BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Subbab ini menyajikan tinjauan terhadap penelitian-penelitian terdahulu yang relevan dengan perancangan arsitektur enterprise dan manajemen risiko TI. Bertujuan untuk memperkuat dasar konseptual dan metodologis penelitian serta mengidentifikasi pendekatan yang telah digunakan sebelumnya. Rangkuman tinjauan pustaka disajikan pada Tabel 2.1.

Tabel 2.1 Penelitian terdahulu

Peneliti dan Judul Penelitian	Hasil Penelitian	Persamaan	Perbedaan
(Anam dkk., 2021) The Analysis and Optimization of Business Processes for Students in Higher Education Based on Togaf 9.2	Pembuatan cetak biru TI untuk proses bisnis mahasiswa. Terdapat beberapa pembaruan di setiap proses, terutama dalam arsitektur sistem informasi, kemudian dalam proses bisnis dan teknologi. Ada juga pembaruan yang perlu dilakukan. Penelitian ini juga memberikan beberapa alasan untuk memperbarui Opportunity and Solutions. Selain itu, penelitian ini memberikan panduan untuk menerapkan pembaruan berdasarkan prioritas yang harus diterapkan dalam perencanaan migrasi.	Menggunakan TOGAF	Fokus pada bisnis proses untuk siswa dan tidak adanya COBIT 2019
(Gormantara dan Emanuel, 2020) Enterprise Architecture Planning Using TOGAF ADM at Scoob Telur Comp	Memberikan desain yang menentukan arsitektur bisnis, arsitektur data, arsitektur aplikasi, arsitektur teknologi dan opportunities and solutions serta juga memberikan usulan rancangan sistem aplikasi sehingga dapat mendukung proses bisnis maupun pembuatan laporan yang terjadi pada Scoob Telur	Menggunakan TOGAF ADM	Fokus pada perencanaan arsitektur Perusahaan telur dan tidak adanya COBIT 2019

Peneliti dan Judul Penelitian	Hasil Penelitian	Persamaan	Perbedaan
(Fadlil dkk., 2021) Integration of Zachman Framework and TOGAF ADM on Academic Information Systems Modeling	Blueprint Arsitektur yang dapat digunakan sebagai acuan dalam pembangunan sistem informasi akademik	Menggunakan TOGAF ADM	Fokus pada sistem modelling pada STMIK MPB dan tidak adanya COBIT 2019
(Girsang dan Abimanyu, 2021) Development of an Enterprise Architecture for Healthcare using TOGAF ADM	Penelitian ini mengembangkan 7 rekomendasi untuk Memperkuat area Bisnis organisasi, 5 rekomendasi untuk Menyelaraskan rencana TI dengan Strategi Bisnis, 16 rekomendasi untuk Menerapkan beberapa solusi TI sebagai Keunggulan Kompetitif bagi organisasi, dan 8 rekomendasi untuk memberikan kinerja yang lebih tinggi dengan memungkinkan pendekatan Manajemen Layanan untuk Operasi TI. Penelitian ini juga menunjukkan bagaimana TOGAF ADM dapat meningkatkan kesadaran pengguna bisnis terhadap bisnis itu sendiri	Menggunakan TOGAF ADM	Fokus pada perencaan arsitektur pada rumah sakit dan tidak adanya COBIT 2019
(Almunadia dkk., 2019) Perancangan Enterprise Architecture Pada Bidang Agroforestry Menggunakan Metode Togaf 9.1 ADM	Blueprint dan IT Roadmap selama 5 tahun yang dapat digunakan sebagai panduan implementasi	Menggunakan TOGAF ADM	Tidak adanya COBIT 2019
(Nugraheni dkk., 2021) Adopting COBIT 2019 for Information Technology Risks	Empat faktor risiko yang sesuai: pengguna akhir, teknologi, infrastruktur, dan keuangan. Faktor risiko Pengguna Akhir diwakili dalam COBIT 2019 oleh ref. 4 (keahlian TI, keterampilan dan	Menggunakan COBIT 2019 untuk evaluasi tata kelola TI	Fokus pada manajemen risiko TI di Universitas Diponegoro dan tidak

Peneliti dan Judul Penelitian	Hasil Penelitian	Persamaan	Perbedaan
in University Online Learning during COVID-19	perilaku). Dalam COBIT 2019, faktor risiko keuangan diwakili oleh ref. 1 (pengambilan keputusan investasi TI, definisi dan pemeliharaan portofolio) dan ref. 3 (definisi dan pemeliharaan portofolio TI) (biaya dan pengawasan TI). Aspek infrastruktur dalam COBIT 2019 ditunjukkan dalam ref. 7 (insiden infrastruktur operasional TI). Aspek teknologi dalam COBIT 2019 diwakili oleh ref. 8 (masalah adopsi/penggunaan perangkat lunak), ref. 9 (insiden perangkat keras), dan ref. 10 (kegagalan perangkat lunak). Keempat faktor risiko tersebut harus diidentifikasi untuk universitas guna mencapai strategi universitas dalam menghadapi pandemi		adanya TOGAF
(Irawan dkk., 2023) Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi menggunakan Framework COBIT 2019 proses EDM03 dan APO12 (Studi Kasus pada PT Bank BRI Unit Bangorejo)	Evaluasi manajemen risiko dan tata kelola TI dengan penerapan domain EDM03 (Ensure Risk Optimization) dan APO12 (Manage Risk). Menilai tingkat kapabilitas proses pengelolaan risiko TI, mengidentifikasi kesenjangan, serta memberikan rekomendasi untuk meningkatkan pengelolaan risiko dan tata kelola TI secara efektif.	Menggunakan framework COBIT 2019	Fokus pada manajemen risiko TI di sektor perbankan dan tidak adanya TOGAF
(Kesuma dkk., 2022) Design Of Information Technology (IT) Governance Using Framework Cobit 2019 Subdomain	Analisis kesenjangan dalam proses APO01 berada pada level 1	Menggunakan framework COBIT 2019 untuk evaluasi tata kelola TI	Fokus pada desain tata kelola TI pada Instidla dan tidak adanya TOGAF

Peneliti dan Judul Penelitian	Hasil Penelitian	Persamaan	Perbedaan
APO01 (Case Study: Instidla)			
(Windasari dkk., 2021) Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019	Hasil level kapabilitas PTOP pada domain MEA dan DSS berada pada level 1 atau performed yang artinya proses yang dilakukan kurang lebih telah mencapai tujuan, namun melalui penerapan serangkaian kegiatan yang tidak lengkap dan tidak terlalu/kurang terorganisir	Menggunakan framework COBIT 2019	Fokus pada tata kelola TI Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support dan tidak adanya TOGAF
(Widjaja dan Andry, 2023) Analisis Multi Computer System Menggunakan Framework COBIT 2019 pada Perusahaan Perkakas	Hasil tiga domain terpenting bagi perusahaan perkakas berdasarkan proses pada design factor yang telah dilakukan adalah EDM05, APO14 (Managed Data) dan BAI09 (Managed Assets)	Menggunakan framework COBIT 2019 untuk evaluasi tata kelola TI	Fokus pada tata kelola TI perusahaan perkakas dan tidak adanya TOGAF

Berdasarkan Tabel 2.1, ditampilkan berbagai studi yang mengaplikasikan kerangka kerja TOGAF ADM dan COBIT dalam berbagai konteks organisasi, seperti universitas, rumah sakit, perusahaan, dan lembaga pendidikan. Sebagian besar penelitian yang menggunakan TOGAF ADM fokus pada perancangan arsitektur enterprise untuk menyelaraskan kebutuhan bisnis dengan teknologi informasi yang digunakan. Hasil dari penelitian tersebut menunjukkan bahwa TOGAF ADM membantu organisasi dalam merancang sistem informasi dan teknologi yang lebih terstruktur dan terintegrasi, meskipun umumnya tidak mencakup pengelolaan risiko atau tata kelola yang lebih komprehensif.

Di sisi lain, penelitian yang menggunakan COBIT, terutama versi 2019, lebih banyak berfokus pada tata kelola dan manajemen risiko teknologi informasi. Penelitian-penelitian ini menilai kemampuan dan kapabilitas organisasi dalam mengelola risiko TI, terutama dalam menghadapi tantangan seperti pandemi, integrasi sistem, dan pengelolaan aset TI. Hasil penelitian ini umumnya

menunjukkan adanya kesenjangan atau tingkat kapabilitas yang perlu ditingkatkan untuk mencapai tata kelola TI yang lebih optimal.

Adapun perbedaan dari penelitian pada Tabel 2.1 adalah sebagai berikut:

A. Kerangka kerja yang digunakan:

1. TOGAF ADM: Sebagian besar penelitian yang menggunakan TOGAF ADM fokus pada perancangan arsitektur enterprise, mencakup berbagai aspek seperti arsitektur bisnis, sistem informasi, dan teknologi. Namun, penelitian ini biasanya tidak mencakup aspek tata kelola dan manajemen risiko secara mendalam.
2. COBIT 2019: Penelitian yang menggunakan COBIT 2019 lebih berfokus pada evaluasi dan pengelolaan risiko TI serta tata kelola secara keseluruhan. COBIT 2019 digunakan untuk mengidentifikasi dan mengelola risiko TI, menyusun strategi TI, serta menilai kapabilitas organisasi dalam mengelola teknologi informasi.

B. Fokus dari penelitian:

1. TOGAF ADM: Fokus utama adalah pada desain dan integrasi sistem informasi dan teknologi untuk memenuhi kebutuhan bisnis. Penelitian ini lebih menekankan pada perancangan arsitektur yang komprehensif.
2. COBIT 2019: Fokus utama adalah pada tata kelola dan manajemen risiko TI, dengan penilaian terhadap kapabilitas organisasi dalam aspek tertentu seperti manajemen risiko, pengelolaan aset, dan audit TI.

2.2 Dasar Teori

2.2.1 Enterprise Architecture Planning

Enterprise Architecture Planning (EAP) merupakan pendekatan sistematis dalam menyusun rencana arsitektur informasi guna mendukung pencapaian tujuan bisnis organisasi. Menurut Stephen H. Spewak dalam bukunya Enterprise Architecture Planning (Spewak dan Steven, 1993), EAP adalah proses penetapan arsitektur untuk penggunaan informasi guna mendukung bisnis dan rencana implementasi arsitektur tersebut. EAP membantu organisasi dalam merancang arsitektur data, aplikasi, dan teknologi secara terstruktur agar selaras dengan strategi bisnis jangka panjang.

EAP menjadi landasan awal bagi penerapan Enterprise Architecture (EA), yaitu suatu kerangka konseptual yang menjembatani antara kebutuhan bisnis dan solusi teknologi informasi. EA mencakup representasi arsitektur dari proses bisnis, data, aplikasi, hingga infrastruktur teknologi yang digunakan oleh organisasi. Menurut (Bernard, 2012), EA adalah pendekatan yang menyediakan prinsip, metode, dan model untuk merancang serta mengelola struktur dan evolusi sistem enterprise. Dengan demikian, EAP dapat dipandang sebagai tahapan perencanaan awal yang mendukung pengembangan EA secara menyeluruh.

Lebih lanjut, (Lankhorst, 2017) menjelaskan bahwa EA menjadi alat penting untuk memodelkan dan mengkomunikasikan struktur internal organisasi, terutama dalam konteks transformasi digital. Di era modern, EA berperan penting dalam menciptakan keterpaduan antara visi strategis organisasi dengan kapabilitas TI yang mendukungnya. Senada dengan pandangan Lin dan MacVittie (Lin dan Macvittie, 2022) yang menyatakan bahwa EA modern harus mampu menyediakan kerangka yang adaptif untuk mengarahkan transformasi digital dan inovasi bisnis.

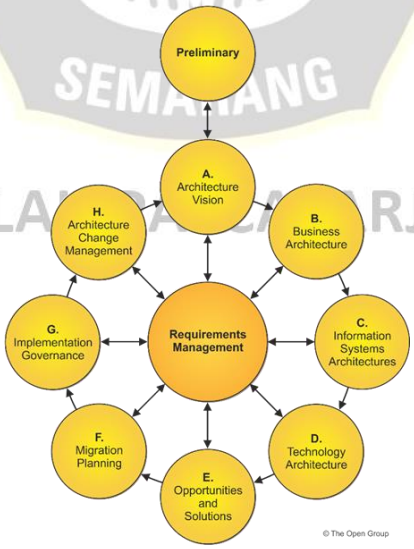
Dalam konteks pengembangannya, jenis-jenis Enterprise Architecture (EA) dapat dikategorikan berdasarkan pendekatan dan kerangka kerja yang digunakan. Beberapa pendekatan yang umum dikenal antara lain Zachman Framework, yang dikembangkan oleh John Zachman dan menggunakan pendekatan tabular untuk memetakan perspektif para pemangku kepentingan (seperti planner, owner, designer, builder) terhadap elemen-elemen sistem informasi seperti data, fungsi, dan jaringan. Selanjutnya, TOGAF (The Open Group Architecture Framework) merupakan salah satu kerangka kerja EA paling populer yang menggunakan siklus pengembangan arsitektur bernama Architecture Development Method (ADM) dan banyak digunakan di berbagai sektor.

Sementara itu, Federal Enterprise Architecture Framework (FEAF) dikembangkan oleh pemerintah Amerika Serikat untuk mengintegrasikan sistem antar instansi pemerintah dengan fokus pada konsistensi dan interoperabilitas. Gartner Enterprise Architecture Framework lebih menekankan pada hasil bisnis dan manajemen perubahan dengan fokus pada penciptaan nilai (*value creation*) serta penyelarasan antara strategi bisnis dan teknologi informasi. Setiap jenis EA

memiliki karakteristik tersendiri tergantung pada kebutuhan, skala organisasi, dan tujuan strategisnya. Dalam penelitian ini, pendekatan TOGAF dipilih karena menawarkan struktur yang sistematis dan fleksibel untuk pengembangan arsitektur enterprise, serta memungkinkan integrasi dengan kerangka tata kelola TI seperti COBIT 2019 guna menciptakan desain arsitektur yang lebih komprehensif dan sadar risiko..

2.2.2 Kerangka Kerja TOGAF

TOGAF (The Open Group Architecture Framework) merupakan salah satu kerangka kerja *enterprise architecture* yang paling banyak digunakan di dunia. TOGAF dikembangkan oleh The Open Group dan menyediakan metode terstruktur untuk merancang, mengembangkan, mengelola, serta mengimplementasikan arsitektur enterprise secara holistik. Menurut (The Open Group, 2018), komponen inti dari TOGAF adalah Architecture Development Method (ADM), yaitu siklus pengembangan arsitektur yang terdiri dari delapan fase utama berurutan dan berulang (iteratif) yang membentuk satu siklus pengembangan arsitektur, serta membimbing organisasi dalam proses perancangan hingga implementasi arsitektur. seperti terlihat pada Gambar 2.1.



Gambar 2.1 Tahap TOGAF ADM (The Open Group, 2018)

Masing-masing fase dalam ADM memiliki tujuan spesifik, yang merupakan serangkaian proses iteratif mulai dari menyusun arsitektur, transisi,

hingga mengelola proses realisasi arsitektur. Sepanjang siklus ADM, harus sering dilakukan validasi hasil terhadap persyaratan awal, baik untuk keseluruhan siklus ADM, maupun untuk fase tertentu dari proses (Antouw dan Andry, 2020), berikut penjelasan tahapnya pada Tabel 2.2.

Tabel 2.2 Fase TOGAF ADM

Fase TOGAF	Penjelasan
Preliminary Phase	Melakukan kegiatan persiapan yang diperlukan untuk memenuhi arahan bisnis untuk arsitektur perusahaan yang baru, termasuk definisi kerangka kerja dan alat bantu arsitektur khusus organisasi, dan definisi prinsip-prinsip.
Phase A: Architecture Vision	Menentukan ruang lingkup, batasan, dan harapan untuk proyek. Rancang visi arsitektur, identifikasi pemangku kepentingan, validasi konteks bisnis dan buat pernyataan pekerjaan arsitektur serta dapatkan persetujuan
Phase B: Business Architecture	Pengembangan arsitektur bisnis untuk mendukung visi arsitektur yang telah disepakati. Pada tahap ini tools dan method umum untuk pemodelan seperti: Integration DEFinition (IDEF) dan Unified Modeling Language (UML) bisa digunakan untuk membangun model yang diperlukan
Phase C: Information Systems Architectures	Bagaimana arsitektur sistem informasi dikembangkan, tentukan jenis data dan aplikasi yang diperlukan untuk mendukung bisnis dan pastikan pemangku kepentingan memahaminya. Teknik yang bisa digunakan dengan yaitu: ER-Diagram, Class Diagram, dan Object Diagram
Phase D: Technology Architecture	Bangun arsitektur teknologi yang diinginkan dengan menentukan jenis teknologi yang diperlukan melalui Technology Portfolio Catalog, mencakup perangkat lunak dan keras, serta mempertimbangkan alternatif dalam pemilihan teknologi
Phase E: Opportunities and Solutions	Evaluasi model arsitektur saat ini, identifikasi proyek utama yang diperlukan untuk mencapai arsitektur tujuan, serta klasifikasikan proyek tersebut sebagai pengembangan baru atau pemanfaatan kembali sistem yang ada
Phase F: Migration and Planning	Menganalisis manfaat biaya dan risiko serta mengembangkan rencana implementasi dan migrasi yang terperinci.
Phase G: Implementation Governance	Memberikan pengawasan arsitektural untuk implementasi
Phase H: Architecture Change Management	Menyediakan pemantauan berkelanjutan dan proses manajemen perubahan untuk memastikan bahwa arsitektur merespons kebutuhan perusahaan dan memaksimalkan nilai arsitektur untuk bisnis.

Fase TOGAF	Penjelasan
Requirements Management	Menguji proses pengelolaan architecture requirements sepanjang siklus ADM berlangsung.

(Anam dkk., 2021) menyatakan bahwa pendekatan sistemik seperti ADM penting untuk menghadapi kompleksitas dalam organisasi modern, karena memungkinkan integrasi antara struktur organisasi, teknologi, dan proses bisnis. Hal ini sejalan dengan penelitian (Girsang dan Abimanyu, 2021), yang menyebutkan bahwa TOGAF ADM memberikan pedoman terstruktur dan fleksibel untuk mengembangkan arsitektur yang adaptif terhadap perubahan lingkungan bisnis dan teknologi. Selain itu, TOGAF ADM dianggap scalable dan dapat disesuaikan dengan kebutuhan organisasi berskala kecil maupun besar.

The Architecture Content Framework merupakan komponen penting yang mendukung proses pengembangan arsitektur dengan menyediakan struktur dan artefak standar yang dibutuhkan untuk mendokumentasikan hasil dari setiap fase ADM (*Architecture Development Method*). Framework ini memastikan bahwa setiap produk arsitektur (output) memiliki konsistensi, kejelasan, dan keterkaitan dengan keseluruhan proses pengembangan enterprise architecture. Menurut (The Open Group, 2018), *Architecture Content Framework* menggunakan tiga kategori berikut untuk menggambarkan tipe hasil kerja arsitektural (*architectural work product*) berdasarkan konteks penggunaanya:

A. Deliverable

Deliverable adalah output formal yang dihasilkan pada setiap tahapan TOGAF Architecture Development Method (ADM). Deliverable biasanya berupa dokumen atau laporan yang disetujui oleh pemangku kepentingan (stakeholders) dan digunakan sebagai dasar untuk pengambilan keputusan atau tindakan lebih lanjut.

B. Artifact

Artifact adalah dokumen atau model aktual yang menangkap dan merepresentasikan informasi arsitektur. Artifacts dikelompokkan sebagai katalog (daftar benda), matriks (menampilkan keterhubungan antar benda), dan diagram (gambar benda). Sebuah deliverable arsitektural dapat berisikan banyak

dan sekumpulan artifacts akan menjadi konten dari repositori arsitektur (Architecture Repository).

C. Building Blocks

Building block mempresentasikan sebuah komponen bisnis, IT, atau kemampuan arsitektural yang mungkin dapat digunakan kembali (re-useable), yang dapat dikombinasikan dengan building blocks lain untuk menyampaikan arsitektur dan solusinya.

2.2.3 Manajemen Risiko

Manajemen risiko adalah proses terintegrasi yang melibatkan identifikasi, penilaian, dan pengendalian terhadap berbagai risiko yang berpotensi menghambat pencapaian tujuan organisasi (Rocha dkk., 2024). Menurut (Vorst dkk., 2018) dalam buku Manajemen Risiko Berbasis SNI ISO 31000, manajemen risiko merupakan bagian integral dari tata kelola organisasi dan harus dilakukan secara terstruktur, sistematis, dan menyeluruh, dengan mempertimbangkan konteks internal maupun eksternal. (Sarjana dkk., 2022) menyatakan bahwa manajemen risiko adalah proses berkelanjutan yang melibatkan seluruh unsur organisasi, tidak hanya untuk menghindari ancaman, tetapi juga untuk mendorong inovasi dan perbaikan berkelanjutan melalui kepemimpinan dan budaya risiko yang kuat.

Dalam buku Strategic Risk Management A Research Overview, (Andersen dan Sax, 2020) menekankan bahwa manajemen risiko strategis harus terintegrasi dengan proses pengambilan keputusan dan strategi organisasi. Risiko tidak hanya harus dikelola secara reaktif, tetapi juga diposisikan sebagai bagian dari upaya menciptakan nilai dan keunggulan kompetitif dalam jangka panjang. (Praja dkk., 2020) menyimpulkan bahwa efektivitas manajemen risiko bergantung pada keterlibatan pimpinan puncak, kebijakan yang jelas, serta penerapan kerangka kerja yang sesuai dengan karakteristik organisasi.

Untuk mendukung penerapan manajemen risiko, berbagai kerangka kerja telah dikembangkan dan diadopsi secara luas oleh organisasi di berbagai sektor. Salah satunya adalah ISO 31000, yaitu standar internasional yang memberikan prinsip dan panduan umum dalam pengelolaan risiko organisasi secara menyeluruh.

Selain itu, terdapat pula COSO ERM yang mengintegrasikan manajemen risiko ke dalam proses strategis dan operasional organisasi untuk menciptakan nilai dan keberlanjutan. Dalam konteks keamanan informasi, NIST Risk Management Framework banyak digunakan, khususnya oleh institusi pemerintah di Amerika Serikat, karena memberikan pendekatan sistematis terhadap pengelolaan risiko TI. Sementara itu, COBIT yang dikembangkan oleh ISACA menjadi kerangka kerja yang komprehensif untuk tata kelola dan manajemen teknologi informasi, termasuk di dalamnya pengelolaan risiko TI secara terstruktur dan selaras dengan tujuan.

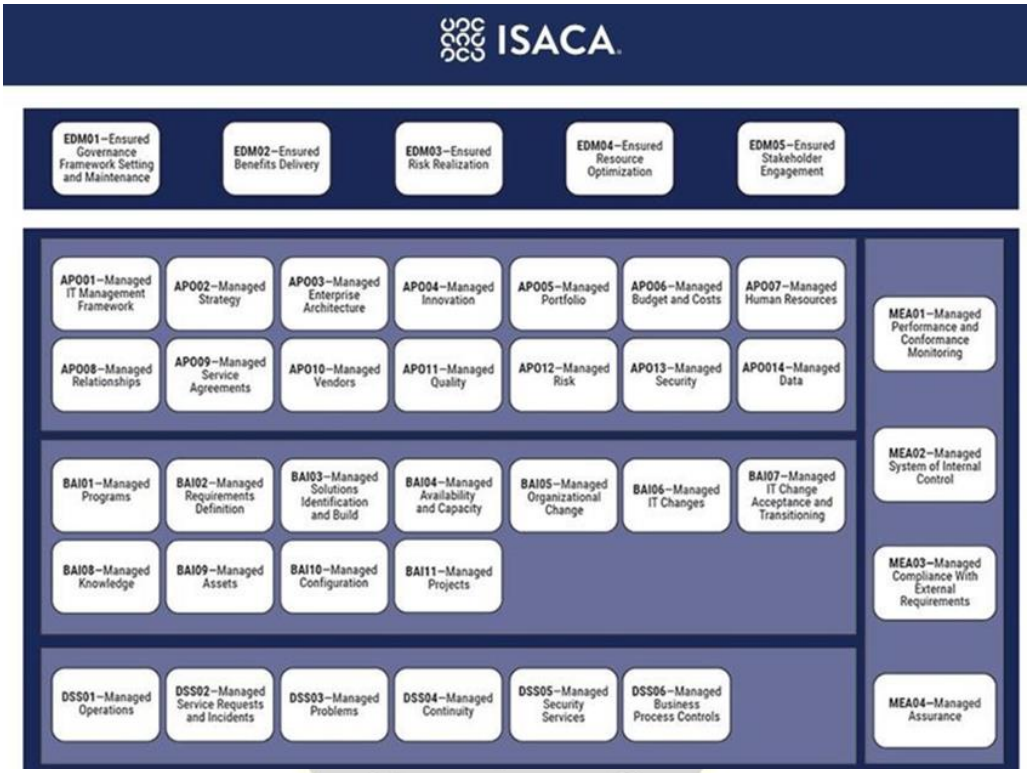
Dalam konteks penelitian ini, kerangka kerja COBIT 2019, khususnya domain APO12 (*Manage Risk*), dipilih sebagai dasar untuk analisis dan pengelolaan risiko teknologi informasi. COBIT 2019 dipilih karena dirancang secara khusus untuk mengelola dan mengawasi sistem informasi dan TI organisasi (Irawan dkk., 2023). Kerangka ini memberikan pedoman yang selaras dengan prinsip tata kelola TI modern, mudah diintegrasikan dengan kerangka kerja arsitektur enterprise seperti TOGAF ADM, serta menyediakan fokus pada pengelolaan risiko yang selaras dengan tujuan bisnis organisasi.

2.2.4 Kerangka Kerja COBIT 2019

COBIT (*Control Objectives for Information and Related Technology*) merupakan kerangka kerja standar yang dikembangkan oleh IT Governance Institute, bagian dari ISACA, untuk mendukung tata kelola dan manajemen teknologi informasi. Versi COBIT 2019, hadir sebagai penyempurnaan dari COBIT 5 dengan penekanan pada pemisahan yang lebih jelas antara fungsi tata kelola dan manajemen (Haes dkk., 2020). Tujuan tata kelola direpresentasikan oleh domain Evaluate, Direct and Monitor (EDM), serta manajemen yang mencakup domain Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), dan Monitor, Evaluate and Assess (MEA).

Domain EDM berfokus dalam evaluasi opsi strategis, pengarahan manajemen senior, dan pemantauan pencapaian strategi. Domain APO menitikberatkan pada penyelarasan strategi TI dengan tujuan bisnis, perencanaan, dan pengorganisasian kegiatan pendukung. Domain BAI terkait definisi, akuisisi,

implementasi solusi TI, serta integrasinya ke dalam proses bisnis. Domain DSS menyoroti penyampaian layanan operasional TI, dukungan, keamanan, dan kontinuitas layanan. Serta domain MEA sebagai pemantau kinerja TI, memastikan kesesuaian dengan target internal, pengendalian, dan persyaratan eksternal. Berikut adalah penggambaran domain Cobit 2019 pada Gambar 2.2.



Gambar 2.2 Model Inti Cobit 2019 (ISACA, 2018b)

Domain APO12 (*Manage Risk*), dirancang untuk menyelaraskan manajemen risiko TI dengan strategi manajemen risiko organisasi. Pada modul COBIT 2019 yang berjudul *Governance and Management Objectives*, domain APO12 mencakup enam subdomain yang membentuk kerangka kerja yang komprehensif untuk mengelola risiko TI secara efektif, memungkinkan organisasi mengidentifikasi, menganalisis, dan merespons risiko selaras terhadap strategi bisnis (ISACA, 2018a). Penjelasan domain APO 12 tersaji pada Tabel 2.3.

Tabel 2.3 Domain APO 12 Manage Risk

Sub Domain		**Penjelasan**
APO12 .01	Collect data (mengumpulkan data)	Menekankan pentingnya mengidentifikasi dan mengumpulkan data yang relevan untuk mendukung proses identifikasi,

Sub Domain		Penjelasan
		analisis, dan pelaporan risiko IdanT secara efektif
APO12 .02	Analyze risk (menganalisis risiko)	Mengembangkan pemahaman berbasis bukti mengenai risiko yang dihadapi organisasi, sehingga dapat mendukung proses pengambilan keputusan yang tepat terkait manajemen risiko
APO12 .03	Maintain a risk profile (memelihara profil risiko)	Organisasi diharapkan mampu memelihara inventaris risiko yang telah teridentifikasi, termasuk atribut-atribut penting seperti frekuensi kejadian, dampak potensial, serta strategi respons yang tersedia. Profil risiko ini juga harus mencakup dokumentasi atas sumber daya, kemampuan, dan aktivitas pengendalian yang telah diterapkan
APO12 .04	Articulate risk (mengartikulasikan risiko)	Mengharuskan organisasi untuk mengkomunikasikan kondisi eksisting terkait paparan risiko dan peluang TI kepada seluruh *stakeholder* secara tepat waktu, guna memastikan respons yang cepat dan akurat
APO12 .05	Define a risk management action portfolio (menetapkan portofolio tindakan manajemen risiko)	Menekankan perlunya pengelolaan berbagai upaya mitigasi risiko dalam bentuk portofolio tindakan yang terencana dan terintegrasi, sehingga risiko dapat ditekan ke tingkat yang dapat diterima
APO12 .06	Respond to risk (menanggapi risiko)	Mengarahkan organisasi untuk merespons peristiwa risiko yang terjadi secara cepat dan efektif, dengan tujuan utama membatasi besarnya kerugian atau dampak yang mungkin ditimbulkan

Risiko TI dikelola melalui identifikasi *risk scenario*, yaitu gambaran terstruktur mengenai kejadian atau rangkaian kejadian yang berpotensi mengganggu pencapaian tujuan organisasi. Pendekatan ini mencakup aktor (pihak yang menyebabkan risiko: karyawan, vendor, atau sistem), ancaman (sumber risiko seperti serangan siber atau bencana alam), peristiwa (kejadian inti seperti pelanggaran data atau gangguan layanan), aset (sumber daya yang terdampak, baik fisik, informasi, maupun manusia), dan waktu (durasi atau periode risiko terjadi dan dampaknya dirasakan) (Moll, 2018). Gambaran Risk Scenario bisa dilihat pada Gambar 2.3.

Gambar 2.3 Risk Skenario (Kohler dan Fragniè, 2021)

Dalam melakukan analisis risiko terdapat dua cara yang dilakukan yaitu menggunakan metode kualitatif atau kuantitatif untuk menilai dampak dan probabilitas (Evrin, 2021). Analisis kualitatif merupakan metode subjektif dalam menilai risiko berdasarkan dampak dan probabilitasnya, dengan melibatkan pemangku kepentingan melalui pendekatan seperti *brainstorming*, wawancara, survei, atau observasi. Risiko yang teridentifikasi kemudian diklasifikasikan berdasarkan tingkat kemungkinan dan dampaknya, dalam kategori rendah, sedang, atau tinggi. Hasil penilaian ini dipetakan dalam matriks risiko untuk membantu memvisualisasikan dan memprioritaskan risiko yang memerlukan perhatian segera.

Matriks risiko menggabungkan *Likelihood* (kemungkinan terjadinya risiko) dan *Impact* (tingkat dampak terhadap organisasi jika risiko tersebut terjadi). *Likelihood* diklasifikasikan mulai dari *Rare* (1) hingga *Almost Certain* (5) dan *Impact* diklasifikasikan dari *Insignificant* (1) hingga *Critical* (5) (Slater dan Hill, 2024) seperti terlihat pada Tabel 2.4.

Tabel 2.4 Risk Matriks

Likelihood	**Impact**				
	Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Critical (5)**
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Hasil perkalian antara *Likelihood* dan *Impact* menghasilkan nilai numerik yang menunjukkan tingkat risiko, yang selanjutnya dikategorikan ke dalam empat zona warna: zona hijau untuk risiko rendah (nilai 1–4) yang tidak memerlukan tindakan segera, zona kuning untuk risiko sedang (nilai 5–9) perlu mitigasi, tetapi tidak darurat, zona oranye untuk risiko tinggi (nilai 10–14) dengan tindakan memerlukan perhatian segera, dan zona merah untuk risiko sangat tinggi atau kritis (nilai 15–25) harus segera ditangani untuk menghindari dampak besar.

Analisis kuantitatif merupakan metode objektif untuk menilai risiko secara numerik menggunakan data dan statistik guna menghasilkan estimasi eksposur risiko yang lebih akurat. Proses dimulai dengan identifikasi risiko, dilanjutkan dengan pengumpulan data historis seperti frekuensi kejadian dan dampak biaya. Probabilitas dan dampak kemudian dianalisis menggunakan teknik seperti distribusi probabilitas, simulasi Monte Carlo, atau Value at Risk (VaR), dengan rumus Risk Exposure = Probabilitas × Dampak (Kiswati dkk., 2020):

$$Risk\ Exposure = Probabilitas * Dampak \quad (2.1)$$

Hasilnya divisualisasikan melalui magnitude matrix atau heat map, dan risiko diprioritaskan berdasarkan nilai eksposur tertinggi untuk tindakan mitigasi yang lebih tepat sasaran.

Setelah skenario risiko berhasil diidentifikasi dan dirumuskan berdasarkan konteks organisasi, selanjutnya dituangkan ke dalam Risk Register sebagai dokumentasi seluruh risiko. Risk register adalah dokumen yang digunakan untuk mencatat dan mengelola risiko yang diidentifikasi dalam proses manajemen risiko. Risk register berisi informasi tentang risiko, termasuk deskripsi risiko, tingkat kemungkinan, dampak, pemilik risiko, serta langkah-langkah mitigasi. Risk register membantu dalam memantau dan mengendalikan risiko secara sistematis sepanjang siklus proyek atau kegiatan tertentu (Evrin, 2021). Risk scenario dan risk register saling terkait dalam proses pengelolaan risiko. Risk scenario menggambarkan potensi kejadian risiko tertentu yang mungkin terjadi, sedangkan risk register adalah dokumen yang mencatat semua risiko yang telah diidentifikasi, termasuk risiko yang didasarkan pada berbagai skenario.