BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu atau tinjauan empiris berisi tentang topik penelitian yang terkait dan mendukung proses penelitian ini sehingga dapat dijadikan acuan dalam prosesnya. Untuk mendukung penelitian ini secara empiris, penulis meninjau sejumlah penelitian terdahulu yang relevan dengan topik yang diangkat. Adapun penelitian-penelitian tersebut adalah sebagai berikut:

2.1.1 Evaluasi Tingkat Keamanan Sistem Informasi Menggunakan Kerangka Kerja COBIT 2019

Penelitian yang dilakukan Nasiri, 2023. Tujuan dari penelitian ini adalah mengevaluasi tingkat kapabilitas keamanan sistem informasi pada universitas XYZ menggunakan *framework* COBIT 2019. Sub-domain yang digunakan dalam penelitian ini yaitu APO12, APO13 dan DSS05 dengan maksud untuk mengidentifikasi berapa tingkat kapabilitas universitas XYZ dalam mengelola keamanan informasi. Hasil yang didapat adalah pengelolaan keamanan sistem informasi pada universitas XYZ untuk persyaratan sub-domain APO13, pengendalian keamanan informasi diperoleh hasil sebesar 28% pada evaluasi tingkat kapabilitasnya di tingkat 2. Hal ini berarti pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI) masih jauh dari persyaratan yang distandarkan oleh COBIT 2019 karena masih sebagian kecil (*partly*) dalam pelaksanaannya. Sedangkan pelaksanaan keamanan informasi untuk sub-domain DSS05 mencapai 69% pada tingkat kapabilitas 2, dengan sebagian besar persyaratan telah dilaksanakan. Pada kedua sub-domain tersebut, pencapaian tingkat kapabilitas masih di tingkat 2 atau tingkat yang paling rendah, dan tingkat kematangannya juga masih di posisi *partly* dan *largely* belum ada yang masuk ke kategori *fully*. Butuh usaha keras untuk bisa memenuhi semua persyaratan COBIT 2019 di level kapabilitas 2 secara penuh. Terdapat 19

rekomendasi perbaikan praktis yang perlu segera dilakukan untuk memenuhi persyaratan tingkat 2 agar dapat naik ke tingkat 3.

2.1.2 Evaluasi Tata Kelola dan Manajemen Infrastruktur TI pada Bank BPD XYZ menggunakan COBIT 2019

Penelitian yang dilakukan Budiana et al., 2024, tujuannya adalah untuk menilai tingkat *capability* dan *maturity level* saat ini, serta menganalisis kesenjangan dengan tingkat yang diharapkan. Analisis ini akan menjadi dasar untuk memberikan rekomendasi perbaikan pada 144 aplikasi yang dikelola mandiri pada *Data Center* dan *Disaster Recovery Center* Bank BPD XYZ yang terindikasi beberapa permasalahan dalam pengelolaan infrastruktur TI berdasarkan laporan monitoring dan audit dari regulator. Sub-domain yang digunakan dalam penelitian ini adalah EDM03, APO12, APO13, MEA03. Rekomendasi perbaikan tata kelola dan manajemen infrastruktur TI Bank BPD XYZ untuk mencapai tingkat kemampuan dan tingkat kematangan guna mencapai standar maksimal *fully*. Hal ini didasarkan pada hasil analisis kesenjangan. Rekomendasi dan saran berdasarkan standar COBIT 2019. Hasil tersebut digunakan sebagai acuan dalam penyusunan inisiatif rekomendasi dan selanjutnya kegiatan rekomendasi dan perbaikan untuk mencapai kondisi keselarasan tata kelola dan manajemen yang diharapkan pada Bank BPD XYZ.

2.1.3 Assessment Penggunaan COBIT 2019 dalam Pengelolaan TI Pada Institusi Perguruan Tinggi

Menurut penelitian yang dilakukan Anadya Tafdhilla et al., 2023, Fokus utama perguruan tinggi dan sekolah tinggi dalam menerapkan *framework* COBIT 2019 adalah pada sub-domain DSS05. Di banyak institusi pendidikan tinggi yang menerapkan framework COBIT 2019, tingkat kapabilitasnya bergantung pada pemahaman yang kuat mengenai praktik-praktik terbaik dalam mengelola operasional TI. Banyak perguruan tinggi belum mencapai target kapabilitas yang diinginkan. Oleh karena itu, institusi-institusi ini perlu terus meningkatkan kemampuan mereka dalam menghadapi perubahan lingkungan TI yang dinamis dan meningkatkan ketahanan sistem operasional mereka.

2.1.4 Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Menggunakan Kerangka Kerja COBIT 2019 Pada RSUD Palembang BARI

Penelitian yang dilakukan Algiffary et al., 2023, mengevaluasi penerapan sistem informasi di RSUD Palembang BARI dengan tujuan meningkatkan keamanan sistem informasi. Dalam konteks ini, audit keamanan dilakukan dengan menggunakan kerangka kerja COBIT 2019 sub-domain EDM03, APO12, APO13, APO14, dan DSS05. Penelitian ini melibatkan identifikasi dan evaluasi risiko keamanan informasi, penentuan kontrol keamanan yang diperlukan, serta memastikan kepatuhan terhadap standar keamanan informasi yang ditetapkan oleh COBIT 2019. Penelitian menyimpulkan bahwa tingkat keamanan sistem informasi RSUD Palembang BARI berada pada tingkat 3 (*Defined*), dengan selisih *gap analysis* sebesar 1 tingkat di bawah tingkat yang diharapkan. Berdasarkan hasil di atas, masih diperlukan upaya perbaikan dan peningkatan keamanan sistem informasi yang harus dilakukan oleh RSUD Palembang BARI.

2.1.5 Penggunaan COBIT 2019 untuk Menilai Aplikasi Sewa Ruangan di Pemerintah Kota Salatiga

Menurut penelitian yang dilakukan Prawesti et al., 2023, adanya mekanisme tata kelola di perusahaan akan menciptakan kondisi yang menguntungkan untuk memantau dan mengevaluasi efektivitas aktivitas TI yang diterapkan di perusahaan. TI merupakan kebutuhan utama bagi instansi pemerintah daerah untuk mempercepat kinerja dan pelayanannya. Pada penelitian ini membahas salah satu aplikasi yang dikembangkan oleh Diskominfo Salatiga yaitu Pinjam Ruang. Aplikasi Peminjaman Ruang merupakan aplikasi yang digunakan untuk mengelola peminjaman ruang di Kota Salatiga. Aplikasi ini memiliki sejumlah masalah, termasuk fakta bahwa beberapa ruang belum terintegrasi dan pengujian keamanan tidak pernah dilakukan pada aplikasi. Meski dikerahkan, aplikasi Pinjam Ruang belum dievaluasi. Berdasarkan permasalahan

tersebut, diperlukan audit sistem informasi untuk menilai tingkat kompetensi penggunaan aplikasi ini.

2.1.6 Audit Sistem Absensi Sidik Jari menggunakan COBIT 5

Menurut penelitian yang dilakukan Agustinus & Zuraidah, 2023, Audit sistem informasi dilakukan untuk memastikan bahwa sistem absensi di instansi berjalan dengan baik. Audit ini menggunakan *framework* Cobit 5 dan dilaksanakan di UPP PKB Samsat Jakarta Timur. Tujuan audit adalah untuk menilai tingkat kapabilitas sistem absensi, pemantauan, evaluasi pengelolaan pengoperasian, serta keamanan dan kinerja sistem absensi. Tujuan penelitian ini adalah untuk menilai sistem absensi secara menyeluruh, meliputi pengendalian, penilaian, dan jaminan independensi. Evaluasi juga akan dilakukan terhadap tingkat keamanan dan kinerja sistem informasi absensi. Metode yang digunakan adalah menggunakan sub-domain dari COBIT 5, ada 3 sub-domain yang digunakan dalam penelitian ini yaitu DSS01 *Managed Operations*, DSS05 *Managed Security Service* dan MEA01 *Monitor, Evaluate and Assess Performance and Conformance*.

2.1.7 Audit TKTI Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau Menggunakan *Framework* COBIT 2019

Penelitian yang dilakukan Triningsih et al., 2024, dengan objek penelitian katalog *online* perpustakaan UIN SUSKA Riau dengan tujuan menentukan menentukan kinerja, analisis nilai dan membuat rekomendasi perbaikan pada sistem informasi katalog tersebut. Tujuan dari Tata Kelola TI adalah memaksimalkan nilai bisnis dengan mengkoordinasikan tujuan perusahaan dengan strategi TI. Proses pengumpulan dan evaluasi informasi dilakukan untuk menjamin keamanan aset perusahaan, integritas data, pencapaian tujuan organisasi, serta penggunaan sumber daya secara efisien. Menggunakan pendekatan COBIT 2019 untuk membantu perusahaan dalam mengoptimalkan pengelolaan tata kelola TI. Terdapat berbagai kerangka kerja yang dapat digunakan untuk melakukan audit dalam kemajuan teknologi informasi. Salah satunya adalah COBIT 2019, kerangka kerja audit TI terbaru dari

ISACA dan ITGI yang membantu menilai kesenjangan antara masalah teknis, risiko, dan pengendalian dalam kemajuan teknologi informasi.

2.1.8 Audit Sistem Informasi Movable Fixed Asset dan Inventory Management dengan Framework COBIT 5

Penelitian yang dilakukan Zuraidah & Sulthon, 2023, dengan mengaudit PT Karya Semesta yang menggunakan Aplikasi Office seperti Word dan Excel untuk aktivitas harian. Mereka beralih ke Aplikasi Movable Fixed Asset dan Inventory Management karena sering kehilangan data saat mati listrik tiba-tiba. Tujuan Audit ini adalah menilai penggunaan dan efisiensi Aplikasi Movable Fixed Asset dan Inventory di Perusahaan. COBIT adalah kerangka kerja yang sering dimanfaatkan oleh auditor, terutama auditor sistem informasi. COBIT dapat digunakan sebagai alat yang komprehensif untuk mengatur teknologi informasi di perusahaan. Hasil dari penelitian tersebut mencakup pengukuran kinerja aplikasi, analisis, pemetaan tingkat kemampuan, dan rekomendasi untuk perusahaan. Standar yang digunakan dalam penelitian ini adalah COBIT 5 yang menitikberatkan pada sub-domain EDM, APO, BAI, DSS, dan MEA.

2.1.9 Audit Tata Kelola Sistem KKN UIN Sultan Syarif Kasim Riau Menggunakan COBIT 2019

Penelitian yang dilakukan Yuda et al., 2024, Tujuannya adalah untuk mengidentifikasi masalah yang ada dan memberikan rekomendasi perbaikan guna meningkatkan tata kelola teknologi informasi di LPPM. Penelitian ini melibatkan tahap perencanaan, pengumpulan data, dan analisis hasil. Penelitian ini berkontribusi dalam meningkatkan tata kelola teknologi informasi di LPPM Universitas Islam Negeri Sultan Syarif Qasim. Rekomendasi perbaikan ini dapat membantu LPPM dalam mengoptimalkan penggunaan teknologi informasi saat memilih lokasi KKN Mahasiswa. Dengan menerapkan rekomendasi ini, penggunaan *website* LPPM diharapkan menjadi lebih efektif. Hal ini akan membantu mengatasi masalah server yang sering down, kesulitan dalam proses *login*, kurangnya integrasi *database*, dan *user interface* yang membingungkan.

2.1.10 Audit TKTI Management Menggunakan Kerangka Kerja COBIT 5 Pada PT Simona

Penelitian yang dilakukan Zuraidah, 2023 di PT Simona yang merupakan perusahaan jasa yang menyediakan layanan pencucian karpet dan sofa untuk perorangan maupun perusahaan. Untuk mendukung pelayanan bisnis, perusahaan menggunakan layanan Teknologi Informasi seperti perangkat lunak dan perangkat keras yang digunakan dalam proses bisnis. Untuk memastikan pengelolaan TI yang optimal, dilakukan pengukuran tingkat tata kelola TI yang sudah berlangsung dan dibandingkan dengan tingkat yang diharapkan manajemen. Pengukuran ini berdasarkan pada sub-domain COBIT 5. Hasil pengolahan data menunjukkan bahwa metode tata kelola infrastruktur TI yang diterapkan di PT Simona masih perlu ditingkatkan. Terbukti dengan nilai *gap* yang signifikan antara tingkat pengelolaan saat ini dan tingkat yang diinginkan oleh manajemen. Audit tata kelola yang dilakukan pada manajemen menunjukkan bahwa semua sub-domain telah mencapai tingkat target yang diinginkan. Penelitian Terdahulu

Tabel 2.1 Penelitian Terdahulu

No	Penulis, Tahun, Judul	Kerangka kerja yang digunakan	Domain	Hasil Penelitian
1	Nasiri, A. (2023). Menilai Tingkat Keamanan Sistem Informasi Menggunakan Kerangka Kerja COBIT 2019. 9, 34–41.	COBIT 2019	APO12, APO13 dan DSS05	1. Hasil audit menunjukkan kapabilitas masih di tingkat 2 dengan tingkat kematangan partly hingga largely, belum mencapai fully sesuai standar COBIT 2019. 2. Implementasi manajemen risiko (APO12) baru 20%, pengendalian keamanan informasi

				(APO13) 28%, dan layanan keamanan informasi (DSS05) 69%. 3. Sebanyak 19 rekomendasi perbaikan praktis perlu segera dilakukan agar dapat naik ke tingkat kapabilitas 3.
2	Budiana, I. W., Aryanto, K. Y. E., & Sunarya, I. M. G. (2024). Evaluasi Tata Kelola dan Manajemen Infrastruktur TI pada Bank BPD XYZ menggunakan COBIT 2019. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(1), 149–161. https://doi.org/10.57152/malcom.v4i1.1043	COBIT 2019	EDM03, APO12, APO13, dan MEA03	Sub-domain EDM03, APO12, APO13, dan MEA03 dianggap paling penting dan mengharuskan mencapai Tingkat kapabilitas 4 sehingga menjadi prioritas dalam penilaian titik kritis selanjutnya.

3	Anandya Tafdhilla, Hasna Iftinan, J., Azzahra Rahmadani, & Anita Wulansari. (2023). Assessment Penggunaan COBIT 2019 dalam Pengelolaan TI Pada Institusi Perguruan Tinggi. *Bulletin of Computer Science Research*, *4*(1), 91–100. https://doi.org/10.47065/bulletincsr.v4i1.314	COBIT 2019	Semua domain	Pengujian dalam artikel-artikel yang direview menggunakan kelima sub-domain COBIT 2019, namun sub-domain yang paling sering muncul dalam penelitian adalah DSS05.
4	Algiffary, M. A., Izman Herdiansyah, M., & Kunang, Y. N. (2023). Audit Keamanan Sistem Informasi Manajemen	COBIT 2019	EDM03, APO12, APO13, APO14, dan DSS05	1. RSUD Palembang BARI sudah mencapai tingkat keamanan yang memadai berdasarkan audit pada sub-domain yang digunakan. 2. Perlu peningkatan kualitas sistem dan mengatasi kerentanan yang teridentifikasi

	Rumah Sakit Menggunakan Kerangka Kerja COBIT 2019 Pada RSUD Palembang BARI. *JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)*, *4*(1), 2723–1453. https://doi.org/10.52158/jacost.505			sehingga dapat dipastikan kepatuhan yang berkelanjutan terhadap standar keamanan informasi.
5	Fika Rizky Prawesti, N., Huning Anwariningsih, S., Ruswanti, D., & Susilo, D. (2023). Penggunaan COBIT 2019 untuk Menilai Aplikasi Sewa Ruangan di Pemerintah Kota	COBIT 2019	DSS05 dan MEA03	1. Aplikasi Pinjam Ruang telah menunjukkan kemajuan dalam hal pengelolaan keamanan. 2. Masih terdapat beberapa area yang perlu ditingkatkan, terutama dalam hal pengujian keamanan dan kepatuhan terhadap peraturan. 3. Untuk mencapai tingkat kematangan yang lebih tinggi, disarankan untuk melakukan asesmen keamanan secara berkala dan menyusun

	Salatiga. *Engineering And Technology International Journal*, *5*(3), 743493. https://doi.org/10.556442			panduan penggunaan aplikasi yang lebih detail
6	Agustinus, M., & Zuraidah, E. (2023). Audit Sistem Absensi Sidik Jari Menggunakan COBIT 5. *Media Online)*, *4*(2), 854–863. https://doi.org/10.30865/klik.v4i2.1082	COBIT 5	DSS01, DSS05, dan MEA01	1. Dari ketiga sub-domain tersebut tidak ada yang mencapai target minimal namun pada sub-domain MEA01 hampir mencapai target. 2. Sistem absensi saat ini telah menunjukkan kemajuan yang signifikan, namun masih perlu ditingkatkan untuk mencapai kinerja optimal. 3. Beberapa area perlu mendapatkan perhatian lebih agar sistem absensi dapat berjalan lebih efektif dan efisien
7	Triningsih, E., Faizah, M., & Yulianti, N. (2024). *Audit TKTI*	COBIT 2019	APO04, DSS01, dan DSS05	1. Tingkat kematangan yang cukup tinggi pada sub-domain APO04 dan DSS01, berada di level 3 dan 4.

	Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau Menggunakan Framework COBIT 2019.			2. Sub-domain DSS05 masih perlu ditingkatkan. Hal ini mengindikasikan bahwa secara umum sistem OPAC telah berjalan dengan baik, tetapi masih terdapat beberapa aspek keamanan yang perlu diperkuat.
8	Zuraidah, E., & Maula Sulthon, B. (2023). Audit Sistem Informasi Movable Fixed Asset dan Inventory Management dengan Framework COBIT 5. *Media Online)*, *3*(6), 1088–1099. https://doi.org/10.30865/klik.v3i6.774	COBIT 5	EDM04, APO10, APO12, BAI09, DSS05, dan MEA01	1. Meskipun sistem Movable Fixed Asset dan Inventory Management telah mencapai tingkat kematangan yang cukup baik pada beberapa sub-domain, namun terdapat *gap* yang signifikan pada sub-domain EDM04, APO12, DSS05, APO10, dan MEA01. 2. Perlunya upaya lebih lanjut untuk meningkatkan kapabilitas organisasi dalam mengoptimalkan sumber daya, mengelola risiko, dan memastikan keselarasan antara TI dan bisnis.
9	Ghufran Yuda, A., Takratama Savra, D.,	COBIT 2019	APO01, APO04, APO06,	1. LPPM UIN Suska Riau telah membangun fondasi yang kuat

	Rahmat Halim, F., Ripaldo Pratama, M., Safiq Tama, N., & Islam Negeri Sultan Syarif Kasim Riau, U. (2024). Audit Tata Kelola Sistem KKN UIN Sultan Syarif Kasim Riau Menggunakan COBIT 2019. In *Jurnal Testing dan Implementasi Sistem Informasi* (Vol. 2, Issue 1).		APO14, dan BAI03	dalam tata kelola teknologi informasi. 2. Disarankan untuk fokus pada peningkatan proses APO06. 3. Dengan melakukan perbaikan pada proses ini, LPPM dapat mengoptimalkan pengelolaan KKN dan memberikan layanan yang lebih baik kepada mahasiswa.
10	Zuraidah, E. (2023). Audit TKTI Management Menggunakan Kerangka Kerja COBIT 5 Pada PT Simona.	COBIT 5	APO01, APO12, DSS01, dan DSS03	1. Terdapat beberapa area yang masih perlu mendapat perhatian lebih. 2. Sub-domain APO01, APO12, dan DSS03 masih memiliki ruang untuk perbaikan. Hal ini mengindikasikan bahwa perusahaan perlu fokus pada

	PROSISKO, 10.			optimalisasi proses-proses tersebut untuk mencapai tingkat kematangan yang lebih tinggi.

2.2 Teori Terkait

2.2.1 Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi (TKTI) atau *IT Governance* merupakan suatu kerangka kerja yang dirancang untuk memastikan bahwa penggunaan Teknologi Informasi (TI) dalam organisasi dapat memberikan nilai tambah yang optimal serta mampu mendukung pencapaian tujuan bisnis secara efektif dan efisien (Suhermawan et al., 2023). TKTI memberikan struktur formal yang memungkinkan strategi TI selaras dengan strategi bisnis, sekaligus menyediakan mekanisme untuk mengarahkan dan mengendalikan sumber daya TI guna meminimalkan risiko yang mungkin timbul dari penggunaan teknologi tersebut.

Gambar 2.1 Kontek TKTI
Sumber: Modul COBIT 2019 Introduction and Methodology (ISACA, 2018b)

Dalam implementasinya, pengelolaan sumber daya TI menjadi salah satu elemen penting dari TKTI. Sumber daya TI, baik berupa infrastruktur, aplikasi, data, maupun sumber daya manusia yang mengelolanya, harus diatur secara sistematis agar dapat mendukung proses bisnis yang berjalan. Tujuan dari pengelolaan ini adalah agar proses bisnis dapat diimplementasikan secara optimal, efektif, dan efisien, serta dapat menjawab tantangan dinamis dalam era digital. Salah satu alat bantu yang sering digunakan dalam menerapkan tata kelola TI adalah kerangka kerja COBIT (*Control Objectives for Information and Related Technology*). COBIT

memberikan pedoman yang komprehensif dalam merancang, mengelola, dan memantau implementasi TI agar sesuai dengan prinsip tata kelola yang baik.

COBIT 2019, sebagai versi terbaru dari kerangka kerja ini, memperkuat integrasi antara tata kelola TI dan manajemen risiko. Hal ini dikarenakan risiko merupakan komponen yang tidak dapat dipisahkan dari pemanfaatan teknologi. Dengan adanya manajemen risiko yang baik, organisasi mampu melakukan identifikasi, pengukuran, pemantauan, serta mitigasi terhadap potensi risiko yang dapat mengganggu kontinuitas layanan TI (Taryana & Ardan, 2024).

Manajemen risiko sendiri didefinisikan sebagai proses sistematis dalam menjalankan aktivitas manajemen untuk menanggulangi kemungkinan terjadinya risiko, baik yang berdampak terhadap organisasi maupun pihak lain yang berkepentingan (Alfiana et al., 2023). Dalam konteks TI, risiko tidak hanya terbatas pada aspek teknis, seperti serangan siber, kerusakan perangkat keras, atau kebocoran data, tetapi juga menyangkut aspek strategis, seperti ketergantungan pada vendor eksternal, kegagalan integrasi sistem, dan ketidakselarasan antara TI dan strategi bisnis.

Fungsi utama dari manajemen risiko adalah untuk mengurangi dampak negatif dari suatu risiko, menghindari risiko sedini mungkin, menampung sebagian atau seluruh konsekuensi dari risiko tersebut, atau bahkan mengalihkan risiko kepada pihak ketiga (misalnya melalui asuransi atau *outsourcing*). Proses ini mencakup identifikasi risiko, penilaian tingkat risiko, penentuan langkah mitigasi, serta pemantauan berkelanjutan terhadap efektivitas strategi pengendalian risiko yang diterapkan.

Pentingnya manajemen risiko dalam tata kelola TI juga ditegaskan oleh Maryam Teymouri (2011), yang menyatakan bahwa organisasi perlu menetapkan kebijakan dan tujuan yang mempertimbangkan risiko dalam seluruh aktivitas bisnisnya. Hal ini bertujuan untuk melindungi kepentingan pemangku kepentingan melalui pengendalian risiko yang terencana dan terukur. Ketika kebijakan manajemen risiko terintegrasi dengan tata kelola TI, organisasi akan memiliki sistem pengambilan

keputusan yang lebih baik, tanggap terhadap insiden, dan mampu menciptakan sistem informasi yang tangguh.

Dalam era digital saat ini, teknologi informasi bukan hanya sebagai pendukung, tetapi telah menjadi sumber daya strategis yang memberikan keunggulan kompetitif bagi organisasi. Organisasi yang mampu mengelola risiko TI dengan baik dapat mempercepat inovasi, meningkatkan efisiensi, serta membangun kepercayaan stakeholder terhadap keandalan sistem informasi yang dimiliki. Sebaliknya, kegagalan dalam mengelola risiko dapat mengakibatkan kerugian finansial, reputasi buruk, serta gangguan operasional yang serius.

Oleh karena itu, integrasi antara tata kelola TI dan manajemen risiko bukanlah pilihan, melainkan keharusan bagi organisasi modern, termasuk lembaga filantropi seperti LAZIS Sabilillah. Dengan mengadopsi kerangka kerja seperti COBIT 2019, organisasi memiliki panduan yang jelas untuk membangun sistem pengendalian dan keamanan informasi yang selaras dengan kebutuhan bisnis serta standar internasional. Implementasi sub-domain seperti APO12 (*Managed Risk*), APO13 (*Managed Security*), dan DSS05 (*Managed Security Services*) dalam COBIT 2019 adalah langkah konkret untuk mewujudkan tata kelola TI yang tidak hanya efisien, tetapi juga aman dan berdaya guna jangka panjang.

2.2.2 Area Fokus TKTI

Dalam penerapan Tata Kelola Teknologi Informasi (TKTI), terdapat lima area utama yang menjadi fokus pengelolaan agar tujuan organisasi dapat tercapai secara efisien dan risiko TI dapat diminimalkan. Area fokus ini menjadi kerangka dasar dalam memastikan bahwa teknologi informasi mendukung strategi bisnis organisasi secara maksimal (Akbar & Saputra, 2023). Adapun kelima area fokus tersebut meliputi:

1. *Strategic Alignment* (Keselarasan Strategis)

   Fokus ini menekankan pentingnya keterkaitan yang erat antara tujuan bisnis dan perencanaan teknologi informasi. Dalam praktiknya, hal ini mencakup aktivitas mendefinisikan, memelihara, serta mengoptimalkan pemanfaatan TI agar sejalan dengan proses

bisnis organisasi. Keselarasan strategis bertujuan memastikan bahwa TI bukan sekadar pendukung operasional, melainkan mitra strategis dalam pencapaian visi perusahaan.

2. *Value Delivery* (Penyampaian Nilai)

Penyampaian nilai berfokus pada upaya untuk mengoptimalkan nilai bisnis dari investasi TI. Ini dilakukan dengan memastikan bahwa seluruh pemanfaatan teknologi menghasilkan manfaat nyata yang mendukung strategi organisasi. *Value Delivery* menuntut efisiensi biaya, manajemen anggaran yang cermat, dan bukti konkret atas kontribusi TI terhadap nilai organisasi.

3. *Risk Management* (Manajemen Risiko)

Manajemen risiko menitikberatkan pada identifikasi, pengendalian, dan mitigasi terhadap risiko-risiko signifikan yang berkaitan dengan TI. Fokus ini menuntut kesadaran kolektif dari seluruh lapisan organisasi atas potensi risiko, serta penetapan tanggung jawab pengelolaan risiko. Tujuannya adalah menjaga kesinambungan layanan dan kepercayaan *stakeholder* terhadap sistem informasi organisasi.

4. *Resource Management* (Manajemen Sumber Daya)

Area ini mencakup pengelolaan seluruh sumber daya TI secara optimal, termasuk infrastruktur, perangkat lunak, data, dan sumber daya manusia. Pengelolaan ini menjadi kunci keberhasilan dalam menjamin ketersediaan dan kapabilitas sumber daya untuk mendukung kebutuhan bisnis dan inovasi. *Resource Management* juga erat kaitannya dengan pengembangan pengetahuan dan kompetensi dalam organisasi.

5. *Performance Measurement* (Pengukuran Kinerja)

Pengukuran kinerja berperan untuk memantau dan mengevaluasi hasil implementasi TI, mencakup pengawasan terhadap pelaksanaan rencana, proyek-proyek TI, penggunaan sumber daya, serta pencapaian hasil. Pengukuran dilakukan melalui indikator-indikator kinerja utama (*Key Performance Indicators*/KPIs)

dan metrik yang terukur agar organisasi dapat melakukan *continuous improvement*.

Kelima area fokus ini bersifat saling melengkapi dan harus dijalankan secara sinergis dalam setiap inisiatif pengelolaan TI. Dalam konteks implementasi kerangka kerja seperti COBIT 2019, area fokus ini terintegrasi dalam domain-domain dan proses tata kelola yang dapat diukur melalui *capability level* dan *maturity level*.

2.2.3 Audit Teknologi Informasi

Audit Teknologi Informasi (TI) merupakan proses sistematis dan objektif yang dilakukan untuk mengumpulkan serta mengevaluasi bukti-bukti terkait aktivitas dan proses yang berjalan dalam sistem informasi. Audit ini bertujuan untuk menilai sejauh mana proses-proses TI telah memenuhi standar, kebijakan, prosedur, dan kriteria yang berlaku. Dengan kata lain, audit TI bertugas untuk menilai apakah sistem informasi yang digunakan dalam suatu organisasi telah mampu melindungi aset, menjaga integritas data, dan mendukung pencapaian tujuan bisnis secara efisien dan efektif (Wardani & Puspitasari, 2014).

Teknologi informasi sendiri mencakup seluruh aspek teknologi yang digunakan untuk mengolah dan menyampaikan informasi, termasuk perangkat keras, perangkat lunak, jaringan komunikasi, serta data. Maka dari itu, audit TI tidak hanya berfokus pada sistem perangkat lunak, namun juga mencakup proses, kebijakan, dan kontrol terhadap seluruh infrastruktur TI (Andri Yantama et al., 2023).

2.2.4 Peranan Audit TI dalam TKTI

Dalam era digital saat ini, peran TI menjadi sangat vital bagi kelangsungan bisnis. TI bukan lagi sekadar alat bantu operasional, melainkan telah menjadi bagian dari strategi bisnis yang menentukan keberhasilan organisasi dalam mencapai visinya. Oleh sebab itu, audit TI memiliki peran penting dalam menilai kualitas pengelolaan TI agar tetap relevan, terkendali, dan terhindar dari risiko yang merugikan (Intan et al.,

2023). Adapun beberapa alasan penting perlunya dilakukan audit TI adalah:

1. Kerugian akibat kehilangan data, yang dapat menyebabkan berhentinya operasional bisnis.
2. Kesalahan pengambilan keputusan, khususnya ketika menggunakan sistem pendukung keputusan atau biasa disebut *Decision Support Systems* (DSS) yang sensitif terhadap input data.
3. Kebocoran data, seperti informasi pelanggan atau keuangan, yang dapat merusak reputasi organisasi.
4. Penyalahgunaan komputer, baik oleh pihak internal maupun eksternal.
5. Kesalahan dalam perhitungan sistem, yang bisa menyebabkan kesalahan besar dalam proses bisnis.
6. Investasi TI yang tinggi, namun tidak sebanding dengan pengelolaan dan hasilnya.

Audit TI membantu organisasi dalam mengantisipasi dan mengendalikan risiko-risiko tersebut melalui penilaian terhadap infrastruktur, kebijakan, dan implementasi TI yang berjalan. Dengan demikian, audit TI berperan sebagai mekanisme pengawasan dan pengendalian internal dalam TKTI.

2.2.5 Hubungan Audit TI dengan COBIT

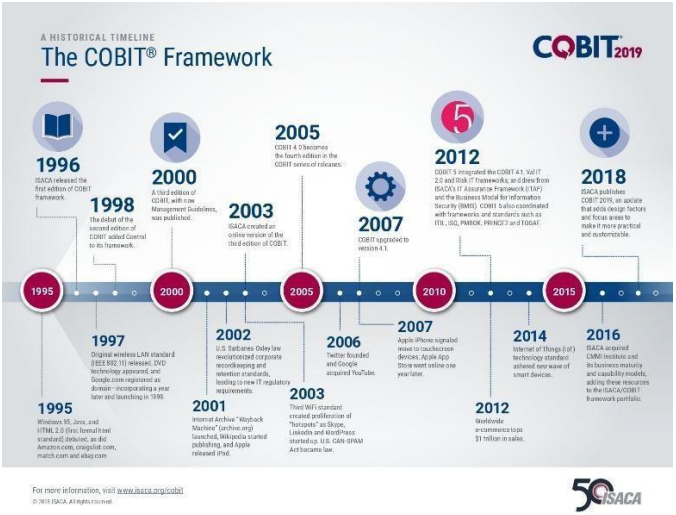
Control Objectives for Information and Related Technology (COBIT) merupakan kerangka kerja (*framework*) yang dirancang untuk mendukung tata kelola dan manajemen TI secara terintegrasi. Dalam konteks audit TI, COBIT digunakan sebagai alat bantu (*tools*) atau pedoman (*guideline*) untuk membantu auditor melakukan evaluasi terhadap proses-proses TI yang ada (Chotijah, 2023). COBIT menyediakan struktur proses yang terdiri dari domain, tujuan kontrol (*control objectives*), dan indikator performa yang dapat digunakan untuk mengidentifikasi kelemahan dan kekuatan dalam sistem TI organisasi. Auditor dapat menggunakan COBIT dalam tiga fungsi utama:

1. Menentukan lingkup audit, dengan memilih domain dan proses yang memiliki risiko tinggi.
2. Menilai kesesuaian proses dengan best practices, apakah setiap process goal dan kriteria kontrol telah terpenuhi.
3. Menentukan tingkat kapabilitas dan kematangan proses, melalui *Capability Maturity Model Integration* (CMMI) yang terdapat dalam COBIT.

Dengan demikian, hubungan antara Audit TI dan COBIT sangat erat, karena COBIT menjadi acuan dalam pelaksanaan audit yang sistematis dan objektif. COBIT tidak hanya memberikan referensi prosedur dan indikator pengukuran, tetapi juga menjadi bagian dari proses perbaikan berkelanjutan melalui rekomendasi hasil audit. Dalam praktiknya, penerapan COBIT dalam audit TI membantu organisasi memastikan bahwa tata kelola dan pengelolaan teknologi informasi telah berjalan secara optimal, terukur, dan selaras dengan tujuan strategis organisasi.

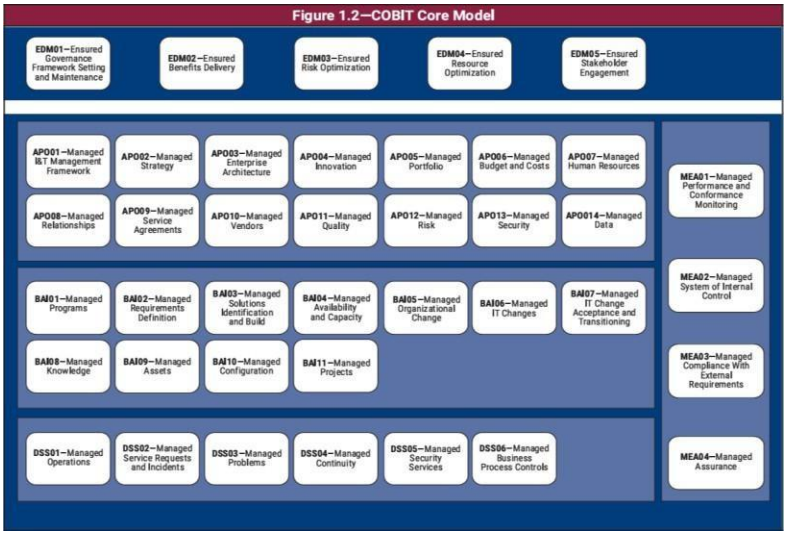
2.2.6 COBIT 2019

COBIT 2019 singkatan dari *Control Objective for Information and Related Technology*, merupakan sebuah kerangka kerja (*framework*) yang dikembangkan untuk mengatur dan mengelola informasi serta teknologi. COBIT menetapkan elemen-elemen penting yang dibutuhkan untuk membangun dan memelihara sistem pengelolaan, seperti proses, struktur organisasi, kebijakan dan prosedur, aliran informasi, budaya dan perilaku, keterampilan, serta infrastruktur yang mendukung (Saleh et al., 2021).



Gambar 2.2 COBIT *Historical Timeline*

COBIT 2019 merupakan pembaruan dari versi sebelumnya yaitu COBIT 5, yang dirilis oleh organisasi profesi internasional yang bergerak dalam bidang tata kelola teknologi informasi yang bernama *Information System Audit and Control Association* (ISACA) sebagai versi terbaru (Fadhilah et al., 2021). Dalam kerangka COBIT 2019, terdapat perbedaan yang jelas antara tata kelola dan manajemen. Tata kelola bertujuan untuk mengevaluasi kebutuhan, kondisi, dan preferensi pemangku kepentingan guna menetapkan tujuan perusahaan yang seimbang dan disepakati. Dalam konteks ini, prioritas ditetapkan, keputusan diambil, serta kinerja dan kepatuhan dipantau berdasarkan arahan dan tujuan yang telah disepakati (Utama et al., 2023). Kerangka ini memberikan panduan lebih rinci terkait tata kelola Teknologi Informasi (TI) dalam suatu organisasi, yang dikenal sebagai Enterprise Governance of IT (EGIT). EGIT mencakup 40 tujuan utama untuk tata kelola dan manajemen, yang disesuaikan dengan kebutuhan unik setiap organisasi. Kumpulan tujuan ini juga dikenal sebagai COBIT Core Model (Zuraidah, 2023).



Gambar 2. 3 COBIT *Core Model*
Sumber: COBIT 2019 Framework: Introduction & Methodology (ISACA, 2018b)

COBIT 2019 merupakan pengembangan dari COBIT 5, dengan pendekatan yang membedakan secara jelas antara tata kelola (*governance*) dan manajemen (*management*) guna memenuhi kebutuhan para pemangku kepentingan (*stakeholders*). Versi ini juga dirancang secara terbuka dan fleksibel, yang berarti memungkinkan penambahan konten baru sesuai kebutuhan tanpa harus secara kaku mengikuti seluruh prinsip yang ada. Fleksibilitas ini menjadikan sistem tata kelola dalam COBIT 2019 mampu beradaptasi secara dinamis dengan perkembangan zaman dan kebutuhan organisasi yang terus berubah.

Tabel 2. 1 Prinsip COBIT

Prinsip	
COBIT 5	**COBIT 2019**
1. Menemukan kebutuhan stakeholder.	**Prinsip berdasarkan sistem tata kelola:**

2. Mencakup ujung ke ujung kebutuhan TI perusahaan. 3. Mengaplikasikan yang tunggal, mengintegrasikan framework. 4. Mengaktifkan pendekatan holistik. 5. Memisahkan tata kelola dengan manajemen.	1. Memenuhi kebutuhan para pemangku kepentingan. 2. Memungkinkan pendekatan yang holistic 3. Penerapan sistem tata kelola yang dinamis 4. Memisahkan tata kelola dengan manajemen 5. Dapat disesuaikan dengan kebutuhan organisasi 6. Mencakup organisasi secara menyeluruh **Prinsip berdasarkan kerangka tata kelola:** 1. Hubungan antar komponen, untuk memaksimalkan konsistensi dan memungkinkan otomatisasi. 2. Untuk mengatasi masalah baru dengan cara yang paling fleksibel, dengan tetap menjaga integritas dan konsistensi. Kerangka tata kelola harus terbuka dan fleksibel. Ini harus memungkinkan penambahan konten baru dan kemampuan. 3. Kerangka tata kelola harus selaras dengan standar, kerangka kerja, dan peraturan utama yang relevan.

COBIT 2019 memiliki sejumlah kelebihan dibandingkan pendahulunya maupun framework lain seperti ITIL, ISO/IEC 27001, atau *The Open Group Architecture Framework* (TOGAF), antara lain:

1. Pendekatan Berbasis Tujuan (Goal-Oriented): COBIT 2019 menyelaraskan tujuan TI dengan tujuan pemangku kepentingan organisasi (enterprise goals) secara eksplisit melalui *cascading goals*.
2. Fleksibilitas dan Kustomisasi: COBIT 2019 menyediakan panduan kustomisasi sesuai kebutuhan spesifik organisasi, baik dari sisi industri, skala, hingga tingkat kematangan TI.
3. Pemodelan *Maturity* dan *Capability* yang Terukur: COBIT 2019 memungkinkan organisasi mengukur secara objektif tingkat kapabilitas setiap proses TI menggunakan skala 0–5 berdasarkan CMMI.
4. Integrasi Standar Internasional: COBIT 2019 mendukung dan kompatibel dengan standar global seperti ISO 27001 (keamanan informasi), *Information Technology Infrastructure Library* ITIL (layanan TI), dan *National Institute of Standards and Technology* (NIST), sehingga memudahkan integrasi lintas kerangka.
5. Berbasis Nilai dan Risiko: COBIT tidak hanya berorientasi pada kontrol internal, tetapi juga pada nilai bisnis dan mitigasi risiko TI.
6. Fokus pada Tata Kelola: Berbeda dengan ITIL yang lebih menekankan pada manajemen layanan TI, COBIT lebih kuat pada sisi tata kelola menyeluruh dan pengambilan keputusan strategis.

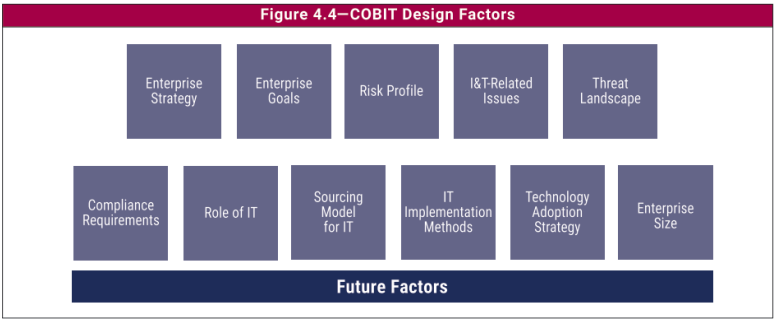
Dengan keunggulan-keunggulan ini, COBIT 2019 menjadi pilihan ideal bagi organisasi yang ingin membangun sistem tata kelola dan keamanan TI yang terstruktur, terukur, dan selaras dengan tujuan strategis. LAZIS Sabilillah sebagai organisasi nirlaba yang mengelola informasi sensitif para donatur membutuhkan pendekatan komprehensif seperti COBIT 2019 untuk menjaga kepercayaan dan keberlangsungan operasional. Sub-domain APO12, APO13, dan DSS05 dalam COBIT 2019 akan digunakan

dalam penelitian ini karena relevansinya dalam mengelola risiko, merancang sistem keamanan informasi, dan mengawasi operasional layanan keamanan secara menyeluruh.

Untuk melindungi data sensitif donatur dan menjaga kelancaran operasional, LAZIS Sabilillah Malang perlu menerapkan sistem keamanan yang kuat. Sub-domain APO12, APO13, dan DSS05 dalam COBIT 2019 menawarkan solusi komprehensif untuk mencapai tujuan ini. Dengan fokus pada aspek teknis keamanan dan pengelolaan layanan keamanan, ketiga sub-domain ini akan membantu LAZIS Sabilillah Malang mencegah serangan siber, dan memastikan kelangsungan operasional. Pada *framework* COBIT 2019 yang merupakan versi terbaru dari COBIT terdiri dari 40 kegiatan yang bisa dijadikan acuan untuk mengelola TI yang baik dari sisi perencanaan, operasional maupun pengawasan kinerja (Suroto & Friadi, 2024). Berdasarkan 40 kegiatan tersebut, hanya terdapat 3 sub-domain yang terkait dengan aspek keamanan yaitu sub-domain APO12 (*managed risk*), APO13 (*managed security*) dan DSS05 (*managed security services*) (Nasiri, 2023).

2.2.7 *Design Factors*

Salah satu pembaruan dalam COBIT 2019 adalah diperkenalkannya *Design Factor*, yaitu sejumlah faktor yang dapat memengaruhi keberhasilan dalam merancang sistem tata kelola, sekaligus menentukan posisinya agar mampu mendukung pencapaian tujuan perusahaan melalui optimalisasi pemanfaatan *Information* & *Technology* (I&T) (ISACA, 2018a). Setiap organisasi tentu memiliki prioritas tujuan dan strategi yang berbeda-beda. Oleh karena itu, proses identifikasi terhadap *Design Factor* perlu dilakukan sejak awal agar implementasi COBIT 2019 dapat disesuaikan dengan kondisi spesifik perusahaan. Dengan begitu, penerapan COBIT 2019 menjadi lebih relevan dan adaptif terhadap karakteristik masing-masing organisasi.



Gambar 2. 4 COBIT 2019 *Design Factors*
Sumber: COBIT® 2019 Framework : introduction and methodology (ISACA, 2018b)

2.2.8 Domain APO

Domain *Align, Plan and Organize* (APO) adalah bagian penting dari *framework* COBIT. Domain APO berfokus pada penyelarasan strategi TI dengan tujuan bisnis, perencanaan inisiatif TI, dan pengorganisasian sumber daya TI untuk memastikan sumber daya tersebut dapat mendukung tujuan organisasi secara keseluruhan. Pada dasarnya, sub-domain APO membantu organisasi memastikan bahwa investasi TI selaras dengan strategi bisnis mereka dan investasi ini direncanakan serta diatur secara efektif untuk mencapai kinerja dan nilai yang optimal. Hal ini memastikan bahwa TI sejalan dengan bisnis sehingga dapat mencapai tujuan yang sama (ISACA, 2019a).

Tujuan utama domain APO12 adalah untuk memastikan bahwa organisasi siap menghadapi segala kemungkinan risiko yang dapat timbul akibat penggunaan teknologi informasi. Hal ini dilakukan melalui serangkaian proses mulai dari pengumpulan data relevan terkait risiko, analisis risiko dengan tujuan memperhitungkan relevansi bisnis dari faktor penyebab risiko, mengelola hasil analisis tersebut menjadi risk profile, memilah risiko yang harus dimitigasi, mengelola peluang meminimalisir risiko, hingga menyiapkan strategi menghadapi risiko (Wahyu et al., 2020).

Sub-domain APO13 merupakan proses yang krusial dalam menjaga keamanan aset informasi perusahaan. Proses APO13 adalah proses mendefinisikan, mengoperasikan, dan memantau sistem yang diterapkan perusahaan untuk mengelola keamanan informasi yang dimilikinya. Tujuan dari proses ini adalah untuk memastikan bahwa dampak insiden keamanan informasi tidak melebihi tingkat risiko yang ditetapkan oleh perusahaan (Aritonang et al., 2018). Selain domain APO, COBIT juga mencakup domain DSS yang tidak kalah penting dalam konteks keamanan informasi dan akan diuraikan pada sub-bab berikutnya.

2.2.9 Domain DSS

Domain DSS, atau "*Deliver, Service, and Support*", adalah salah satu dari lima sub-domain utama dalam kerangka kerja COBIT 2019 yang berfokus pada penyampaian layanan TI yang efektif dan efisien, mendukung pengguna, serta memastikan bahwa layanan TI memenuhi kebutuhan bisnis dan pengguna (Lestari & Adha, 2022). Beberapa aspek penting dari sub-domain DSS meliputi memastikan bahwa operasi TI berjalan lancar dan sesuai dengan standar yang ditetapkan, menangani insiden dan masalah yang muncul untuk meminimalkan dampak pada bisnis, melindungi layanan TI dari ancaman keamanan dan memastikan kepatuhan terhadap kebijakan keamanan, menjamin bahwa layanan TI dapat terus berjalan meskipun terjadi gangguan atau bencana. Singkatnya, sub-domain DSS memastikan bahwa layanan TI disampaikan dengan cara yang mendukung tujuan bisnis dan memberikan nilai tambah bagi organisasi (ISACA, 2018b).

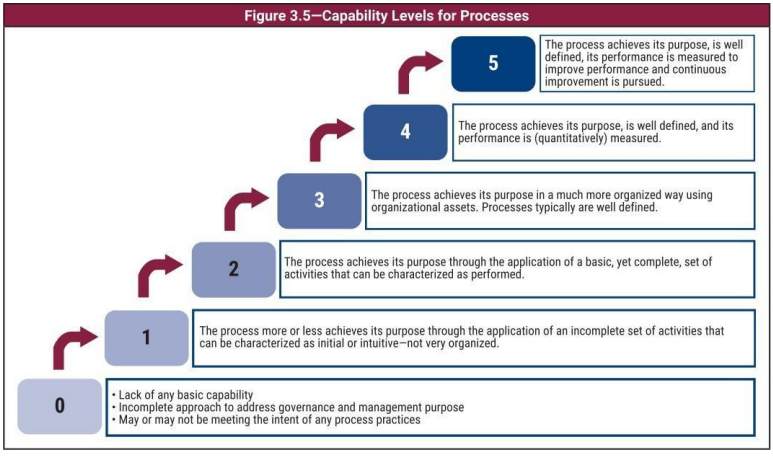
Sub-domain DSS05 merupakan serangkaian proses yang berfokus pada pengelolaan keamanan data pada organisasi dengan tujuan mempertahankan risiko keamanan informasi berada pada batas aman yang sudah ditentukan oleh perusahaan (Imany et al., 2019). Untuk mempermudah penetapan tanggung jawab dalam implementasi sub-domain, digunakan alat bantu RACI chart.

2.2.10 RACI *Chart*

Penentuan klasifikasi peran dan tanggung jawab dalam suatu proses atau proyek RACI Chart sering digunakan khususnya dalam penerapan COBIT 2019. Ini bertujuan untuk menentukan siapa yang bertanggung jawab (R: *Responsible*), siapa yang harus memberikan persetujuan (A: *Accountable*), siapa yang perlu diinformasikan (C: *Consulted*), dan siapa yang perlu diberitahu (I: *Informed*) (Prasetya et al., 2024). Penilaian efektivitas proses dalam kerangka COBIT 2019 dilakukan melalui analisis capability level yang dijelaskan berikut.

2.2.11 *Capability Level Analysis*

Analisis tingkat kapabilitas proses merupakan indikator dari seberapa baik suatu proses berlangsung. Semakin tinggi tingkat kapabilitasnya, semakin optimal proses tersebut dilaksanakan. Kenaikan tingkat kapabilitas bersifat kumulatif, artinya setiap tingkat membangun fondasi untuk tingkat berikutnya (Sukamto et al., 2021).



Gambar 2. 5 *Capability levels for process*
Sumber: (ISACA, COBIT 2019 Framework: Introduction & Methodology, 2018)

COBIT 2019 mendukung skema kapabilitas proses berbasis *Capability Maturity Model Integration* (CMMI) untuk menilai proses dalam setiap tujuan tata kelola dan pengendalian dapat berjalan pada tingkat fungsional yang berbeda, dari 0 hingga 5 (ISACA, 2018c). Untuk memahami setiap tingkatan kapabilitas proses pada gambar 2.2 diatas, akan dijelaskan pada table 2.2 berikut:

Tabel 2. 2 Penjelasan tingkat kapabilitas proses

Level	Penjelasan
Level 0	Kurang kapabilitas dasar, pendekatan yang tidak lengkap, mungkin memenuhi atau tidak memenuhi maksud praktik proses.
Level 1	Proses kurang lebih mencapai tujuannya melalui serangkaian kegiatan yang tidak lengkap, tidak terlalu terorganisir.
Level 2	Proses mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap, dikategorikan beroperasi.
Level 3	Proses mencapai tujuannya secara terorganisir. Proses biasanya telah didefinisikan dengan baik.
Level 4	Proses mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya dapat diukur secara kuantitatif.
Level 5	Proses mencapai tujuannya, didefinisikan dengan baik, kinerjanya diukur, dan perbaikan berkelanjutan dilakukan.

Perhitungan level atau tingkatan capaian kapabilitas adalah dengan mengukur *gap* antara tingkat kapabilitas saat ini dengan tingkat kapabilitas target (Suroto & Friadi, 2024).

Menurut (Neto et al., 2019), pada bagian 7.2.4.1 COBIT 2019 *Design Guide* menjelaskan hubungan skor capaian kapabilitas dengan tingkat kapabilitas, sebagaimana pada tabel berikut:

Tabel 2. 3 Hubungan Skor Capaian Kapabilitas dengan Tingkat Kapabilitas

Skor Capaian Kapabilitas	Tingkat Kapabilitas / *Capability Level*
>=75%	4
>= 50% dan < 75%	3
>= 25% dan < 50%	2
<25%	1

Berdasarkan artikel ISACA yang dipaparkan oleh (Neto et al., 2019) menjelaskan bahwa terdapat referensi yang sudah ditetapkan oleh ISACA dalam menentukan target kapabilitas untuk setiap sub-domain. Adapun target kapabilitas yang sesuai dengan sub-domain yang digunakan dalam penelitian ini adalah sebagai berikut:

Tabel 2. 4 Panduan Target *Capability Level*

Reference	***Governance/Management Objective***	***Target Process Capability Level***
APO12	*Managed risk*	3
APO13	*Managed security*	4
DSS05	*Managed security services*	3

Agar strategi peningkatan kapabilitas lebih terarah, dilakukan analisis kesenjangan (*gap analysis*) seperti dijelaskan di bawah ini.

2.2.12 *Gap Analysis*

Analisis kesenjangan digunakan untuk membandingkan kondisi saat ini suatu organisasi dengan kondisi ideal yang diinginkan. Dengan kata lain, tujuan dari analisis ini adalah untuk menemukan perbedaan antara apa yang sudah ada dan apa yang seharusnya ada. Dengan melakukan perbandingan ini, kita dapat menemukan bagian mana yang perlu ditingkatkan atau diperbarui. Selanjutnya, hasil analisis kesenjangan ini dapat digunakan sebagai dasar untuk membuat rencana tindakan yang lebih fokus dan efisien. Sederhananya, analisis kesenjangan membantu kita memahami di mana kita saat ini dan apa yang harus kita lakukan untuk mencapai tujuan yang telah ditetapkan (Sukamto et al., 2021). Untuk menentukan tingkat keberhasilan implementasi setiap proses, digunakan metode penilaian aktivitas proses sebagai berikut.

2.3 Gambaran Umum Obyek Penelitian

LAZIS Sabilillah adalah Lembaga Amil Zakat, Infak, dan Sedekah yang berbasis di Malang, Indonesia. Dengan fokus pada pengelolaan dana zakat, infak, sedekah, serta dana sosial lainnya. Lembaga ini bertujuan untuk

menghimpun dan menyalurkan bantuan kepada masyarakat yang membutuhkan, baik dalam bentuk bantuan sosial, pendidikan, maupun pemberdayaan ekonomi. Sebagai lembaga filantropi, LAZIS Sabilillah berupaya menjaga transparansi dan akuntabilitas dalam pengelolaan dana, serta memanfaatkan teknologi informasi untuk meningkatkan efisiensi dan keamanan dalam proses pengelolaan dan distribusi dana kepada penerima manfaat.

Dalam operasionalnya, LAZIS Sabilillah memanfaatkan teknologi digital berupa penggunaan aplikasi penerimaan zakat, infak, sedekah berbasis android dan Sistem Informasi Mustahik (SIM) untuk pengelolaan data penerima manfaat. Dengan pengelolaan data secara digital, organisasi ini perlu menerapkan prinsip keamanan informasi yaitu *confidentiality, integrity,* dan *availability.*

2.3.1 Visi, Misi, dan Core Value

Visi :

Menjadi lembaga zakat yang Profesional, Amanah, Transparan dan Terdepan.

Misi :

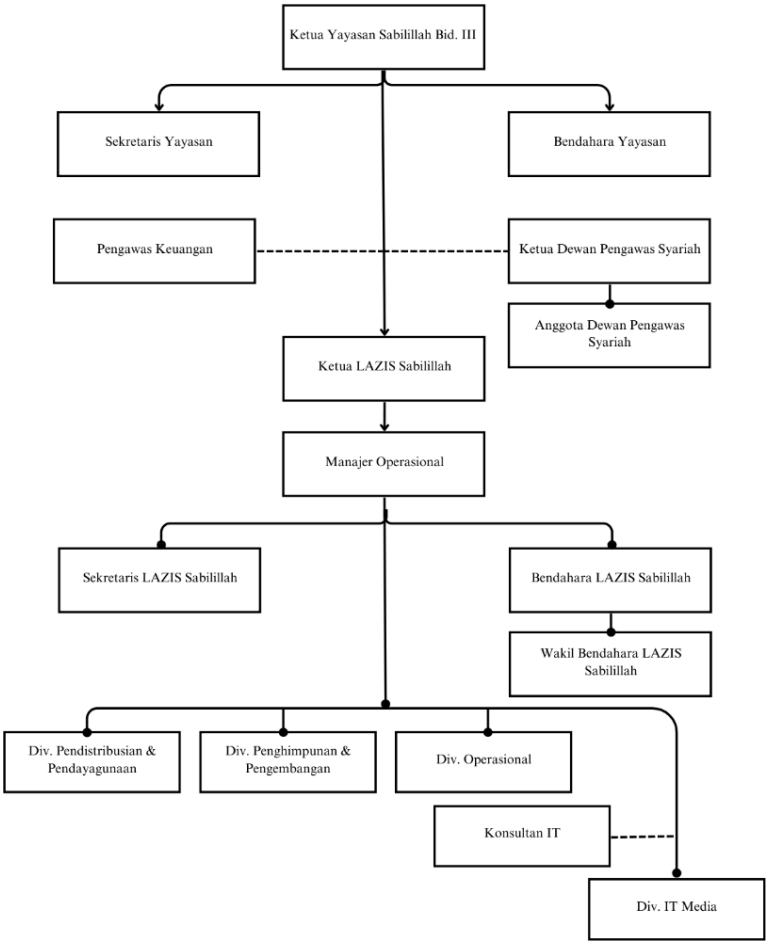
Mengoptimalkan dana Zakat, Infaq, dan Shodaqoh untuk pemberdayaan masyarakat dan pengentasan kemiskinan.

Core Value :

1. Visioner
2. Transformasional
3. Amanah
4. Profesional
5.

2.3.2 Struktur LAZIS Sabilillah

Dalam mewujudkan visi dan misi yang telah direncanakan dengan menerapkan nilai-nilai yang dianut, maka disusunlah struktur organisasi LAZIS Sabilillah Malang sebagaimana pada gambar 2.3 berikut :



Gambar 2. 6 Struktur Organisasi LAZIS Sabilillah Malang
Sumber: Profil LAZIS Sabilillah 2024