

BAB II

KAJIAN LITERATUR

2.1 Tata Kelola Teknologi Informasi

Saat ini keberhasilan suatu organisasi sangat dipengaruhi oleh pemanfaatan teknologi informasi. Meskipun teknologi terus berkembang dan maju, namun seringkali menghadapi berbagai masalah, terutama ketika menghadapi tantangan yang semakin kompleks dan intensif. Para pemimpin dan pembuat kebijakan dalam organisasi dituntut agar berpikir kreatif dalam menemukan strategi yang inovatif agar dapat menciptakan suatu sinergi yang memberikan kontribusi optimal dalam mencapai tujuan organisasi. Namun, seringkali penggunaan TI hanya menghabiskan sumber daya organisasi, sementara hasil yang diharapkan tidak tercapai. Untuk itu, diperlukannya manajemen informasi yang efektif dan pemanfaatan yang terencana. Dari hal tersebut semakin menyadarkan pentingnya tata kelola TI. Konsep tata kelola TI (*IT Governance*) awalnya hampir tidak dikenal beberapa tahun yang lalu karena fungsi Teknologi Informasi (TI) pada organisasi sebelumnya hanya dianggap sebagai fungsi pendukung yang sangat penting dan bukan merupakan aktivitas bisnis utama organisasi [4]. Namun saat ini, tata kelola TI menjadi bagian yang tidak dapat dipisahkan dari Tata Kelola Perusahaan (*Good Corporate Governance*).

Tata kelola teknologi informasi (TI) adalah praktik pengelolaan teknologi informasi yang tepat dan terukur di dalam organisasi [5]. Tata kelola TI mencakup beberapa prinsip, seperti akuntabilitas, transparansi, keadilan, dan tanggung jawab. Tujuan utama dari tata kelola TI adalah memastikan penggunaan teknologi informasi yang efektif dalam mencapai tujuan bisnis organisasi [6]. Dalam tata kelola TI, terdapat kerangka kerja untuk mengelola dan mengawasi penggunaan teknologi informasi, termasuk aspek strategi, manajemen risiko, kepatuhan, manajemen sumber daya TI, dan pengukuran kinerja. Dengan menerapkan prinsip-prinsip dan kerangka kerja tata kelola TI, organisasi dapat memastikan bahwa penggunaan teknologi informasi diintegrasikan secara efektif dalam operasi bisnis dan memungkinkan organisasi mencapai keunggulan kompetitif serta keberlanjutan jangka panjang. [7]

2.1.1 Tujuan dan Manfaat Tata Kelola Teknologi Informasi

Tujuan tata kelola teknologi informasi adalah mengontrol penerapan dalam kinerja TI organisasi sudah memenuhi dengan tujuannya sebagai berikut:

1. Menyelaraskan teknologi informasi dengan strategi organisasi dan mencapai manfaat-manfaat yang dijanjikan dari penerapan teknologi informasi.
2. Penggunaan teknologi informasi memungkinkan organisasi untuk memanfaatkan peluang yang ada dan teknologi informasi secara maksimal dengan mengoptimalkan manfaat penerapan TI.
3. Penggunaan sumber daya TI yang bertanggung jawab.
4. Mengelola manajemen risiko teknologi informasi secara tepat dan efektif [6].

Tata kelola TI berfokus pada penyampaian nilai dari transformasi digital yang dilakukan pada organisasi serta menangani risiko bisnis yang berkemungkinan terjadi pada proses transformasi digital. Secara spesifik, terdapat tiga hasil yang dapat diharapkan setelah sukses mengadopsi tata kelola teknologi informasi organisasi[1]:

1. Realisasi Manfaat (*Benefits Realization*)

Manfaat yang diberikan dalam menciptakan nilai untuk perusahaan melalui teknologi informasi adalah mempertahankan dan meningkatkan nilai yang diperoleh dari investasi teknologi informasi yang sudah dimiliki oleh organisasi, serta menghilangkan inisiatif dan aset TI yang tidak menciptakan nilai yang cukup. Prinsip dasar TI adalah memberikan layanan dan solusi yang sesuai dengan tujuan, tepat waktu, dan sesuai anggaran, sehingga menghasilkan manfaat finansial dan non-finansial. Nilai yang dihasilkan harus sejalan langsung dengan nilai-nilai yang menjadi fokus bisnis, serta harus diukur dengan cara yang menunjukkan dampak dan kontribusi investasi yang diaktifkan oleh TI dalam proses penciptaan nilai perusahaan [6].

2. Optimalisasi Risiko (*Risk Optimization*)

Hal ini mencakup manajemen risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh, dan adopsi teknologi informasi dalam organisasi. Risiko bisnis terkait dengan TI terdiri dari peristiwa terkait TI yang berpotensi mempengaruhi bisnis. Sementara penyampaian nilai berfokus pada penciptaan nilai, manajemen risiko berfokus pada preservasi nilai. Manajemen risiko terkait TI harus diintegrasikan dalam pendekatan manajemen risiko perusahaan untuk memastikan fokus pada TI oleh perusahaan. Hal itu juga harus diukur dengan cara yang

menunjukkan dampak dan kontribusi dari mengoptimalkan risiko bisnis terkait TI pada preservasi nilai [6].

3. Optimalisasi Sumber Daya (*Resources Optimization*)

Memastikan bahwa kemampuan yang tersedia untuk melaksanakan rencana strategis dan sumber daya yang cukup, tepat, serta efektif. Optimalisasi sumber daya memastikan infrastruktur TI yang terintegrasi dan ekonomis, teknologi baru yang diadopsi sesuai dengan kebutuhan bisnis, dan memperbaharui sistem yang ada.

Selain *hardware* dan *software*, sumber daya manusia juga penting dalam keberlangsungan organisasi sehingga penyediaan pelatihan, penerapan retensi, dan memastikan kapabilitas kompetensi personel kunci juga menjadi elemen penting dalam tata kelola teknologi informasi. Selain itu, elemen penting dari optimalisasi sumber daya adalah pemanfaatan data dan informasi untuk mendapatkan nilai optimal [6].

Penyelarasan strategis dan pengukuran kinerja sangat penting dan berlaku pada setiap aktivitas organisasi untuk memastikan bahwa tujuan TI sejalan dengan tujuan yang diinginkan oleh organisasi. Penerapan tata kelola teknologi informasi sendiri memberikan banyak keuntungan, seperti biaya terkait TI yang lebih rendah secara berkelanjutan, meningkatnya kapasitas inovasi terhadap TI, keselarasan terhadap investasi digital, tujuan dan strategi bisnis organisasi, meningkatkan kepercayaan bisnis terhadap TI, serta pergeseran pola pikir yang lebih baik tentang aset digital [6].

Sebaliknya, implementasi tata kelola TI yang tidak efektif memberikan hasil kinerja yang buruk terhadap penyelarasan bisnis, strategi, dan proses TI. Akibatnya, organisasi semakin sulit untuk mencapai tujuan dan strategi organisasi yang diharapkan serta mewujudkan nilai bisnis yang diinginkan dari transformasi digital [6].

2.2 Audit Teknologi Informasi

Istilah audit, menurut ISACA, merujuk pada pemeriksaan dan verifikasi formal untuk memeriksa apakah standar atau seperangkat pedoman sedang diikuti, catatan akurat, atau target efisiensi dan efektivitas terpenuhi. Audit TI dapat didefinisikan sebagai pemeriksaan formal, independen, dan objektif terhadap infrastruktur TI sebuah organisasi untuk menentukan apakah aktivitas (misalnya, prosedur, kontrol, dll.) yang terlibat dalam pengumpulan, pemrosesan, penyimpanan, distribusi, dan penggunaan informasi mematuhi pedoman, melindungi aset, mempertahankan integritas data, dan beroperasi secara efektif dan efisien untuk mencapai tujuan organisasi. Audit TI memberikan keyakinan yang wajar (tidak pernah mutlak) bahwa informasi yang dihasilkan oleh aplikasi dalam organisasi

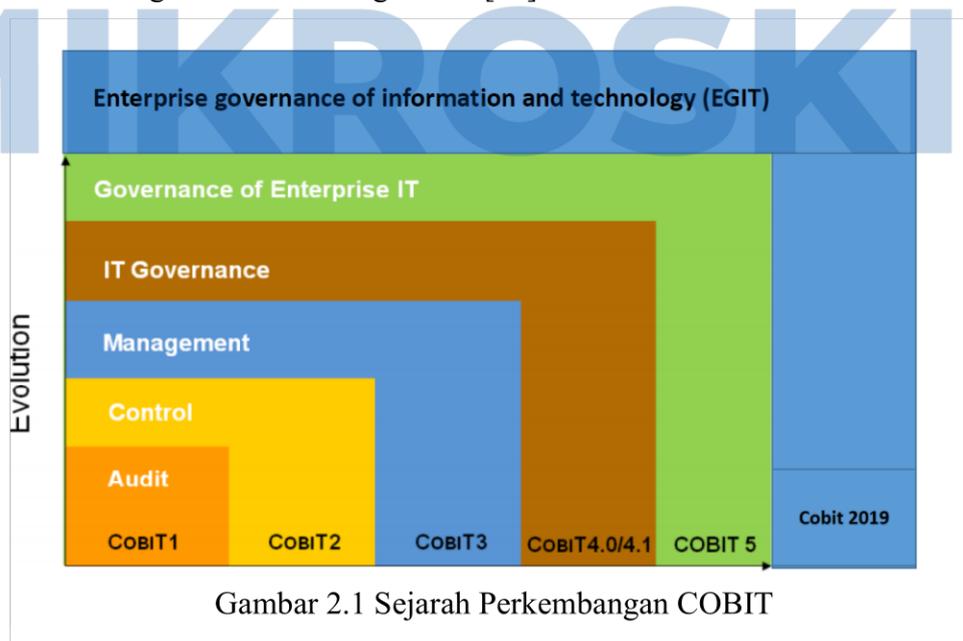
akurat, lengkap, dan mendukung pengambilan keputusan yang efektif sesuai dengan sifat dan ruang lingkup keterlibatan yang telah disepakati sebelumnya [8][2].

2.3 Penjelasan COBIT

2.3.1 Sejarah dan Perkembangan COBIT

COBIT (*Control Objectives for Information and Related Technology*) yang dikembangkan oleh ISACA (*Information System Audit and Control Association*) adalah sekumpulan dokumentasi dan panduan yang mengarahkan pada tata kelola TI dan manajemen TI yang dapat membantu auditor, manajemen dan pengguna untuk menjembatani antara risiko bisnis, kebutuhan kontrol dan permasalahan-permasalahan teknis yang ada pada organisasi [9].

Versi pertama COBIT diterbitkan pada tahun 1996 sebagai kerangka kerja untuk melaksanakan tugas audit TI, kemudian diikuti oleh versi 2 pada tahun 1998 yang menekankan tahap pengendalian. Versi 3 COBIT dirilis pada tahun 2000 dengan menekankan aspek manajemen. Versi 4 COBIT dirilis pada tahun 2005, kemudian dilanjutkan versi 4.1 pada tahun 2007 yang mengarah pada tata kelola TI sebagai penerus sebelumnya. Versi 5 COBIT dirilis pada tahun 2012 dengan menekankan sebagai kerangka kerja praktik baik yang terintegrasi untuk tata kelola dan manajemen TI, dan versi terbaru yaitu COBIT 2019 yang diterbitkan pada tahun 2018 sebagai penerus COBIT 5. COBIT 2019 merupakan pembaharuan terbesar dari pendahulunya dimana COBIT 2019 lebih fleksibel dan dapat menyesuaikan perkembangan terhadap teknologi pada saat ini dan dapat menyesuaikan dengan kebutuhan organisasi [10].



Gambar 2.1 Sejarah Perkembangan COBIT

2.4 Kerangka Kerja COBIT 2019

COBIT 2019 merupakan versi terbaru dari *framework* COBIT dan merupakan penyempurnaan dari versi sebelumnya. COBIT 2019 merupakan kerangka kerja untuk menilai tata kelola dan manajemen TI, serta berperan dalam melakukan kontrol dan memaksimalkan nilai informasi dan teknologi. Tujuannya adalah untuk membantu organisasi mencapai optimalisasi risiko, merealisasikan keuntungan, dan mencapai optimalisasi sumber daya [2].

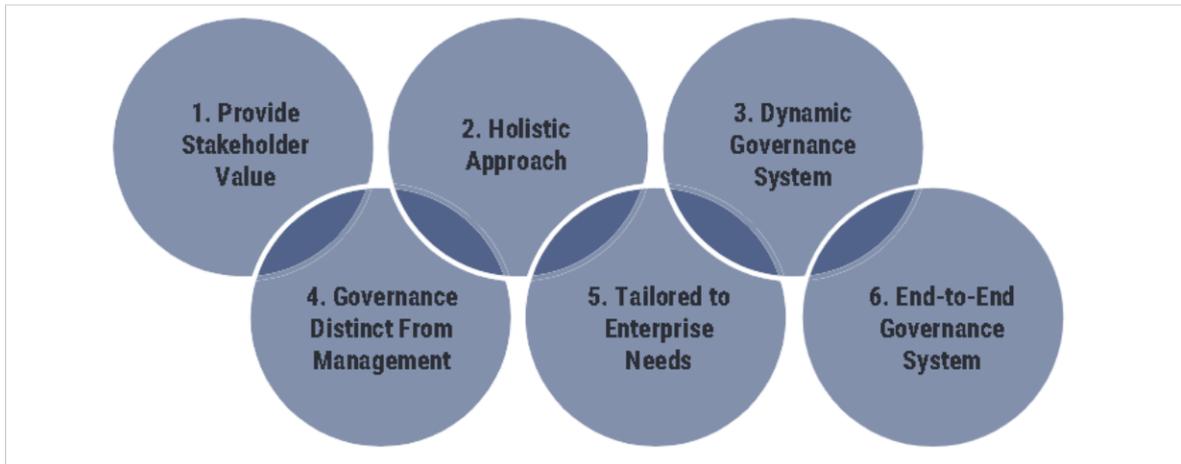
COBIT 2019 memiliki peningkatan dari versi sebelumnya dalam area berikut:

1. Fleksibilitas dan keterbukaan - Definisi dan penggunaan faktor desain memungkinkan COBIT disesuaikan untuk lebih sejalan dengan konteks pengguna tertentu. Arsitektur terbuka COBIT memungkinkan penambahan area fokus baru atau modifikasi yang ada, tanpa implikasi langsung terhadap struktur dan konten dari model inti COBIT.
2. Kebaruan dan relevansi - Model COBIT mendukung referensi dan kesejajaran dengan konsep-konsep yang berasal dari sumber lain (misalnya, standar IT dan peraturan kepatuhan terbaru).
3. Aplikasi preskriptif - Model seperti COBIT dapat bersifat deskriptif dan preskriptif. Model konseptual COBIT dibangun dan disajikan sedemikian rupa sehingga instansiasinya (yaitu, aplikasi komponen pengelolaan IT yang disesuaikan COBIT) dianggap sebagai resep untuk sistem pengelolaan IT yang disesuaikan.
4. Pengelolaan kinerja IT - Struktur model pengelolaan kinerja COBIT terintegrasi ke dalam model konseptual. Konsep-konsep kematangan dan kemampuan diperkenalkan untuk lebih sejalan dengan CMMI.
5. Panduan COBIT menggunakan istilah *Governance of Enterprise Information and Technology*, *Enterprise Governance of Information and Technology*, *Governance of IT* dan *IT Governance* secara bergantian.

2.4.1 Prinsip COBIT 2019

COBIT 2019 dikembangkan berdasarkan 2 prinsip, yaitu [6]:

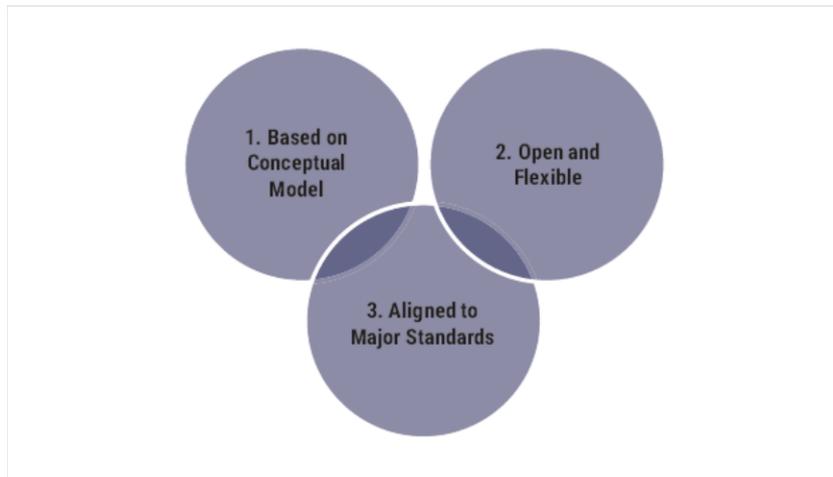
1. Prinsip-prinsip yang menjelaskan persyaratan inti dari suatu sistem tata kelola untuk informasi perusahaan dan teknologi.
2. Prinsip-prinsip untuk sebuah kerangka kerja tata kelola dapat digunakan untuk membangun sistem tata kelola perusahaan.



Gambar 2.2 Enam Prinsip Sistem Tata Kelola

Terdapat enam prinsip untuk sistem tata kelola, yaitu [6]:

1. Memberikan Nilai Bagi *Stakeholder* - Setiap perusahaan memerlukan sistem tata kelola untuk memuaskan kebutuhan *stakeholder* dan menciptakan nilai dari penggunaan TI. Nilai ini mencakup manfaat, risiko, dan sumber daya, dan perusahaan membutuhkan strategi dan sistem tata kelola yang baik untuk merealisasikan nilai tersebut [6].
2. Pendekatan Holistik - Sistem tata kelola TI untuk perusahaan harus didasarkan pada beberapa jenis komponen yang berbeda dan harus dapat bekerja secara keseluruhan [6].
3. Sistem Tata Kelola Dinamis - Sistem tata kelola harus bersifat dinamis, artinya setiap kali ada perubahan pada faktor desain, dampaknya terhadap sistem tata kelola TI harus dipertimbangkan. Pendekatan dinamis mengarah pada sistem tata kelola TI yang efektif dan terbukti di masa depan [6].
4. Tata Kelola Berbeda dari Manajemen - Sistem tata kelola harus dengan jelas membedakan antara aktivitas dan struktur tata kelola dan manajemen [6].
5. Disesuaikan dengan Kebutuhan Perusahaan - Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan, dengan menggunakan sejumlah faktor desain sebagai parameter untuk menyesuaikan dan memprioritaskan komponen sistem tata kelola [6].
6. Sistem Tata Kelola *End-to-End* - Sistem tata kelola harus mencakup seluruh perusahaan dari awal hingga akhir, tidak hanya berfokus pada fungsi TI tetapi juga pada semua teknologi dan pemrosesan informasi yang dilakukan oleh perusahaan untuk mencapai tujuannya, terlepas dari di mana pemrosesan itu berada di perusahaan [6].



Gambar 2.3 Tiga Prinsip Kerangka Kerja Tata Kelola

Terdapat tiga prinsip untuk kerangka kerja tata kelola, yaitu[1]:

1. Kerangka tata kelola sebaiknya didasarkan pada model konseptual yang mengidentifikasi komponen-komponen kunci dan hubungan antara komponen untuk memaksimalkan konsistensi dan memungkinkan otomatisasi.
2. Kerangka tata kelola sebaiknya terbuka dan fleksibel. Ini harus memungkinkan penambahan konten baru dan kemampuan untuk menangani isu-isu baru dengan cara yang paling fleksibel, sambil tetap mempertahankan integritas dan konsistensi.
3. Kerangka tata kelola sebaiknya sejalan dengan standar, kerangka kerja, dan regulasi terkait utama yang relevan.

2.4.2 Perbedaan COBIT 5 dengan 2019

Terdapat beberapa perbedaan antara *framework* COBIT 5 dengan COBIT 2019 dimana perbedaannya adalah sebagai berikut [9]:

Tabel 2.1 Perbandingan COBIT 5 dengan COBIT 2019

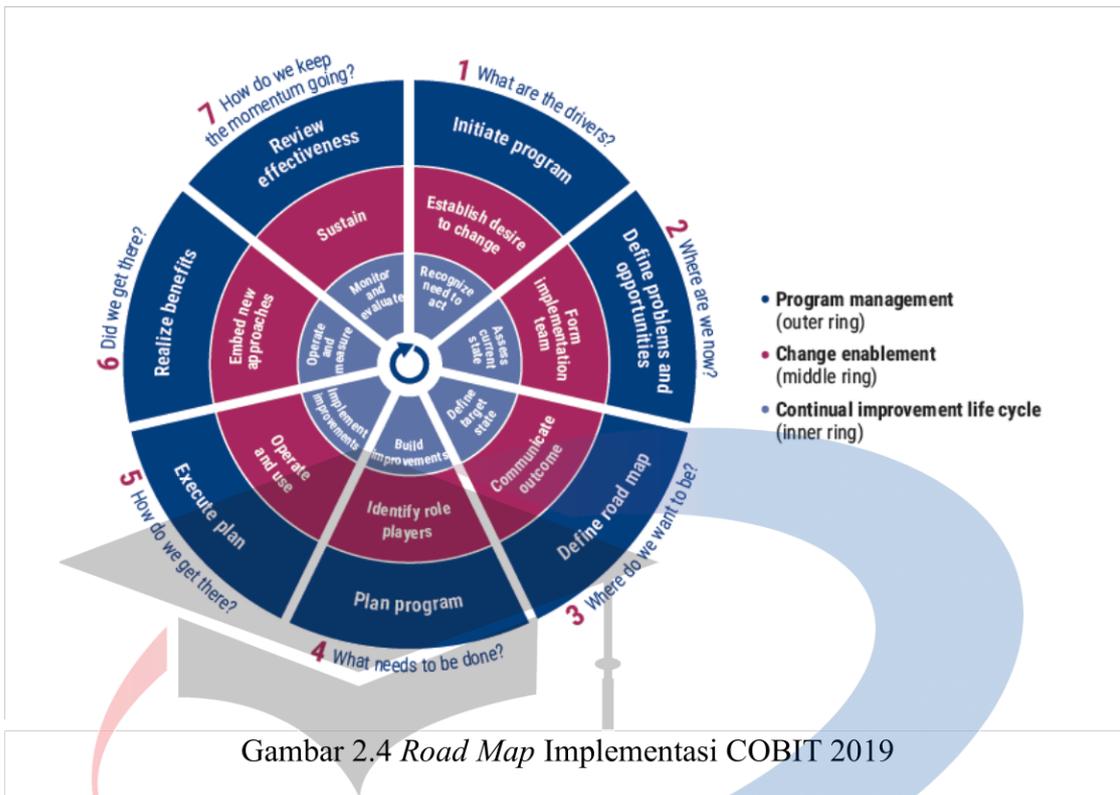
Perbandingan	COBIT 5	COBIT 2019
Gambaran	Tidak memiliki faktor desain	Memiliki faktor desain
Prinsip	Memiliki 5 prinsip	Memiliki 9 prinsip
Detail Domain Proses	Disebut proses tata kelola TI	Disebut <i>Objective</i> tata kelola TI
	Memiliki 37 domain proses	Memiliki 40 domain proses
<i>Goals Cascade</i>	Terdapat 5 <i>Goals Cascade</i>	Terdapat 4 <i>Goals Cascade</i>
Perhitungan tingkat kematangan	<i>Capability Level</i>	<i>Maturity Level</i> dan <i>Capability Level</i>
Tata kelola	<i>Enabler</i>	Komponen sistem tata kelola

Berdasarkan tabel perbandingan yang terlampir terlihat beberapa perbedaan, yaitu: pada COBIT 5 belum memiliki faktor desain, sedangkan COBIT 2019 sudah memiliki faktor desain yang dapat menyesuaikan apa yang diperlukan oleh perusahaan; prinsip-prinsip COBIT 5 lebih sederhana, sehingga memudahkan dalam implementasinya, sedangkan COBIT 2019 memiliki lebih banyak prinsip yang lebih fleksibel. Domain COBIT 5 lebih berfokus pada proses, sedangkan pada COBIT 2019 domain lebih objektif dan detail dengan beberapa tambahan, serta menekankan pada hasil yang dicapai. Tujuan COBIT 5 adalah untuk menetapkan tujuan TI setelah menetapkan tujuan perusahaan, sedangkan pada COBIT 2019 tujuan TI harus selaras terlebih dahulu dengan tujuan perusahaan. COBIT 5 menggunakan tingkat kemampuan (*capability level*) untuk mengukur kinerja, karena disesuaikan dengan ISO 15504/ISO 33000, sedangkan pada COBIT 2019, pengukuran kinerja menggunakan *maturity level* dan *key performance indicators* (KPIs). COBIT 5 memiliki 7 *enabler* yang digunakan untuk tujuan tata kelola, sedangkan COBIT 2019 menggunakan 7 komponen tata kelola [9].

Salah satu kekurangan COBIT 5 adalah kurang fleksibel dan tidak menyesuaikan dengan perkembangan zaman. Selain itu, domain proses hanya fokus pada proses itu sendiri dan tidak mempertimbangkan hasil akhir. COBIT 5 juga tidak memiliki desain faktor sebelum implementasi, yang dapat menyulitkan perusahaan untuk mengintegrasikan tata kelola dengan strategi mereka. Namun, kelebihan COBIT 5 adalah telah banyak diimplementasikan dan domain proses yang ringkas, sehingga mudah diaplikasikan [9].

Sementara itu, kekurangan COBIT 2019 termasuk jumlah domain proses yang lebih banyak, sehingga dapat menyulitkan dalam proses audit dan implementasi. COBIT 2019 juga memiliki lebih banyak prinsip yang membuatnya lebih sulit untuk diterapkan. Namun, kelebihan COBIT 2019 adalah lebih fleksibel dalam menyesuaikan dengan perubahan zaman, penekanan pada hasil yang dicapai dalam setiap domain, dan lebih lengkapnya proses dalam setiap domain. COBIT 2019 juga menyesuaikan tujuan perusahaan dan memiliki desain faktor sebelum implementasi, sehingga memudahkan perusahaan untuk mengintegrasikan tata kelola dengan strategi mereka [9].

2.4.3 Implementasi COBIT 2019



Banyak implementasi sistem tata kelola yang gagal karena tidak diinisiasikan dan dikelola dengan benar sebagai program yang memastikan manfaatnya direalisasikan. Untuk memastikan keberhasilan, program tata kelola harus didukung oleh manajemen eksekutif, dikembangkan dengan baik, dan menetapkan tujuan yang dapat dicapai. Dengan begitu, perusahaan dapat dengan mudah menyesuaikan diri dengan perubahan yang direncanakan. Oleh karena itu, manajemen program harus dianggap sebagai bagian penting dari siklus implementasi. Ada 7 fase dalam implementasi COBIT 2019, yaitu [6]:

1. Fase 1 – Apa yang menjadi pendorong? (*What are the drivers?*)
Fase 1 dari pendekatan implementasi bertujuan untuk mengidentifikasi pendorong perubahan dan menciptakan keinginan untuk berubah di level manajemen eksekutif melalui konsep dasar kasus bisnis. Pendorong perubahan bisa berupa peristiwa, kondisi, atau masalah internal atau eksternal yang merangsang perubahan. Konsep dasar bisnis harus dipantau dan dipelihara dengan disiplin untuk memastikan hasil yang sukses dari setiap inisiatif termasuk peningkatan sistem tata kelola [6].
2. Fase 2 – Dimana kita berada sekarang? (*Where are we now?*)
Fase 2 bertujuan untuk menyelaraskan tujuan terkait TI dengan strategi dan risiko perusahaan serta memprioritaskan tujuan perusahaan yang paling penting dan proses yang mendasarinya. Perusahaan harus mengidentifikasi tujuan tata kelola dan

manajemen yang kritis serta proses yang mendasarinya untuk memastikan keberhasilan. Untuk mengetahui kemampuan saat ini dan kekurangan yang mungkin ada, perlu dilakukan penilaian kemampuan proses dari status saat ini dari proses yang dipilih. Panduan Desain COBIT 2019 menyediakan faktor desain untuk membantu dalam pemilihan tujuan dan proses yang tepat [6].

3. Fase 3 – Ke mana kita ingin mencapai? (*Where do we want to be?*)

Pada Fase 3, tujuan perbaikan ditetapkan dengan menganalisis kesenjangan dan mengidentifikasi solusi potensial. Prioritas diberikan pada proyek yang mudah dicapai dan memberikan manfaat terbesar. Tugas jangka panjang dibagi menjadi bagian-bagian yang mudah dikelola [6].

4. Fase 4 – Apa yang harus dilakukan? (*What needs to be done?*)

Fase 4 melibatkan merencanakan solusi praktis dengan membuat rencana perubahan dan *business case* yang didukung [6].

5. Fase 5 – Bagaimana kita bisa mencapainya? (*How do we get there?*)

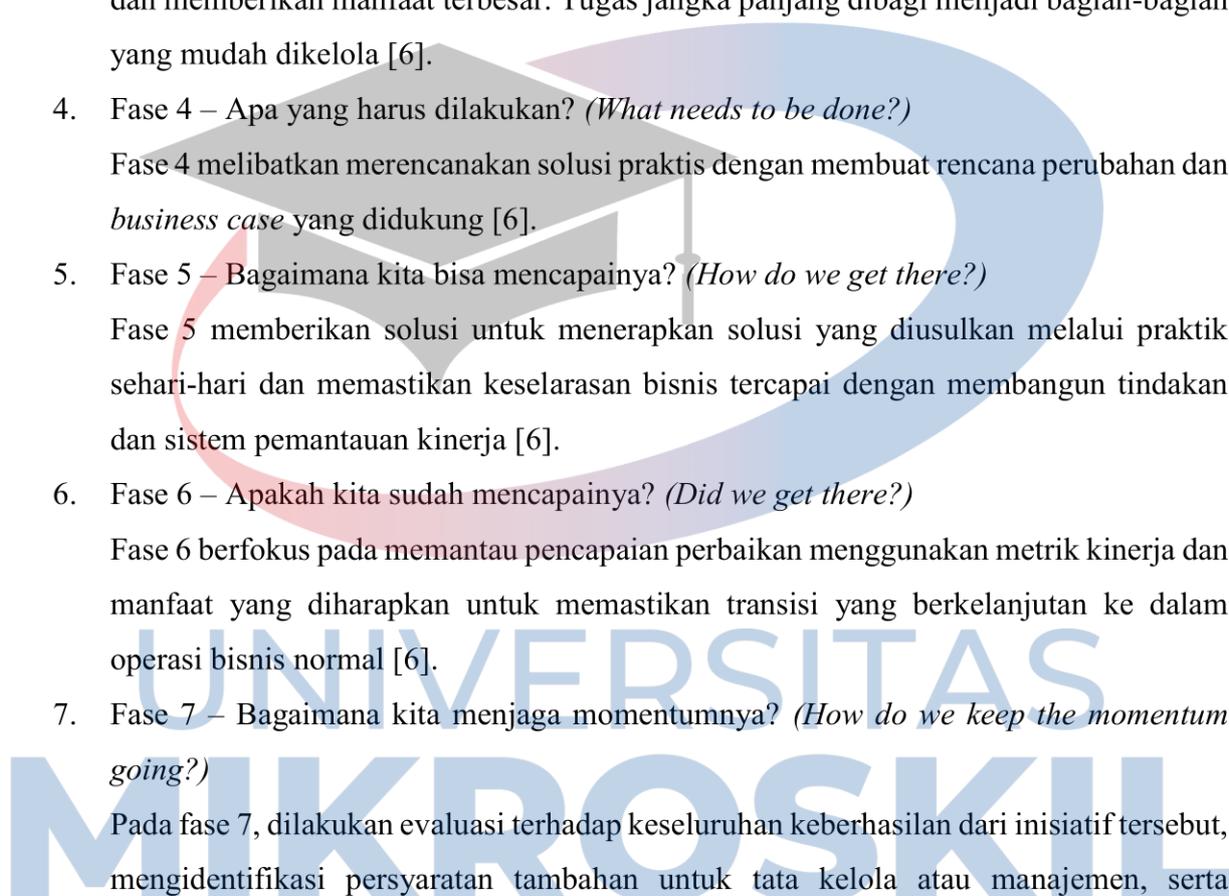
Fase 5 memberikan solusi untuk menerapkan solusi yang diusulkan melalui praktik sehari-hari dan memastikan keselarasan bisnis tercapai dengan membangun tindakan dan sistem pemantauan kinerja [6].

6. Fase 6 – Apakah kita sudah mencapainya? (*Did we get there?*)

Fase 6 berfokus pada memantau pencapaian perbaikan menggunakan metrik kinerja dan manfaat yang diharapkan untuk memastikan transisi yang berkelanjutan ke dalam operasi bisnis normal [6].

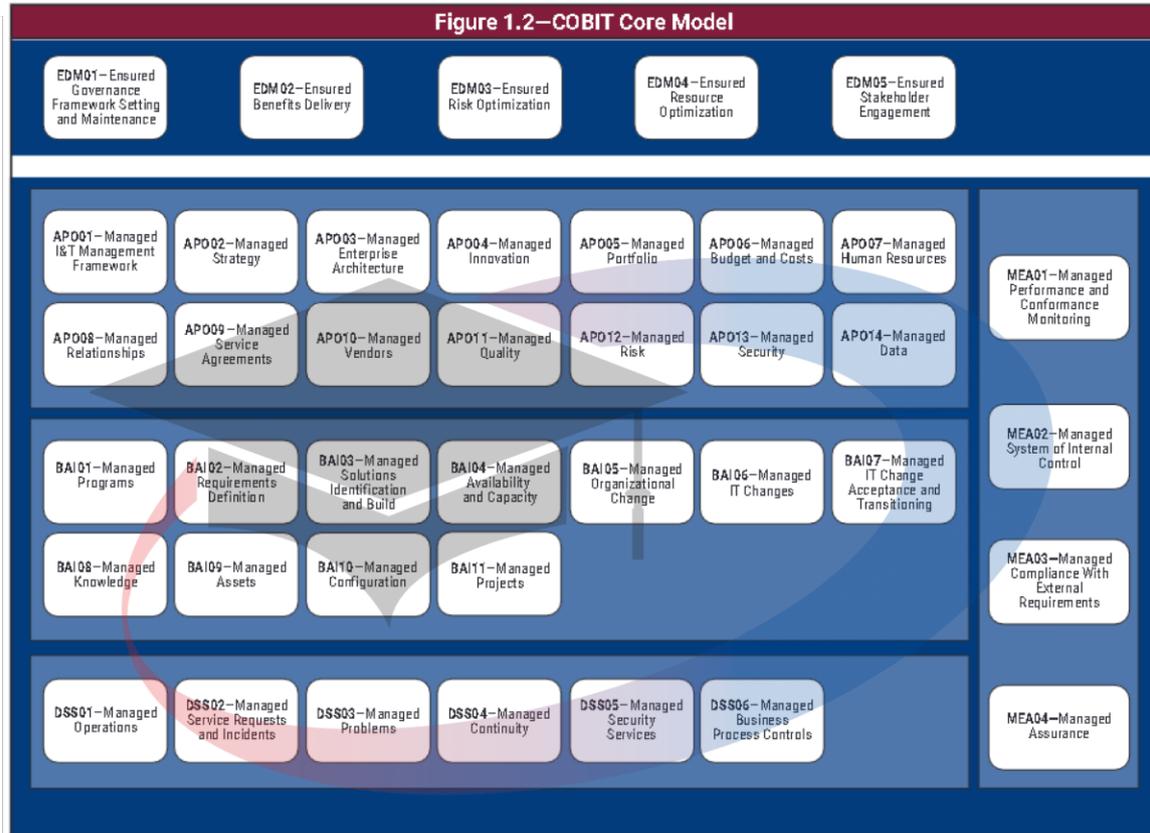
7. Fase 7 – Bagaimana kita menjaga momentumnya? (*How do we keep the momentum going?*)

Pada fase 7, dilakukan evaluasi terhadap keseluruhan keberhasilan dari inisiatif tersebut, mengidentifikasi persyaratan tambahan untuk tata kelola atau manajemen, serta memperkuat kebutuhan untuk melakukan perbaikan secara berkelanjutan. Di tahap ini juga ditekankan pada prioritas peluang tambahan untuk meningkatkan sistem tata kelola [6].



2.5 Model Referensi Proses COBIT 2019

Objektif tata kelola dan manajemen pada COBIT dikelompokkan menjadi 5 domain dan terdiri atas 40 proses. Domain-domain tersebut memiliki nama yang mendeskripsikan tujuan dan aktivitas dari domain tersebut [6].



Gambar 2.5 Domain dan Proses pada COBIT 2019

1. Tata Kelola

Dalam kategori ini terdapat domain *Evaluate, Direct and Monitor* (EDM). Aktivitas yang dilakukan dalam domain ini adalah mengevaluasi pilihan strategis yang diberikan, mengarahkan pilihan strategis yang dievaluasi dan mengawasi tercapainya strategi yang direncanakan [6]. Proses dari EDM, yaitu:

- a. EDM01 : *Ensured Governance Framework Setting and Maintenance*
- b. EDM02 : *Ensured Benefits Delivery*
- c. EDM03 : *Ensured Risk Optimization*
- d. EDM04 : *Ensured Resource Optimization*
- e. EDM05 : *Ensured Stakeholder Engagement*

2. Manajemen

Area ini dikelompokkan dalam 4 domain, yaitu [6]:

a. *Align, Plan and Organize (APO)*

Domain APO membahas secara keseluruhan organisasi, strategi dan aktivitas pendukung untuk TI. Lebih dalamnya domain ini mencakup tentang pengelolaan anggaran dan biaya, sumber daya manusia, pemasok, kualitas, inovasi, risiko, keamanan, dan data[1]. Domain APO terdiri dari 14 proses, yaitu:

- i. APO01 : *Managed I&T Management Framework*
- ii. APO02 : *Managed Strategy*
- iii. APO03 : *Managed Enterprise Architecture*
- iv. APO04 : *Managed Innovation*
- v. APO05 : *Managed Portfolio*
- vi. APO06 : *Managed Budget and Costs*
- vii. APO07 : *Managed Human Resource*
- viii. APO08 : *Managed Relationships*
- ix. APO09 : *Managed Service Agreements*
- x. APO10 : *Managed Vendors*
- xi. APO11 : *Managed Quality*
- xii. APO12 : *Managed Risk*
- xiii. APO13 : *Managed Security*
- xiv. APO14 : *Managed Data* [1].

b. *Build, Acquire and Implement (BAI)*

BAI membahas tentang pendefinisian, akuisisi, dan implementasi dari solusi dan integrasi TI dalam proses bisnis. Secara spesifik domain ini membahas tentang pengelolaan program, perubahan TI, pengetahuan, *asset*, konfigurasi, dan proyek. Domain BAI terdiri dari 11 proses, yaitu [6]:

- i. BAI01 : *Managed Programs*
- ii. BAI02 : *Managed Requirements Definition*
- iii. BAI03 : *Managed Solution Identification and Build*
- iv. BAI04 : *Managed Availability and Capacity*
- v. BAI05 : *Managed Organizational Change*
- vi. BAI06 : *Managed IT Changes*
- vii. BAI07 : *Managed IT Change Acceptance and Transitioning*
- viii. BAI08 : *Managed Knowledge*
- ix. BAI09 : *Managed Assets*

- x. BAI10 : *Managed Configuration*
- xi. BAI11 : *Managed Projects*[1].

c. *Deliver, Service and Support (DSS)*

DSS membahas tentang pemberian layanan dan dukungan TI, termasuk keamanan. Domain ini mengacu pada pengelolaan operasional. masalah, kontinuitas, layanan keamanan, dan pengendalian proses bisnis. Domain DSS terdiri dari 6 proses, yaitu [6]:

- i. DSS01 : *Managed Operations*
- ii. DSS02 : *Managed Service Requests and Incidents*
- iii. DSS03 : *Managed Problems*
- iv. DSS04 : *Managed Continuity*
- v. DSS05 : *Managed Security Services*
- vi. DSS06 : *Managed Business Process Controls*[1].

d. *Monitor, Evaluate and Assess (MEA)*

MEA membahas tentang monitoring kinerja, kesesuaian TI dengan target kinerja internal, kebutuhan pengendalian objektif internal dan eksternal. Lebih lanjutnya domain ini berbicara tentang manajemen kinerja, pengendalian sistem internal, kepatuhan terhadap peraturan, dan jaminan. Domain MEA terdiri dari 4 proses, yaitu [6]:

- i. MEA01 : *Managed Performance and Conformance Monitoring*
- ii. MEA02 : *Managed System of Internal Control*
- iii. MEA03 : *Managed Compliance with External Requirements*
- iv. MEA04 : *Managed Assurance.*

2.6 Penentuan Domain Proses COBIT 2019

2.6.2 Pemetaan *Goals Cascade*

Goals Cascade pada COBIT 2019 telah diperbaharui dari versi sebelumnya, dimana kali ini *goals cascade* nya mendukung terjemahan tujuan perusahaan menjadi prioritas untuk tujuan keselarasan.



Gambar 2.6 *Goal Cascade*

Berikut penjelasan mengenai *Goals Cascade* COBIT 2019[1]:

1. *Stakeholder Drivers and Needs cascade to Enterprise Goals*

Menurut ISACA, tata kelola teknologi informasi bertujuan untuk memenuhi kebutuhan *stakeholders* dan menciptakan nilai dari penerapan teknologi informasi pada organisasi. *Goals Cascade* COBIT menunjukkan bagaimana pencapaian tujuan tata kelola dan manajemen berkontribusi untuk memenuhi kebutuhan pemangku kepentingan. Pada bagian ini kebutuhan *stakeholder* harus diubah dan diselaraskan menjadi strategi perusahaan yang dapat ditindak lanjuti. Penyelarasan ini sangat penting untuk menciptakan nilai dan memenuhi kebutuhan *stakeholder*. Dikarenakan banyak *stakeholder* dan "penciptaan nilai", pastinya akan banyak setiap nilai yang dihasilkan berbeda atau bahkan bertentangan pada masing-masing *stakeholder*. Tujuan perusahaan

ini dikembangkan dengan menggunakan *Balanced Scorecard (BSC)* 1 dimensi yang mewakili daftar tujuan umum yang dapat didefinisikan oleh perusahaan [6].

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Gambar 2.7 Enterprise Goals

2. Enterprise Goals cascade to Alignment Goals

		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 2.8 Enterprise Goals to Alignment Goals

Setelah kebutuhan *stakeholder* diselaraskan dengan tujuan perusahaan maka selanjutnya adalah melakukan kaskade ke *alignment goals*. COBIT 2019 menyediakan tabel panduan yang berisikan daftar generik *enterprise goals*, *alignment goals*, dan hubungannya. Hubungan ini didefinisikan dengan menentukan tujuan penyaluran mana yang berkontribusi dengan cara primer dan sekunder ke pencapaian tujuan perusahaan [6].

3. Alignment Goals cascade to Governance and Management Objectives

Tahapan ini merupakan tahapan yang diperbaharui dari COBIT 5, bertujuan untuk menghindari kesalahpahaman yang sering terjadi dimana perusahaan yang telah dipetakan sebelumnya hanya murni menunjukkan departemen TI saja. Untuk kaskade ini, digunakan hasil pemetaan dari tahap sebelumnya dengan menentukan keterkaitannya dengan cara primer dan sekunder [6].

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
AP001	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
AP002	Managed strategy			S		S	S		P				S	S
AP003	Managed enterprise architecture			S		S	P	S	P					
AP004	Managed innovation			S			P		S				S	P
AP005	Managed portfolio			P		P	S		S	S				
AP006	Managed budget and costs			S	P					P	S			
AP007	Managed human resources			S		S				S			P	P
AP008	Managed relationships			S		P	P		S	S			P	P
AP009	Managed service agreements					P			S					
AP010	Managed vendors					P	S			S				
AP011	Managed quality			S	S	S				P	P			
AP012	Managed risk		P					P						
AP013	Managed security	S	S					P						
AP014	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

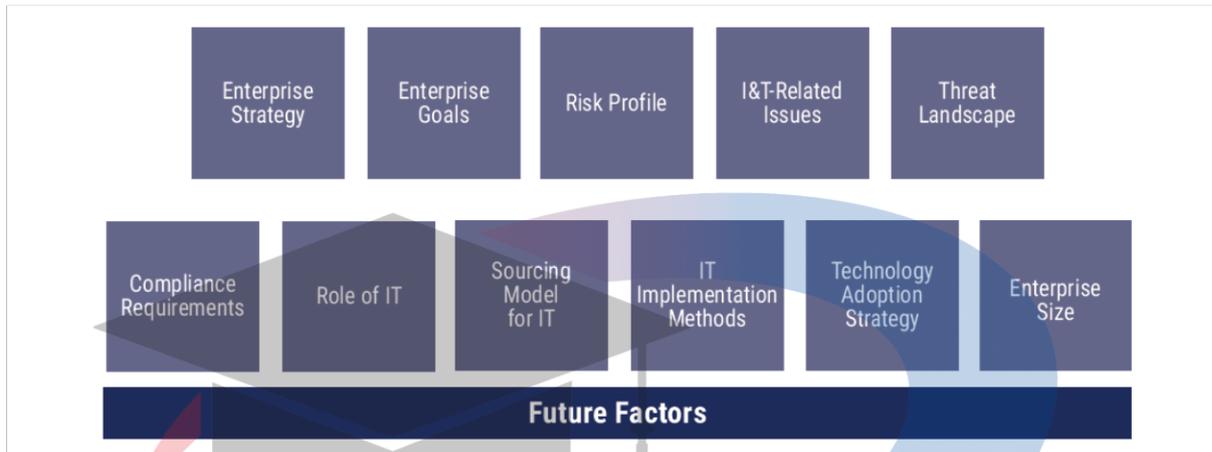
Gambar 2.9 Alignment Goals to Governance and Management Objectives

Untuk keterangannya adalah sebagai berikut:

- Primary*: memiliki hubungan penting dan merupakan pendorong utama untuk mencapai tujuan yang berhubungan dengan TI. *Primary* adalah aktivitas yang harus dilakukan

- b. *Secondary*: masih memiliki hubungan yang kuat namun tidak terlalu menjadi prioritas. Karena perannya sebagai pendukung sekunder sehingga aktivitas ini bisa dilakukan ataupun tidak [6].

2.6.2 Design Factor COBIT 2019



Gambar 2.10 Design Factor

Faktor desain adalah faktor-faktor yang dapat mempengaruhi desain sistem tata kelola perusahaan dan memosisikannya untuk sukses dalam TI. Terdapat sebelas faktor desain yang dipertimbangkan yaitu [6]:

1. *Enterprise Strategy* – Sebuah perusahaan dapat memiliki beberapa strategi dalam mencapai tujuannya, yaitu: 1. Fokus pada Pertumbuhan (*Growth/Acquisition*); 2. Fokus pada Inovasi (*Innovation/Differentiation*); 3. Fokus pada minimalisasi biaya dalam jangka pendek (*Cost Leadership*); 4. Fokus pada Pelayanan klien yang stabil (*Client Service/Stability*). Ukuran penilaian yang digunakan dalam faktor desain ini adalah 1. Tidak Penting; 2. Cukup Penting; 3. Penting; 4. Sangat Penting; 5. Paling Penting [11].
2. *Enterprise Goals* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi tujuan perusahaan yang ingin dicapai. COBIT 2019 menetapkan 13 tujuan perusahaan secara umum. Tujuan perusahaan harus selaras dengan strategi perusahaan. Terkait tujuan yang dipilih, *stakeholder* harus membuat pilihan dengan alasan yang jelas untuk dapat diterapkan pada tata kelola TI [11].
3. *IT Risk Profile* – COBIT 2019 menyediakan 19 kategori skenario risiko, untuk menganalisis risiko tingkat tinggi dan identifikasi risiko yang terkait pada perusahaan. Dalam penilaian untuk profil risiko, ada 2 penilaian yaitu penilaian dampak (*risk*

impact) dengan penilaian, yaitu: 1. *Very Low*; 2. *Low*; 3. *Medium*; 4. *High*; 5. *Very High*, dan penilaian peluang terjadi (*likelihood*) dengan penilaian, yaitu: 1. *Rare* (1%-20%); 2. *Unlikely* (21%-40%); 3. *Possible* (41%-60%); 4. *Likely* (61%-80%); 5. *Almost* (81%-100%) [11].

4. *I&T Related Issues* – Pada tahap ini terdapat 20 permasalahan terkait TI yang didaftarkan oleh COBIT 2019. Tahapan faktor desain ini merupakan tahap untuk mengidentifikasi masalah perusahaan terkait TI [11].
5. *Threat Landscape* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi ancaman yang berpotensi dialami perusahaan. Penilaian pada faktor desain ini dinilai antara 0% dan 100% dan jumlah keseluruhan nilai harus 100% [11].
6. *Compliance Requirements* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi kebutuhan kepatuhan yang perlu dipenuhi oleh perusahaan. Penilaian pada faktor desain ini dinilai antara 0% dan 100% dan jumlah keseluruhan nilai harus 100% [11].
7. *Role of IT* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi peran IT dalam perusahaan. Peran TI disini dibagi menjadi 3, yaitu *strategic*, *support*, dan *factory*. Tingkat penilaian dalam faktor desain ini adalah: 1. *Tidak penting*; 2. *Cukup penting*; 3. *Penting*; 4. *Sangat penting*; 5. *Paling penting*[3].
8. *Sourcing Model of IT* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi sumber model TI yang diterapkan oleh perusahaan. Model TI yang biasanya diterapkan seperti *outsourcing*, *cloud*, *insourced*, dan *hybrid*. Penilaian pada faktor desain ini dinilai antara 0% dan 100% dan jumlah keseluruhan nilai harus 100% [11].
9. *IT Implementation Methods* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi metode implementasi TI yang diterapkan perusahaan. Beberapa tipe model implementasi TI seperti *Agile*, *DevOps*, *Traditional*, dan *Hybrid*. Penilaian pada faktor desain ini dinilai antara 0% dan 100% dan jumlah keseluruhan nilai harus 100% [11].
10. *Technology Adoption Strategy* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi strategi yang digunakan perusahaan dalam mengadopsi TI seperti, *first mover*: perusahaan selalu ingin mengadopsi teknologi baru secepat mungkin; *follower*: perusahaan menerapkan teknologi setelah perusahaan lain terlebih dahulu menerapkannya; dan *slow adopter*: perusahaan sangat lambat dalam mengadopsi

teknologi tersebut. Penilaian pada faktor desain ini dinilai antara 0% dan 100% dan jumlah keseluruhan nilai harus 100% [11].

11. *Enterprise Size* – Tahapan faktor desain ini bertujuan untuk mengidentifikasi ukuran perusahaan berdasarkan jumlah karyawan dari perusahaan tersebut [11].

Dengan adanya faktor desain COBIT 2019, perusahaan dapat lebih fokus dalam menentukan strategi, lebih fleksibel dalam menciptakan solusi tata kelola yang efisien dan dapat memberikan rekomendasi terhadap perusahaan dalam mengatur tata Kelola TI.

2.7 COBIT Performance Management (CPM)

Manajemen kinerja merupakan bagian yang sangat penting dalam sistem tata kelola dan manajemen. Manajemen kinerja mencakup semua aktivitas dan metode yang berhubungan dengan cara kerja sistem tata kelola dan manajemen serta seluruh komponen perusahaan, dan bagaimana cara meningkatkan kinerjanya untuk mencapai hasil yang diinginkan. COBIT menggunakan istilah *COBIT Performance Management (CPM)* yang merupakan bagian yang tidak dapat terpisahkan dari *framework* COBIT[4]. CPM mencakup *capability level* dan *maturity level*. Prinsip CPM sendiri didasarkan pada prinsip-prinsip berikut [6]:

1. CPM harus sederhana, mudah dipahami dan digunakan.
2. CPM harus konsisten dalam mendukung model konseptual COBIT.
3. CPM harus memungkinkan manajemen kinerja terhadap semua komponen sistem tata kelola.
4. CPM harus memberikan hasil yang dapat diandalkan, dapat diulang, dan relevan.
5. CPM harus fleksibel sehingga dapat mendukung persyaratan dari berbagai organisasi dengan prioritas dan kebutuhan yang berbeda.
6. CPM harus mendukung berbagai jenis evaluasi maupun penelitian.

Pada COBIT 5 sebelumnya proses ini dikenal sebagai proses model *capability* yang berdasarkan pada ISO/IEC 15540 (saat ini menjadi ISO/IEC 33000). Dalam versi COBIT sebelumnya, *capability level* yang dinilai hanyalah bagian proses. Namun pada CPM COBIT 2019 menggunakan rujukan CMMI (*Capability Maturity Model Integration*) versi 2.0 yang mana terdapat 2 jenis penilaian yaitu *capability* (berhubungan dengan *process area*) dan *maturity* (berhubungan dengan kemampuan pada proses area yang ada). Model CMMI digunakan sebagai kerangka kerja untuk menilai proses *maturity level*. Dalam *capability* dan

maturity apabila tingkatan yang ditunjukkan semakin tinggi *level* yang dicapai, maka semakin baik [6].

Ada beberapa penyesuaian terhadap proses CPM dari COBIT 5 ke COBIT 2019:

1. Hasil proses sekarang terhubung satu-ke-satu dengan praktik proses.
2. *Base Practice* pada COBIT 5 sama dengan COBIT 2019 untuk setiap tujuan tata kelola dan manajemen.
3. *Work Product* pada COBIT 5 mengalami perubahan menjadi *Information Flow and Item* dibawah komponen C pada setiap tujuan tata kelola atau manajemen [6].

2.8 Fokus Area Audit Tata Kelola TI pada Organisasi

Penentuan domain dilakukan berdasarkan identifikasi kebutuhan *stakeholder* dan permasalahan yang ada pada organisasi. Tujuannya agar proses audit yang dilakukan dapat memberikan hasil yang efisien dan tepat sasaran.

2.8.1 Proses Mendapatkan Domain Audit Tata Kelola TI

Proses penentuan ruang lingkup pada penelitian ini merujuk pada COBIT 2019 yaitu menggunakan *goals cascade* dan *design factor*. Untuk mendapatkan domain proses yang akan digunakan, dilakukan beberapa aktivitas sebagai berikut:

1. Melakukan *pra-riset* pada awalnya untuk mengetahui kondisi terkini terkait tata kelola Universitas Mikroskil. Kegiatan ini pada awalnya dilakukan dengan wawancara terhadap *stakeholder*. Kemudian dilanjutkan menyebarkan kuesioner terhadap beberapa *stakeholder* Universitas Mikroskil untuk mengumpulkan informasi yang dibutuhkan. Kuesioner yang berhasil dikumpulkan kemudian diolah kembali dan dianalisa untuk proses berikutnya.
2. Berdasarkan hasil analisis dari kuesioner dan wawancara yang telah dikumpulkan dan dirangkum, dilakukan tahap pemetaan (*mapping*) menggunakan *goals cascade* COBIT 2019. Tahap pertama yang dilakukan adalah mengidentifikasi kebutuhan *stakeholder*. Kebutuhan *stakeholder* berhubungan dengan *enterprise goals*. Hasil selanjutnya dipetakan ke *alignment goals* kemudian melakukan identifikasi *design factor*.
3. Hasil *mapping* kemudian disesuaikan kembali menggunakan tahapan *design factor*. Tujuan penentuan faktor desain adalah untuk mengetahui proses mana yang memiliki prioritas lebih baik dalam organisasi atau pengaruh yang berpotensi muncul jika proses tersebut tidak ditindaklanjuti secepatnya. Pengambilan data pada *design factor* mengacu pada *Design Toolkit* yang telah disediakan oleh ISACA untuk COBIT 2019.

4. Dari keseluruhan 40 proses yang ada dalam COBIT 2019 terpilih proses domain APO12 yang memiliki nilai prioritas yang tinggi dan sesuai dengan kebutuhan organisasi.
5. Setelah didapatkan objektif tata kelola dari proses sebelumnya, dilakukan kembali konfirmasi terhadap *stakeholder* untuk mengetahui proses mana yang paling sesuai dengan kebutuhan organisasi dan *stakeholder* serta proses tersedia saat dievaluasi nantinya. Yang menjadi fokus utama adalah domain proses APO12 (*Managed Risk*) karena paling sesuai dengan kebutuhan organisasi dan *stakeholder* saat ini.

2.8.2 Manajemen Risiko

Ketidakmampuan dalam mengelola risiko dapat membawa biaya yang sangat besar. Akhir-akhir ini, bisnis telah mengalami banyak kejadian yang berhubungan dengan risiko yang mengakibatkan kerugian finansial yang besar, penurunan nilai pemegang saham, kerusakan pada reputasi organisasi, pemecatan manajemen senior, dan dalam beberapa kasus terburuk terjadi pembubaran bisnis. Lingkungan yang semakin berisiko ini mendorong manajemen agar dapat mengadopsi perspektif yang lebih proaktif dalam pengelolaan risiko.

Manajemen risiko berperan untuk memastikan bahwa kerugian tidak menghalangi manajemen organisasi untuk mencapai tujuannya dalam menjaga aset serta mewujudkan nilai yang diharapkan dari investasi. *Special Publication (SP) 800-30** dari *The National Institute of Standards and Technology (NIST)* mendefinisikan manajemen risiko sebagai proses mengidentifikasi dan menilai risiko, diikuti dengan menerapkan prosedur yang diperlukan untuk mengurangi risiko tersebut menjadi tingkat yang dapat diterima. Manajemen risiko memiliki peran penting dalam melindungi informasi organisasi dari ancaman TI. Proses manajemen risiko TI yang dirancang dengan baik sangat penting untuk mengembangkan program keamanan yang berhasil melindungi aset TI suatu organisasi. Ketika digunakan secara efektif, metodologi manajemen risiko yang terstruktur dengan baik akan membantu manajemen organisasi dalam mengidentifikasi kontrol yang memadai untuk mendukung sistem TI mereka [8].

Terdapat empat langkah dalam manajemen risiko perusahaan yang efektif, diantaranya:

1. Penilaian dan perencanaan risiko
2. Identifikasi dan analisis risiko
3. Memanfaatkan dan mengembangkan strategi respons risiko
4. Pemantauan risiko [8]

Manajemen risiko harus menciptakan nilai dan menjadi bagian integral dari proses organisasi. Juga harus menjadi bagian dari proses pengambilan keputusan dan disesuaikan secara sistematis dan terstruktur untuk secara eksplisit mengatasi ketidakpastian yang dihadapi oleh perusahaan berdasarkan informasi terbaik yang tersedia. Selain itu, proses manajemen risiko harus dinamis, iteratif, dan responsif terhadap perubahan dengan kemampuan perbaikan dan peningkatan [8].

2.8.3 APO12 - *Management Risk*

Deskripsi dari domain APO12 adalah terus mengidentifikasi, menilai, dan mengurangi risiko terkait TI dalam batas toleransi yang ditetapkan oleh manajemen eksekutif perusahaan. Tujuan dari APO12 ini adalah mengintegrasikan pengelolaan risiko perusahaan yang terkait dengan TI dengan ERM secara keseluruhan, perusahaan dapat memastikan bahwa semua risiko diidentifikasi, dinilai, dan dikelola dengan tepat, dan bahwa sumber daya dialokasikan dengan cara yang mengoptimalkan upaya pengelolaan risiko [12].

Subdomain pada domain ini adalah sebagai berikut:

1. APO12.01 – Pengumpulan Data (*Collect data*)

Praktik pada proses ini adalah mengidentifikasi dan mengumpulkan data yang relevan untuk memungkinkan identifikasi, analisis, dan pelaporan risiko terkait TI yang efektif [12].

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut:

- a. Menetapkan dan menjaga metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI.
- b. Merekam data terkait risiko TI yang relevan dan signifikan pada lingkungan operasional internal dan eksternal perusahaan.
- c. Mengadopsi atau menentukan taksonomi risiko untuk definisi yang konsisten dari skenario risiko dan kategori dampak dan kemungkinan.
- d. Merekam data pada peristiwa risiko yang telah atau mungkin menyebabkan dampak bisnis sesuai dengan kategori dampak yang didefinisikan dalam taksonomi risiko. Menangkap data yang relevan dari isu terkait, insiden, masalah, dan investigasi terkait.
- e. Meninjau dan menganalisis data risiko TI historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui catatan peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.

- f. Untuk kelas peristiwa yang serupa, mengelola data yang terkumpul dan menyoroti faktor-faktor yang berkontribusi. Menentukan faktor kontribusi yang umum di beberapa peristiwa.
- g. Menentukan kondisi khusus yang ada atau tidak ada ketika peristiwa risiko terjadi dan cara kondisi tersebut mempengaruhi frekuensi peristiwa dan besarnya kerugian.
- h. Melakukan analisis peristiwa dan faktor risiko secara berkala untuk mengidentifikasi isu risiko baru atau muncul dan untuk memahami faktor risiko internal dan eksternal yang terkait.

2. APO12.02 – Analisis Risiko (*Analyze Risk*)

Praktik pada proses ini adalah mengembangkan pandangan yang dapat diperkuat tentang risiko TI yang sebenarnya memerlukan pemahaman yang komprehensif tentang lingkungan TI perusahaan, termasuk aset, kerentanan, ancaman, dan kontrolnya.

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut [12]:

- a. Tentukan ruang lingkup yang tepat untuk upaya analisis risiko, mempertimbangkan semua faktor risiko dan/atau kritisnya aset bisnis.
- b. Bangun dan secara teratur memperbarui skenario risiko TI; paparan kerugian terkait TI; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis ancaman dan peristiwa yang saling terkait atau bersamaan. Kembangkan harapan untuk aktivitas pengendalian dan kemampuan untuk mendeteksinya.
- c. Estimasi frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Pertimbangkan semua faktor risiko yang berlaku dan evaluasi pengendalian operasional yang diketahui.
- d. Bandingkan risiko saat ini (paparan kerugian terkait TI) dengan nafsu risiko dan toleransi risiko yang dapat diterima. Identifikasi risiko yang tidak dapat diterima atau meningkat.
- e. Usulkan tanggapan risiko untuk risiko yang melebihi tingkat nafsu risiko dan toleransi yang dapat diterima.
- f. Tentukan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan tanggapan risiko yang dipilih. Identifikasi persyaratan dan harapan untuk pengendalian kunci yang sesuai untuk respons mitigasi risiko.
- g. Validasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Konfirmasi bahwa analisis sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan baik dan diperiksa untuk bias.

- h. Analisis biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/mitigasi, mentransfer, dan menerima dan memanfaatkannya. Konfirmasi respons risiko optimal.

3. APO12.03 – Mempertahankan Profil Risiko (*Maintain a Risk Profile*)

Praktik pada proses ini adalah memelihara daftar risiko dan atribut risiko yang diketahui, termasuk frekuensi yang diharapkan, dampak potensial, dan respon yang diberikan. Dokumentasikan sumber daya terkait, kemampuan, dan aktivitas pengendalian saat ini yang terkait dengan item risiko.

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut [12]:

- a. Menyusun daftar proses bisnis dan mendokumentasikan ketergantungan mereka pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual kritis, *vendor*, pemasok, dan penyedia layanan luar.
- b. Tentukan dan sepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk menjaga operasi proses bisnis. Analisis ketergantungan dan identifikasi titik lemah.
- c. Gabungkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.
- d. Secara teratur, tangkap semua informasi profil risiko dan konsolidasikan ke dalam profil risiko yang teragregasi.
- e. Tangkap informasi tentang status rencana tindakan risiko untuk dimasukkan ke dalam profil risiko TI perusahaan.
- f. Berdasarkan semua data profil risiko, tentukan satu set indikator risiko yang memungkinkan identifikasi dan pemantauan cepat dari risiko saat ini dan tren risiko.
- g. Tangkap informasi tentang kejadian risiko TI yang telah terjadi untuk dimasukkan ke dalam profil risiko TI perusahaan.

4. APO12.04 – Artikulasi Risiko (*Articulate Risk*)

Mengkomunikasikan informasi tentang keadaan terkini dari paparan dan peluang yang berkaitan dengan teknologi informasi dan telekomunikasi dengan tepat waktu kepada semua pemangku kepentingan yang diperlukan agar dapat memberikan respons yang sesuai.

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut[6]:

- a. Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat kepercayaan, untuk memungkinkan manajemen menyeimbangkan risiko dan pengembalian.
 - b. Memberikan pemimpin keputusan pemahaman tentang skenario terburuk dan skenario yang paling mungkin, paparan kerugian yang berkaitan dengan TI, dan pertimbangan reputasi, hukum, dan regulasi yang signifikan, atau kategori dampak lainnya sesuai dengan taksonomi risiko.
 - c. Melaporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas kontrol, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya pada profil risiko.
 - d. Secara periodik, untuk area dengan risiko relatif dan kapasitas risiko yang seimbang, identifikasi peluang yang berkaitan dengan TI yang akan memungkinkan penerimaan risiko yang lebih besar dan pertumbuhan dan pengembalian yang lebih baik.
 - e. Tinjau hasil penilaian pihak ketiga objektif dan tinjauan audit internal dan jaminan kualitas. Sertakan hasilnya dalam profil risiko. Tinjau kesenjangan yang diidentifikasi dan paparan kerugian yang berkaitan dengan TI untuk menentukan kebutuhan untuk analisis risiko tambahan.
5. APO12.05 – Mendefinisikan Portofolio Tindakan Manajemen Risiko (*Define a Risk Management Portfolio*)

Mengelola peluang untuk mengurangi risiko menjadi tingkat yang dapat diterima sebagai sebuah portofolio. Hal ini dapat dicapai dengan mengidentifikasi, mengevaluasi, dan memprioritaskan peluang yang ada dan mengelolanya sebagai suatu kesatuan yang terintegrasi.

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut [12]:

- a. Menjaga daftar kegiatan pengendalian yang diterapkan untuk memitigasi risiko dan yang memungkinkan risiko diambil sesuai dengan toleransi dan nafsu risiko. Mengklasifikasikan kegiatan pengendalian dan memetakan ke skenario risiko TI spesifik dan agregasi dari skenario risiko TI.

- b. Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individual dan portofolio mereka.
 - c. Mendefinisikan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang strategis bagi perusahaan, dengan mempertimbangkan biaya, manfaat, efek pada profil risiko saat ini, dan peraturan yang berlaku.
6. APO12.06 – Merespon Risiko (*Respond to Risk*)

Menanggapi kejadian risiko yang terjadi dengan cepat dengan tindakan yang efektif untuk membatasi besarnya kerugian.

Adapun aktivitas yang dilakukan pada subdomain ini adalah sebagai berikut [12]:

- a. Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah khusus yang harus diambil ketika kejadian risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.
- b. Mengaplikasikan rencana respons yang tepat untuk meminimalkan dampak ketika kejadian risiko terjadi.
- c. Mengategorikan insiden dan membandingkan paparan kerugian yang terkait dengan TI terhadap ambang toleransi risiko. Berkomunikasi mengenai dampak bisnis kepada para pembuat keputusan sebagai bagian dari pelaporan dan memperbarui profil risiko.
- d. Meninjau kembali peristiwa/kerugian buruk di masa lalu dan kesempatan yang terlewatkan dan menentukan penyebab akar masalah.
- e. Berkomunikasi mengenai penyebab akar masalah, persyaratan respon risiko tambahan, dan perbaikan proses kepada para pembuat keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses termasuk dalam proses tata kelola risiko.

2.9 RACI (*Responsible, Accountable, Consulted, Informed*)

RACI *Chart* merupakan sebuah tabel yang berisi responden yang tepat pada masing-masing domain. RACI *Chart* menjelaskan tugas dan tingkat tanggung jawab yang disarankan untuk praktik proses pada peran dan struktur yang berbeda pada kerangka kerja COBIT 2019 [6].

RACI Chart terdiri dari beberapa bagian yang memiliki peran yang berbeda, yaitu:

1. R – *Responsible*: Bagian ini mengambil peran utama dalam memenuhi daftar sehingga menciptakan hasil yang diinginkan.
2. A – *Accountable*: Bagian ini menetapkan akuntabilitas keseluruhan peran lain sehingga tugas dapat diselesaikan. Peran ini dapat dimintai pertanggungjawaban.
3. C – *Consulted*: Bagian ini berperan dalam memberikan masukan atau saran.
4. I – *Informed*: Bagian ini berperan dalam memperoleh informasi tentang pencapaian dan/atau kiriman tugas.

B. Component: Organizational Structures																	
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
Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference																
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 1); Appendix A: Roles and Responsibilities																

Gambar 2.11 Tabel RACI

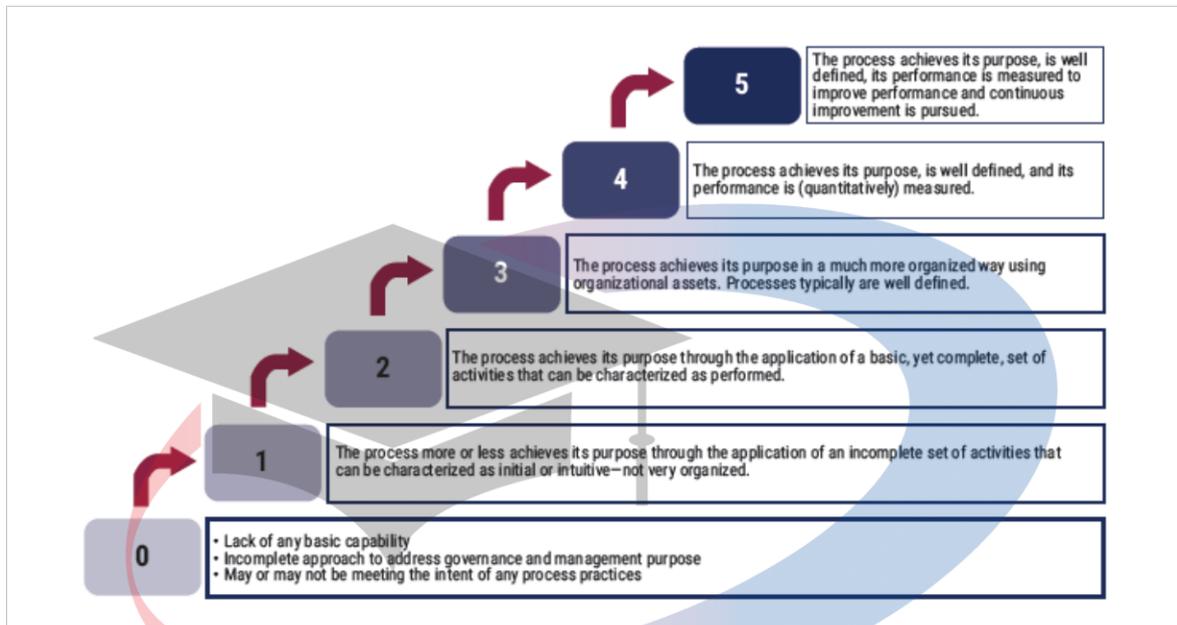
RACI Chart di atas menggambarkan aktivitas yang akan dilakukan setiap bagian yang terlibat. *Key Management Practice* (KPM) menyebutkan aktivitas apa saja yang berlangsung pada setiap domain COBIT 2019. Penjelasan mengenai struktur organisasi berdasarkan RACI Chart COBIT 2019 dijelaskan sebagai berikut:

1. *Chief Risk Officer* (CRO), merupakan jabatan tertinggi yang bertanggung jawab atas semua aspek manajemen total perusahaan.
2. *Chief Information Officer* (CIO), adalah jabatan yang bertanggung jawab dalam menyelaraskan TI dan strategi bisnis, serta bertanggung jawab dalam setiap aspek manajemen risiko pada perusahaan.
3. *Chief Technology Officer* (CTO), jabatan ini yang bertanggung jawab dalam setiap aspek teknis TI, termasuk di dalamnya mengelola dan memantau keputusan terkait dengan layanan TI, solusi dan infrastruktur.

4. *Chief Digital Officer (CDO)*, adalah jabatan yang berfokus pada mendorong pertumbuhan di perusahaan menggunakan informasi digital dan teknologi dalam menciptakan nilai bisnis perusahaan.
5. *Enterprise Risk Committee (ERC)*, merupakan jabatan yang bertanggung jawab untuk membantu *Board of Directors* dalam memenuhi tanggung jawabnya untuk mengawasi kualitas dan integritas praktik manajemen risiko perusahaan.
6. *Chief Information Security Officer (CISO)*, adalah jabatan yang mengawasi keamanan informasi, dunia maya, dan teknologi organisasi termasuk mengembangkan, menerapkan, dan menegakkan kebijakan keamanan untuk melindungi data penting perusahaan.
7. *Business Process Owners (BPO)*, jabatan ini bertanggung jawab dalam melakukan proses, mewujudkan tujuan proses, mendorong peningkatan proses serta menyetujui perubahan proses.
8. *Project Management Officer*, jabatan ini bertanggung jawab untuk mendukung manajer program dan proyek untuk mengumpulkan, menilai serta melaporkan informasi tentang pelaksanaan program dan proyek konstituen.
9. *Data Management Function*, adalah jabatan yang bertanggung jawab untuk mendukung aset data perusahaan di seluruh siklus hidup data dan mengelola strategi data, infrastruktur, dan repositori.
10. *Head Architect*, jabatan yang bertanggung jawab dalam proses arsitektur perusahaan.
11. *Head Development*, jabatan ini bertanggung jawab dalam proses pengembangan terkait dengan TI.
12. *Head IT Operations*, merupakan jabatan yang bertanggung jawab terhadap lingkungan dan infrastruktur operasional TI perusahaan.
13. *Head IT Administration*, bertanggung jawab atas catatan terkait TI dan mendukung masalah administrasi terkait TI.
14. *Service Manager*, jabatan yang mengelola pengembangan, implementasi, evaluasi serta *maintenance* dari produk dan layanan baru atau yang sudah ada untuk *user* tertentu.
15. *Information Security Manager*, jabatan yang bertanggung jawab dalam mengelola, mendesain, mengawasi, dan/atau menilai keamanan informasi perusahaan.
16. *Business Continuity Manager*, adalah jabatan yang bertugas dalam mengelola, merancang, mengawasi, dan/atau menilai kemampuan keberlangsungan bisnis perusahaan, serta memastikan bahwa fungsi penting perusahaan dapat tetap beroperasi.

17. *Privacy Officer*, merupakan jabatan yang bertanggung jawab dalam memantau risiko dan dampak bisnis dari undang-undang privasi dan untuk memandu dan mengkoordinasi penerapan kebijakan dan aktivitas yang memastikan kepatuhan terhadap arahan privasi.

2.10 Metode Pengukuran Capability Level



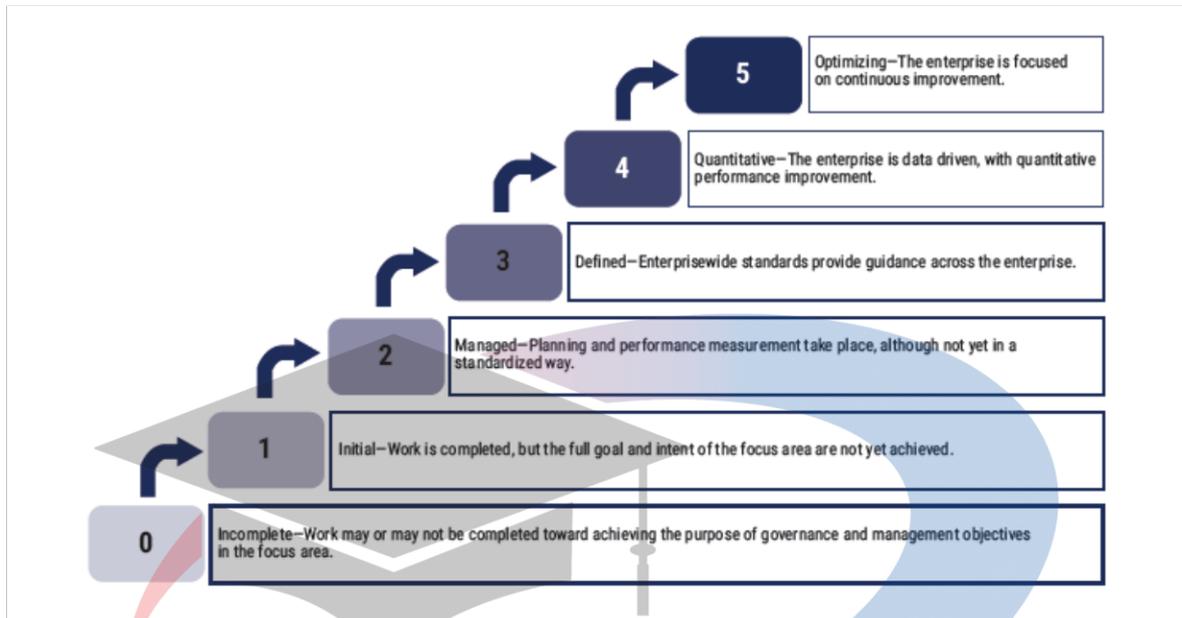
Gambar 2.12 *Capability Levels*

Tingkat kapabilitas proses (*Capability level*) merupakan sebuah skala penilaian untuk menilai seberapa baik diimplementasikan dan dilakukannya suatu proses. Tingkat kapabilitas dapat dicapai apabila tingkat yang di bawahnya telah tercapai. Berikut karakteristik tingkat kapabilitas proses [13]:

1. Level 0 – Proses ini tidak memiliki kapabilitas dasar sangat kurang dan mencerminkan pendekatan yang kurang memadai dalam mengatasi tujuan tata kelola dan manajemen, memenuhi atau tidak memenuhi maksud dari praktik.
2. Level 1 – Proses ini lebih atau kurang mencapai tujuannya melalui adopsi satu set kegiatan yang tidak lengkap yang dapat dikategorikan sebagai awal atau intuitif dan kurang terorganisir.
3. Level 2 – Proses ini mencapai tujuannya melalui implementasi serangkaian kegiatan dasar, tetapi lengkap, yang dapat dikategorikan sebagai dilakukan.
4. Level 3 – Proses mencapai tujuannya dengan cara yang lebih terorganisir menggunakan aset organisasi. Proses biasanya terdefinisi dengan baik.
5. Level 4 – Proses mencapai tujuannya terdefinisi dengan baik, dan kinerjanya diukur secara kuantitatif.

6. Level 5 – Proses mencapai tujuannya, terdefinisi dengan baik, kinerjanya diukur untuk meningkatkan kinerja, dan perbaikan berkelanjutan dilakukan.

2.11 Metode Pengukuran *Maturity Level*



Gambar 2.13 *Maturity Levels*

COBIT 2019 mendefinisikan tingkat kematangan berkaitan dengan area fokus (yaitu, kumpulan objektif tata kelola dan manajemen; dan komponen yang mendasarinya). Tingkat kematangan tertentu dicapai ketika semua proses yang terkandung dalam area fokus mencapai tingkat kemampuan tertentu. Berikut karakteristik tingkat kematangan area fokus [13]:

1. Tingkat 0 – *Incomplete*: Pekerjaan mungkin atau mungkin tidak diselesaikan untuk mencapai tujuan tata kelola dan manajemen dalam area fokus tersebut.
2. Tingkat 1 – *Initial*: Pekerjaan diselesaikan, tetapi tujuan dan maksud penuh dari area fokus belum tercapai sepenuhnya.
3. Tingkat 2 – *Managed*: Perencanaan dan pengukuran kinerja dilakukan, meskipun belum dalam cara yang terstandarisasi.
4. Tingkat 3 – *Defined*: Standar perusahaan menyediakan panduan di seluruh perusahaan.
5. Tingkat 4 – *Quantitative*: Perusahaan digerakkan oleh data, dengan peningkatan kinerja secara kuantitatif.
6. Tingkat 5 – *Optimizing*: Perusahaan difokuskan pada pengembangan berkelanjutan.

2.12 *Rating Scale*

Proses *Rating Scale* merupakan suatu tingkat kapabilitas dapat dicapai dengan derajat yang berbeda-beda, yang dapat diekspresikan dengan serangkaian peringkat yaitu [2] [13]:

1. N – *Not achieved* atau tidak tercapai – tingkat kapabilitas dicapai < 15%
2. P – *Partially achieved* – tingkat kapabilitas dicapai antara 15-50%
3. L – *Largely Achieved* – tingkat kapabilitas dicapai antara 50-85%
4. F – *Fully Achieved* – tingkat kapabilitas dicapai > 85%

2.13 Model Penilaian *Capability Process*

Untuk penilaian setiap aktivitas dimulai pada level 0, setelah organisasi mencapai level tertentu maka penilaian akan dilanjutkan pada level berikutnya, tetapi jika hasil penilaian terhadap level kapabilitas tersebut belum memenuhi standar maka penilaian tidak akan dilanjutkan dan berhenti pada level kapabilitas terakhir penilaian dilakukan [6]. Pengelolaan dan perhitungan data kuesioner dalam menentukan capability level COBIT 2019 dari setiap aktivitas yang dihitung dan diolah menggunakan rumus sebagai berikut:

1. Menghitung *capability level* pada masing-masing subdomain

$$Capability\ level = \frac{Jumlah\ aktivitas\ yang\ telah\ dilakukan}{Jumlah\ aktivitas} \dots\dots\dots(1)$$

2. Setelah menghitung masing-masing nilai kapabilitas subdomain APO12,

$$Capability\ level\ APO12 = \frac{\sum APO12.01 + \sum APO12.02 + \dots + \sum APO12.06}{\sum Subdomain\ proses} \dots\dots\dots(2)$$

Jika level 0 tercapai, maka dapat dilanjutkan pada level selanjutnya sampai level 5.

2.14 Model Penilaian *Maturity Level*

Metode *maturity model* merupakan metode yang digunakan untuk mengukur level pengembangan manajemen proses sejauh mana kapabilitas manajemen tersebut. Terdapat enam tingkat kematangan tata kelola TI suatu perusahaan, diantaranya adalah [14]:

Tabel 2.2 Indeks Tingkat Kematangan

Indeks	Tingkat Kematangan
4,50 – 5,00	Optimal
3,50 – 4,49	Terkelola
2,50 – 3,49	Ditetapkan
1,50 – 2,49	Dapat Diulang
0,50 – 1,49	Inisialisasi
0 – 0,49	Tidak Ada

Model penilaian *maturity level* dilakukan dengan menggunakan rumus:

1. Indeks *maturity subdomain APO12*

$$\text{Maturity Level Subdomain} = \frac{\text{Jumlah jawaban kuesioner}}{\text{Aktivitas subdomain}} \dots\dots\dots(1)$$

2. Menghitung *maturity level* keseluruhan APO12

$$\text{Maturity Level APO12} = \frac{\sum \text{Maturity Level Subdomain}}{\text{Banyak proses}} \dots\dots\dots(2)$$

2.15 Gap Analysis

Gap analysis merupakan selisih antara tingkat kematangan saat ini dengan yang diharapkan. Analisis ini dapat membantu memahami kondisi apa yang dialami oleh organisasi saat ini dan membantu dalam menentukan tindakan apa yang harus diambil untuk memperbaiki dan meningkatkan kinerja tata kelola TI. *Gap analysis* dapat dihitung menggunakan rumus [14]:

$$\text{Gap} = A - B \dots\dots\dots(1)$$

Dengan A = tingkat dari kematangan diharapkan, B = tingkat dari kematangan saat ini. Analisis terhadap kesenjangan ini dilakukan untuk mengidentifikasi kegiatan dan untuk memberikan rekomendasi perbaikan dalam mencapai tingkat kematangan yang diharapkan organisasi

2.16 Metode Perhitungan Skala Guttman

Skala *Guttman* adalah skala pengukuran dengan data yang diperoleh berupa data interval. Jawaban dapat dibuat dengan skor tertinggi 1 (satu) dan terendah (0). Tipe cara pemberian bobot nilai, yaitu 1 untuk jawaban “ya” dan 0 untuk jawaban “tidak”.

2.17 Penelitian Terdahulu

Penelitian terdahulu dilakukan dengan menelusuri serta mempelajari dari berbagai referensi bacaan yang berhubungan dengan tema penelitian. Referensi dapat berupa jurnal, skripsi, buku-buku, dan penelitian sebelumnya dengan harapan dapat membantu dalam mengembangkan penelitian yang akan dilakukan. Penelitian terdahulu terkait dengan tata kelola teknologi informasi berdasarkan kerangka kerja COBIT 2019 yaitu:

Tabel 2.3 Penelitian Terdahulu

Judul Penelitian	Penulis	Tahun Terbit	Domain	Kesimpulan

<p><i>Evaluasi Tata Kelola TI Office 365 pada ITB STIKOM Bali menggunakan Framework COBIT 5 [10]</i></p>	<p>Dian Pramana, Ni Made Rai Masita Dewi, Odie Kharisma Putra.</p>	<p>2022</p>	<p>EDM03, APO01, APO07, DSS05, MEA01.</p>	<p>Dalam penelitian ini didapatkan hasil tingkat kapabilitas saat ini untuk domain EDM03, MEA02, APO01, DSS05 dan APO07 berada I level 4. Kemudian untuk tingkat kapabilitas yang diharapkan berada pada level 5. Hasil perbandingan antara tingkat kapabilitas saat ini dengan yang diharapkan untuk domain EDM03, AP01, MEA01 memiliki <i>gap</i> dengan nilai level 1. Rekomendasi yang diberikan adalah melakukan perbaikan tata kelola pada proses yang diteliti, kemudian menggabungkan beberapa <i>framework</i> dalam melakukan audit TI agar hasil rekomendasi dapat lebih spesifik.</p>
<p><i>Evaluation Of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI 11 Domain [2]</i></p>	<p>A. B. Sipayung, R. Yunis, and E. Elly</p>	<p>2022</p>		<p>Berdasarkan hasil penelitian, didapatkan hasil proses kapabilitas BAI 11 berada pada level 1, untuk maturity level mendapatkan nilai 2,1. Untuk <i>gap</i> sendiri saat ini <i>capability level</i> berada pada level 2 dengan target level perusahaan yaitu level 3, sedangkan untuk <i>maturity</i></p>

					<p><i>level</i> saat ini yang didapatkan adalah level 1 dengan target level yang diharapkan adalah level 3. Rekomendasi yang diberikan adalah untuk melakukan perbaikan pada level 2 untuk mencapai target yang diharapkan yaitu level 3, kemudian melakukan dokumentasi yang tidak terstandarisasi pada setiap subdomain BAI 11 untuk mendukung implementasi aktivitas proses.</p>
<p>Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: UPT TIK Universitas Tanjungpura Pontianak) [13]</p>	<p>Anggi Srimurdianti Sukamto, Haried Novriando, Aldi Reynaldi</p>	<p>2021</p>	<p>APO08, APO09, APO11</p>	<p>Dalam penelitian ini menghasilkan tingkat kapabilitas proses tata kelola dan manajemen TI pada beberapa domain sebagai berikut: APO08 (tingkat 5), APO09 (tingkat 1), dan APO11 (tingkat 2). Sedangkan pada analisis kesenjangan yang diperoleh adalah sebagai berikut: APO08 (0), APO09 (-1, dan APO11 (-1). Untuk kesenjangan pada proses APO09 dan APO11 masing-masing pada nilai 2% dan 8%. Rekomendasi yang diberikan adalah dengan membuat dokumentasi untuk setiap</p>	

				proses yang ada, yang diharapkan dengan rekomendasi tersebut proses dan kesesuaiannya dapat dikelola dengan baik.
<i>Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PSI Universitas Muria Kudus [14]</i>	Keszya Wabang, Yusiana Rahma, Aris Puji Widodo, Fajar Nugraha	2021	EDM04, APO01, APO02, APO07, APO11, APO12, APO14, DSS01, DSS05, MEA01, MEA02	Berdasarkan hasil penelitian, didapatkan dari 11 domain proses yang digunakan dalam pengukuran tingkat kematangan dan analisis kesenjangan, APO07 berada dalam tingkat kematangan terendah dengan skor 3.25 sedangkan indeks tertinggi berada pada DSS05 dengan skor 3.48 dengan rata-rata tingkat kematangan pada 3.37 dan berada pada level 3. Untuk nilai kesenjangan, yang paling besar terdapat pada APO07 dengan skor 1.75 dan terkecil pada DSS05 dengan skor 1.52 dengan rata-rata skor kesenjangan di nilai 1.63. Rekomendasi yang diberikan seperti organisasi perlu menetapkan ukuran dan parameter manajemen kinerja proses pengelolaan TI dengan menyediakan sumber daya TI yang memadai dan mengelola komunikasi antar pihak yang terlibat, menentukan peran

			<p>dan tanggung jawab, membuat perencanaan, tujuan, dan menyelaraskan proses dengan perencanaan yang sudah dibuat, mengoptimalkan koordinasi dengan semua bidang terkait TI agar selaras dengan tujuan organisasi, meningkatkan kemampuan TI untuk tujuan bisnis, dan membuat laporan <i>monitoring</i> seluruh kegiatan secara rutin agar organisasi dapat lebih dekat dengan target tata kelola TI yang diharapkan.</p>
--	--	--	---

UNIVERSITAS MIKROSKIL