BAB II
KAJIAN LITERATUR

2.1 Manajemen Risiko Teknologi Informasi *(IT Risk Management)*

IT Risk Management merupakan suatu proses sistematis yang dilakukan oleh organisasi untuk mengidentifikasi, menganalisis, menilai, menanggapi, serta memantau risiko-risiko yang muncul akibat penggunaan dan pengelolaan teknologi informasi dalam kegiatan operasional perusahaan. Risiko TI mencakup berbagai bentuk ketidakpastian yang dapat berdampak negatif terhadap tujuan bisnis, mulai dari gangguan operasional, kehilangan data, serangan siber, hingga kegagalan sistem dan jaringan. Tujuan utama manajemen risiko TI adalah memastikan bahwa aset informasi organisasi terlindungi, layanan tetap beroperasi secara andal, dan keputusan bisnis dapat diambil dengan mempertimbangkan aspek keamanan serta keberlanjutan teknologi[14].

Manajemen risiko menjadi krusial karena perkembangan teknologi yang pesat telah meningkatkan potensi terjadinya ancaman seperti gangguan layanan, kebocoran data, serta serangan siber yang dapat menghambat kelancaran operasional bisnis dan menurunkan kepercayaan pelanggan. Dalam era digital, ketergantungan organisasi terhadap sistem dan infrastruktur TI membuat setiap gangguan kecil dapat berdampak besar terhadap kontinuitas operasional, reputasi, serta stabilitas keuangan perusahaan. Oleh karena itu, penerapan manajemen risiko TI berfungsi untuk memastikan bahwa seluruh potensi ancaman dapat diidentifikasi, dianalisis, dan dikendalikan secara efektif melalui proses yang terukur dan terdokumentasi dengan baik. Sebuah penelitian menjelaskan bahwa manajemen risiko TI yang diterapkan secara terstruktur dapat meningkatkan kesiapan organisasi dalam menghadapi insiden teknologi serta menjaga kesinambungan layanan[15]. Penerapan praktik manajemen risiko yang efektif memungkinkan organisasi untuk mengidentifikasi potensi gangguan sejak dini dan menetapkan strategi mitigasi yang tepat, sehingga mengurangi dampak negatif terhadap kinerja bisnis dan keandalan sistem[16]. Penelitian lain menegaskan bahwa pengelolaan risiko TI yang terstruktur juga membantu meningkatkan efisiensi proses pengambilan keputusan dan mendukung pencapaian tujuan strategis perusahaan melalui peningkatan kapabilitas pengendalian serta ketahanan terhadap insiden teknologi[17].

Secara umum, manajemen risiko teknologi informasi dapat dikategorikan ke dalam beberapa jenis utama sebagai berikut:

1. Manajemen Risiko Kepatuhan *(Compliance Risk Management)*

Manajemen risiko kepatuhan merupakan proses penting untuk memastikan seluruh kegiatan organisasi berjalan sesuai hukum, regulasi, dan standar industri agar terhindar dari sanksi maupun kerugian reputasi. Dalam konteks lembaga publik seperti Direktorat Jenderal Pajak (DJP), pendekatan ini diterapkan melalui sistem klasifikasi wajib pajak berdasarkan tingkat risiko kepatuhan sehingga pengawasan dapat dilakukan lebih efisien, dan hasilnya terbukti meningkatkan efektivitas pemeriksaan serta penerimaan pajak[18]. Penerapan *compliance risk management* juga dibuktikan melalui peningkatan capaian penerimaan pajak di KPP Pratama Senen. Hasil pengukuran efektivitasnya menunjukkan bahwa empat kriteria utama seperti efektivitas, efisiensi, perataan, dan kecukupan telah berjalan cukup baik, mencerminkan peningkatan kinerja pengawasan pajak secara umum. Namun, dari sisi responsivitas dan ketepatan, masih terdapat kekurangan karena proses tindak lanjut terhadap pelanggaran wajib pajak belum sepenuhnya cepat dan akurat dalam menentukan prioritas risiko kepatuhan, seperti pelaporan pendapatan secara menyeluruh[19]. Pada sektor perbankan, penerapan manajemen risiko kepatuhan menjadi elemen penting untuk memastikan seluruh kegiatan usaha berjalan sesuai dengan prinsip syariah serta peraturan yang berlaku. Risiko kepatuhan dapat berdampak signifikan terhadap reputasi, pendapatan, dan kepercayaan nasabah apabila tidak dikelola dengan baik[20]. Selain itu, penerapan manajemen risiko kepatuhan yang terintegrasi dalam kerangka *Governance, Risk, and Compliance (GRC)* juga mampu memperkuat tata kelola, transparansi, dan akuntabilitas organisasi di berbagai sektor, menjadikan fungsi audit internal tidak hanya berperan sebagai pengawas kepatuhan, tetapi juga sebagai mitra strategis dalam mitigasi risiko dan peningkatan nilai organisasi[21].

2.* Manajemen Risiko Bahaya *(Hazard Risk Management)

Hazard risk management adalah pengelolaan risiko dari potensi bahaya atau kerusakan yang dapat menyebabkan kerugian fisik, kesehatan, atau lingkungan. Risiko ini bersifat murni negatif dan tidak menimbulkan peluang keuntungan, seperti kecelakaan kerja, bencana alam, atau kebakaran[22].

Sebuah penelitian menunjukkan bahwa risiko bahaya di industri pembuatan kapal tradisional *"Phinisi"* merupakan ancaman serius terhadap keselamatan dan kesehatan pekerja. Risiko seperti terjatuh, tertimpa benda, hingga paparan bahan berbahaya menjadi faktor utama yang dapat menyebabkan kecelakaan kerja fatal. Studi ini menekankan bahwa identifikasi dan pengendalian *hazard risk* harus menjadi bagian inti dalam sistem manajemen keselamatan kerja, karena kegagalan dalam mitigasi dapat menyebabkan kerugian besar,

baik dari sisi manusia (cedera/kematian) maupun material (kerusakan alat dan keterlambatan produksi)[21]. Penelitian serupa dilakukan di PT Barokah Galangan Perkasa yang bergerak di bidang manufaktur, perbaikan dan perawatan kapal dengan metode HIRARC *(Hazard Identification, Risk Assessment and Risk Control),* menemukan adanya 40 potensi bahaya di area akomodasi atas dan 37 potensi bahaya di area tangki minyak yang terdiri dari risiko rendah hingga tinggi, seperti tersengat listrik dan kebakaran akibat hubungan arus pendek. Risiko ini dikendalikan melalui pengawasan administratif, penggunaan alat pelindung diri (APD), pengendalian rekayasan teknis, hingga pemberian peringatan atau perubahan bonus dan upah bagi pekerja yang tidak patuh[23]. Penelitian serupa pada proyek konstruksi menunjukkan bahwa 76% kecelakaan kerja didominasi oleh kasus tersengat listrik, tertimpa material, dan jatuh dari ketinggian, yang menegaskan bahwa penerapan manajemen K3 menjadi aspek krusial dalam melindungi keselamatan tenaga kerja dan menjaga produktivitas[24].

Hazard Risk Management dalam konteks teknologi informasi merupakan proses sistematis untuk mengidentifikasi, menilai, mengendalikan, dan memantau potensi bahaya yang dapat mengganggu atau merusak infrastruktur TI, data, maupun layanan digital organisasi. Bahaya ini tidak hanya mencakup kecelakaan fisik, tetapi juga mencakup kegagalan perangkat keras secara tiba-tiba, kesalahan konfigurasi sistem, *overloading* jaringan, paparan *malware*, hingga gangguan lingkungan seperti pemadaman listrik atau cuaca ekstrem yang berdampak pada operasional sistem[25,26,27]. Oleh karena itu, penerapan manajemen risiko bahaya dalam bidang TI menjadi elemen penting untuk menjaga kontinuitas layanan, keamanan data, dan stabilitas sistem organisasi secara menyeluruh.

3. Manajemen Risiko Peluang *(Opportunity Risk Management)*

Opportunity Risk Management adalah pengelolaan risiko yang timbul dari pengambilan peluang yang secara sengaja dilakukan organisasi dengan harapan mendapatkan hasil positif, namun di sisi lain ada kemungkinan kerugian atau kegagalan. Risiko ini bersifat spekulatif yaitu organisasi memilih suatu strategi atau investasi yang bisa menguntungkan tetapi sekaligus membawa potensi kerugian. Risiko ini juga meliputi risiko kehilangan peluang terbaik jika organisasi memilih jalan yang kurang optimal[28].

Beberapa studi menyoroti bahwa ketidakpastian dan risiko tidak selalu bersifat negatif, melainkan dapat mendorong inovasi dan peluang strategis. Di sektor industri China, ketidakpastian kebijakan lingkungan mendorong perusahaan manufaktur dan energi untuk mengembangkan inovasi ramah lingkungan, sekaligus menghadapi risiko finansial jika

implementasi gagal[28]. Hal serupa terjadi pada perusahaan intensitas karbon tinggi, di mana CEO dengan orientasi risiko memandang perubahan iklim sebagai peluang untuk meningkatkan efisiensi energi, memperkuat citra perusahaan, dan mengembangkan inovasi hijau[29]. Pada sektor keuangan Malaysia, keberadaan komite manajemen risiko dan struktur kepemilikan difokuskan tidak sekadar menghindari risiko, tetapi mengelolanya secara strategis agar mampu meningkatkan kinerja perusahaan[30].

Dalam bidang TI, manajemen risiko peluang berarti organisasi tidak hanya mengelola potensi kerugian, tetapi juga memanfaatkan peluang yang muncul dari teknologi baru dan inovasi layanan digital. Misalnya, metode *ROAM (Risky Opportunity Analysis Method)* membantu organisasi menilai risiko dan peluang saat melakukan digitalisasi infrastruktur kritikal, sehingga bisa memilih solusi yang aman sekaligus inovatif [31]. Di sektor keuangan, adopsi kecerdasan buatan (AI) dapat meningkatkan efisiensi dan inovasi, tetapi harus didukung manajemen risiko agar tidak menimbulkan masalah, seperti pelanggaran regulasi atau kebocoran data[32]. Penelitian di sektor *fintech* juga menunjukkan bahwa pertumbuhan teknologi, seperti pengembangan aplikasi pembayaran digital, pinjaman *online*, dan layanan investasi berbasis teknologi, harus dibarengi strategi mitigasi risiko, seperti pengelolaan kredit dan kepatuhan regulasi, agar peluang TI bisa dimanfaatkan secara optimal tanpa merugikan perusahaan[33].

Dengan demikian, pengelolaan risiko peluang tidak hanya memungkinkan organisasi memanfaatkan ketidakpastian sebagai dorongan inovasi, tetapi juga memastikan bahwa langkah-langkah strategis yang diambil tetap aman dan terukur. Dalam bidang TI, hal ini berarti setiap pengembangan teknologi atau layanan digital harus seimbang antara potensi keuntungan dan mitigasi risiko, sehingga inovasi dapat diterapkan secara efektif tanpa menimbulkan kerugian operasional atau reputasi[31,32,33].

4. Manajemen Risiko Pengendalian *(Control Risk Management)*

Control Risk Management adalah pengelolaan risiko pada potensi di mana sistem pengendalian internal dan proses pengendalian organisasi gagal mencegah, mendeteksi, atau memperbaiki kerugian atau penyimpangan secara tepat waktu. Dengan kata lain, meskipun organisasi telah mengidentifikasi risiko atau ancaman yang mungkin timbul, kontrol yang ada mungkin tidak cukup efektif untuk memastikan bahwa risiko tersebut dikendalikan sehingga tujuan organisasi dapat tercapai[34].

Penelitian pada sektor korporasi non-keuangan di Prancis yang terdaftar di indeks SBF 120 meneliti pengaruh kualitas pengendalian internal terhadap praktik manajemen laba, baik berbasis aktual maupun aktivitas operasional nyata[35]. Penelitian serupa pada sektor

jasa keuangan dan bisnis swasta di Indonesia juga menemukan bahwa peran audit internal dan efektivitas sistem pengendalian internal berpengaruh positif terhadap kualitas laporan keuangan[36]. Hasil penelitian keduanya menunjukkan bahwa perusahaan dengan sistem pengendalian internal yang kuat cenderung lebih sedikit melakukan manipulasi laporan keuangan, sedangkan kelemahan dalam kontrol internal meningkatkan risiko penyimpangan[35,36]. Kepatuhan terhadap sistem pengendalian internal, khususnya pada aktivitas pengendalian, informasi, komunikasi, dan pemantauan, berpengaruh positif terhadap keberlanjutan kinerja keuangan bank, sehingga memperkuat peran pengendalian internal dalam menjaga stabilitas operasional[37]. Efektivitas pengendalian internal juga terbukti mampu menekan risiko audit yang timbul dari investasi teknologi informasi, menunjukkan pentingnya kontrol internal dalam menjaga keandalan sistem dan mengurangi risiko pengendalian[38]. Sementara itu, penelitian di sektor layanan teknologi informasi global menemukan bahwa gangguan layanan jaringan dapat diminimalkan melalui penerapan kontrol internal yang ketat dalam proses pengadaan dan pemeliharaan sistem, guna memastikan kontinuitas operasional dan keamanan layanan[39].

Sebagai *dealer* resmi merek terkemuka, seperti *Daihatsu, Kubota,* dan *UD Trucks,* PT. Capella Medan menjalankan proses bisnis yang sangat bergantung pada layanan jaringan dan sistem informasi yang terintegrasi. Aktivitas seperti pemrosesan penjualan kendaraan, pencatatan administrasi, pelaporan keuangan, hingga komunikasi antar cabang seluruhnya memerlukan konektivitas yang stabil dan aman, namun sering kali operasional perusahaan mengalami hambatan akibat gangguan jaringan, seperti terjadinya *downtime* yang berdampak pada keterlambatan proses administrasi, terganggunya transaksi penjualan, kendala dalam pelaporan data, serta tersendatnya komunikasi baik antar divisi maupun dengan pihak eksternal. Oleh karena itu, pengendalian terhadap risiko yang muncul dari gangguan layanan jaringan menjadi sangat penting untuk memastikan operasional berjalan lancar. Kelemahan dalam sistem pengendalian internal atau keterlambatan dalam mendeteksi gangguan dapat mengakibatkan terhambatnya pelayanan pelanggan, kesalahan data, hingga menurunnya efisiensi bisnis. Dengan demikian, pembahasan mengenai manajemen risiko di PT. Capella Medan menjadi relevan karena menjadi dasar dalam mitigasi dampak gangguan jaringan.

2.2 Gangguan Layanan Jaringan

Gangguan layanan jaringan merupakan kondisi ketika sistem jaringan yang berfungsi sebagai tulang punggung konektivitas data dan komunikasi dalam organisasi mengalami penurunan performa atau bahkan berhenti beroperasi, sehingga layanan teknologi informasi

tidak dapat diakses sebagaimana mestinya[40]. Gangguan ini dapat memengaruhi berbagai aktivitas bisnis yang bergantung pada ketersediaan jaringan, termasuk proses administrasi, transaksi digital, pengiriman data, hingga komunikasi antarcabang. Penyebab gangguan jaringan dapat diklasifikasikan ke dalam beberapa faktor, yakni serangan siber, seperti *Distributed Denial-of-Service (DDoS)*, kerusakan perangkat keras, serta kesalahan konfigurasi jaringan yang mengakibatkan peningkatan *latency* atau *downtime* berkepanjangan[41]. Ketidakstabilan jaringan dapat menurunkan kepercayaan pengguna terhadap layanan digital, sehingga diperlukan pemantauan berkelanjutan untuk mendeteksi gangguan sejak dini. Sistem pemantauan jaringan secara *real-time* terbukti mampu meningkatkan keandalan layanan dengan mendeteksi anomali performa lebih awal sebelum menimbulkan gangguan serius[42].

Gangguan layanan jaringan merupakan permasalahan yang umum terjadi dan berdampak signifikan terhadap kinerja operasional suatu organisasi. Penelitian menunjukkan bahwa klasifikasi gangguan jaringan dapat membantu dalam mengidentifikasi sumber permasalahan secara lebih akurat sehingga langkah penanganan dapat dilakukan lebih cepat dan tepat. Sebagai contoh, studi yang menganalisis gangguan *low bandwidth* pada jaringan Bank Tabungan Negara (BTN) menemukan bahwa penggunaan pendekatan analitis berbasis *machine learning* mampu meningkatkan efektivitas deteksi dan mempercepat proses pemulihan jaringan[43]. Selain itu, hasil penelitian di Badan Penghubung Provinsi Lampung memperlihatkan bahwa gangguan layanan jaringan juga dapat disebabkan oleh faktor eksternal, seperti cuaca ekstrem dan peningkatan beban trafik, yang berpengaruh terhadap parameter *throughput, delay,* dan *packet loss*[25]. Temuan ini menegaskan bahwa gangguan jaringan dapat bersumber dari aspek teknis maupun lingkungan, dan keduanya sama-sama berpotensi menurunkan performa layanan serta menghambat kelancaran arus komunikasi dan data dalam sistem jaringan[25,43].

Dalam era digitalisasi layanan publik, stabilitas dan keamanan jaringan menjadi elemen penting yang menentukan keberhasilan sistem informasi di berbagai sektor, salah satunya bidang kesehatan. RSUD Kabupaten Kediri menghadapi sejumlah kendala berupa gangguan layanan jaringan, keterbatasan kapasitas server, serta belum optimalnya sistem keamanan data pasien, yang menyebabkan terhambatnya akses dan sinkronisasi data antarunit serta berdampak langsung pada kelancaran pelayanan kesehatan[44].

Gangguan jaringan seperti ini bersifat krusial karena dapat menghambat kegiatan operasional organisasi, memperlambat aliran informasi antarunit kerja, dan berpotensi mengganggu layanan publik yang bergantung pada konektivitas jaringan, termasuk pada

sektor lain, seperti PT Capella Medan. Gangguan jaringan serupa dapat berdampak langsung pada proses administrasi penjualan, transaksi keuangan, serta koordinasi antar cabang. Oleh karena itu, penelitian ini menegaskan pentingnya penerapan audit manajemen risiko dalam sistem jaringan. Audit ini dibutuhkan untuk mengidentifikasi titik rawan gangguan, mengevaluasi efektivitas kontrol yang ada, serta memastikan adanya mekanisme mitigasi yang mampu mengantisipasi gangguan serupa sebelum berdampak luas terhadap kinerja operasional perusahaan.

2.3 Audit Teknologi Informasi

Audit Teknologi Informasi (TI) merupakan proses evaluasi yang dilakukan secara sistematis, terstruktur, dan objektif untuk memastikan bahwa penerapan serta pengelolaan sistem informasi dalam suatu organisasi telah sesuai dengan tujuan strategis, standar, dan kebijakan yang berlaku. Audit teknologi informasi mencakup evaluasi sistematis terhadap kepatuhan standar teknis, mekanisme keamanan data, efisiensi operasional, keandalan layanan, serta integrasi informasi dengan tujuan menilai sejauh mana penerapan dan pengelolaan teknologi informasi telah sesuai dengan prinsip-prinsip tata kelola TI yang baik dalam mendukung pencapaian sasaran strategis organisasi[45].

Audit TI berperan penting dalam meningkatkan efektivitas pengendalian internal dan kualitas operasional sistem, karena kemampuan auditor dan kapabilitas TI organisasi menentukan sejauh mana audit memberikan hasil yang andal[46]. Tata kelola TI yang baik memungkinkan audit menilai kepatuhan terhadap standar, sekaligus meningkatkan transparansi dan akuntabilitas informasi, sehingga menjadi alat strategis untuk pengawasan dan penjaminan kualitas TI[47]. Selain itu, Audit TI juga membantu organisasi memanfaatkan sumber daya TI dengan efisien, menemukan ketidaksesuaian operasional, dan menjaga kelancaran proses bisnis[48]. Lebih jauh, audit TI beradaptasi dengan perkembangan teknologi baru, menjaga integritas data, dan memastikan kepatuhan terhadap prinsip tata kelola modern, sehingga organisasi siap menghadapi kompleksitas digital[49].

Dengan demikian, audit TI menjadi alat strategis untuk menilai kualitas pengelolaan TI secara keseluruhan, memastikan sistem informasi mendukung pencapaian tujuan organisasi secara efektif, efisien, dan berkelanjutan[50]. Fungsi ini menjadikan audit TI sangat penting, terutama ketika layanan digital memegang peran besar dalam keberlangsungan operasi perusahaan.

Dalam konteks penelitian ini, audit TI difokuskan pada aspek manajemen risiko gangguan layanan TI untuk memberikan gambaran tingkat kesiapan sistem dalam

mengendalikan risiko, meminimalkan gangguan operasional, dan menjaga kualitas layanan yang diterima pengguna. Oleh karena itu, audit manajemen risiko gangguan layanan TI dipilih sebagai langkah strategis untuk memastikan sistem TI tetap andal, aman, dan mendukung keberlanjutan operasional perusahaan secara optimal.

2.4 Audit Manajemen Risiko Teknologi Informasi

Audit manajemen risiko teknologi informasi adalah suatu proses sistematis yang bertujuan mengevaluasi efektivitas pengendalian terhadap ancaman dan kelemahan yang terkait TI dalam rangka mendukung pencapaian tujuan organisasi secara efektif dan efisien [51]. Melalui audit, organisasi dapat mengidentifikasi, menganalisis, dan mengevaluasi risiko TI, kemudian memastikan bahwa mekanisme mitigasi, kebijakan, dan prosedur yang berlaku sudah memadai dan diimplementasikan dengan baik sehingga potensi kerugian akibat gangguan teknologi dapat diminimalkan[15].

Pelaksanaan audit manajemen risiko TI biasanya dilakukan dengan pendekatan yang sistematis, mencakup tahapan identifikasi risiko, evaluasi kontrol yang ada, dan penilaian efektivitas kebijakan organisasi dalam menangani ancaman yang mungkin timbul. Auditor akan mengumpulkan bukti dan data yang relevan untuk menilai apakah sistem keamanan, pengelolaan data, dan proses operasional sudah berjalan sesuai standar yang berlaku. Melalui audit ini, organisasi dapat memperoleh gambaran menyeluruh mengenai kondisi aktual pengendalian risiko serta menentukan langkah-langkah peningkatan yang diperlukan untuk memperkuat keamanan dan keandalan sistem informasi [52].

Selain sebagai bentuk evaluasi, audit manajemen risiko TI juga berfungsi sebagai alat pengawasan dan peningkatan berkelanjutan terhadap kualitas teknologi informasi di dalam organisasi. Hasil audit dapat digunakan sebagai dasar pengambilan keputusan manajemen dalam merancang kebijakan baru, memperbaiki prosedur kerja, serta meningkatkan kesadaran risiko di kalangan karyawan. Dengan demikian, audit ini tidak hanya membantu menemukan kelemahan yang ada, tetapi juga berperan proaktif dalam membangun budaya organisasi yang lebih tangguh terhadap ancaman teknologi dan perubahan lingkungan digital yang dinamis[52].

Mengingat pentingnya fungsi proaktif audit risiko TI, perlu diperhatikan bahwa kerangka kerja evaluasi harus mampu menangkap aspek manajemen risiko secara komprehensif. Penelitian terdahulu pada tahun 2013 menggunakan kerangka kerja COBIT 4.1 domain *Plan and Organize* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS), dan *Monitor and Evaluate* (ME), *IT Balanced Scorecard* dan *Key Performance*

Indicator (KPI) untuk menilai efektivitas tata kelola teknologi informasi di PT Capella Medan. Fokus utama penelitian ini adalah pada evaluasi kinerja TI secara umum, tanpa menguraikan secara mendalam aspek pengelolaan risiko atau keberlanjutan layanan jaringan. Kesenjangan yang muncul adalah bahwa COBIT 4.1 belum memiliki domain khusus yang membahas manajemen risiko secara komprehensif, sehingga tidak mampu menggambarkan secara detail bagaimana organisasi mengidentifikasi, mengendalikan, dan memitigasi gangguan pada infrastruktur TI[8]. Penelitian selanjutnya dilakukan pada tahun 2025 menggunakan COBIT 2019 dengan domain EDM05 *(Ensure Stakeholder Transparency),* APO06 *(Manage Budget and Costs),* BAI09 *(Manage Assets),* dan MEA03 *(Monitor, Evaluate, and Assess Compliance with External Requirements).* Fokus penelitian ini bertumpu pada penilaian tata kelola dan kepatuhan TI, bukan pada risiko operasional jaringan. Dari kedua hasil penelitian ini, belum terdapat evaluasi terhadap pengelolaan risiko gangguan layanan jaringan, yang justru menjadi faktor penting dalam menjaga ketersediaan dan stabilitas sistem informasi perusahaan[9].

Oleh karena itu, pelaksanaan penelitian yang berfokus pada domain APO12 *(Managed Risk)* menjadi esensial. Domain ini secara spesifik memprioritaskan identifikasi risiko, analisis dampak, perumusan tindakan mitigasi, dan pemantauan efektivitas kontrol teknologi informasi secara berkelanjutan. Dengan demikian, audit manajemen risiko gangguan layanan jaringan yang menggunakan kerangka APO12 *(Managed Risk)* ini penting untuk dilaksanakan agar PT Capella Medan dapat memperoleh kerangka pengendalian risiko yang lebih adaptif, selaras dengan standar COBIT 2019, serta relevan untuk mengatasi tantangan infrastruktur jaringan modern yang memiliki kompleksitas dan kerentanan yang tinggi terhadap gangguan.

2.5 Kerangka Kerja Audit Teknologi Informasi

Kerangka kerja audit teknologi informasi merupakan landasan sistematis yang digunakan untuk mengevaluasi efektivitas tata kelola, pengelolaan, serta pengendalian atas sistem informasi dan teknologi di dalam suatu organisasi. Audit TI berperan sebagai mekanisme evaluatif untuk menilai kesesuaian implementasi TI terhadap kebijakan internal maupun regulasi eksternal, sekaligus mengukur sejauh mana penerapan teknologi tersebut mendukung pencapaian tujuan strategis organisasi[13].

Dalam konteks *Enterprise Information and Technology (I&T),* pengelolaan TI mencakup seluruh aktivitas dan infrastruktur organisasi tanpa terbatas pada satu unit tertentu. Oleh karena itu, proses audit harus mencerminkan pendekatan menyeluruh yang

tidak hanya meninjau aspek teknis, tetapi juga menilai bagaimana sistem informasi berkontribusi terhadap efektivitas bisnis, keamanan data, dan keberlanjutan strategi organisasi[13].

Sejumlah penelitian menunjukkan bahwa kerangka kerja audit TI seperti COBIT 2019 menjadi instrumen yang efektif untuk menilai kapabilitas tata kelola TI secara sistematis. Audit manajemen risiko TI harus mencakup identifikasi risiko, kematangan proses, dan kesenjangan kapabilitas[53,54]. Studi pada unit pengembangan TI di lingkungan perguruan tinggi menggunakan domain COBIT 2019 seperti APO11 *(Managed Quality)*, APO14 *(Managed Data)* dan BAI08 *(Managed Knowledge)* dengan menetapkan alokasi hari audit untuk merancang audit berbasis tingkat risiko masing masing domain[55]. Hasil ini menegaskan bahwa kerangka kerja audit TI tidak hanya melihat aspek teknis saja tetapi juga mencakup tata kelola, pengukuran kapabilitas dan kematangan proses TI.

Sebuah perusahaan *fintech* menggunakan COBIT 2019 menemukan bahwa meskipun sistem sudah berjalan, masih terdapat *gap* dalam dokumentasi dan prosedur yang terstandarisasi, yang menghambat efektivitas TI dalam mendukung bisnis. Temuan ini menegaskan bahwa audit TI harus dijalankan secara *end to end*, mulai dari merancang ruang lingkup audit, mengidentifikasi proses kunci, penilaian kapabilitas, menemukan celah *(gap),* hingga penyusunan rekomendasi perbaikan yang terukur agar teknologi informasi memberikan nilai optimal bagi organisasi[56].

2.6 COBIT 2019

COBIT 2019 menjadi kerangka kerja yang tepat dalam pelaksanaan audit dalam penelitian ini karena menyediakan pendekatan evaluasi risiko yang komprehensif untuk memastikan layanan TI tetap berfungsi secara andal dalam mendukung aktivitas bisnis perusahaan. *Framework* ini membantu auditor menilai sejauh mana risiko seperti *downtime* jaringan, gangguan sistem, hingga ancaman keamanan telah diidentifikasi dan dimitigasi secara tepat. Dukungan dari penelitian sebelumnya juga memperkuat relevansi penggunaannya, yang menunjukkan bahwa audit berbasis COBIT mampu meningkatkan ketahanan layanan jaringan melalui pengukuran risiko yang lebih akurat dan terstruktur.

2.6.1 Perkembangan COBIT

COBIT dikembangkan oleh *Information Systems Audit and Control Association* (ISACA) sebagai seperangkat panduan, prinsip, dan praktik terbaik yang berfungsi untuk membantu organisasi dalam mengelola, mengendalikan, serta meningkatkan kinerja TI agar selaras dengan tujuan bisnis dan peraturan yang berlaku. Melalui kerangka kerja ini,

organisasi dapat membangun sistem tata kelola yang terukur dan terdokumentasi dengan baik, sehingga setiap aktivitas TI dapat dievaluasi dari sisi efektivitas, efisiensi, keamanan, dan kepatuhan terhadap regulasi[3].

COBIT berperan penting sebagai alat bantu bagi auditor, manajer TI, dan pihak manajemen untuk memastikan bahwa penerapan TI di dalam organisasi tidak hanya mendukung kegiatan operasional, tetapi juga menciptakan nilai tambah yang dapat diukur secara objektif. Selain itu, COBIT menyediakan metodologi audit dan pengendalian yang komprehensif, mencakup aspek pengukuran kinerja, manajemen risiko, serta kepatuhan terhadap standar industri dan kebijakan internal organisasi. Dengan demikian, COBIT tidak hanya menjadi alat pengendali, tetapi juga panduan strategis dalam upaya peningkatan pengelolaan TI secara menyeluruh[3].

Seiring transformasi teknologi informasi, ISACA terus memperbarui COBIT agar tetap relevan dengan kebutuhan organisasi. Perkembangannya dimulai dari COBIT 1.0 pada tahun 1996 yang berfokus pada pengawasan dan kontrol lingkungan teknologi informasi. Dua tahun kemudian, COBIT 2.0 memperluas cakupan dari sekadar audit menjadi pengendalian sistem TI yang lebih menyeluruh. Perubahan signifikan hadir pada COBIT 3 yang dirilis pada tahun 2003 dengan diperkenalkannya konsep *IT Governance* yang memperluas fokus dari kontrol menuju manajemen dan tata kelola TI dalam organisasi. Kemudian, COBIT 4.0 dirilis pada tahun 2005 untuk menjawab kebutuhan praktik tata kelola yang lebih matang dan disempurnakan menjadi COBIT 4.1 pada tahun 2007 dengan integrasi standar lain, seperti ITIL, ISO/IEC 27001, *Val IT,* dan *Risk IT* sehingga banyak diadopsi oleh organisasi [57].

2.6.2 Perbedaan COBIT 5 dan COBIT 2019

Berikut beberapa perbedaan antara COBIT 5 dan COBIT 2019 [57]:

1. COBIT 5 dibangun atas lima prinsip tata kelola, sedangkan COBIT 2019 memperbarui dan mengembangkan prinsip-prinsip tersebut menjadi enam prinsip yang terbagi dalam dua klasifikasi, yaitu *governance system principles* (prinsip sistem tata kelola) dan *governance framework principles* (prinsip kerangka kerja tata kelola).
2. Pada COBIT 5 terdapat 37 proses yang terbagi menjadi *governance objectives* dan *management objectives*. Pada COBIT 2019 jumlah proses meningkat menjadi 40 proses melalui penambahan pada tiga domain utama, yaitu *Align, Plan and Organize* (APO14), *Build, Acquire and Implement* (BAI11), serta *Monitor, Evaluate and Assess* (MEA04).

3. Dalam terminologi proses, COBIT 5 menggunakan bentuk kata kerja seperti *"manage"* dan *"ensure"* untuk menunjukkan tindakan aktif dalam pelaksanaan tata kelola dan manajemen teknologi informasi. Namun, pada COBIT 2019 terminologi tersebut diubah menjadi bentuk kata sifat seperti *"managed"* dan *"ensured"*.
4. COBIT 5 menggunakan konsep *"enablers"* sebagai elemen pendukung tata kelola, seperti proses dan struktur organisasi. Pada COBIT 2019, konsep ini digantikan dengan *"components"* yang lebih luas serta dilengkapi *design factors* sebagai variabel yang memengaruhi rancangan sistem tata kelola organisasi.
5. Manajemen kinerja pada COBIT 2019 menggunakan CMMI *(Capability Maturity Model Integration)* dengan skala kapabilitas dan kematangan 0 hingga 5, sedangkan COBIT 5 masih mengacu pada standar ISO/IEC 33000 *Software Process Improvement and Capability Determination.*
6. COBIT 2019 memperkenalkan konsep *"Focus Areas",* yang memberikan panduan penerapan *framework* sesuai kebutuhan organisasi tertentu, seperti keamanan siber, privasi, manajemen risiko, *DevOps*, atau *cloud*. Sementara itu, COBIT 5 tidak memiliki konsep ini. COBIT 2019 secara eksplisit menyediakan panduan untuk integrasi dengan *framework* lain seperti ITIL, ISO *27001, DevOps,* dan *Agile,* sementara COBIT 5 belum mengatur keterkaitan tersebut secara sistematis.

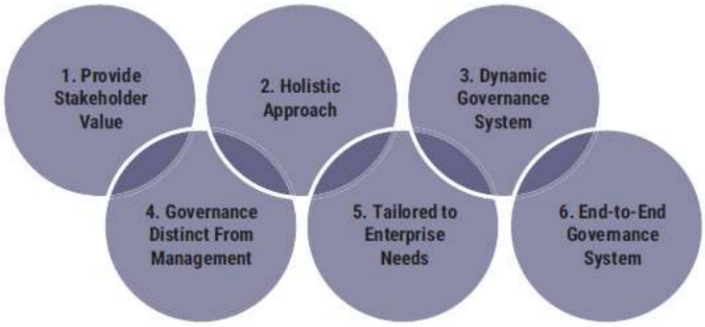
2.6.3 Prinsip-prinsip COBIT 2019

COBIT 2019 merupakan kerangka kerja tata kelola dan manajemen teknologi informasi yang dikembangkan untuk membantu organisasi mencapai tujuan bisnis melalui pemanfaatan informasi dan teknologi secara optimal. *Framework* ini tidak hanya menyediakan panduan untuk mengatur dan mengendalikan sumber daya TI, tetapi juga menekankan pentingnya keselarasan antara strategi bisnis dan strategi teknologi agar organisasi dapat menghasilkan nilai yang berkelanjutan. Untuk mencapai hal tersebut, COBIT 2019 disusun dengan fondasi prinsip-prinsip yang menjadi pedoman utama dalam pembentukan sistem tata kelola yang efektif, efisien, dan adaptif terhadap perubahan lingkungan bisnis dan teknologi[3].

Prinsip COBIT 2019 terdiri dari dua kelompok utama, yaitu[3]

1. ***Governance System Principles***

   Berfokus pada struktur dan karakteristik internal dari sistem tata kelola teknologi informasi dan bagaimana memastikan bahwa sistem tersebut efektif untuk memenuhi tujuan organisasi. *Six principles for a governance system* terdiri dari:



Gambar 2. 1 Prinsip *Governance System*

a. Menyediakan Nilai bagi Pemangku Kepentingan *(Provide Stakeholder Value)*

COBIT 2019 menegaskan bahwa pengelolaan informasi dan teknologi harus difokuskan pada penciptaan nilai nyata bagi para pemangku kepentingan. Nilai ini dihasilkan melalui keseimbangan antara manfaat bisnis, penggunaan sumber daya yang efisien, dan pengelolaan risiko yang terkendali. Dengan kata lain, sistem pengelolaan berfungsi untuk memastikan bahwa seluruh keputusan dan investasi teknologi informasi berkontribusi langsung pada pencapaian tujuan strategis organisasi serta memberikan dampak positif bagi semua pihak yang berkepentingan.

Dengan pendekatan ini, COBIT 2019 memastikan pengelolaan risiko gangguan layanan jaringan TI harus diarahkan pada penciptaan nilai bagi pemangku kepentingan melalui peningkatan keandalan sistem, kontinuitas layanan, serta kepuasan pengguna. Prinsip ini menjadi dasar bagi audit manajemen risiko pada organisasi.

b. Pendekatan Holistik *(Holistic Approach)*

Pengelolaan efektif tidak dapat berdiri dari satu komponen saja, melainkan dibangun dari interaksi berbagai elemen seperti proses, struktur organisasi, kebijakan, budaya, dan informasi. Prinsip ini menekankan pentingnya pendekatan holistik di mana seluruh komponen tersebut saling memengaruhi dan bekerja secara terpadu, sehingga menghasilkan sistem pengelolaan yang utuh dan berkesinambungan.

Beberapa kajian menunjukkan bahwa audit risiko yang menerapkan pendekatan holistik mampu meningkatkan efektivitas pengendalian karena menilai risiko dari berbagai dimensi, termasuk proses kerja, sumber daya manusia, dan budaya organisasi. Dengan demikian, audit tidak hanya bersifat reaktif terhadap insiden, tetapi juga proaktif dalam membangun sistem pengelolaan risiko yang terintegrasi dan berorientasi pada peningkatan berkelanjutan.

c. Sistem Tata Kelola yang Dinamis *(Dynamic Governance System)*

Dalam lingkungan bisnis yang cepat berubah, sistem tata kelola perlu memiliki kemampuan untuk menyesuaikan diri terhadap perubahan strategi, risiko, teknologi, atau kebutuhan regulasi. COBIT 2019 memandang tata kelola sebagai sistem yang terus berkembang. Oleh karena itu, organisasi harus secara berkala meninjau dan memperbarui desain tata kelola agar tetap relevan dan responsif terhadap perubahan lingkungan eksternal maupun internal.

Audit TI berperan sebagai mekanisme evaluatif yang memastikan pengelolaan risiko gangguan layanan tetap adaptif terhadap dinamika ancaman dan kemajuan teknologi, sehingga sistem tata kelola mampu mempertahankan stabilitas layanan sekaligus mendukung peningkatan kinerja organisasi secara berkelanjutan.

d. Pemisahan antara Tata Kelola dan Manajemen *(Governance Distinct from Management)*

Prinsip ini memperjelas batas tanggung jawab antara fungsi tata kelola dan manajemen. Tata kelola berfokus pada penetapan arah strategis, evaluasi opsi, serta pemantauan pencapaian tujuan organisasi, yang biasanya menjadi kewenangan dewan direksi. Sementara itu, manajemen bertanggung jawab untuk menjalankan keputusan tersebut melalui perencanaan, pengelolaan, dan pelaksanaan operasional sehari-hari. Pemisahan ini memastikan adanya keseimbangan antara pengawasan strategis dan pelaksanaan taktis.

Audit berfungsi untuk menilai sejauh mana pemisahan peran antara penetapan arah strategis oleh manajemen puncak dan pelaksanaan operasional oleh unit TI telah diterapkan secara efektif dalam mekanisme pengendalian risiko gangguan layanan, sehingga tata kelola dan manajemen dapat berjalan selaras dalam mendukung stabilitas serta keandalan layanan teknologi informasi.

e. Penyesuaian terhadap Kebutuhan Organisasi *(Tailored to Enterprise Needs)*

Setiap organisasi memiliki konteks, tujuan, dan tingkat risiko yang berbeda. Karena itu, sistem tata kelola tidak dapat diterapkan secara seragam. COBIT 2019 mendorong proses desain yang menyesuaikan tata kelola berdasarkan faktor-faktor seperti ukuran perusahaan, strategi bisnis, model operasional, serta tingkat regulasi yang berlaku. Prinsip ini memungkinkan organisasi mengimplementasikan tata kelola yang relevan dan efisien sesuai dengan realitas bisnisnya.

Pengelolaan risiko difokuskan pada kondisi nyata organisasi, khususnya pada aspek layanan TI yang mendukung operasional bisnis sehingga audit dan mekanisme

pengendalian yang diterapkan dapat disesuaikan secara kontekstual untuk memastikan efektivitas pengelolaan risiko serta keberlanjutan layanan jaringan perusahaan.

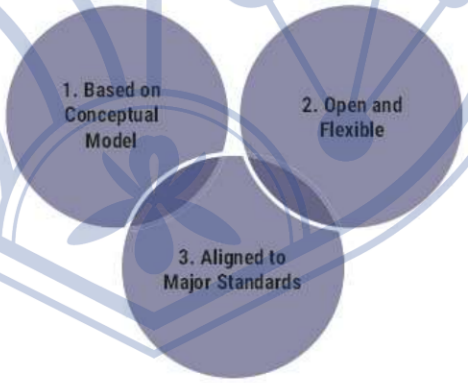
f. Cakupan Menyeluruh terhadap Organisasi *(End-to-End Governance System)*

Tata kelola informasi dan pengelolaan teknologi harus bersifat menyeluruh, tidak hanya terbatas pada departemen TI. COBIT 2019 menekankan bahwa seluruh proses bisnis yang melibatkan pengelolaan informasi, baik yang bersifat strategis maupun operasional, merupakan bagian dari ekosistem tata kelola. Dengan cakupan yang komprehensif ini, organisasi dapat memastikan bahwa setiap unit kerja ikut mendukung tercapainya tujuan bisnis secara keseluruhan.

Audit berperan dalam menilai sejauh mana keterlibatan lintas fungsi di seluruh unit organisasi telah terintegrasi dalam mekanisme pengendalian risiko layanan TI, sehingga upaya mitigasi gangguan tidak hanya menjadi tanggung jawab divisi IT, tetapi menjadi bagian dari komitmen kolektif perusahaan dalam menjaga keandalan dan kontinuitas layanan.

2. *Governance Framework Principles*

COBIT 2019 berfokus pada bagaimana kerangka kerja untuk membangun dan mengimplementasikan sistem tata kelola dapat disusun agar lebih terstruktur, fleksibel, dan sesuai dengan standar yang ada. *Three Principles for a Governance Framework* terdiri dari:



Gambar 2. 2 *Principles for a Governance Framework*

a. Berbasis pada Model Konseptual *(Based on Conceptual Model)*

COBIT 2019 dirancang menggunakan model konseptual yang jelas dan sistematis untuk menggambarkan bagaimana setiap komponen tata kelola saling berhubungan. Pendekatan ini membantu organisasi dalam memahami struktur tata

kelola secara menyeluruh, sekaligus mempermudah proses penerapan, evaluasi, dan peningkatan berkelanjutan. Model konseptual ini juga memastikan bahwa setiap elemen dalam *framework* memiliki posisi dan peran yang logis dalam sistem keseluruhan.

Dengan adanya model konseptual yang terstruktur dalam COBIT 2019, proses audit manajemen risiko gangguan layanan TI dapat dilaksanakan secara lebih sistematis dan berbasis pada hubungan antarkomponen tata kelola yang telah terdefinisi dengan jelas. Pendekatan ini memungkinkan auditor untuk menilai efektivitas peran dan keterkaitan setiap elemen pengendalian risiko dalam mendukung keandalan serta keberlanjutan layanan TI, sekaligus memastikan bahwa praktik tata kelola yang diterapkan selaras dengan prinsip integrasi dan perbaikan berkelanjutan yang ditekankan dalam *framework* tersebut.

b. Terbuka dan Mudah Disesuaikan *(Open and Flexible)*

Salah satu keunggulan COBIT 2019 adalah fleksibilitasnya dalam menghadapi perkembangan teknologi dan kebutuhan organisasi yang terus berubah. Prinsip ini menegaskan bahwa kerangka kerja COBIT dirancang secara terbuka sehingga dapat diperbarui, diperluas, atau dikombinasikan dengan praktik-praktik baru tanpa kehilangan integritas dasar *framework* nya. Dengan demikian, COBIT dapat terus relevan dalam berbagai konteks industri dan generasi teknologi.

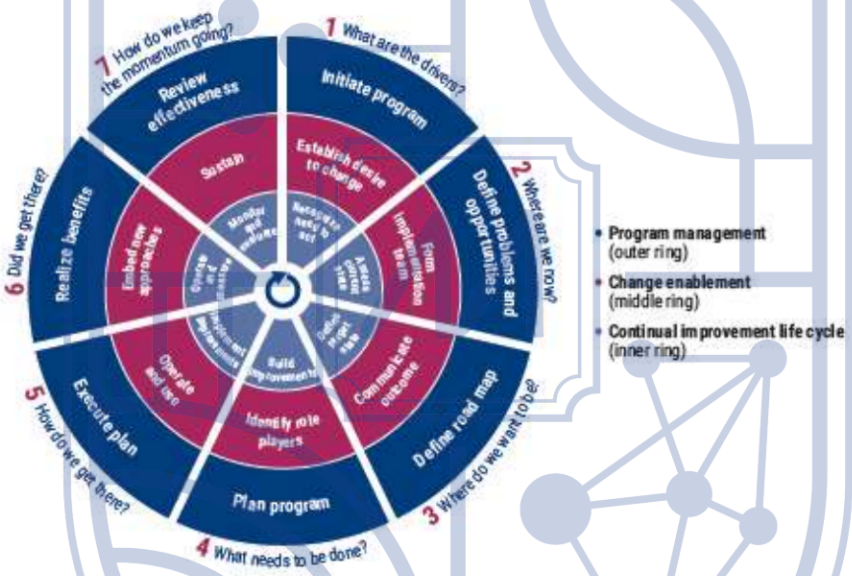
Karakteristik fleksibel yang dimiliki COBIT 2019 menjadikan proses audit manajemen risiko layanan TI mampu beradaptasi terhadap dinamika perubahan lingkungan teknologi dan kebutuhan organisasi. Dengan kerangka yang terbuka dan mudah disesuaikan, auditor dapat terus meninjau serta memperbarui pendekatan pengendalian risiko sesuai dengan evolusi ancaman dan inovasi teknologi, sehingga penerapan tata kelola dan pengawasan terhadap layanan TI tetap efektif, kontekstual, dan berkelanjutan dalam mendukung tujuan strategis organisasi.

c. Selaras dengan Standar dan Regulasi Utama *(Aligned to Major Standards)*

COBIT 2019 dirancang agar dapat diterapkan secara selaras dengan prinsip, kebijakan, dan tujuan tata kelola yang sudah ada di dalam organisasi. Keselarasan ini memastikan bahwa *framework* dapat memperkuat praktik tata kelola yang telah berjalan tanpa menimbulkan tumpang tindih. Dengan demikian, penerapan COBIT membantu menciptakan sinergi antara pengelolaan teknologi dan tujuan strategis organisasi secara terpadu.

Kemampuan COBIT 2019 untuk berintegrasi dengan berbagai standar tata kelola dan keamanan informasi internasional memperkuat relevansinya dalam pelaksanaan audit manajemen risiko layanan TI. Pendekatan yang selaras ini memungkinkan auditor menilai efektivitas pengendalian tidak hanya dari perspektif internal organisasi, tetapi juga berdasarkan kesesuaian terhadap praktik terbaik global dan regulasi yang berlaku, sehingga hasil audit dapat memberikan jaminan yang lebih komprehensif terhadap keandalan, keamanan, dan kepatuhan layanan TI dalam mendukung tujuan strategis perusahaan.

2.6.4 Implementasi COBIT 2019



Gambar 2. 3 COBIT *Implementation*

Implementasi COBIT 2019 merupakan proses yang terstruktur dan berkelanjutan untuk membangun, mengoptimalkan, serta memelihara tata kelola dan manajemen teknologi informasi yang selaras dengan tujuan organisasi. Kerangka ini tidak hanya berfokus pada penerapan awal, tetapi juga memastikan keberlanjutan dan peningkatan nilai yang dihasilkan dari investasi teknologi informasi. ISACA memperkenalkan pendekatan *Continual Improvement Life Cycle*, di mana setiap fasenya memiliki tujuan, aktivitas, dan hasil yang spesifik untuk membantu organisasi dalam menilai kondisi saat ini, menentukan arah strategis, serta mencapai tata kelola teknologi informasi yang efektif dan berkelanjutan [3].

Berikut ini merupakan tujuh tahapan implementasi COBIT 2019, yaitu[3]:

1. ***Phase 1 — What Are the Drivers?***

   Fase ini bertujuan untuk mengidentifikasi faktor pendorong dilakukannya audit manajemen risiko layanan teknologi informasi. Tingginya ketergantungan operasional perusahaan terhadap layanan jaringan dan sistem TI menjadikan setiap potensi gangguan berisiko menurunkan kualitas pelayanan serta menghambat proses bisnis. Oleh karena itu, diperlukan audit yang memastikan pengelolaan risiko telah berjalan secara memadai dalam menjaga keberlangsungan layanan TI.

2. ***Phase 2 — Where Are We Now?***

   Pada fase ini, dilakukan penilaian kondisi aktual pengelolaan risiko layanan teknologi informasi untuk mengetahui kesenjangan antara praktik yang berjalan dengan kondisi ideal yang diharapkan. Evaluasi difokuskan pada sejauh mana pengendalian risiko terhadap gangguan layanan TI telah diterapkan serta efektivitas proses dalam menjaga keandalan jaringan. Hasil penilaian ini menjadi dasar penentuan tingkat kapabilitas saat ini dan mengidentifikasi area yang memerlukan peningkatan dalam upaya menjaga kontinuitas layanan teknologi informasi.

3. ***Phase 3 — Where Do We Want to Be?***

   Fase ketiga difokuskan pada penetapan visi dan sasaran teknologi informasi di masa depan. Organisasi mendefinisikan target *maturity level* atau tingkat kemampuan yang ingin dicapai untuk setiap proses atau domain COBIT 2019. Tahap ini juga mencakup penyelarasan tujuan TI dengan tujuan strategis bisnis *(enterprise goals)* agar arah pengembangan EGIT memiliki dasar yang kuat. *Output* dari fase ini adalah penetapan target kemampuan pengelolaan risiko gangguan layanan TI, sekaligus menyelaraskannya dengan tujuan strategis bisnis untuk menghasilkan rencana dan prioritas inisiatif peningkatan layanan TI.

4. ***Phase 4 — What Needs to Be Done?***

   Fase ini menyusun rencana aksi untuk menutup kesenjangan pengelolaan risiko gangguan layanan TI, termasuk identifikasi aktivitas utama, prioritas, pembagian tanggung jawab, dan estimasi sumber daya, sehingga tercipta panduan implementasi yang terukur dan realistis.

5. ***Phase 5 — How Do We Get There?***

   Fase ini merupakan tahap pelaksanaan nyata dari rencana implementasi yang telah disusun. Organisasi mulai menjalankan program dan proyek peningkatan pengelolaan risiko gangguan layanan teknologi informasi dengan dukungan sumber

daya manusia, teknologi, serta kebijakan yang relevan sehingga program berjalan sesuai rencana dan tercipta pengawasan yang memadai.

6. ***Phase 6 — Did We Get There?***

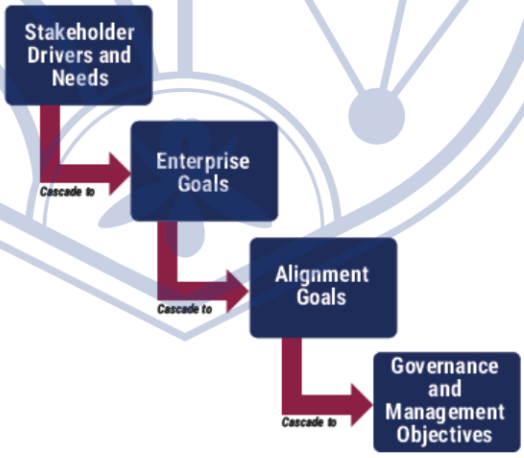
   Fase keenam merupakan tahap evaluasi hasil implementasi. Organisasi menilai sejauh mana inisiatif pengelolaan risiko gangguan layanan TI telah mencapai target, dengan membandingkan hasil aktual terhadap sasaran dan melakukan tindakan korektif jika diperlukan.

7. ***Phase 7 — How Do We Keep the Momentum Going?***

   Fase terakhir bertujuan untuk mempertahankan dan mengoptimalkan manajemen risiko gangguan layanan TI, melalui *monitoring* berkala, perbaikan berkelanjutan, dan penerapan praktik terbaik agar hasil yang dicapai tetap efektif dan berkembang seiring waktu. Hasil dari tahap ini adalah siklus perbaikan berkelanjutan *(continuous improvement)* yang memastikan nilai dari manajemen risiko gangguan layanan TI terus berkembang seiring waktu.

2.6.5 *Goals Cascade*

Goals cascade merupakan mekanisme yang digunakan untuk menerjemahkan kebutuhan dan harapan para pemangku kepentingan menjadi strategi dan tujuan yang dapat ditindaklanjuti oleh organisasi. Proses ini dilakukan secara bertahap melalui empat tingkatan utama, yaitu[3]



Gambar 2. 4 *Goals Cascade* COBIT 2019

1. *Stakeholder Drivers and Needs to Enterprise Goals*

Tahapan ini merupakan langkah awal dalam proses *goal cascade*, di mana kebutuhan para pemangku kepentingan disesuaikan dan diterjemahkan menjadi strategi perusahaan yang dapat diimplementasikan.

Dalam audit manajemen risiko gangguan layanan TI, kebutuhan ini terkait dengan keandalan layanan, keamanan informasi, dan keberlangsungan operasional. COBIT 2019 menyediakan 13 *Enterprise Goals* berbasis *Balanced Scorecard* (BSC) sebagai acuan agar pengelolaan risiko layanan TI benar-benar memberikan nilai bagi *stakeholder*.

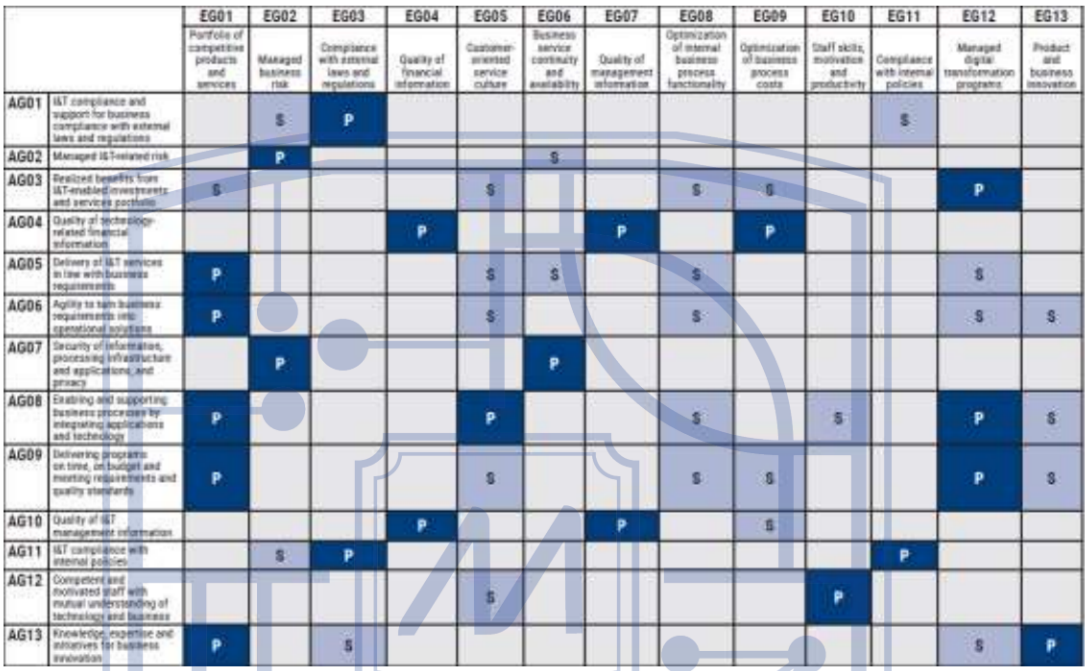
Tabel 2. 1 *Enterprise Goals* COBIT 2019

Acuan	Dimensi BSC	Tujuan Perusahaan
EG01	*Financial*	Portofolio produk dan layanan yang kompetitif.
EG02	*Financial*	Risiko bisnis dikelola dengan baik.
EG03	*Financial*	Kepatuhan terhadap hukum dan regulasi eksternal.
EG04	*Financial*	Kualitas informasi keuangan yang andal.
EG05	*Customer*	Budaya layanan yang berfokus pada pelanggan.
EG06	*Customer*	Keberlangsungan dan ketersediaan layanan bisnis.
EG07	*Customer*	Kualitas informasi manajemen yang akurat.
EG08	*Internal*	Optimalisasi fungsi proses bisnis internal.
EG09	*Internal*	Efisiensi biaya proses bisnis.
EG10	*Internal*	Peningkatan keterampilan, motivasi, dan produktivitas staf.
EG11	*Internal*	Kepatuhan terhadap kebijakan internal.
EG12	*Growth*	Pengelolaan program transformasi digital secara efektif.
EG13	*Growth*	Inovasi produk dan bisnis yang berkelanjutan.

2. *Enterprise Goals to Alignment Goals*

Pada tahap ini, *enterprise goals* diteruskan menjadi *alignment goals* agar pengelolaan TI selaras dengan kebutuhan bisnis. Langkah ini memastikan bahwa upaya pengendalian risiko dan peningkatan keandalan layanan benar-benar mendukung tujuan organisasi dan kepentingan stakeholder. Hubungan tersebut diklasifikasikan menjadi dua jenis, yaitu:

- **P *(Primary),*** yaitu hubungan yang memiliki tingkat kepentingan utama karena berperan sebagai pendorong utama dalam pencapaian tujuan yang berkaitan dengan teknologi informasi. Hubungan ini mencerminkan aktivitas yang bersifat prioritas.
- **S *(Secondary),*** yaitu hubungan yang memiliki tingkat kepentingan lebih rendah dan berfungsi sebagai aktivitas pendukung terhadap pencapaian tujuan utama.

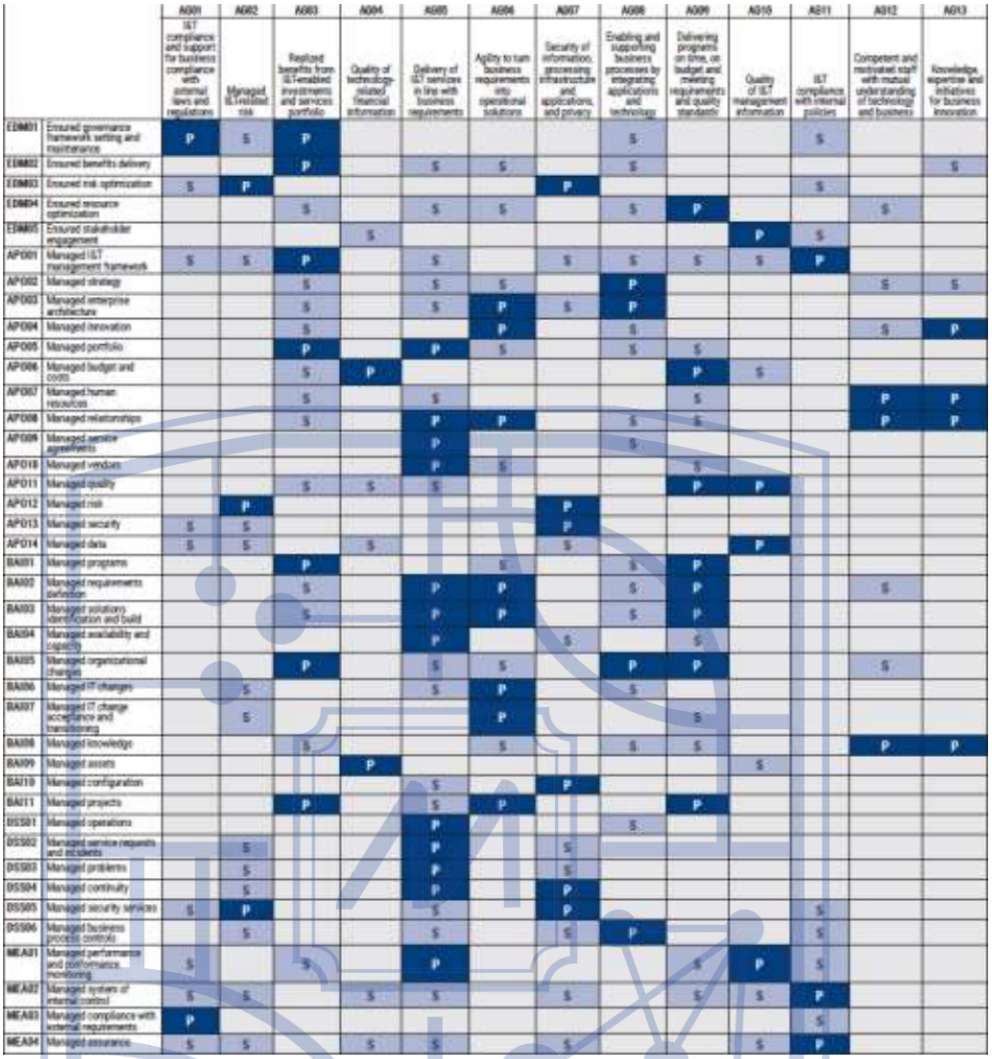


		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

Gambar 2. 5 *Cascade of Enterprise Goals to Alignment Goals*

3. *Alignment Goals* to *Governance and Management Objectives*

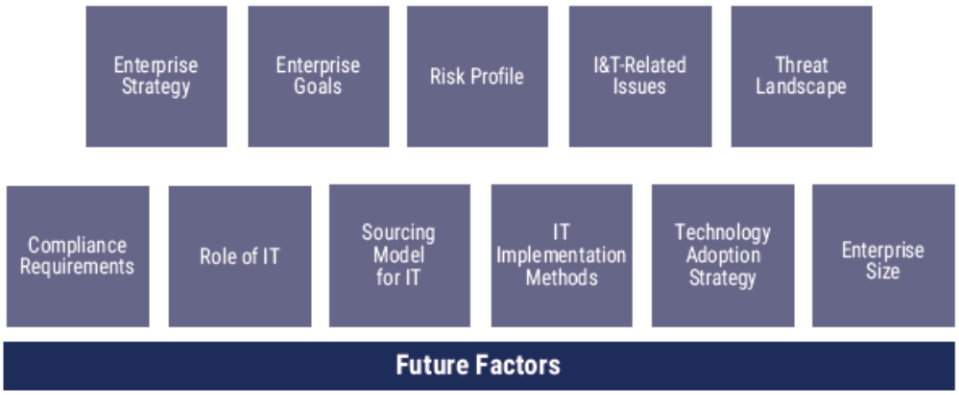
Tahapan ini merupakan penyempurnaan dari versi COBIT sebelumnya. Tujuan dari pembaruan ini adalah untuk menghindari kesalahpahaman yang sering muncul, di mana hasil pemetaan perusahaan sebelumnya dianggap hanya menggambarkan tanggung jawab dari departemen teknologi informasi semata. Pada tahap ini, dilakukan pemetaan *alignment goals* ke dalam domain proses COBIT 2019 untuk menentukan area TI yang perlu diawasi. Dengan demikian, auditor dapat mengidentifikasi proses yang paling berpengaruh terhadap pengendalian risiko gangguan layanan TI, baik sebagai *Primary* (P) maupun *Secondary* (S).



Gambar 2. 6 *Cascade of Alignment Goals to Governance and Management Objectives*

2.6.6 *Design Factors (DF)*

Design factors dapat dipahami sebagai komponen yang memengaruhi perancangan dan penentuan prioritas dalam penerapan tata kelola dan manajemen TI, sehingga penerapan *framework* COBIT tidak bersifat universal, tetapi disesuaikan dengan karakteristik, kebutuhan, serta sasaran spesifik masing-masing organisasi.



Gambar 2. 7 *Design Factors* COBIT 2019

Dalam COBIT 2019, terdapat 11 *design factors* yang menjadi dasar penyesuaian sistem tata kelola untuk membantu organisasi merancang pengelolaan informasi dan teknologi yang relevan, efektif, serta sesuai dengan konteks dan kebutuhan masing-masing organisasi[58].

Berikut merupakan *design factors* COBIT 2019[58]:

1. *Enterprise Strategy*

Menggambarkan arah strategis utama organisasi yang menentukan bagaimana sistem tata kelola TI mendukung pencapaian tujuan bisnis, baik melalui pertumbuhan, inovasi, maupun efisiensi biaya.

Dalam konteks layanan jaringan, audit manajemen risiko memastikan infrastruktur tetap stabil dan aman, sehingga potensi gangguan seperti *downtime* atau ancaman keamanan tidak menghambat pencapaian tujuan strategis organisasi.

Tabel 2. 2 *Design Factor 1*

Tipe Strategi	**Penjelasan**
Growth/Acquisition	Berfokus pada peningkatan pendapatan dan ekspansi bisnis.
Innovation/Differentiation	Berfokus pada produk atau layanan yang unik dan inovatif.
Cost Leadership	Berfokus pada efisiensi dan pengurangan biaya.
Client Service/Stability	Berfokus pada pelayanan yang stabil dan berorientasi pelanggan.

2. *Enterprise Goals*

Menunjukkan sasaran utama organisasi yang ingin dicapai dan menjadi dasar dalam menetapkan prioritas pengelolaan serta evaluasi kinerja tata kelola TI.

Audit manajemen risiko dilakukan untuk memastikan layanan TI tetap andal sehingga tujuan bisnis dapat tercapai tanpa gangguan operasional.

Tabel 2. 3 *Design Factor 2*

Acuan	**Dimensi BSC**	**Tujuan Perusahaan**
EG01	*Financial*	Portofolio produk dan layanan yang kompetitif
EG02	*Financial*	Risiko bisnis dikelola dengan baik
EG03	*Financial*	Kepatuhan terhadap hukum dan regulasi eksternal
EG04	*Financial*	Kualitas informasi keuangan yang andal
EG05	*Customer*	Budaya layanan yang berfokus pada pelanggan
EG06	*Customer*	Keberlangsungan dan ketersediaan layanan bisnis
EG07	*Customer*	Kualitas informasi manajemen yang akurat
EG08	*Internal*	Optimalisasi fungsi proses bisnis internal
EG09	*Internal*	Efisiensi biaya proses bisnis
EG10	*Internal*	Peningkatan keterampilan, motivasi, dan produktivitas staf
EG11	*Internal*	Kepatuhan terhadap kebijakan internal
EG12	*Growth*	Pengelolaan program transformasi digital secara efektif
EG13	*Growth*	Inovasi produk dan bisnis yang berkelanjutan

3. *Risk Profile*

Mencerminkan tingkat dan jenis risiko yang dihadapi organisasi sehingga sistem tata kelola dapat menyesuaikan pengendalian untuk menjaga stabilitas dan keberlanjutan bisnis.

Dalam konteks gangguan layanan jaringan, pemahaman profil risiko diperlukan untuk menetapkan fokus audit manajemen risiko dalam menjaga keberlanjutan layanan dan mencegah *downtime.*

Tabel 2. 4 *Design Factor 3*

Acuan	Kategori Risiko
1	Keputusan investasi TI dan pengelolaan portofolio
2	Manajemen siklus hidup program dan proyek
3	Biaya dan pengawasan TI
4	Keahlian, keterampilan, dan perilaku TI
5	Arsitektur perusahaan/TI
6	Insiden infrastruktur operasional TI
7	Tindakan tidak sah
8	Masalah adopsi atau penggunaan perangkat lunak
9	Insiden perangkat keras
10	Kegagalan perangkat lunak
11	Serangan logis (peretasan, malware, dsb.)
12	Insiden pihak ketiga/pemasok
13	Ketidakpatuhan terhadap peraturan
14	Isu geopolitik
15	Aksi industri
16	Bencana alam
17	Inovasi berbasis teknologi
18	Lingkungan
19	Manajemen data dan informasi

4. *I&T Related Issues*

Mengidentifikasi permasalahan dan tantangan utama terkait penggunaan teknologi informasi yang dapat memengaruhi efektivitas penerapan tata kelola.

Identifikasi ini penting untuk mengetahui area yang berpotensi menimbulkan gangguan layanan, sehingga dapat dilakukan pengelolaan risiko yang tepat guna menjaga keandalan layanan TI.

Tabel 2. 5 *Design Factor 4*

Acuan	Deskripsi
A	Terjadi ketidakharmonisan antar unit TI di dalam organisasi akibat persepsi bahwa TI memberikan kontribusi yang rendah terhadap nilai bisnis. Ketidakharmonisan antar unit TI karena dianggap kurang memberi nilai bagi bisnis.

B	Terdapat ketegangan antara unit bisnis dan departemen TI yang disebabkan oleh kegagalan inisiatif atau rendahnya kontribusi TI terhadap pencapaian nilai bisnis.
C	Terjadi insiden signifikan terkait TI, seperti kehilangan data, pelanggaran keamanan, kegagalan proyek, maupun kesalahan aplikasi.
D	Muncul permasalahan dalam penyediaan layanan oleh pihak penyedia jasa TI eksternal *(outsourcer).*
E	Kegagalan organisasi dalam memenuhi ketentuan regulasi atau persyaratan kontraktual yang berkaitan dengan TI.
F	Terdapat temuan audit atau laporan berkala yang menunjukkan kinerja TI yang rendah serta permasalahan pada kualitas layanan.
G	Adanya pengeluaran TI yang tidak resmi atau tidak tercatat dalam anggaran yang telah disetujui.
H	Ditemukan adanya duplikasi inisiatif atau tumpang tindih proyek yang menyebabkan pemborosan sumber daya TI.
I	Keterbatasan sumber daya TI, baik dari segi jumlah maupun kompetensi personel yang belum memadai.
J	Proyek atau perubahan berbasis TI sering kali tidak memenuhi kebutuhan bisnis, mengalami keterlambatan, atau melebihi anggaran yang ditetapkan.
K	Kurangnya dukungan dan keterlibatan dari jajaran eksekutif atau manajemen puncak terhadap kegiatan dan strategi TI.
L	Struktur operasional TI yang kompleks serta mekanisme pengambilan keputusan yang tidak terdefinisi dengan jelas.
M	Biaya operasional TI yang relatif tinggi dan tidak sebanding dengan nilai manfaat yang dihasilkan.
N	Kegagalan inovasi yang disebabkan oleh arsitektur dan sistem TI yang sudah usang atau tidak relevan dengan kebutuhan saat ini.
O	Adanya kesenjangan pengetahuan dan pemahaman antara pihak bisnis dan teknis dalam penerapan solusi TI.
P	Permasalahan terkait kualitas data dan kurangnya integrasi antar sistem informasi.

Q	Tingginya tingkat penggunaan sistem komputasi oleh pengguna akhir yang menyebabkan kurangnya pengawasan dan kontrol kualitas aplikasi.
R	Unit bisnis mengembangkan solusi TI secara mandiri tanpa koordinasi atau keterlibatan dari departemen TI utama.
S	Ketidaktahuan atau ketidakpatuhan terhadap peraturan dan kebijakan yang berkaitan dengan perlindungan data dan privasi.
T	Ketidakmampuan organisasi dalam memanfaatkan teknologi baru maupun berinovasi melalui penerapan teknologi informasi.

5. *Threat Landscape*

Menggambarkan kondisi ancaman eksternal yang berpotensi mengganggu keamanan dan operasional organisasi, seperti risiko siber atau gangguan sistem.

Semakin tinggi tingkat ancaman, semakin penting audit manajemen risiko dilakukan untuk menjaga layanan tetap stabil dan aman.

Tabel 2. 6 *Design Factor 5*

Kategori	**Penjelasan**
Normal	Organisasi beroperasi dalam kondisi ancaman yang tergolong normal, di mana tingkat risiko keamanan dan gangguan eksternal masih dalam batas kewajaran umum.
High	Organisasi beroperasi dalam lingkungan dengan tingkat ancaman yang tinggi, disebabkan oleh faktor seperti kondisi geopolitik, karakteristik industri, atau profil perusahaan yang berisiko tinggi terhadap serangan dan gangguan eksternal.

6. *Compliance Requirements*

Menilai tingkat kompleksitas kewajiban hukum dan regulasi yang harus dipatuhi dalam pengelolaan teknologi informasi.

Semakin tinggi tuntutan kepatuhan, semakin diperlukan audit manajemen risiko untuk memastikan layanan TI tetap sesuai standar dan terhindar dari potensi pelanggaran.

Tabel 2. 7 *Design Factor 6*

Kategori	**Penjelasan**
Low Compliance Requirements	Organisasi berada dalam lingkungan dengan kewajiban kepatuhan yang minimal dan tidak kompleks.

Normal Compliance Requirements	Organisasi tunduk pada ketentuan regulasi yang umum berlaku di berbagai sektor industry.
High Compliance Requirements	Organisasi beroperasi di bawah regulasi yang ketat dan memiliki persyaratan kepatuhan yang tinggi.

7. *Role of IT*

Menunjukkan seberapa besar kontribusi dan posisi teknologi informasi dalam mendukung atau menggerakkan kegiatan bisnis organisasi.

Semakin besar perannya, semakin penting audit manajemen risiko dilakukan agar potensi gangguan layanan TI tidak menghambat operasional.

Tabel 2. 8 *Design Factor 7*

Peran TI	**Penjelasan**
Support	TI berperan mendukung proses bisnis, namun tidak bersifat kritis terhadap operasional atau inovasi.
Factory	TI menjadi elemen penting bagi kelangsungan operasional, tetapi belum menjadi pendorong inovasi bisnis.
Turnaround	TI berperan sebagai penggerak inovasi bisnis, namun belum sepenuhnya menjadi faktor utama keberlangsungan operasional.
Strategic	TI memiliki peran strategis yang krusial bagi kelangsungan dan pengembangan bisnis organisasi.

8. *Sourcing Model for IT*

Menentukan bagaimana organisasi memperoleh layanan dan sumber daya teknologi informasi, baik secara *internal, eksternal*, atau kombinasi keduanya.

Pemilihan model yang tepat perlu diaudit agar risiko gangguan dari pihak penyedia layanan dapat terkendali dan tidak menghambat operasional organisasi.

Tabel 2. 9 *Design Factor 8*

Model	**Penjelasan**
Outsourcing	Layanan TI disediakan oleh pihak ketiga melalui kontrak kerja sama.
Cloud	Organisasi memanfaatkan layanan berbasis komputasi awan untuk memenuhi kebutuhan TI.

Insourced	Seluruh layanan TI dikelola dan dijalankan oleh sumber daya internal organisasi.
Hybrid	Organisasi menggunakan kombinasi antara sumber daya internal, *outsourcing*, dan layanan *cloud.*

9. *IT Implementation Methods*

Menggambarkan pendekatan yang digunakan organisasi dalam mengembangkan dan menerapkan solusi teknologi, seperti metode tradisional atau *agile*.

Audit diperlukan untuk memastikan bahwa metode penerapan TI yang dipilih mampu meminimalkan risiko kegagalan dan gangguan layanan dalam operasional organisasi.

Tabel 2. 10 *Design Factor 9*

Model	**Penjelasan**
Agile	Pendekatan iteratif yang menekankan fleksibilitas, kolaborasi, dan kemampuan beradaptasi terhadap perubahan kebutuhan.
DevOps	Metode yang mengintegrasikan pengembangan dan operasional untuk mempercepat rilis serta meningkatkan stabilitas sistem.
Traditional	Pendekatan pengembangan sistem yang dilakukan secara berurutan dari tahap perencanaan hingga implementasi.
Hybrid	Kombinasi antara metode tradisional dan modern yang disesuaikan dengan karakteristik proyek TI.

10. *Technology Adoption Strategy*

Menunjukkan seberapa cepat organisasi mengadopsi teknologi baru sesuai dengan kesiapan dan orientasi bisnisnya.

Tabel 2. 11 *Design Factor 10*

Kategori	**Penjelasan**
First Mover	Organisasi menjadi pihak pertama yang mengadopsi dan menerapkan teknologi baru untuk memperoleh keunggulan kompetitif.
Follower	Organisasi mengadopsi teknologi setelah terbukti efektif digunakan oleh pihak lain di industri.
Slow Adopter	Organisasi berhati-hati dan cenderung lambat dalam menerapkan teknologi baru untuk meminimalkan risiko.

11. *Enterprise Size*

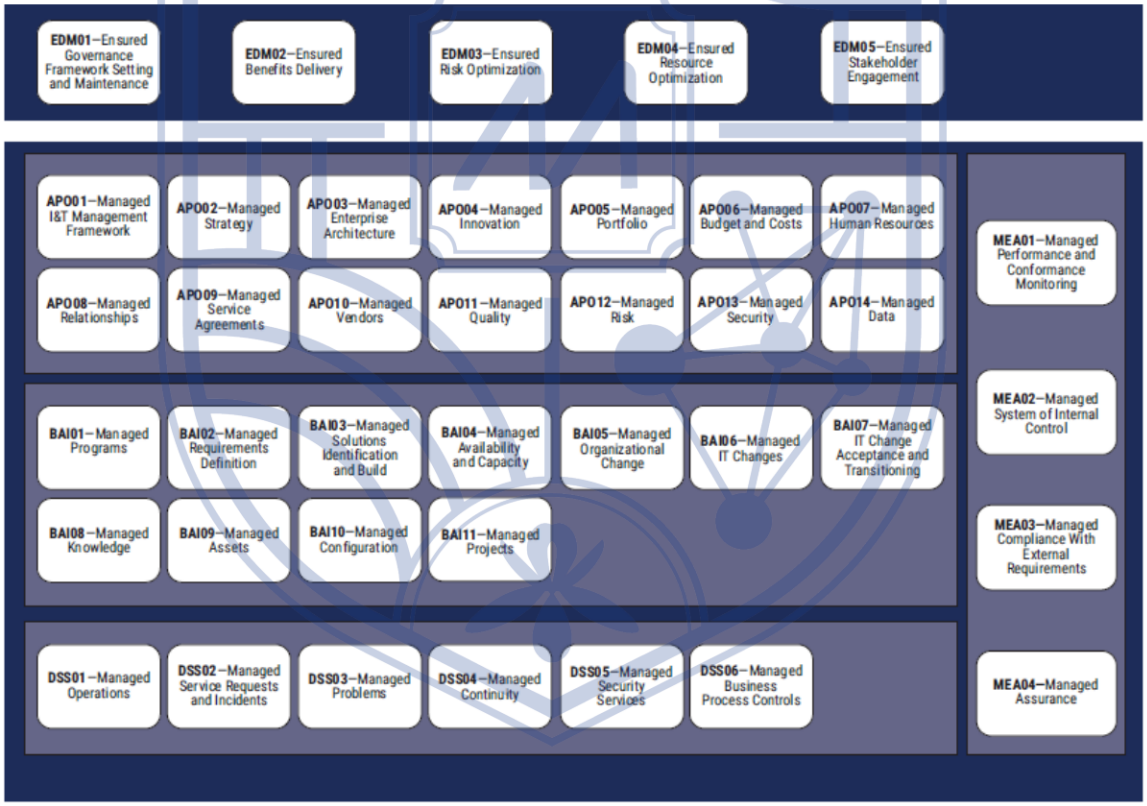
Mewakili ukuran organisasi yang memengaruhi skala kompleksitas, struktur, dan kebutuhan sistem tata kelola teknologi informasi.

Tabel 2. 12 *Design Factor 11*

Ukuran	**Penjelasan**
Small to Medium	Perusahaan dengan lebih dari 250 karyawan tetap.
Large	Perusahaan dengan lebih dari 250 karyawan tetap.

2.6.7 Domain COBIT 2019

COBIT 2019 membagi keseluruhan tata kelola dan manajemen teknologi informasi ke dalam lima domain utama, yang masing-masing merepresentasikan area aktivitas dan tanggung jawab berbeda dalam pengelolaan informasi dan teknologi di organisasi[3].



Gambar 2. 8 Domain COBIT 2019

1. *Governance System Principles*

a. Domain EDM *(Evaluate, Direct, and Monitor)* yang berfokus pada tata kelola strategis, pengawasan, serta evaluasi kinerja TI agar sejalan dengan kebutuhan dan tujuan bisnis.

Tabel 2. 13 Domain EDM *(Evaluate, Direct, and Monitor)*

***Sub*-Domain**	**Nama**	**Penjelasan**
EDM01	*Ensured Governance Framework Setting and Maintenance*	Menetapkan dan memelihara kerangka kerja tata kelola TI yang efektif.
EDM02	*Ensured Benefits Delivery*	Memastikan manfaat dari investasi TI tercapai sesuai tujuan bisnis.
EDM03	*Ensured Risk Optimization*	Memastikan risiko TI dikelola secara optimal.
EDM04	*Ensured Resource Optimization*	Memastikan sumber daya TI digunakan secara efisien.
EDM05	*Ensured Stakeholder Engagement*	Memastikan kebutuhan dan harapan pemangku kepentingan terpenuhi.

2. *Governance Framework Principles*

a. Domain APO *(Align, Plan, and Organize),* menangani perencanaan strategis, tata kelola sumber daya, serta pengorganisasian fungsi TI agar mendukung strategi dan sasaran perusahaan.

Tabel 2. 13 Domain APO *(Align, Plan, and Organize)*

***Sub*-Domain**	**Nama**	**Penjelasan**
APO01	*Managed I&T Management Framework*	Mengelola kerangka kerja manajemen TI yang konsisten.
APO02	*Managed Strategy*	Menyusun dan mengelola strategi TI yang mendukung tujuan bisnis.
APO03	*Managed Enterprise Architecture*	Mengelola arsitektur perusahaan agar TI dan bisnis selaras.
APO04	*Managed Innovation*	Mengelola inovasi agar memberikan nilai tambah bagi organisasi.

APO05	*Managed Portfolio*	Mengelola portofolio investasi dan inisiatif TI.
APO06	*Managed Budget and Costs*	Mengelola anggaran dan biaya TI secara efisien.
APO07	*Managed Human Resources*	Mengelola sumber daya manusia di bidang TI.
APO08	*Managed Relationships*	Mengelola hubungan antara unit TI dan pihak terkait.
APO09	*Managed Service Agreements*	Mengelola perjanjian layanan TI.
APO10	*Managed Vendors*	Mengelola hubungan dan kinerja vendor TI.
APO11	*Managed Quality*	Menjamin kualitas proses dan layanan TI.
APO12	*Managed Risk*	Mengidentifikasi dan mengelola risiko TI.
APO13	*Managed Security*	Mengelola keamanan informasi dan aset TI.
APO14	*Managed Data*	Mengelola siklus hidup dan kualitas data organisasi.

b. Domain BAI *(Build, Acquire, and Implement),* merupakan perancangan, akuisisi, pengembangan, serta penerapan solusi TI dan perubahan yang terjadi dalam sistem.

Tabel 2. 14 Domain BAI *(Build, Acquire, and Implement)*

Sub-Domain	**Nama**	**Penjelasan**
BAI01	*Managed Programs*	Mengelola program dan proyek untuk menghasilkan hasil bisnis yang diinginkan.
BAI02	*Managed Requirements Definition*	Menetapkan kebutuhan bisnis dan persyaratan solusi TI.

BAI03	*Managed Solutions Identification and Build*	Mengembangkan dan mengonfigurasi solusi TI yang sesuai.
BAI04	*Managed Availability and Capacity*	Menjamin ketersediaan dan kapasitas layanan TI.
BAI05	*Managed Organizational Change*	Mengelola perubahan organisasi akibat penerapan TI.
BAI06	*Managed IT Changes*	Mengatur perubahan sistem TI dengan risiko minimal.
BAI07	*Managed IT Change Acceptance and Transitioning*	Memastikan solusi baru diterima dan diintegrasikan dengan lancer.
BAI08	*Managed Knowledge*	Mengelola pengetahuan dan pembelajaran organisasi TI.
BAI09	*Managed Assets*	Mengelola aset TI sepanjang siklus hidupnya.
BAI10	*Managed Configuration*	Mengelola konfigurasi dan versi sistem TI.
BAI11	*Managed Projects*	Mengelola proyek agar mencapai sasaran tepat waktu dan anggaran.

c. Domain *DSS (Deliver, Service, and Support),* berfokus pada penyampaian layanan TI, operasi harian, dukungan pengguna, serta pengelolaan insiden dan masalah.

Tabel 2. 15 Domain DSS *(Deliver, Service, and Support)*

Sub-Domain	Nama	Penjelasan
DSS01	*Managed Operations*	Menjalankan operasi TI sehari-hari secara andal dan efisien.
DSS02	*Managed Service Requests and Incidents*	Menangani permintaan layanan dan insiden pengguna.

DSS03	*Managed Problems*	Mengidentifikasi dan menyelesaikan akar penyebab masalah TI.
DSS04	*Managed Continuity*	Memastikan kelangsungan layanan TI dalam kondisi darurat.
DSS05	*Managed Security Services*	Menyediakan layanan keamanan operasional.
DSS06	*Managed Business Process Controls*	Mengelola kontrol proses bisnis berbasis TI.

d. Domain MEA *(Monitor, Evaluate, and Assess),* mengatur proses pemantauan dan evaluasi kinerja, kepatuhan, serta efektivitas kontrol *internal* TI.

Tabel 2. 16 Domain MEA *(Monitor, Evaluate, and Assess)*

***Sub*-Domain**	**Nama**	**Penjelasan**
MEA01	*Managed Performance and Conformance Monitoring*	Memantau kinerja dan kepatuhan sistem TI.
MEA02	*Managed System of Internal Control*	Mengevaluasi efektivitas sistem pengendalian internal TI.
MEA03	*Managed Compliance With External Requirements*	Memastikan kepatuhan terhadap peraturan eksternal.
MEA04	*Managed Assurance*	Menyediakan penilaian independen terhadap tata kelola dan manajemen TI.

2.6.8 Domain APO12 *(Managed Risk)*

Domain APO12 *(Managed Risk)* membahas proses pengelolaan risiko yang terkait dengan penggunaan teknologi informasi dalam organisasi. Tujuan utama dari domain ini adalah untuk mengidentifikasi, menilai, dan mengendalikan risiko teknologi informasi sehingga potensi dampak negatif terhadap pencapaian tujuan bisnis dapat diminimalkan. Proses ini menekankan pentingnya pemahaman menyeluruh terhadap sumber risiko, baik

yang berasal dari faktor internal maupun eksternal, serta perlunya mekanisme pemantauan yang berkelanjutan agar profil risiko organisasi selalu mutakhir[13].

APO12 juga mendorong penerapan kebijakan dan kerangka kerja manajemen risiko yang terintegrasi dengan tata kelola perusahaan secara keseluruhan, sehingga keputusan yang diambil selalu mempertimbangkan tingkat risiko yang dapat diterima *(risk tolerance).* Dengan demikian, penerapan domain ini membantu organisasi dalam menjaga keseimbangan antara pencapaian nilai bisnis dan pengelolaan risiko teknologi informasi secara efektif serta berkesinambungan[13].

Subdomain yang terdapat dalam domain APO12 dapat diuraikan sebagai berikut[13]:

1. **APO12.01 - *Collect Data***

   Pada sub-domain ini, dilakukan identifikasi dan pengumpulan data yang relevan untuk memungkinkan proses identifikasi, analisis, dan pelaporan risiko yang berkaitan dengan teknologi informasi dan teknologi secara efektif.

   Aktivitas :

   a. Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data yang berkaitan dengan risiko I&T.
   b. Mencatat data yang relevan dan signifikan mengenai risiko I&T yang terkait dengan lingkungan operasional internal dan eksternal perusahaan.
   c. Mengadopsi atau menetapkan taksonomi risiko untuk memastikan konsistensi dalam definisi skenario risiko, serta kategori dampak dan kemungkinan terjadinya.
   d. Mencatat data tentang kejadian risiko yang telah atau mungkin menimbulkan dampak terhadap bisnis, sesuai dengan kategori dampak yang telah ditetapkan dalam taksonomi risiko.
   e. Melakukan survei dan analisis terhadap data risiko I&T historis serta pengalaman kerugian yang tersedia secara eksternal, termasuk tren industri, rekan sejawat, dan basis data peristiwa industri atau perjanjian pengungkapan peristiwa umum.
   f. Untuk kelompok peristiwa yang serupa, mengorganisasi data yang telah dikumpulkan serta menyoroti faktor-faktor penyebabnya. Identifikasi faktor-faktor umum yang berkontribusi terhadap beberapa peristiwa yang berbeda.
   g. Menentukan kondisi spesifik yang ada atau tidak ada ketika peristiwa risiko terjadi**,** serta bagaimana kondisi tersebut memengaruhi frekuensi kejadian dan besarnya kerugian.

h. Melakukan analisis berkala terhadap peristiwa dan faktor risiko untuk mengidentifikasi isu risiko baru atau yang sedang muncul, serta memahami faktor risiko internal dan eksternal yang terkait.

2. APO12.02 – *Analyze Risk*

Mengembangkan pandangan yang terukur dan berbasis bukti mengenai risiko yang berkaitan dengan teknologi informasi dan teknologi guna mendukung proses pengambilan keputusan terkait risiko.

Aktivitas :

a. Menetapkan cakupan yang tepat dari upaya analisis risiko, dengan mempertimbangkan seluruh faktor risiko dan/atau tingkat pentingnya aset bagi bisnis.
b. Menyusun dan memperbarui secara berkala skenario risiko I&T, paparan kerugian yang berkaitan dengan I&T, serta skenario risiko reputasi, termasuk skenario gabungan yang melibatkan ancaman beruntun *(cascading)* atau kejadian yang terjadi bersamaan. Selain itu, mengembangkan ekspektasi yang jelas terhadap aktivitas serta kapabilitas pengendalian yang diperlukan untuk mendeteksi potensi ancaman tersebut.
c. Memperkirakan frekuensi (atau kemungkinan) dan besarnya potensi kerugian atau keuntungan yang terkait dengan setiap skenario risiko TI. Mempertimbangkan seluruh faktor risiko yang relevan serta evaluasi kontrol operasional yang telah ada.
d. Membandingkan tingkat risiko saat ini (paparan risiko TI) dengan tingkat *risk appetite* dan *risk tolerance* yang dapat diterima oleh organisasi, serta mengidentifikasi risiko yang tidak dapat diterima atau yang memiliki tingkat paparan tinggi.
e. Mengusulkan tindakan respons risiko bagi risiko yang melebihi batas *risk appetite* dan *risk tolerance.*
f. Menentukan persyaratan umum untuk proyek atau program yang akan melaksanakan respons risiko yang dipilih. Identifikasi pula kebutuhan dan ekspektasi terhadap kontrol utama *(key controls)* yang diperlukan untuk mendukung mitigasi risiko tersebut.
g. Memvalidasi hasil analisis risiko dan analisis dampak bisnis *(Business Impact Analysis/BIA)* sebelum digunakan dalam proses pengambilan keputusan.

Pastikan bahwa hasil analisis selaras dengan kebutuhan organisasi serta bahwa estimasi dilakukan secara tepat dan bebas dari bias.

h. Melakukan analisis biaya dan manfaat *(cost/benefit analysis)* terhadap berbagai opsi respons risiko, seperti menghindari *(avoid),* mengurangi atau memitigasi *(reduce/mitigate),* mentransfer atau berbagi *(transfer/share),* menerima *(accept),* dan memanfaatkan peluang *(exploit/seize).* Konfirmasi opsi yang paling optimal sebagai respons risiko.

3. APO12.03 – *Maintain a Risk Profile*

Memelihara daftar inventaris risiko yang diketahui beserta atribut risikonya, termasuk frekuensi yang diharapkan, potensi dampak, serta respons yang direncanakan. Selain itu, mendokumentasikan sumber daya, kapabilitas, dan aktivitas pengendalian yang berkaitan dengan setiap item risiko.

Aktivitas :

a. Melakukan inventarisasi proses bisnis dan mendokumentasikan ketergantungan proses tersebut terhadap proses manajemen layanan teknologi informasi serta sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan penyedia jasa alih daya *(outsourcer).*

b. Menentukan dan menyepakati layanan dan sumber daya infrastruktur TI yang penting untuk mendukung keberlangsungan proses bisnis. Analisis hubungan ketergantungan tersebut dan identifikasi titik lemah yang berpotensi menimbulkan risiko.

c. Menggabungkan skenario risiko yang ada berdasarkan kategori, lini bisnis, dan area fungsional.

d. Secara berkala mengumpulkan seluruh informasi profil risiko dan mengonsolidasikannya ke dalam profil risiko agregat.

e. Mencatat informasi mengenai status rencana tindakan risiko *(risk action plan)* untuk dimasukkan ke dalam profil risiko teknologi informasi organisasi.

f. Berdasarkan seluruh data profil risiko, menetapkan serangkaian indikator risiko *(risk indicators)* yang memungkinkan identifikasi cepat serta pemantauan terhadap risiko dan tren risiko yang sedang berlangsung.

g. Mencatat informasi mengenai kejadian risiko yang telah terwujud, untuk dimasukkan ke dalam profil risiko teknologi informasi organisasi.

4. APO12.04 – *Articulate Risk*

Menyampaikan informasi mengenai kondisi terkini dari paparan dan peluang yang berkaitan dengan I&T secara tepat waktu kepada seluruh pemangku kepentingan yang relevan, agar dapat dilakukan respons yang sesuai.

Aktivitas :

a. Melaporkan hasil analisis risiko kepada seluruh pemangku kepentingan yang terdampak dalam bentuk dan format yang berguna untuk mendukung pengambilan keputusan organisasi. Jika memungkinkan, sertakan probabilitas serta rentang kerugian atau keuntungan, beserta tingkat keyakinannya, agar manajemen dapat menyeimbangkan antara risiko dan imbal hasil *(risk-return).*
b. Memberikan kepada pengambil keputusan pemahaman mengenai skenario terburuk *(worst-case)* dan skenario paling mungkin terjadi *(most-probable),* paparan kerugian yang terkait dengan I&T, serta pertimbangan penting lainnya seperti reputasi, hukum, peraturan, atau kategori dampak lain sesuai taksonomi risiko.
c. Melaporkan profil risiko terkini kepada seluruh pemangku kepentingan. Menyertakan informasi mengenai efektivitas proses manajemen risiko, efektivitas kontrol, kesenjangan, inkonsistensi, redundansi, status perbaikan *(remediation status),* serta dampaknya terhadap profil risiko.
d. Secara berkala, untuk area yang memiliki kesetaraan antara risiko relatif dan kapasitas risiko, identifikasi peluang terkait I&T yang memungkinkan penerimaan risiko lebih besar guna meningkatkan pertumbuhan dan pengembalian *(growth and return).*
e. Meninjau hasil penilaian dari pihak ketiga yang independen, serta hasil audit internal dan tinjauan jaminan mutu *(quality assurance reviews).* Menyertakan temuan-temuan tersebut ke dalam profil risiko, kemudian tinjau kesenjangan dan paparan kerugian terkait I&T untuk menentukan kebutuhan akan analisis risiko tambahan.

5. APO12.05 – *Define a Risk Management Action Portfolio*

Mengelola berbagai peluang untuk mengurangi risiko hingga pada tingkat yang dapat diterima, melalui pendekatan portofolio yang seimbang.

Aktivitas :

a. Memelihara daftar inventaris aktivitas pengendalian yang telah diterapkan untuk memitigasi risiko serta memungkinkan pengambilan risiko sesuai

dengan tingkat *risk appetite* dan *risk tolerance* organisasi. Mengklasifikasikan aktivitas pengendalian tersebut dan petakan terhadap skenario risiko yang spesifik maupun terhadap agregasi dari beberapa skenario risiko teknologi informasi.

b. Menentukan apakah setiap entitas organisasi melakukan pemantauan terhadap risiko dan menerima tanggung jawab atas operasionalnya dalam batas toleransi risiko individu maupun portofolionya.

c. Menetapkan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau memungkinkan terciptanya peluang strategis bagi organisasi, dengan mempertimbangkan biaya, manfaat, dampak terhadap profil risiko saat ini, serta kepatuhan terhadap peraturan yang berlaku.

6. APO12.06 - *Respond to Risk*

Merespons secara tepat waktu terhadap kejadian risiko yang telah terwujud, dengan menerapkan langkah-langkah efektif untuk membatasi besarnya kerugian yang mungkin timbul.

Aktivitas :

a. Menyiapkan, memelihara, dan menguji rencana respons yang mendokumentasikan langkah-langkah spesifik yang harus dilakukan ketika suatu kejadian risiko berpotensi menimbulkan insiden operasional atau insiden pengembangan yang signifikan serta berdampak serius terhadap bisnis. Pastikan bahwa rencana tersebut mencakup jalur eskalasi yang jelas di seluruh organisasi.

b. Menerapkan rencana respons yang sesuai untuk meminimalkan dampak ketika insiden risiko benar-benar terjadi.

c. Mengategorikan setiap insiden dan membandingkan paparan kerugian yang berkaitan dengan teknologi informasi terhadap ambang batas *risk tolerance*. Mengkomunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari proses pelaporan, serta perbarui profil risiko sesuai hasil evaluasi.

d. Meninjau kejadian merugikan atau kerugian yang telah terjadi di masa lalu, termasuk peluang yang terlewatkan, dan menentukan akar penyebabnya.

e. Mengomunikasikan akar penyebab, kebutuhan tambahan atas respons risiko, serta usulan perbaikan proses kepada pengambil keputusan yang relevan.

Pastikan bahwa penyebab, kebutuhan respons, dan peningkatan proses tersebut diintegrasikan ke dalam proses tata kelola risiko organisasi.

2.6.9 COBIT *Performance Management (CPM)*

Manajemen kinerja merupakan bagian penting dari sistem tata kelola dan manajemen. Istilah ini mencakup seluruh kegiatan dan metode yang digunakan untuk menilai sejauh mana sistem tata kelola serta seluruh komponen dalam organisasi berfungsi, dan bagaimana peningkatan dapat dilakukan guna mencapai tingkat kinerja yang diharapkan[3].

COBIT menggunakan istilah COBIT *Performance Management* (CPM) untuk menggambarkan aktivitas ini. Konsep tersebut meliputi berbagai metode seperti pengukuran tingkat kapabilitas *(capability levels)* dan tingkat kematangan *(maturity levels).* Secara keseluruhan, manajemen kinerja menjadi bagian integral dari kerangka kerja COBIT karena berperan dalam mengukur efektivitas penerapan tata kelola dan manajemen TI dalam organisasi[3].

COBIT 2019 mendasarkan COBIT *Performance Management* (CPM) pada beberapa prinsip utama berikut[3]:

1. Kesederhanaan dan Kemudahan Penggunaan

   CPM harus dirancang agar mudah dipahami dan digunakan oleh seluruh pihak yang terlibat dalam tata kelola dan manajemen teknologi informasi.
2. Konsistensi dengan Model Konseptual COBIT

   CPM harus selaras dan mendukung model konseptual COBIT. Sistem ini memungkinkan pengelolaan kinerja seluruh komponen dalam sistem tata kelola, baik pada tingkat proses maupun komponen lainnya seperti struktur organisasi dan informasi.
3. Keandalan dan Relevansi Hasil Penilaian

   CPM harus menghasilkan hasil penilaian yang andal, dapat diulang, serta relevan dengan kondisi organisasi.
4. Fleksibilitas dalam Penerapan

   CPM harus cukup fleksibel untuk memenuhi kebutuhan beragam organisasi yang memiliki prioritas dan tujuan yang berbeda-beda.
5. Dukungan terhadap Berbagai Jenis Penilaian

   CPM harus dapat mendukung berbagai bentuk evaluasi, baik penilaian mandiri (*self-assessment*) maupun penilaian formal melalui audit atau peninjauan eksternal.

Pada COBIT 2019, pengelolaan kinerja tidak hanya menilai pencapaian hasil, tetapi juga sejauh mana kapabilitas proses dan komponen tata kelola serta manajemen dapat mendukung pencapaian tujuan organisasi. Sejalan dengan model sebelumnya, COBIT 2019 mengadopsi pendekatan berbasis *Capability Levels* yang disesuaikan dengan standar internasional ISO/IEC 33000 (pembaruan dari ISO/IEC 15504)[3].

Adapun perbedaan dan penyempurnaan yang terdapat dalam COBIT 2019 adalah sebagai berikut[3]:

1. Hasil proses *(process outcomes)* kini dihubungkan secara langsung dengan praktik proses *(process practices).* Artinya, keberhasilan suatu proses ditentukan oleh penyelesaian praktik-praktik yang telah ditetapkan. Contohnya, APO01.01 - *Design the management system for enterprise I&T*, hasilnya adalah sistem manajemen TI perusahaan yang dirancang secara efektif.
2. Praktik dasar *(base practices)* disetarakan dengan praktik proses COBIT 2019 untuk setiap tujuan tata kelola dan manajemen.
3. Produk kerja *(work products)* disesuaikan dengan alur informasi *(information flows)* dan item-item dalam setiap komponen tujuan tata kelola dan manajemen.

2.7 RACI *Chart (Responsible, Accountable, Consulted, Informed)*

RACI merupakan singkatan dari *Responsible, Accountable, Consulted,* dan *Informed*, yang digunakan untuk menjelaskan peran dan tanggung jawab setiap pihak dalam suatu aktivitas atau proses[59].

1. *Responsible* (R), pihak yang melakukan pekerjaan langsung atau bertanggung jawab dalam pelaksanaan tugas.
2. *Accountable* (A), pihak yang memiliki tanggung jawab akhir terhadap hasil dan memastikan tugas berjalan dengan benar.
3. *Consulted* (C), pihak yang dilibatkan untuk memberikan masukan atau keahlian teknis dalam pelaksanaan tugas.
4. *Informed* (I), pihak yang diberi informasi atau laporan hasil kegiatan, namun tidak terlibat langsung dalam pelaksanaannya.

Dalam praktiknya, penerapan RACI memungkinkan organisasi untuk mengidentifikasi dengan tepat siapa yang harus terlibat dalam setiap langkah proses, mulai dari pengambilan keputusan, pelaksanaan teknis, hingga pelaporan hasil sehingga alur kerja menjadi lebih efisien dan akuntabel. Dengan penerapan yang tepat, RACI dapat mendukung kolaborasi yang lebih baik antar pemangku kepentingan dan memperkuat kontrol *internal*

atas pelaksanaan proses. Namun, model ini juga menuntut pendekatan yang sistematik, meliputi definisi peran yang jelas, komunikasi yang terbuka, serta evaluasi berkala untuk memastikan semua pihak memahami dan menjalankan perannya[60].

Tabel 2. 17 *RACI Chart* APO12 *(Managed Risk)*

Key Management Practice	*Chief Risk Officer*	*Chief Information Officer*	*Chief Technology Officer*	*Chief Digital Officer*	*Enterprise Risk Committee*	*Chief Information Security Officer*	*Business Process Owners*	*Project Management Office*	*Data Management Function*	*Head Architect*	*Head Development*	*Head IT Operations*	*Head IT Administration*	*Service Manager*	*Information Security Manager*	*Business Continuity Manager*	*Privacy Officer*
APO12.01 Collect data	*A*	*R*	*R*	*R*		*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*
APO12.02 Analyze risk	*A*	*R*			*R*		*R*										
APO12.03 Maintain a risk profile	*A*	*R*			*R*		*R*										
APO12.04 Articulate risk	*A*	*R*			*R*		*R*										
APO12.05 Define a risk management action portfolio	*A*	*R*			*R*		*R*										
APO12.06 Respond to risk	*R*	*A*	*R*	*R*		*R*	*R*	*R*		*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*

Dalam konteks audit manajemen risiko gangguan layanan teknologi informasi, model RACI digunakan untuk menetapkan dengan jelas siapa yang berperan dalam mengidentifikasi, menganalisis, menangani, dan memantau risiko yang dapat mengganggu keberlangsungan layanan TI. Dengan kata lain, RACI membantu auditor dan manajemen memahami siapa yang harus melakukan apa ketika terjadi potensi gangguan pada sistem, jaringan, atau infrastruktur layanan TI. Berikut merupakan peran masing-masing pihak[60]:

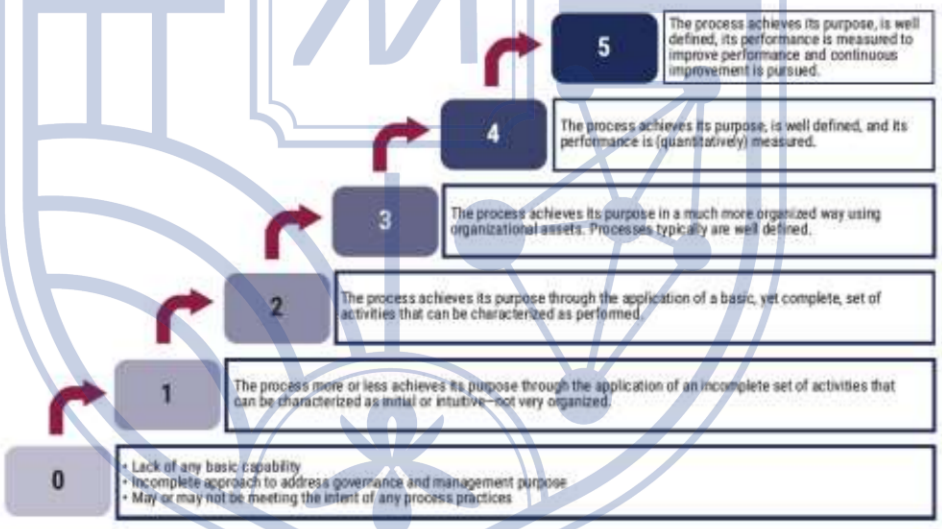
1. *Chief Risk Officer (CRO),* jabatan ini mengawasi keseluruhan proses manajemen risiko, termasuk risiko gangguan layanan TI, serta memastikan kebijakan mitigasi dan kontrol risiko diterapkan secara konsisten di seluruh unit.
2. *Chief Information Officer (CIO),* kedudukan ini bertanggung jawab terhadap ketersediaan dan keandalan layanan TI, memastikan strategi teknologi selaras dengan kebutuhan bisnis serta memiliki rencana pemulihan saat gangguan terjadi.

3. *Chief Technology Officer (CTO),* jabatan ini menjamin kesiapan infrastruktur dan sistem teknologi agar mampu beroperasi stabil serta cepat dipulihkan bila terjadi gangguan teknis.
4. *Chief Digital Officer (CDO),* berperan mengawasi kelangsungan layanan digital berbasis TI dan memastikan inovasi digital tidak menimbulkan risiko tambahan terhadap stabilitas sistem.
5. *Enterprise Risk Committee,* jabatan ini menetapkan arah dan kebijakan strategis pengelolaan risiko gangguan TI, serta meninjau hasil audit untuk memastikan risiko signifikan ditangani sesuai tingkat prioritasnya.
6. *Chief Information Security Officer (*CISO*),* bertugas mengelola aspek keamanan informasi dan jaringan untuk mencegah gangguan layanan akibat ancaman siber, serta mengoordinasikan respons terhadap insiden keamanan.
7. *Business Process Owners,* berperan menilai dampak gangguan layanan TI terhadap proses bisnis utama, memastikan setiap proses memiliki kontrol dan prosedur pemulihan yang memadai.
8. *Project Management Office (PMO),* bertugas memastikan proyek TI yang sedang berjalan memperhitungkan risiko gangguan layanan, serta mengoordinasikan mitigasi selama pelaksanaan proyek.
9. *Data Management Function,* jabatan ini menjamin keamanan, integritas, dan ketersediaan data selama maupun setelah gangguan, serta memastikan mekanisme *backup* dan *recovery* berjalan efektif.
10. *Head Architect,* bertugas merancang arsitektur sistem dan jaringan yang tangguh terhadap gangguan, serta memastikan desain teknologi mendukung ketahanan layanan TI.
11. *Head Development,* memastikan aplikasi dikembangkan dengan mempertimbangkan aspek keandalan dan pemulihan cepat ketika terjadi gangguan layanan atau kegagalan sistem.
12. *Head IT Operations,* mengelola kegiatan operasional TI sehari-hari dan mengoordinasikan penanganan insiden untuk menjaga kontinuitas layanan selama gangguan terjadi.
13. *Head IT Administration,* berperan dalam pengelolaan sumber daya administrasi TI seperti akun, akses, dan konfigurasi sistem agar tidak menjadi penyebab atau celah dalam gangguan layanan.

14. *Service Manager,* bertugas mengawasi kinerja layanan TI, memimpin proses pemulihan *(service recovery),* serta memastikan pengguna mendapatkan dukungan saat layanan terganggu.
15. *Information Security Manager,* melaksanakan kebijakan keamanan jaringan di lapangan, mengidentifikasi potensi ancaman, dan melakukan tindakan preventif untuk mencegah gangguan.
16. *Business Continuity Manager (BCM),* berperan mengembangkan dan menguji rencana kesinambungan bisnis (BCP) agar layanan TI dapat tetap beroperasi atau segera dipulihkan pascagangguan.
17. *Privacy Officer,* memastikan perlindungan data pribadi tetap terjaga selama dan setelah gangguan layanan TI, serta menilai risiko kebocoran atau pelanggaran privasi.

2.8 *Capability Levels*

2.8.1 Konsep *Capability Levels*



Gambar 2. 9 *Capability Levels*

Capability Levels digunakan untuk menilai sejauh mana suatu proses tata kelola dan manajemen TI dijalankan secara efektif di dalam organisasi. Setiap tingkat menunjukkan perbedaan proses, mulai dari yang belum memiliki kemampuan sama sekali hingga yang sudah terukur dan terus mengalami perbaikan berkelanjutan. Berikut merupakan tingkat kapabilitas proses *(Capability Levels)* dalam COBIT[3]:

1. Level 0 - Organisasi belum memiliki kapabilitas dasar. Pendekatan terhadap tata kelola dan manajemen masih tidak lengkap atau bahkan tidak ada sama sekali, sehingga proses belum berjalan sesuai dengan tujuannya.
2. Level 1 - Proses sudah mulai dijalankan, namun masih bersifat tidak terorganisasi, reaktif, dan belum konsisten. Aktivitas yang dilakukan masih belum cukup untuk mencapai tujuan proses secara berkelanjutan.
3. Level 2 - Proses dijalankan melalui serangkaian aktivitas dasar yang dapat dikatakan telah dilakukan secara rutin, meskipun belum sepenuhnya terdokumentasi atau distandarisasi.
4. Level 3 - Proses mulai berjalan dengan lebih terstruktur dan sistematis. Aktivitas serta hasilnya sudah terdefinisi dengan baik dan biasanya didukung oleh dokumentasi formal.
5. Level 4 - Proses telah distandarisasi dengan baik dan hasil kinerjanya diukur secara kuantitatif. Organisasi mampu memprediksi hasil proses karena telah memiliki data pengukuran yang konsisten dan dapat diandalkan.
6. Level 5 - Proses mencapai tujuannya secara optimal, kinerjanya terukur dengan baik, serta terus ditingkatkan melalui upaya perbaikan berkelanjutan untuk mencapai efisiensi dan efektivitas yang lebih tinggi.

Setiap level kapabilitas dapat dicapai dengan tingkat pencapaian yang berbeda-beda. COBIT menyediakan panduan untuk menilai sejauh mana suatu proses memenuhi kriteria di level tertentu, yang umumnya digunakan untuk melakukan evaluasi atau peningkatan kinerja, dengan kategori penilaian sebagai berikut[3]:

1. *Fully Achieved* (Tercapai Sepenuhnya), tingkat kapabilitas telah terpenuhi secara menyeluruh dengan pencapaian lebih dari 85%.
2. *Largely Achieved* (Sebagian Besar Tercapai), tingkat kapabilitas sebagian besar kriteria telah terpenuhi dengan tingkat pencapaian antara 50% - 85%, di mana proses sudah dijalankan dengan baik namun masih terdapat beberapa area yang memerlukan penyempurnaan.
3. *Partially Achieved* (Sebagian Tercapai), tingkat kapabilitas memenuhi sekitar 15% - 50% dari kriteria yang diharapkan, di mana sebagian aktivitas sudah dijalankan namun belum terstruktur secara menyeluruh.
4. *Not Achieved* (Belum Tercapai), tingkat kapabilitas masih sangat rendah, yaitu kurang dari 15%, di mana proses belum diterapkan secara efektif.

2.8.2 Rumus Perhitungan *Capability Level*

Pengelolaan dan perhitungan data kuesioner dalam penentuan tingkat kapabilitas *(capability level)* dalam COBIT 2019 pada setiap aktivitas yang dilaksanakan melalui proses pengolahan dan perhitungan data menggunakan rumus yang telah ditetapkan sebagai berikut[9,61]:

a) Perhitungan Tingkat Kapabilitas Sub-domain Berdasarkan Penilaian Responden

1. **Menghitung *capability level* pada masing – masing sub-domain**

$$\textbf{Capability Level} = \frac{\sum \text{Rata-rata Aktivitas dan Dokumen yang Telah Terpenuhi}}{\text{Total Responden}} \quad \text{.....(1)}$$

2. **Menghitung masing – masing nilai kapabilitas sub-domain APO12**

$$\textbf{Capability Level APO12} = \frac{\sum CLR\ APO12\ 1 + CLR\ APO12\ 2 + \ldots CLR\ APO12\ n}{\text{Total Responden}} \quad \text{.....(2)}$$

Perhitungan ini berfokus pada penilaian yang diberikan oleh masing-masing responden. Nilai *capability level* dihitung dari rata-rata aktivitas yang dinilai telah dilakukan oleh responden, kemudian dijumlahkan dan dibagi dengan total responden. Rumus ini menghasilkan tingkat kapabilitas yang mencerminkan persepsi individu terhadap seberapa jauh aktivitas pada tiap sub-domain APO12 *(Managed Risk)* yang telah dilaksanakan.

b) Perhitungan Tingkat Kapabilitas Berdasarkan Pemenuhan Aktivitas Setiap Sub-domain

1. **Menghitung *capability level* pada masing – masing sub-domain**

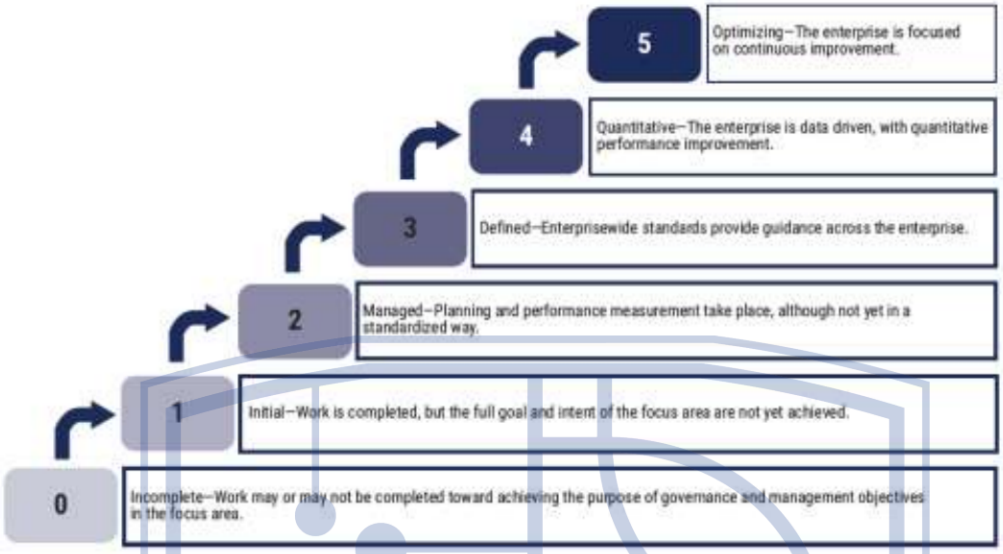
$$\textbf{Capability Level} = \frac{\sum \text{Aktivitas Terpenuhi Sub Domain Lv n}}{\text{Jumlah Sub Domain APO12 Lv n}} \quad \text{.....(3)}$$

2. **Menghitung masing – masing nilai kapabilitas sub-domain APO12**

$$\textbf{Capability Level} = \frac{\sum \text{APO12.01} + \cdots + \text{APO12.n}}{\text{Jumlah Sub Domain APO12 Lv n}} \quad \text{.....(4)}$$

Perhitungan dilakukan dengan membagi jumlah aktivitas yang benar-benar terpenuhi dengan jumlah total sub-domain pada *level* tersebut sehingga hasilnya mencerminkan kecapaian struktural proses, bukan lagi penilaian responden. Dengan kata lain, rumus ini menggambarkan tingkat kapabilitas proses APO12 berdasarkan pencapaian objektif setiap sub-domain pada *level* n.

2.9 *Maturity Levels*



Gambar 2. 10 *Maturity Levels*

2.9.1 Konsep *Maturity Levels*

Maturity levels atau tingkat kematangan menggambarkan sejauh mana suatu proses tata kelola dan manajemen telah dikembangkan, diterapkan, serta disempurnakan di dalam organisasi. Konsep ini digunakan untuk menilai kemampuan organisasi dalam menjalankan proses secara konsisten, terukur, dan berkesinambungan[3].

Berikut merupakan tingkat kematangan dalam COBIT 2019[3]:

1. Level 0 *(Incomplete)* - Proses belum sepenuhnya dilaksanakan dan belum mendukung pencapaian tujuan tata kelola serta manajemen pada area yang dimaksud.
2. Level 1 *(Initial)* - Proses telah dilakukan, namun tujuan utama belum tercapai secara menyeluruh dan pelaksanaannya belum terarah dengan baik.
3. Level 2 *(Managed)* - Perencanaan dan pengukuran kinerja telah dilakukan, tetapi belum diterapkan secara konsisten dan terstandarisasi di seluruh organisasi.
4. Level 3 *(Defined)* - Proses telah memiliki standar dan pedoman yang diterapkan secara konsisten di seluruh organisasi.
5. Level 4 *(Quantitative)* - Organisasi telah menggunakan pendekatan berbasis data dengan pengukuran kinerja kuantitatif untuk meningkatkan efektivitas proses.
6. Level 5 *(Optimizing)* - Organisasi berfokus pada perbaikan berkelanjutan untuk mencapai kinerja dan efisiensi yang optimal.

2.9.2 Rumus Perhitungan *Maturity Level*

Penentuan tingkat kematangan *(maturity level)* dalam kerangka kerja COBIT 2019 melibatkan pengolahan dan perhitungan data kuesioner secara sistematis. Proses ini, yang dilaksanakan untuk setiap aktivitas dalam suatu proses, menggunakan rumus baku yang telah ditetapkan untuk menghasilkan skor akhir yang mencerminkan tingkat kematangan proses tersebut[61].

a) Perhitungan *Maturity Level* Berdasarkan Penilaian Responden

1. Menghitung *maturity level* pada masing – masing sub-domain

$$\textbf{Maturity Level} = \frac{\sum \text{R1} + \sum \text{R2} + \sum \text{R3} + \sum \text{R4} + \sum \text{R5} + \sum \text{R6}}{\text{Jumlah Responden}} \quad \textbf{.....(5)}$$

2. Menghitung masing-masing *maturity level* sub-domain APO12

$$\textbf{Maturity Level} = \frac{\sum APO12.01 + \sum APO12.02 + \cdots + \sum APO12.06}{\textit{Jumlah Responden APO12}} \quad \textbf{.....(6)}$$

Perhitungan ini berfokus pada penilaian yang diberikan oleh masing-masing responden. Nilai *maturity level* dihitung dari rata-rata skor aktivitas yang dinilai telah dilakukan, kemudian dijumlahkan dan dibagi dengan total responden. Pendekatan ini menghasilkan tingkat kematangan yang mencerminkan persepsi individu mengenai sejauh mana aktivitas pada setiap sub-domain APO12 *(Managed Risk)* telah diterapkan dalam praktik.

b) Perhitungan *Maturity Level* Berdasarkan Pemenuhan Aktivitas Sub-domain

1. Menghitung *maturity level* pada masing – masing sub-domain

$$\textbf{Maturity Level} = \frac{\sum \text{Rata–rata Aktivitas dan Dokumen yang telah terpenuhi}}{\sum \text{Aktivitas dan Dokumen Domain Proses}} \quad \textbf{.....(7)}$$

2. Menghitung masing-masing *maturity level* sub-domain APO12

$$\textbf{Maturity Level} = \frac{\sum \text{APO12.01} + \sum \text{APO12.02} + \cdots + \sum \text{APO12.06}}{\sum \text{Aktivitas dan Dokumen Domain APO12}} \quad \textbf{.....(8)}$$

Perhitungan berbasis pemenuhan aktivitas proses dilakukan dengan membandingkan jumlah aktivitas yang terlaksana dengan total aktivitas pada sub-domain APO12 *(Managed Risk)*. Pendekatan ini menghasilkan tingkat kematangan yang objektif karena menunjukkan pencapaian aktual proses tanpa dipengaruhi penilaian subjektif responden.

2.10 Analisa Kesenjangan *(Gap Analysis)*

Gap analysis adalah suatu metode atau proses sistematis untuk mengidentifikasi kesenjangan *(gap)* antara kondisi saat ini dengan kondisi yang diharapkan atau ditargetkan.

Tujuannya adalah untuk mengetahui apa saja yang belum tercapai, mengapa hal tersebut terjadi, dan apa yang perlu dilakukan untuk menutup kesenjangan tersebut[62]

2.10.1 Rumus Perhitungan Kesenjangan Tingkat Kapabilitas/ *Capability Level*

Proses ini diterapkan pada setiap aktivitas dalam suatu proses guna mengidentifikasi perbedaan antara kondisi aktual dan kondisi yang diharapkan. Perhitungan dilakukan menggunakan rumus baku yang telah ditetapkan untuk memperoleh hasil akhir yang menggambarkan tingkat kesenjangan pada proses tersebut[62]

$$\boldsymbol{Gap = Expected\ Capability - Current\ Capability} \text{.....(9)}$$

Peneliti akan terlebih dahulu meminta pihak perusahaan untuk menetapkan level kapabilitas yang menjadi target pencapaian. Selanjutnya, nilai kesenjangan *(gap)* akan dihitung dengan mengurangkan nilai rata-rata kapabilitas aktual perusahaan saat ini dari level kapabilitas yang diharapkan[62].

2.10.2 Rumus Perhitungan Kesenjangan Tingkat Kematangan/ *Maturity Level*

$$\boldsymbol{Gap = Expected\ Maturity - Current\ Maturity} \text{.....(10)}$$

Dari perhitungan ini, akan didapatkan selisih antara tingkat kematangan proses yang diharapkan *(Expected Maturity)* dengan tingkat kematangan saat ini *(Current Maturity).* Melalui identifikasi perbedaan antara kondisi aktual dan target yang telah ditetapkan, organisasi dapat menyusun langkah-langkah strategis dan rencana perbaikan yang lebih terarah. Proses ini juga membantu dalam menentukan prioritas peningkatan pada area yang masih lemah, sehingga upaya pengembangan dapat dilakukan secara efektif dan berkesinambungan untuk mencapai kinerja manajemen yang optimal.

2.11 Pengukuran *Capability Levels* Menggunakan Skala *Guttman*

Skala ini digunakan untuk memperoleh jawaban yang bersifat tegas dan pasti dari responden terhadap setiap pernyataan yang diberikan, seperti pilihan “ya” dan “tidak”, “setuju” dan “tidak setuju”, atau “yakin” dan “tidak yakin”[63].

Penerapan skala *Guttman* dalam penelitian ini bertujuan untuk mengukur tingkat penerapan manajemen risiko gangguan layanan teknologi informasi di PT Capella Medan, khususnya pada domain APO12 *(Managed Risk)* berdasarkan kerangka COBIT 2019. Setiap butir pernyataan untuk menilai *capability level* dalam kuesioner disusun sesuai dengan indikator aktivitas proses yang terdapat pada domain APO12, seperti identifikasi risiko, penilaian risiko, serta pengelolaan respons risiko terhadap gangguan layanan jaringan. Jawaban responden kemudian diberi skor berdasarkan sistem penilaian sebagai berikut[63]:

Tabel 2. 18 Skala *Guttman*

Jawaban	Nilai	Keterangan
Ya/ Sudah dilakukan	1	Menunjukkan bahwa aktivitas atau kontrol telah diterapkan sesuai dengan indikator proses.
Tidak/ Belum dilakukan	0	Menunjukkan bahwa aktivitas atau kontrol belum diterapkan atau belum berjalan optimal.

Hasil dari pengisian kuesioner dengan skala *Guttman* akan diolah untuk menentukan tingkat pencapaian aktivitas proses dan tingkat kapabilitas *(capability level)* pada domain APO12. Semakin banyak jawaban "Ya" yang diperoleh, maka semakin tinggi tingkat penerapan proses manajemen risiko di perusahaan[63].

Penilaian setiap aktivitas dimulai dari level 0, dan setelah organisasi berhasil mencapai suatu level tertentu, proses penilaian akan dilanjutkan ke level berikutnya. Namun, apabila hasil evaluasi pada level kapabilitas tersebut belum memenuhi standar yang ditetapkan, maka proses penilaian tidak akan dilanjutkan dan akan berhenti pada level kapabilitas terakhir yang telah dinilai[10].

2.12 Penelitian Terdahulu (Studi Empiris)

Tinjauan penelitian terdahulu mencakup audit tata kelola TI pernah dilakukan PT Capella Medan pada tahun 2013 dan 2025. Selain itu, terdapat beberapa penelitian relevan lainnya yang mendukung penelitian ini sebagai berikut:

Tabel 2. 19 Penelitian Terdahulu

No	Judul, Nama, dan Tahun Penelitian	Kerangka Kerja dan Domain	Hasil Penelitian	Kesenjangan Penelitian
1.	Penerapan IT *Balanced Scorecard* dan *Competency Gap Index* dalam Tata Kelola IT : Studi Kasus PT. Capella Medan Oleh : Hoga Saragih, Waisen, dan	**COBIT 4.1 Domain:** *1.Planning and Organization (PO)* *2.Acquisition and Implementation (AI)* *3.Delivery and Support (DS)* *4.Monitoring and Evaluate (ME)*	***Maturity*** Berada di bawah Level 3 dan memerlukan perbaikan signifikan.	Hanya terbatas pada pengukuran tingkat kematangan tata kelola TI menggunakan COBIT 4.1. dan tidak lagi relevan dibandingkan COBIT 2019.
			Analysis Gap Seluruh nilai kesenjangan berada di atas Level 1, mengindikasikan	Belum ada penilaian mendalam terhadap risiko gangguan layanan TI yang berpotensi menghambat operasional.

	Bobby Reza (2013) [8]	***IT Balanced Scorecard & Key Performance Indicator (KPI)***	perlunya tindakan perbaikan segera.	
			Faktor Pendukung Dukungan manajemen terhadap pengembangan TI masih rendah, dan pemanfaatan sistem informasi perlu ditingkatkan agar selaras dengan strategi bisnis perusahaan.	Analisis sebelumnya bersifat umum dan gagal memprioritaskan area risiko kritikal yang membutuhkan mitigasi segera.
				Memfokuskan kajian pada audit manajemen risiko gangguan layanan TI untuk menghasilkan rekomendasi yang lebih tepat sasaran guna meningkatkan keamanan, keandalan, dan ketersediaan layanan TI.
2.	Evaluasi Tata Kelola Teknologi Informasi dengan *Framework* COBIT 2019 pada PT Capella Medan Oleh : Ramiro (2025) [9]	**COBIT 2019 Domain:** 1. EDM.05 – *Ensured Stakeholder Engagement* 2. APO.06 – *Managed Budget and Costs* 3. BAI.09 – *Managed Assets* 4. MEA.03 – *Managed Compliance with External Requirements*	***Capability*** 1. EDM.05 *(Ensured Stakeholder Engagement)* berada pada Level 3 *(Defined Process)*. 2. APO.06 *(Managed Budget and Costs),* BAI.09 *(Managed Assets),* dan MEA.03 *(Managed Compliance with External Requirements)* masing-masing berada pada Level 2 *(Managed Process).*	Sebagian besar proses (APO.06, BAI.09, MEA.03) masih berada pada Level 2, jauh dari target Level 5, menunjukkan tata kelola TI belum matang sepenuhnya.

			Analysis Gap Terdapat kesenjangan antara kondisi saat ini (*as-is*) dan target yang diharapkan (*to-be*) yaitu: 1. EDM.05 memiliki gap sebesar 1 2. APO.06, BAI.09, dan MEA.03 masing-masing memiliki gap sebesar 3. Kesenjangan ini menunjukkan perlunya peningkatan signifikan agar mencapai target kapabilitas Level 5 sesuai standar COBIT 2019.	Aspek anggaran, aset, dan kepatuhan *eksternal* belum dikelola secara optimal untuk mendukung strategi bisnis perusahaan.
			Rekomendasi PT Capella Medan perlu meningkatkan pengelolaan anggaran, aset, dan kepatuhan eksternal agar tata kelola TI lebih efektif dan selaras dengan tujuan perusahaan.	EDM.05 (*Ensured Stakeholder Engagement)* masih berada di Level 3, menandakan komunikasi dan koordinasi antar *stakeholder* belum konsisten dan terukur.
				Belum terdapat pendekatan sistematis untuk menutup *gap* kapabilitas dan meningkatkan tata kelola TI hingga Level 5 sesuai standar COBIT 2019.
3.	Evaluasi Tata Kelola Teknologi Informasi Pada PT Indako Trading Coy Dengan Menggunakan	**COBIT 2019** **Domain:** APO12 (*Managed Risk)*	***Analysis Gap*** Tingkat kemampuan *(capability)* dan kematangan *(maturity)* berada pada Level 2, dengan selisih 1 level dari target yang diharapkan (Level 3).	Penelitian cenderung deskriptif, tanpa eksplorasi mendalam terhadap faktor penyebab rendahnya tingkat kapabilitas/kematangan dan belum melibatkan analisis kuantitatif.

	Framework COBIT 2019 Domain APO12 Oleh : Stanley Howard, Tomy Wijaya, Roni Yunis, dan Megawati (2023) [11]		**Implikasi** Proses manajemen risiko TI belum terkelola secara optimal dan belum distandardisasi dengan baik.	Rekomendasi yang diberikan masih bersifat umum dan belum diukur efektivitas implementasinya.
			Rekomendasi Utama Perusahaan perlu meningkatkan pendokumentasian, pengawasan risiko, dan penyelarasan aktivitas TI dengan tujuan bisnis untuk mencapai target Level 3.	Diperlukan perluasan evaluasi ke domain COBIT 2019 lainnya dan kombinasi metode dengan analisis risiko berbasis data empiris untuk strategi tata kelola yang lebih komprehensif dan terukur.
4.	Audit Tata Kelola TI Menggunakan COBIT 2019 Domain APO12 Pada Universitas Mikroskil Oleh : Chandra Wijaya, Mario Sukamto, Roni Yunis, Megawati (2023) [10]	**COBIT 2019 Domain:** APO12 (*Managed Risk)*	***Analysis Gap*** *Capability level* berada pada Level 1 (Dasar), dengan *Maturity Level* 2 baru mencapai 56% *(Largely Achieved).* Kesenjangan ini menunjukkan proses belum tersusun secara menyeluruh.	Fokus terbatas hanya menjelaskan tingkat kemampuan dan kematangan tanpa membahas penyebab rendahnya nilai atau dampaknya terhadap pengelolaan TI sehingga penelitian kurang mendalam.
			Implikasi Penerapan manajemen risiko TI masih bersifat dasar dan membutuhkan peningkatan signifikan dalam hal keteraturan dan kelengkapan proses.	Diperlukan perluasan pembahasan domain COBIT 2019 lain untuk hasil yang lebih lengkap.
			Rekomendasi Utama Peningkatan fokus pada konsistensi dan standarisasi proses manajemen risiko TI di seluruh organisasi, terutama untuk memastikan	Diperlukan penguji efektivitas implementasi rekomendasi yang diberikan.

			keseragaman dalam perencanaan, dokumentasi, dan pemantauan.	
5.	Analisis Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 Domain BAI03 (Studi Kasus: PT. Berlian Tangguh Sejahtera) Oleh : Shella Yolanda, Hendra, Hita, Tri Wulandari Ginting (2023) [12]	**COBIT 2019 Domain** BAI03 *(Managed Solutions Identification and Build)*	***Analysis Gap*** *Capability Level* berada pada Level 2 (93%), namun masih terdapat kesenjangan pada standarisasi proses bisnis yang belum sepenuhnya dilakukan.	Belum membahas secara mendalam faktor penyebab rendahnya tingkat kematangan serta dampaknya terhadap efektivitas proses bisnis.
			Implikasi Meskipun proses sudah direncanakan dan dinilai, ketidakadaan standarisasi penuh dapat menyebabkan inefisiensi dan variasi dalam pelaksanaan proses bisnis.	Memperluas cakupan ke domain lain (misalnya, APO12 atau DSS01) agar hasil lebih komprehensif.
			Rekomendasi Perusahaan perlu fokus pada standarisasi menyeluruh terhadap proses bisnis, serta memperbaiki sistem dan pengelolaan biaya entertainment agar menjadi lebih efisien dan terukur.	Menggabungkan pendekatan kuantitatif untuk menilai efektivitas rekomendasi dalam peningkatan tata kelola TI.
6.	*IT Risk Management: Towards a System for Enhancing*	**1.*Cyber Security Culture Framework* (CSCF)** **2.COBIT 2019**	**Temuan Utama** Pendekatan ini berhasil meningkatkan objektivitas dalam proses penilaian risiko TI.	Fokus terbatas dan hanya bertumpu pada sisi teknis implementasi tata kelola TI.

	Objectivity in Asset Valuation That Engenders a Security Culture Oleh : Bilgin Metin, Sefa Duran, Eda Telli, Meltem Mutlutürk, dan Martin Wynn (2024) [64]	Domain BAI09 *(Managed Assets)* **3.ISO 27001** **4.ISO 27005** **5.ISO 31000**	**Manfaat Sistem** Sistem yang dikembangkan mampu meminimalkan bias pribadi dan kesalahan subjektif saat menentukan nilai aset.	Belum menyoroti peran faktor organisasi, budaya kerja, dan kesiapan sumber daya manusia terhadap keberhasilan implementasi.
			Validasi Hasil validasi survei (terhadap 16 praktisi) menunjukkan metode ini efektif dalam meningkatkan kesadaran keamanan informasi dan mendukung pengambilan keputusan berbasis risiko.	Metodologi kurang komprehensif dan pendekatan masih terbatas pada satu kerangka kerja saja.
			Keterbatasan Penerapan Pendekatan ini lebih sesuai untuk organisasi menengah hingga besar yang telah memiliki fungsi manajemen risiko dan sumber daya khusus.	Diperlukan integrasi pendekatan multidimensi dan perbandingan *framework* untuk rekomendasi aplikatif.
7.	*Implementation Of The* COBIT 2019 *Framework On Information Technology Goveranance and Risk Management (Study Case: CV. Syntax Corporation Indonesia)*	**COBIT 2019** **Domain:** 1.APO12 *(Managed Risk)* 2.BAI09 *(Managed Assets)*	***Capability*** APO12 *(Managed Risk)* berada pada Level 3 *(Defined Process).* BAI09 *(Managed Assets)* berada pada Level 2 *(Managed Process).*	Penelitian belum menganalisis secara sistematis akar penyebab *(root cause)* dari kesenjangan kapabilitas.
			Analysis Gap Terdapat kesenjangan signifikan karena kondisi aktual masih di bawah target Level 5 yang diharapkan perusahaan.	Tidak terdapat studi komparatif antar organisasi untuk melihat perbedaan penerapan.

	Oleh : Mar'atus Solikhah, Lena Magdalena, Muhammad Hatta (2024) [65]		**Faktor Pendukung** Adanya penerapan awal tata kelola TI dan pemetaan tanggung jawab melalui model RACI.	Perlu dilakukan analisis mendalam terhadap faktor penyebab kesenjangan serta evaluasi dampak penerapan rekomendasi terhadap hasil bisnis dan keberlangsungan layanan.
			Faktor Penghambat Kurangnya dokumentasi, evaluasi terstruktur, dan keselarasan praktik TI dengan strategi bisnis.	Penelitian selanjutnya diharapkan menghasilkan strategi tata kelola TI yang lebih komprehensif dan adaptif melalui studi lintas domain COBIT 2019.
8.	*IT Infrastructure Assessment using the* COBIT 2019 *Framework* oleh Aulia Faqih Rifa'i, Sumarsono, Muhammad Fauzan, Al Baihaqi, Yazid Azfa Yasa (2025) [1]	**COBIT 2019 Domain:** 1.APO12 *(Managed Risk)* 2.BAI10 *(Managed Configuration)* 3.DSS02 *(Managed Service Requests & Incidents)* 4.DSS03 *(Managed Problems)* *5.*DSS04 *(Managed Continuity).*	***Capability*** Seluruh domain (APO12, BAI10, DSS02, DSS03, DSS04) berada pada *level* 1 *(Initial Process),* sedangkan target yang diharapkan adalah *level* 4 *(Quantitatively Managed).*	Penelitian hanya menilai tingkat kematangan secara deskriptif tanpa analisis mendalam terhadap faktor penyebab rendahnya kapabilitas.
			Analysis Gap Terdapat kesenjangan besar antara kondisi aktual dan target yang diharapkan, menunjukkan rendahnya tingkat kematangan infrastruktur TI dan perlunya peningkatan signifikan.	Tidak dilakukan analisis komparatif antar organisasi untuk melihat perbedaan tingkat kapabilitas.
			Faktor Pendukung Adanya kesadaran awal terhadap pentingnya tata kelola infrastruktur TI di lingkungan universitas.	Penelitian selanjutnya disarankan mengombinasikan metode evaluasi kuantitatif dan kualitatif.
			Faktor Penghambat Keterbatasan dokumentasi, proses	Diperlukan eksplorasi mendalam terhadap akar masalah dan analisis

			pemantauan, serta manajemen risiko dan insiden yang belum terstruktur.	komparatif untuk menghasilkan rekomendasi yang lebih spesifik, terukur, dan meningkatkan kualitas penelitian.
9.	*Enhancing Risk Management in an IT Service Company: A* COBIT 2019 *Framework Approach* Oleh : Emmanuel Enrique, Melissa Indah Fianty (2023) [17]	**COBIT 2019** **Domain :** 1. APO12 *(Managed Risk)* 2. BAI10 *(Managed Congiguration)* 3. DSS04 *(Managed Continuity)*	***Capability*** 1. APO12 *(Managed Risk)* berada pada *level* 3 *(Defined Process)* 2. BAI10 *(Managed Configuration)* berada pada *level* 3 *(Defined Process)* 3. DSS04 *(Managed Continuity)* berada pada *level* 2 *(Managed Process)* Target yang diharapkan masing-masing berada pada *level* 4, 4, dan 3.	Penelitian masih terbatas pada pendekatan kualitatif melalui wawancara dan analisis literatur.
			Analysis Gap Terdapat *gap* 1 *level* pada setiap domain, menunjukkan perlunya peningkatan untuk mencapai target kematangan yang diharapkan.	Belum dilakukan analisis kuantitatif mendalam maupun perbandingan antar domain COBIT 2019.
			Faktor Pendukung Perusahaan telah memiliki dasar pengelolaan risiko dan konfigurasi yang cukup baik serta kesadaran terhadap pentingnya kontinuitas layanan.	Penelitian selanjutnya dapat mengeksplorasi domain tambahan seperti APO13 *(Managed Security)* atau konfigurasi layanan lanjutan.
			Faktor Penghambat Masih terdapat kelemahan dalam	Disarankan mengombinasikan metode kuantitatif dan komparatif

			pengelolaan risiko TI, aset, dan keberlanjutan layanan yang menyebabkan keterlambatan pengiriman dan penurunan kepuasan pelanggan.	untuk menghasilkan strategi pengelolaan risiko yang lebih terukur dan adaptif terhadap perkembangan teknologi.
10.	*Assessment of Capability Levels and Improvement Recommendations Using* COBIT 2019 *for the IT Consulting Industry* Oleh : Saus Carlos Immanuel Simatupang, Melissa Indah Fianty (2023) [59]	**COBIT 2019** **Domain:** 1.APO12 *(Managed Risk)* 2.DSS01 *(Managed Operations)* 3.DSS02 *(Managed Service Requests and Incidents)*	***Capability Level*** 1. APO12 *(Managed Risk)* dan DSS02 *(Managed Service Requests & Incidents)* berada pada *level* 2. 2. DSS01 *(Managed Operations)* berada pada *level* 3 dan telah mencapai target.	Penelitian belum membahas secara spesifik aspek risiko terkait keberlangsungan layanan TI secara menyeluruh.
			Analysis Gap Terdapat *gap* 1 *level* pada APO12 dan DSS02 terhadap target *level* 3.	Membuka peluang penelitian signifikan untuk mengevaluasi efektivitas pengelolaan risiko TI pada domain APO12 *(Managed Risk).*
			Faktor Pendukung Proses operasional perusahaan sudah berjalan stabil dan terkelola baik.	Fokus penelitian mendatang dapat diarahkan pada penguatan kontinuitas layanan dalam organisasi.
			Faktor Penghambat Kurangnya dokumentasi risiko dan penanganan insiden yang belum terintegrasi dengan strategi perusahaan.	Tujuannya untuk menghasilkan strategi mitigasi risiko yang lebih terukur dan berorientasi pada kesinambungan bisnis.
11.	*Performance Analysis of Information*	**COBIT 2019** **Domain:**	***Capability Level*** Seluruh domain DSS01 *(Managed Operations)*,	Penelitian hanya berfokus pada satu perguruan tinggi negeri sehingga hasilnya

	Technology Services in Higher Education using COBIT 2019 Oleh : Eva Hariyanti, Nania Nuzulita, Muhammad Erza Ranandha, Ima Tri Indari (2025) [66]	1.DSS01 *(Managed Operations)* 2.DSS02 *(Managed Service Requests and Incidents)* 3.*DSS03 (Managed Problems)*	DSS02 *(Managed Service Requests & Incidents),* dan DSS03 *(Managed Problems)* berada pada Level 3 *(Defined Process).*	sulit digeneralisasikan ke institusi lain.
			Analysis Gap Masih terdapat ruang peningkatan menuju level kematangan lebih tinggi, terutama pada integrasi dengan penyedia layanan eksternal dan evaluasi risiko lingkungan.	Metodologi penelitian terlalu menitikberatkan pada pendekatan kuantitatif tanpa eksplorasi aspek kualitatif.
			Faktor Pendukung Proses layanan TI sudah terdefinisi baik dengan validitas instrumen tinggi (skor 4,14).	Penelitian selanjutnya dapat melakukan studi komparatif antar berbagai institusi pendidikan.
			Faktor Penghambat Beberapa aktivitas layanan TI belum optimal, khususnya dalam integrasi eksternal dan penilaian risiko operasional.	Disarankan mengadopsi pendekatan campuran untuk menganalisis faktor penyebab kesenjangan kematangan layanan dan merumuskan transformasi TI yang lebih aplikatif.
12.	*IT Governance Design in XY University using* COBIT 2019 *Framework* Oleh : Willson Mangoki, Danny Manongga, dan Ade Iriani (2024) [38]	**COBIT 2019 Domain:** 1.APO04 *(Managed Innovation)* 2.APO03 *(Managed Enterprise Architecture)* 3.APO07 *(Managed Human Resources)*	***Capability Level*** Empat domain utama APO04, APO03, APO07, dan BAI07 berada pada *level* 3 dan 4.	Penelitian belum membahas secara optimal peran faktor manusia dan budaya organisasi dalam penerapan tata kelola TI.
			Analysis Gap Perlu peningkatan kapabilitas untuk memperkuat keselarasan TI dengan strategi universitas.	Fokus penelitian masih dominan pada aspek teknis dan struktural berdasarkan kerangka COBIT 2019.

		4.BAI07 *(Managed IT Change Acceptance and Transitioning)*	**Faktor Pendukung** Adanya dukungan manajemen dan penerapan desain tata kelola TI berbasis COBIT 2019.	Belum dieksplorasi bagaimana kesiapan SDM, pola komunikasi, dan budaya kerja memengaruhi efektivitas implementasi tata kelola.
			Faktor Penghambat Beberapa proses TI belum terdokumentasi dan distandardisasi secara menyeluruh.	Penelitian selanjutnya disarankan mengintegrasikan aspek perilaku dan organisasi agar model tata kelola TI lebih realistis dan berkelanjutan.

Kajian terhadap berbagai penelitian terdahulu mengidentifikasi bahwa tata kelola dan manajemen risiko TI merupakan tantangan fundamental di berbagai sektor, termasuk pendidikan, jasa, dan korporasi. Berbagai penelitian secara konsisten menunjukkan bahwa area ini masih menjadi tantangan utama di beragam jenis organisasi. Untuk mengatasi tantangan ini, kerangka kerja COBIT digunakan sebagai alat standar untuk menilai tingkat kapabilitas dan kematangan proses tata kelola TI. Namun, terdapat beberapa kesenjangan dalam penelitian sebelumnya yang dapat dikembangkan untuk memperoleh penelitian yang lebih baik di studi kali ini:

1. Kesenjangan Pembaruan Kerangka Kerja di PT Capella Medan

   Penelitian awal mengenai tata kelola TI di PT Capella Medan masih menggunakan kerangka kerja COBIT 4.1 yang kini dianggap sudah usang dan telah digantikan oleh versi yang lebih mutakhir. COBIT 2019 menawarkan model COBIT *Performance Management* yang lebih modern, detail, dan relevan dengan praktik tata kelola dan manajemen risiko TI saat ini yang juga menekankan pada integrasi risiko dengan tujuan bisnis.

2. Kesenjangan dalam Kajian Spesifik Manajemen Risiko TI Domain APO12 *(Managed Risk)*

   Kajian penelitian terhadap domain APO12 cenderung tidak dilakukan secara mendalam terhadap risiko spesifik yang paling kritis dan berdampak langsung pada kontinuitas layanan, seperti risiko gangguan layanan jaringan. Risiko ini sangat krusial di lingkungan korporasi, namun minim dieksplorasi secara terfokus. Penelitian ini akan

mengisi kesenjangan tersebut dengan melakukan audit mendalam pada APO12, secara eksplisit menargetkan dan menganalisis risiko gangguan layanan jaringan di PT Capella Medan.

3. Kesenjangan Solusi Implementasi

   Sebagian besar studi terdahulu cenderung menghasilkan temuan yang bersifat deskriptif (misalnya, menyatakan bahwa tingkat kapabilitas berada di Level 2), tetapi kurang memberikan rekomendasi aksi atau peningkatan yang komprehensif dan terstruktur sesuai dengan *process practices* COBIT 2019. Penelitian ini tidak hanya akan menilai tingkat kapabilitas *(as-is),* tetapi juga akan merumuskan rekomendasi peningkatan *(to-be)* yang terperinci dan berbasis kerangka kerja COBIT 2019. Hal ini bertujuan untuk meningkatkan keandalan, keamanan, dan ketahanan infrastruktur TI di PT Capella Medan, menyediakan kontribusi yang lebih bernilai praktis dan ekonomis.

Dengan mengatasi ketiga kesenjangan di atas, penelitian yang berjudul "Audit Manajemen Risiko Gangguan Layanan Jaringan pada PT Capella Medan Menggunakan *Framework* COBIT 2019 Domain APO12 *(Managed Risk)*" memiliki posisi yang kuat dan kontribusi yang jelas, yaitu:

1. Relevansi Metodologis: Mengadopsi kerangka kerja yang modern, yakni COBIT 2019 di PT Capella Medan.
2. Fokus Analitis: Menyediakan audit yang spesifik dan mendalam pada domain APO12 *(Managed Risk)*, dengan fokus utama pada risiko gangguan layanan jaringan yang merupakan risiko operasional kritikal.
3. Dampak Praktis: Menghasilkan rekomendasi yang terperinci dan terstruktur untuk meningkatkan kapabilitas manajemen risiko, memindahkan hasil penelitian dari sekadar deskriptif menjadi panduan implementasi yang nyata.