berbagai peristiwa terkait risiko TI.		
3	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besaran kerugian.		
4	Melakukan peristiwa berkala dan analisis faktor risiko untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.		
5	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mencari bias.		
6	Berdasarkan semua data profil risiko, perusahaan menentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan cepat atas risiko dan tren risiko saat ini.		
7	Menangkap informasi tentang peristiwa risiko TI yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan.		
8	Menangkap informasi tentang peristiwa risiko TI yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan.		
9	Menentukan sekumpulan proposal proyek yang dirancang untuk mengurangi risiko dan proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, efek pada profil risiko dan peraturan saat ini.		
10	Mengategorikan insiden dan membandingkan eksposur kerugian terkait TI dengan ambang batas toleransi risiko. Mengkomunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan dan perbaruan profil risiko.		
11	Memeriksa kejadian buruk/kerugian masa lalu dan peluang yang hilang dan menentukan akar penyebabnya.		

Tabel 5. Pertanyaan *Capability* APO12 Level 5

No	Pertanyaan Capability Level 5	Jawaban	
		Yes	No
1	Menganalisis biaya /manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi, mentransfer/berbagi, dan menerima dan mengeksploitasi / menyita. Konfirmasikan respons risiko yang optimal.		
2	Mengkomunikasikan akar masalah, persyaratan respons risiko tambahan, dan perbaikan proses kepada pengambil keputusan yang tepat. Memastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.		

3.2.2. Pertanyaan Capability APO13

Daftar pertanyaan *capability* APO13 Level 2 pada tabel 6, daftar pertanyaan *capability* APO13 Level 3 pada tabel 7, daftar pertanyaan *capability* APO13 Level 4 pada tabel 8 berikut.

Tabel 6. Pertanyaan *Capability* APO13 Level 2

No	Pertanyaan Capability Level 2	Jawaban	
		Yes	No
1	Menentukan ruang lingkup dan batasan sistem manajemen keamanan informasi dalam kaitannya dengan karakteristik perusahaan, organisasi, lokasinya, aset, dan teknologinya. Menyertakan detail, dan alasan untuk, pengecualian apa pun dari cakupan.		
2	Menentukan sistem manajemen keamanan informasi yang sesuai dengan kebijakan perusahaan dan konteks di mana perusahaan beroperasi.		
3	Menyelaraskan sistem manajemen keamanan informasi dengan pendekatan perusahaan secara keseluruhan untuk manajemen keamanan.		
4	Mendapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan atau mengubah sistem manajemen keamanan informasi		
5	Mempersiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup sistem manajemen keamanan informasi		
6	Mendefinisikan dan mengkomunikasikan peran dan tanggung jawab manajemen keamanan informasi.		
7	Mengkomunikasikan pendekatan sistem manajemen keamanan informasi.		

Tabel 7. Pertanyaan Capability APO13 Level 3

No	Pertanyaan Capability Level 3	Jawaban	
		Yes	No
1	Merumuskan dan memelihara rencana perlakuan risiko keamanan informasi yang selaras dengan tujuan strategis dan arsitektur perusahaan. Memastikan bahwa rencana tersebut mengidentifikasi praktik manajemen dan solusi keamanan yang tepat dan optimal, dengan sumber daya, tanggung jawab, dan prioritas terkait untuk mengelola risiko keamanan informasi yang teridentifikasi		
2	Menjaga sebagai bagian dari arsitektur perusahaan inventaris komponen solusi yang ada untuk mengelola risiko terkait keamanan.		
3	Mengembangkan proposal untuk mengimplementasikan rencana perlakuan risiko keamanan informasi, didukung oleh kasus bisnis yang sesuai yang mencakup pertimbangan pendanaan dan alokasi peran dan tanggung jawab.		
4	Memberikan masukan untuk desain dan pengembangan praktik manajemen dan solusi yang dipilih dari rencana perlakuan risiko keamanan informasi		
5	Menerapkan keamanan informasi dan pelatihan privasi dan program kesadaran		
6	Mengintegrasikan perencanaan, desain, implementasi, dan pemantauan prosedur keamanan dan privasi informasi serta kontrol lain yang mampu memungkinkan pencegahan yang cepat, deteksi peristiwa keamanan, dan respons terhadap insiden keamanan.		

Tabel 8. Pertanyaan Capability APO13 Level 4

No	Pertanyaan Capability Level 4	Jawaban	
		Yes	No
1	Menentukan bagaimana mengukur keefektifan praktek manajemen yang dipilih dalam menilai keefektifan untuk menghasilkan hasil yang sebanding dan dapat direproduksi		
2	Melakukan peninjauan berkala terhadap keefektifan sistem manajemen keamanan informasi. Menyertakan pemenuhan kebijakan dan tujuan sistem manajemen keamanan informasi dan meninjau praktik keamanan dan privasi.		
3	Melakukan audit sistem manajemen keamanan informasi pada interval yang direncanakan		
4	Melakukan tinjauan sistem manajemen keamanan informasi secara teratur untuk memastikan bahwa ruang lingkup tetap memadai dan perbaikan dalam proses sistem manajemen keamanan informasi teridentifikasi.		
5	Mencatat tindakan dan peristiwa yang dapat berdampak pada keefektifan atau kinerja sistem manajemen keamanan informasi		

3.3. Perhitungan APO12 – Managed Risk

Tabel 9. RACI Chart untuk Control Objective APO12

APO12	Kepala Perwakilan	Sekretaris Bendahara	Pranata Komputer	Perencana Ahli Muda
Mengidentifikasi dan mengumpulkan data yang relevan	A	I		R
Menganalisis resiko	A	I	R	R
Mempertahankan prodil risiko	A	I	R	R
Mengartikulasi risiko	A	I	R	R

APO12	Kepala Perwakilan	Sekretaris Bendahara	Pranata Komputer	Perencana Ahli Muda
Menentukan dan mengelola portofolio tindakan manajemen risiko	A	I	R	R
Menanggapi risiko	A	I	R	

Berdasarkan RACI chart pada tabel 9, kami mengambil Pranata Komputer dan Perencana Ahli Muda sebagai responden untuk proses audit di sistem ini hal ini dikarenakan perannya sebagai *responsible* pada sistem.

3.3.1. Perhitungan *Capability* Level 2-5 (Responden 1)

Berikut merupakan rekapitulasi hasil perhitungan data kuesioner level 2-5 oleh responden 1 yang ditampilkan pada tabel 10 berikut.

Tabel 10. Perhitungan Capability APO12 Level 2-5 (Responden 1)

Level	Kalimat	Yes	No.	Score
2	1	X		1
	2	X		1
	3	X		1
	4	X		1
	5	X		1
	6	X		1
	Total			6
Capability Level				100%

Level	Kalimat	Yes	No.	Score
3	1	X		1
	2	X		1
	3	X		1
	4	X		1
	5	X		1
	6	X		1
	7	X		1
	8	X		1
	9	X		1
	10	X		1
	11	X		1
	12	X		1
	13	X		1
	14	X		1
	15	X		1
	16	X		1
	17	X		1
	Total			17
Capability Level				100%

Level	Kalimat	Yes	No	Score
4	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	6	x		1
	7	x		1
	8	x		1
	9	x		1
	10	x		1
	11	x		1
	Total			11
Capability Level				100%

Level	Kalimat	Yes	No.	Score
5	1	x		1
	2	x		1
	Total			2
Capability Level				100%

Berdasarkan perhitungan di atas, didapatkanlah bahwa *Capability* APO12 Level 2, *Capability* Level 3, *Capability* Level 4, dan *Capability* Level 5 pada APO12 mendapatkan *Score* 100%.

3.3.2. Perhitungan *Capability* Level 2-5 (Responden 2)

Berikut merupakan rekapitulasi hasil perhitungan data kuesioner level 2-5 oleh responden 2 yang ditampilkan pada tabel 11 berikut.

Tabel 11. Perhitungan Capability APO12 Level 2-5 (Responden 2)

Level	Kalimat	Yes	No.	Score
2	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	6	x		1
	Total			6
Capability Level				100%

Level	Kalimat	Yes	No.	Score
3	1	X		1
	2	X		1
	3	X		1
	4	X		1
	5	X		1
	6		X	0
	7	X		1
	8	X		1
	9		X	0
	10	X		1
	11	X		1
	12	X		1
	13	X		1
	14	X		1
	15	X		1
	16	X		1
	17	X		1
	Total			15
Capability Level				88,23%

Level	Kalimat	Yes	No	Score
4	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	6	x		1
	7	x		1
	8	x		1
	9	x		1
	10		x	0
	11	x		1
	Total			10
Capability Level				90,90%

Level	Kalimat	Yes	No.	Score
5	1	x		1
	2	x		1
	Total			2
Capability Level				100%

Berdasarkan perhitungan di atas, didapatkanlah bahwa *Capability* APO12 Level 2 dan *Capability* Level 5 mendapatkan *Score* 100%, sedangkan untuk *Capability* Level 3 mendapatkan *Score* 88,23% dan *Capability* Level 4 mendapatkan Score 90,90%.

3.3.3. Hasil Capability Level 2-5 Objektif APO12

Hasil *capability* dihitung menggunakan rumus capability level pada rumus 1 untuk setiap level adalah sebagai berikut.

$$\text{Rumus Capability Level } (CLi) = \frac{\text{R1+R2}}{\sum \text{R}} x100\% \quad (1)$$

Keterangan :

Cli : Nilai Capability Level pada level x
R1 : Nilai Capability Level dari Responden 1 pada level x
R2 : Nilai Capability Level dari Responden 2 pada level x
$\sum$R : Jumlah Responden

1. Hasil *Capability* Level 2 Objektif APO12

$$CLi = \frac{100 + 100}{2} x100\% = \frac{200}{2} x100\% = 100\%$$

2. Hasil *Capability* Level 3 Objektif APO12

$$CLi = \frac{100 + 88}{2} x100\% = \frac{188}{2} x100\% = 94\%$$

3. Hasil *Capability* Level 4 Objektif APO12

$$CLi = \frac{100 + 91}{2} x100\% = \frac{191}{2} x100\% = 95{,}5\%$$

4. Hasil *Capability* Level 5 Objektif APO12

$$CLi = \frac{100 + 100}{2} x100\% = \frac{200}{2} x100\% = 100\%$$

3.4. Perhitungan APO13 – Managed Security

Tabel 12. RACI Chart untuk Control Objective APO13

APO13	Kepala Perwakilan	Sekretaris Bendahara	Pranata Komputer	Perencana Ahli Muda
Membangun dan memelihara sistemmanajemen keamanan informasi	A	I	R	
Menentukan dan mengelola perawatanrisiko keamanan dan privasi keamanan dan privasi informasi	A	I	R	R
Memantau dan meninjau sistem manajemen keamanan informasi	A	I	R	R

Berdasarkan RACI chart pada tabel 12, kami mengambil Pranata Komputer dan Perencana Ahli Muda sebagai responden untuk proses audit di sistem ini hal ini dikarenakan perannya sebagai *responsible* pada sistem.

3.4.1. Perhitungan Capability Level 2-5 (Responden 1)

Tabel 13. Perhitungan Capability APO13 Level 2-4 (Responden 1)

Level	Kalimat	Yes	No.	Score
2	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	6	x		1
	7	x		1
	Total			7
Capability Level				100%

Level	Kalimat	Yes	No.	Score
3	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	6	x		1
	Total			6
Capability Level				100%

Level	Kalimat	Yes	No	Score
4	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	Total			5
Capability Level				100%

Berdasarkan perhitungan pada tabel 13, didapatkanlah bahwa *Capability* APO13 Level 2, *Capability* Level 3 dan *Capability* Level 4 mendapatkan *Score* 100%.

3.4.2. Perhitungan Capability Level 2-5 (Responden 2)

Tabel 14. Perhitungan *Capability* APO13 Level 2-4 (Responden 2)

Level	Kalimat	Yes	No.	Score
2	1	x		1
	2	x		1
	3	x		1
	4		x	0
	5	x		1
	6	x		1
	7	x		1
	Total			6
Capability Level				85,71%

Level	Kalimat	Yes	No	Score
3	1	x		1
	2	x		1
	3	x		1
	4		x	0
	5	x		1
	6	x		1
	Total			6
Capability Level				83,33%

Level	Kalimat	Yes	No	Score
4	1	x		1
	2	x		1
	3	x		1
	4	x		1
	5	x		1
	Total			5
Capability Level				100%

Berdasarkan perhitungan pada tabel 14, didapatkanlah bahwa *Capability* APO13 Level 2 mendapatkan *Score* 85,71%, Capability Level 3 mendapatkan *Score* 83,33% dan *Capability* Level 4 mendapatkan *Score* 100%.

3.4.3. Hasil Capability Level 2-5 Objektif APO13

Hasil *capability* dihitung menggunakan rumus *capability* level pada rumus 1 untuk setiap level adalah sebagai berikut.

1. Hasil *Capability* Level 2 Objektif APO13

$$CLi = \frac{100 + 86}{2} x100\% = \frac{186}{2} x100\% = 93\%$$

2. Hasil *Capability* Level 3 Objektif APO13

$$CLi = \frac{100 + 83}{2} x100\% = \frac{183}{2} x100\% = 91{,}5\%$$

3. Hasil *Capability* Level 4 Objektif APO13

$$CLi = \frac{100 + 100}{2} x100\% = \frac{200}{2} x100\% = 100\%$$

3.5. Kesimpulan Hasil Capability Level Objektif

Berdasarkan tabel 15, dapat diketahui bahwa seluruh objektif yang dievaluasi merupakan domain Align, Plan and Organize (APO). Pada Proses APO12 – *Managed Risk*, tata kelola TI mendapatkan tingkat kemampuan berada pada level 5 dan APO13 –

Managed Security, tata kelola TI mendapat tingkat kemampuan yang berada pada level 4.

Tabel 15. Hasil Capability Level Objektif

Governance and Management Objective		Level	Keterangan Pencapaian
APO12	Managed Risk	5	Proses ini mencapai tujuannya, mendefinisikan dan meningkatkan dengan baik kinerjanya yang dapat diukur secara kuantitatif serta melakukan perbaikan terus-menerus.
APO13	Managed Security	4	Proses ini mencapai tujuannya dan mendefinisikan dengan baik kinerjanya yang dapat diukur secara kuantitatif.

Berdasarkan hasil evaluasi data kuesioner dari tiap-tiap responden yang terdiri dari 2 (dua) responden, didapatkan rekapitulasi dan hasil *capability* level 2 APO12 adalah 100%. Selanjutnya rekapitulasi dan hasil *capability* level 3 APO12 adalah 94%. Kemudian rekapitulasi dan hasil *capability* level 4 APO12 adalah 95,5%, dan rekapitulasi dan hasil *capability* level 5 APO12 adalah 100%.

Sedangkan untuk APO 13 hasil evaluasi data kuesioner yang didapatkan dari tiap-tiap responden yang terdiri dari 2 (dua) responden, rekapitulasi dan hasil *capability* level 2 APO13 adalah 93%. Selanjutnya rekapitulasi dan hasil *capability* untuk level 3 APO13 adalah 91,5%. Kemudian rekapitulasi dan hasil *capability* level 4 APO13 adalah 100%.

3.6. Rekomendasi

APO12 (*Managed Risk*) Level 5 pada COBIT 2019 merepresentasikan level *Optimized*, yaitu level kematangan tertinggi untuk sebuah proses. Pada tingkat ini, organisasi terus meningkatkan proses mereka untuk mencapai hasil terbaik. Berikut beberapa rekomendasi implementasi APO12 Level 5 di COBIT 2019[15]. Membangun Budaya Cerdas Risiko, Menumbuhkan budaya dalam organisasi yang menghargai dan memprioritaskan manajemen risiko. Mempromosikan kesadaran, akuntabilitas, dan kepemilikan risiko di semua tingkatan, dan memastikan bahwa praktik manajemen risiko tertanam dalam DNA organisasi[16]. Dengan menerapkan rekomendasi ini, organisasi dapat mencapai tingkat kematangan yang tinggi dalam mengelola risiko, memungkinkan mereka untuk secara proaktif mengidentifikasi dan mengatasi potensi ancaman terhadap tujuan perusahaan mereka.

Setelah dilakukan perhitungan dan audit sistem informasi kami dapat memberikan rekomendasi APO13 level 4. Berikut ini beberapa rekomendasi yang kami berikan.

1. Kebijakan dan Prosedur

   Pastikan organisasi memiliki kebijakan dan prosedur yang jelas terkait penggunaan sistem APO13 level 4. Kebijakan ini harus mencakup penggunaan yang benar, perlindungan data, dan tanggung jawab pengguna.
2. Pengelolaan Akses

Menerapkan sistem autentikasi yang kuat dan pengendalian akses yang tepat untuk memastikan hanya pengguna yang ter otorisasi yang mampu mengakses sistem. Periksa penggunaan kata sandi yang kuat dan sikap yang disarankan tentang penggantian kata sandi secara berkala[17]. Berikan akses sesuai kebutuhan kepada setiap pengguna dan pastikan pengguna memiliki hak yang tepat sesuai dengan tanggung jawab mereka dalam organisasi.

3. Keamanan Data

   Pastikan bahwa data yang disimpan dalam sistem APO13 level 4 dilindungi dengan teknologi enkripsi yang kuat, baik dalam transit maupun saat disimpan. Lakukan pengujian keamanan secara berkala untuk mengidentifikasi kerentanan potensial dan perbaiki mereka segera[18]. Tetapkan kebijakan penghapusan data yang aman untuk menghapus data yang tidak diperlukan lagi atau data yang telah melewati masa retensi yang ditentukan.

4. Manajemen Perubahan

   Terapkan proses manajemen perubahan yang baik untuk memastikan bahwa perubahan dalam sistem APO13 level 4 direncanakan, diaudit, dan dilakukan dengan hati-hati untuk meminimalkan risiko dan dampak yang tidak diinginkan.

5. Pemantauan dan Pendeteksian

   Pasang sistem pemantauan yang memadai untuk mengawasi aktivitas sistem dan mendeteksi upaya tidak sah atau aktivitas yang mencurigakan. Lakukan audit log secara rutin untuk memastikan kepatuhan dan memeriksa adanya aktivitas yang mencurigakan atau melanggar kebijakan.

6. Pemulihan Bencana

   Pastikan rencana pemulihan bencana yang sesuai untuk sistem APO13 level 4, termasuk cadangan data yang teratur dan pengujian pemulihan yang rutin

7. Pelatihan Pengguna

   Sediakan pelatihan yang memadai kepada pengguna tentang kebijakan, prosedur, dan praktik terbaik yang berkaitan dengan penggunaan sistem APO13 level 4. Dorong pengguna untuk melaporkan segala bentuk pelanggaran keamanan atau aktivitas mencurigakan yang mereka temui. Ingatlah bahwa ini hanya beberapa rekomendasi umum dan tidak menggantikan audit yang komprehensif oleh profesional keamanan informasi yang berkualifikasi.

4. KESIMPULAN

Dari penelitian yang dilakukan, dapat diketahui seluruh objektif yang dievaluasi adalah domain Align, Plan and Organize (APO). Kemudian pada Proses APO12 – Managed Risk, tata kelola TI mendapatkan tingkat kemampuan yang berada pada level 5 dan APO13 – Managed Security, serta tata kelola TI mendapat tingkat kemampuan yang berada pada level 4.

5. SARAN

Terdapat batasan pada penelitian ini karena hanya berfokus pada domain APO 12 dan APO 13. Selanjutnya dapat digunakan berbagai domain sehingga dapat memeriksa tata kelola IT secara keseluruhan *domain*-nya di COBIT–19.

DAFTAR PUSTAKA

[1] M. Khairul Anam, S. Dwi Putri, D. Yuliana, E. Yumami, and T. P. Lestari, "Application of the Cobit 2019 Framework To Analyse the Security of Academic Information Systems," *Decod. J. Pendidik. Teknol. Inf. ISSN*, vol. 3, no. 2, pp. 296–309, 2023.

[2] T. H. Thabit, "The Impact of Implementing COBIT 2019 Framework on Reducing the Risks of e-Audit," *Buhuth Mustaqbaliya Sci. Period. J.*, 2021, [Online]. Available: https://www.iasj.net/iasj/download/48792fe8bdb882af

[3] L. H. Atrinawati *et al.*, "Assessment of Process Capability Level in University XYZ Based on COBIT 2019," *J. Phys. Conf. Ser.*, vol. 1803, no. 1, 2021, doi: 10.1088/1742-6596/1803/1/012033.

[4] E. Nachrowi, Yani Nurhadryani, and Heru Sukoco, "Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 764–774, 2020, doi: 10.29207/resti.v4i4.2265.

[5] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu)," *2020 3rd Int. Conf. Comput. Informatics Eng. IC2IE 2020*, pp. 236–241, 2020, doi: 10.1109/IC2IE50715.2020.9274599.

[6] A. Fernandes, R. Almeida, and M. M. da Silva, "A flexible method for COBIT 2019 process selection," *26th Am. Conf. Inf. Syst. AMCIS 2020*, pp. 0–10, 2020.

[7] N. Sakron, G. Firmansyah, H. Akbar, and B. Tjahjono, "Audit of Information Technology Governance on School Operational Cost Flow in SMKN West Jakarta Using COBIT 2019," *J. Indones. Sos. Sains*, vol. 4, no. 09, pp. 763–772, 2023, doi: 10.59141/jiss.v4i09.881.

[8] M. Kesuma, R. H. Saputra, M. A. Syaputra, and J. Fitra, "Design Of Information Technology (IT) Governance Using Framework Cobit 2019 Subdomain APO01 (Case Study : Instidla)," vol. 01, 2019.

[9] M. H. Qolby, R. Mulyana, and W. A. Nurtrisha, "Perancangan Manajemen Pengembangan TI Agile Untuk Transformasi Digital InsurCo Dengan COBIT 2019 DevOps," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 1, pp. 462–475, 2023, doi: 10.30865/klik.v4i1.1152.

[10] A. A. Mariatama, L. H. Atrinawati, and M. G. L. Putra, "Perancangan Tata Kelola Teknologi Informasi Dengan Menggunakan Framework Cobit 2019 Pada Pt Jwt Global Logistics Indonesia," *J. Sist. Inf. dan Inform.*, vol. 5, no. 1, pp. 19–29, 2022, doi: 10.47080/simika.v5i1.1423.

[11] ISACA Governance and Manajement, *COBIT 2019 Governance and Management Objectives (ISACA)*. 2019. [Online]. Available: https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

[12] T. A. Karo Karo and A. Faza, "Evaluation of Integration and Human Resources in Information Technology Governance using COBIT 2019: PT. Pelabuhan Indonesia

Tanjung Priok Branch," *J. Inf. Syst. Informatics*, vol. 5, no. 3, pp. 902–914, 2023, doi: 10.51519/journalisi.v5i3.538.

[13] K. S. Gunawan, "Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector," *G-Tech J. Teknol. Terap.*, vol. 7, no. 3, pp. 1026–1036, 2023.

[14] M. A. Saputra and M. R. Redo, "Penerapan Framework Cobit 2019 Untuk Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi," *J. Sci. Soc. Res.*, vol. 4, no. 3, p. 352, 2021, doi: 10.54314/jssr.v4i3.715.

[15] Y. Megasyah and A. A. Arifnur, "Academic Information System Security Audits Using Cobit," *J. Appl. Eng. Technol. Sci.*, vol. 1, no. 2, pp. 124–135, 2020.

[16] S. Carlos, I. Simatupang, M. I. Fianty, S. Carlos, and I. Simatupang, "G-Tech : Jurnal Teknologi Terapan Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry," vol. 7, no. 4, pp. 1391–1400, 2023.

[17] W. Adi Nugroho and R. Sutomo, "Evaluation Of Information System Governance Capability Level Of Engineering Construction Services Firm Using Cobit Framework 5," *Int. J. Sci. Technol. Manag.*, vol. 4, no. 4, pp. 1015–1022, 2023, doi: 10.46729/ijstm.v4i4.879.

[18] C. A. Kasodu, A. D. Manuputty, and Sakiwan, "Evaluasi Penerapan Manajemen Layanan TI Menggunakan Framework COBIT 5 pada Subdomain APO09 Manage Service Agreements (Studi Kasus: Satuan …," *JuTISI (Jurnal Tek. …*, vol. 4, pp. 207–218, 2018.