

BAB II

TINJAUAN PUSTAKA

2.1 Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi adalah sebuah kerangka kerja tata kelola perusahaan atau organisasi yang berkonsentrasi pada sumber daya teknologi informasi yang strategis pada sebuah pengelolaan dan penilaian [11]. Tata kelola teknologi informasi merupakan kumpulan berbagai metode dan aturan dalam menjalankan sebuah prosedur untuk mencapai tujuan strategis yang disepakati [8]. Tata kelola teknologi informasi memberikan beberapa manfaat bagi perusahaan atau instansi, berikut manfaat tata kelola teknologi informasi bagi perusahaan atau instansi :

1. Realisasi manfaat

Manfaat ini membangun nilai (performa) bagi perusahaan atau instansi

2. Manfaat pengoptimalan risiko

Manfaat ini mencakup risiko-risiko yang terkait dengan penggunaan, kepemilikan, operasi, interaksi, pengaruh dan adopsi teknologi informasi dalam suatu perusahaan atau instansi.

3. Manfaat pengoptimalan sumber daya

Manfaat ini memastikan bahwa kapabilitas yang sesuai tersedia untuk melaksanakan rencana dan tersedia sumber daya yang memadai, tepat dan efektif.

2.2 COBIT

COBIT (control objective information technology) adalah kerangka kerja untuk meninjau tata kelola dan pengelolaan teknologi informasi perusahaan atau instansi. COBIT 2019 diterbitkan sebagai pedoman bagi setiap organisasi untuk dapat bergerak cepat, dinamis, dan berinovasi [12]. COBIT 2019 merupakan pengembangan dari COBIT 5. Kerangka COBIT 2019 membuat perbedaan jelas

antara tata kelola dan manajemen, perbedaan tersebut memiliki aktivitas yang berbeda, struktur yang berbeda, dan tujuan yang berbeda.

Berikut enabling process dari tata kelola dan manajemen :

1. Tata kelola
 - a. Memastikan bahwa kebutuhan, kondisi, dan pilihan pemangku kepentingan dievaluasi untuk menentukan tujuan yang disepakati.
 - b. Arah ditentukan melalui pembuatan prioritas dan pengambilan keputusan.
 - c. Kinerja dipantau berdasarkan arah dan tujuan yang disepakati [13].
2. Manajemen

Mengatur, membangun, menjalankan dan mengelola aktivitas yang sejalan dengan arah yang telah ditetapkan untuk mencapai tujuan perusahaan atau instansi [13].

Selain itu COBIT 2019 juga mengidentifikasi komponen untuk membangun dan menopang sistem tata kelola, proses, struktur instansi, kebijakan dan prosedur, arus informasi, budaya dan perilaku serta keterampilan dan infrastruktur [13].

2.3 COBIT 5 dan COBIT 2019

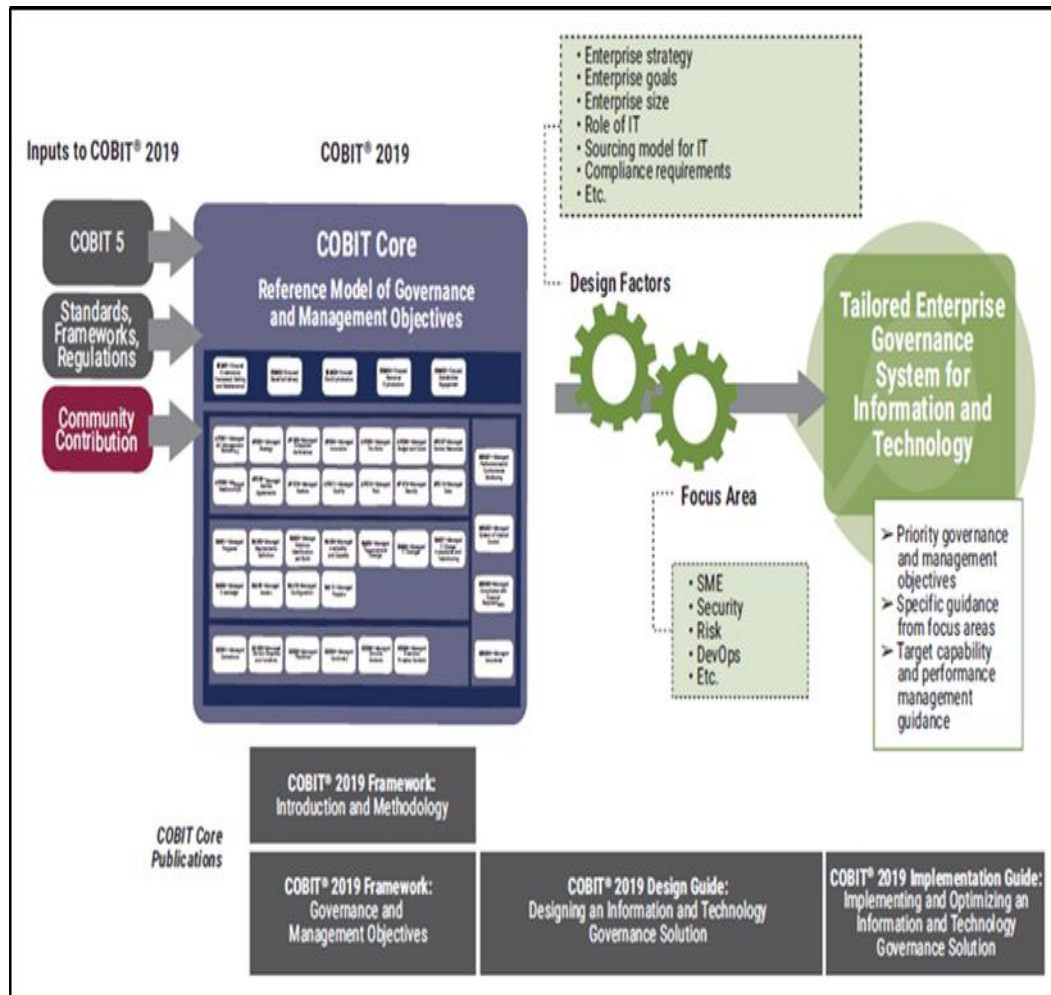
Perbedaan antara COBIT 5 dan COBIT 2019 adalah sebagai berikut :

Tabel 2.1 Perbedaan COBIT 5 dan COBIT 2019 [13]

COBIT 5	COBIT 2019
Setiap domain disebut sebagai <i>process</i>	Setiap domain memiliki <i>objectives</i> dan <i>process</i> , dan di dalam <i>process</i> memiliki serangkaian <i>activity</i>
Terdiri dari 37 domain	Terdiri dari 40 domain
Memiliki 5 prinsip <i>governance system</i>	Memiliki 7 prinsip <i>governance system</i> dan 3 prinsip <i>governance framework</i> .
<i>Governance system</i> belum dinamis	Memiliki <i>governance system</i> yang dinamis
Kebutuhan organisasi belum sesuai	Sesuai dengan kebutuhan organisasi
Berbasis kontekstual	Berbasis konseptual
Penggunaannya belum fleksibel	Penggunaannya lebih fleksibel
Belum selaras dengan standar <i>framework</i> lainnya	Selaras dengan standar <i>framework</i> lainnya

2.4 Gambaran COBIT 2019

COBIT 2019 memiliki 5 domain yang menggambarkan tujuan tata kelola dan manajemen teknologi informasi. Berikut gambaran dari COBIT 2019 :



Gambar 2.1 Gambaran COBIT 2019 [13]

Supaya teknologi informasi dapat berkontribusi pada perusahaan atau instansi, maka sejumlah tujuan tata kelola dan manajemen harus dicapai. Konsep dasar yang berkaitan dengan tujuan tata kelola dan manajemen teknologi informasi adalah sebagai berikut :

1. Tujuan tata kelola atau manajemen selalu berkaitan dengan satu proses dan serangkaian komponen terkait dari jenis lain untuk membantu mencapai tujuan

2. Tujuan tata kelola berkaitan dengan proses tata kelola sedangkan tujuan manajemen berkaitan dengan proses manajemen [13].

Tujuan tata kelola dan manajemen dalam COBIT 2019 dikelompokkan menjadi lima domain. Domain memiliki nama dengan kata kerja yang mengungkapkan tujuan utama dan bidang kegiatan tujuan yang terkandung di dalamnya. Berikut adalah kelima domain dari COBIT 2019 :

1. Tujuan tata kelola dikelompokkan dalam domain EDM (*evaluated, direct and monitor*). Domain EDM sebagai pengatur dan mengevaluasi opsi strategis serta mengarahkan manajemen senior pada opsi strategis yang dipilih guna pencapaian yang strategis. Berikut pembagian domain EDM kedalam domain obyektif, domain proses beserta deskripsinya:

Tabel 2.2 Governance Objectives Domain EDM [13].

<i>Objectives Domain</i>	<i>Descriptions</i>	<i>Processes Domain</i>	<i>Descriptions</i>
<i>EDM 01</i>	<i>Ensured governance framework setting and maintenance</i>	<i>EDM 01.01</i>	<i>Evaluate the governance system</i>
		<i>EDM 01.02</i>	<i>Direct the governance system</i>
		<i>EDM 01.03</i>	<i>Monitor the governance system</i>
<i>EDM 02</i>	<i>Ensured benefit delivery</i>	<i>EDM 02.01</i>	<i>Establish the target investment mix</i>
		<i>EDM 02.02</i>	<i>Evaluate value optimization</i>
		<i>EDM 02.03</i>	<i>Direct value optimization</i>
		<i>EDM 02.04</i>	<i>Monitor value optimization</i>
<i>EDM 03</i>	<i>Ensured risk monitor</i>	<i>EDM 03.01</i>	<i>Evaluate risk management</i>
		<i>EDM 03.02</i>	<i>Direct risk management</i>
		<i>EDM 03.03</i>	<i>Monitor risk management</i>
<i>EDM 04</i>	<i>Ensured resource optimization</i>	<i>EDM 04.01</i>	<i>Evaluate resource management</i>
		<i>EDM 04.02</i>	<i>Direct resource management</i>
		<i>EDM 04.03</i>	<i>Direct resource management</i>
<i>EDM 05</i>	<i>Ensured stakeholder engagement</i>	<i>EDM 05.01</i>	<i>Evaluate stakeholder engagement and reporting requirements</i>
		<i>EDM 05.02</i>	<i>Direct stakeholder engagement communication and reporting</i>
		<i>EDM 05.03</i>	<i>Monitor stakeholder engagement</i>

2. Tujuan manajemen dikelompokkan kedalam empat domain yaitu APO (*Align, plan and organize*), BAI (*build, acquire and implement*), DSS (*deliver, service and support*), dan MEA (*monitor, evaluate, and assess*). Domain APO membahas keseluruhan organisasi, strategi dan kegiatan pendukung untuk teknologi informasi. Domain BAI memahami definisi, akuisisi, dan implementasi solusi teknologi informasi dalam proses bisnis. Domain DSS membahas pengiriman operasional dan dukungan layanan teknologi informasi termasuk keamanan dan Domain MEA membahas pemantauan kinerja dan kesesuaian teknologi informasi dengan target kinerja internal, mengendalikan tujuan internal dan persyaratan eksternal [13]. Berikut pembagian domain APO, BAI, DSS dan MEA kedalam domain obyektif, domain proses beserta deskripsinya :

Tabel 2.3 *Management Objectives Domain APO [13].*

<i>Objectives Domain</i>	<i>Descriptions</i>	<i>Processes Domain</i>	<i>Descriptions</i>
<i>APO 01</i>	<i>Managed IT Management Framework</i>	<i>APO 01.01</i>	<i>Design the management system for enterprise IT</i>
		<i>APO 01.02</i>	<i>Communicate management objectives, direction and decisions made</i>
		<i>APO 01.03</i>	<i>Implement management processes</i>
		<i>APO 01.04</i>	<i>Define and implement the organizational structures</i>
		<i>APO 01.05</i>	<i>Establish roles and responsibilities</i>
		<i>APO 01.06</i>	<i>Optimize the placement of the IT function</i>
		<i>APO 01.07</i>	<i>Define information (data) and system ownership</i>
		<i>APO 01.08</i>	<i>Define target skills and competencies</i>
		<i>APO 01.09</i>	<i>Define and communicate policies procedures</i>
		<i>APO 01.10</i>	<i>Define and implement infrastructure, service and application to support the</i>

			<i>governance and management system</i>
		<i>APO 01.11</i>	<i>Manage continual improvement of the IT management system</i>
<i>APO 02</i>	<i>Managed strategy</i>	<i>APO 02.01</i>	<i>Understand enterprise context and direction</i>
		<i>APO 02.02</i>	<i>Assess current capabilities, performance and digital maturity of the enterprise</i>
		<i>APO 02.03</i>	<i>Define target digital capabilities</i>
		<i>APO 02.04</i>	<i>Conduct a gap analysis</i>
		<i>APO 02.05</i>	<i>Define the strategic plan and road map</i>
		<i>APO 02.06</i>	<i>Communicate the IT strategy and direction</i>
<i>APO 03</i>	<i>Managed enterprise architecture</i>	<i>APO 03.01</i>	<i>Develop the enterprise architecture vision</i>
		<i>APO 03.02</i>	<i>Define reference architecture</i>
		<i>APO 03.03</i>	<i>Select opportunities and solutions</i>
		<i>APO 03.04</i>	<i>Define architecture implementation</i>
		<i>APO 03.05</i>	<i>Provide enterprise architecture service</i>
<i>APO 04</i>	<i>Managed innovation</i>	<i>APO 04.01</i>	<i>Create an environment conducive to innovation</i>
		<i>APO 04.02</i>	<i>Maintain an understanding of the enterprise environment</i>
		<i>APO 04.03</i>	<i>Monitor and scan the technology environment</i>
		<i>APO 04.04</i>	<i>Assess the potential of emerging technologies and innovative ideas</i>
		<i>APO 04.05</i>	<i>Recommended appropriate further initiatives</i>
		<i>APO 04.06</i>	<i>Monitor the implementation and use innovation</i>
<i>APO 05</i>	<i>Managed portfolio</i>	<i>APO 05.01</i>	<i>Determine the availability and sources of funds</i>
		<i>APO 05.02</i>	<i>Evaluated and select program to fund</i>
		<i>APO 05.03</i>	<i>Monitor, optimize and report of</i>

			<i>investment portfolio performance</i>
		<i>APO 05.04</i>	<i>Maintain portfolio</i>
		<i>APO 05.05</i>	<i>Manage benefit achievement</i>
<i>APO 06</i>	<i>Managed budget and cost</i>	<i>APO 06.01</i>	<i>Manage finance and accounting</i>
		<i>APO 06.02</i>	<i>Prioritize resource allocation</i>
		<i>APO 06.03</i>	<i>Create and maintain budgets</i>
		<i>APO 06.04</i>	<i>Model and allocate cost</i>
		<i>APO 06.05</i>	<i>Manage cost</i>
<i>APO 07</i>	<i>Managed human resources</i>	<i>APO 07.01</i>	<i>Acquire and maintain adequate and appropriate staffing</i>
		<i>APO 07.02</i>	<i>Identify key IT personnel</i>
		<i>APO 07.03</i>	<i>Maintain the skill and competencies of personnel</i>
		<i>APO 07.04</i>	<i>Assess and recognize / reward employee job performance</i>
		<i>APO 07.05</i>	<i>Plan and track the usage of IT and business human resource</i>
		<i>APO 07.06</i>	<i>Manage contract staff</i>
<i>APO 08</i>	<i>Managed relationships</i>	<i>APO 08.01</i>	<i>Understand business expectations</i>
		<i>APO 08.02</i>	<i>Align IT strategy with business expectations and identify opportunities for IT to change the business</i>
		<i>APO 08.03</i>	<i>Manage the business relationship</i>
		<i>APO 08.04</i>	<i>Coordinate and communicate</i>
		<i>APO 08.05</i>	<i>Provide input to the continual improvement of service</i>
<i>APO 09</i>	<i>Managed service agreements</i>	<i>APO 09.01</i>	<i>Identify IT service</i>
		<i>APO 09.02</i>	<i>Catalog IT enabled service</i>
		<i>APO 09.03</i>	<i>Define and prepare service agreements and contract</i>
		<i>APO 09.04</i>	<i>Monitor and report service levels</i>
		<i>APO 09.05</i>	<i>Review service agreements and contract</i>
<i>APO 10</i>	<i>Managed vendor</i>	<i>APO 10.01</i>	<i>Identify and evaluate vendor relationships and contracts</i>
		<i>APO 10.02</i>	<i>Select vendor</i>
		<i>APO 10.03</i>	<i>Manage vendor relationships</i>

			<i>and contracts</i>
		<i>APO 10.04</i>	<i>Manage vendor risk</i>
		<i>APO 10.05</i>	<i>Monitor vendor performance and compliance</i>
<i>APO 11</i>	<i>Managed quality</i>	<i>APO 11.01</i>	<i>Establish a quality management system (QMS)</i>
		<i>APO 11.02</i>	<i>Focus quality management on customer</i>
		<i>APO 11.03</i>	<i>Manage quality standards, practice and procedures and integrate quality management into key process and solutions</i>
		<i>APO 11.04</i>	<i>Perform quality monitoring, control and reviews</i>
		<i>APO 11.05</i>	<i>Maintain continuous improvement</i>
<i>APO 12</i>	<i>Managed risk</i>	<i>APO 12.01</i>	<i>Collect data</i>
		<i>APO 12.02</i>	<i>Analyze risk</i>
		<i>APO 12.03</i>	<i>Maintain a risk profile</i>
		<i>APO 12.04</i>	<i>Articulate risk</i>
		<i>APO 12.05</i>	<i>Define a risk management action portfolio</i>
		<i>APO 12.06</i>	<i>Respond to risk</i>
<i>APO 13</i>	<i>Managed security</i>	<i>APO 13.01</i>	<i>Establish and maintain in information security management system (ISMS)</i>
		<i>APO 13.02</i>	<i>Define and manage information security and privacy risk treatment plan</i>
		<i>APO 13.03</i>	<i>Monitor and review the information security management system (ISMS)</i>
<i>APO 14</i>	<i>Managed data</i>	<i>APO 14.01</i>	<i>Define and communicate the organization's data management strategy and roles and responsibility</i>
		<i>APO 14.02</i>	<i>Define and maintain a consistent business glossary</i>
		<i>APO 14.03</i>	<i>Establish the processes and infrastructure for metadata management</i>
		<i>APO 14.04</i>	<i>Define a data quality strategy</i>
		<i>APO 14.05</i>	<i>Establish data profiling</i>

			<i>methodologies, processes and tools</i>
		<i>APO 14.06</i>	<i>Ensure a data quality assessment approach</i>
		<i>APO 14.07</i>	<i>Define a data cleansing approach</i>
		<i>APO 14.08</i>	<i>Manage the life cycle of data assets</i>
		<i>APO 14.09</i>	<i>Support data archiving and retention</i>
		<i>APO 14.10</i>	<i>Manage data backup and storage arrangements</i>

Tabel 2.4 Management Objectives Domain BAI [13]

<i>Objectives Domain</i>	<i>Descriptions</i>	<i>Processes Domain</i>	<i>Descriptions</i>
<i>BAI 01</i>	<i>Managed programs</i>	<i>BAI 01.01</i>	<i>Maintain a standard approach for program management</i>
		<i>BAI 01.02</i>	<i>Initiate a program</i>
		<i>BAI 01.03</i>	<i>Manage stakeholder engagement</i>
		<i>BAI 01.04</i>	<i>Develop and maintain the program plan</i>
		<i>BAI 01.05</i>	<i>Launch and execute the program</i>
		<i>BAI 01.06</i>	<i>Monitor, control and report on the program outcomes</i>
		<i>BAI 01.07</i>	<i>Manage program quality</i>
		<i>BAI 01.08</i>	<i>Manage program risk</i>
		<i>BAI 01.09</i>	<i>Close a program</i>
<i>BAI 02</i>	<i>Manage requirements definition</i>	<i>BAI 02.01</i>	<i>Define and maintain business functional and technical requirements</i>
		<i>BAI 02.02</i>	<i>Perform a feasibility study and technical requirements</i>
		<i>BAI 02.03</i>	<i>Manage requirements risk</i>
		<i>BAI 02.04</i>	<i>Obtain approval of requirements and solutions</i>
<i>BAI 03</i>	<i>Manage solutions identification and build</i>	<i>BAI 03.01</i>	<i>Design high level solutions</i>
		<i>BAI 03.02</i>	<i>Design detailed solutions components</i>

		<i>BAI 03.03</i>	<i>Develop solution components</i>
		<i>BAI 03.04</i>	<i>Procure solution components</i>
		<i>BAI 03.05</i>	<i>Build solutions</i>
		<i>BAI 03.06</i>	<i>Perform quality assurance (QA)</i>
		<i>BAI 03.07</i>	<i>Prepare for solution testing</i>
		<i>BAI 03.08</i>	<i>Execute solution testing</i>
		<i>BAI 03.09</i>	<i>Manage change to requirements</i>
		<i>BAI 03.10</i>	<i>Maintain solutions</i>
		<i>BAI 03.11</i>	<i>Define IT product and service and maintain the service portfolio</i>
		<i>BAI 03.12</i>	<i>Design solutions based on the defined development methodology</i>
<i>BAI 04</i>	<i>Managed availability and capacity</i>	<i>BAI 04.01</i>	<i>Assess current availability, performance and capacity and create a baseline</i>
		<i>BAI 04.02</i>	<i>Assess business impact</i>
		<i>BAI 04.03</i>	<i>Plan for new changed service requirements</i>
		<i>BAI 04.04</i>	<i>Monitor review and availability and capacity</i>
		<i>BAI 04.05</i>	<i>Investigate and address availability, performance and capacity issues</i>
		<i>BAI 05.01</i>	<i>Establish the desired to change</i>
		<i>BAI 05.02</i>	<i>Form an effective implementation team</i>
		<i>BAI 05.03</i>	<i>Communicate desired vision</i>
		<i>BAI 05.04</i>	<i>Empower role players and identify short-term wins</i>
		<i>BAI 05.05</i>	<i>Enable operation and use</i>
		<i>BAI 05.06</i>	<i>Embed new approaches</i>
		<i>BAI 05.07</i>	<i>Sustain changes</i>
<i>BAI 06</i>	<i>Managed IT changes</i>	<i>BAI 06.01</i>	<i>Evaluate, prioritize and authorize change requests</i>
		<i>BAI 06.02</i>	<i>Manage emergency changes</i>
		<i>BAI 06.03</i>	<i>Track and report change status</i>
		<i>BAI 06.04</i>	<i>Close and document the changes</i>
<i>BAI 07</i>	<i>Managed IT change acceptance and transitioning</i>	<i>BAI 07.01</i>	<i>Establish in implementation plan</i>
		<i>BAI 07.02</i>	<i>Plan business process, system</i>

			<i>and data conversion</i>
		<i>BAI 07.03</i>	<i>Plan acceptance test</i>
		<i>BAI 07.04</i>	<i>Establish a test environment</i>
		<i>BAI 07.05</i>	<i>Perform acceptance test</i>
		<i>BAI 07.06</i>	<i>Promote to production and manage releases</i>
		<i>BAI 07.07</i>	<i>Provide early production support</i>
		<i>BAI 07.08</i>	<i>Perform a post-implementation review</i>
<i>BAI 08</i>	<i>Managed knowledge</i>	<i>BAI 08.01</i>	<i>Identify and classify resources of information for governance and management of IT</i>
		<i>BAI 08.02</i>	<i>Organize and contextualize information into knowledge</i>
		<i>BAI 08.03</i>	<i>Use and share knowledge</i>
		<i>BAI 08.04</i>	<i>Evaluate and update or retire information</i>
<i>BAI 09</i>	<i>Managed assets</i>	<i>BAI 09.01</i>	<i>Identify and record current assets</i>
		<i>BAI 09.02</i>	<i>Manage critical assets</i>
		<i>BAI 09.03</i>	<i>Manage the assets life cycle</i>
		<i>BAI 09.04</i>	<i>Optimize assets value</i>
		<i>BAI 09.05</i>	<i>Manage license</i>
<i>BAI 10</i>	<i>Managed configuration</i>	<i>BAI 10.01</i>	<i>Establish and maintain a configuration model</i>
		<i>BAI 10.02</i>	<i>Establish and maintain a configuration repository and baseline</i>
		<i>BAI 10.03</i>	<i>Maintain and control configuration item</i>
		<i>BAI 10.04</i>	<i>Produce status and configuration report</i>
		<i>BAI 10.05</i>	<i>Verify and review integrity of the configuration repository</i>
<i>BAI 11</i>	<i>Managed projects</i>	<i>BAI 11.01</i>	<i>Maintain a standard approach for project management</i>
		<i>BAI 11.02</i>	<i>Start up and initiate a project</i>
		<i>BAI 11.03</i>	<i>Manage stakeholder engagement</i>
		<i>BAI 11.04</i>	<i>Develop and maintain the project plan</i>
		<i>BAI 11.05</i>	<i>Manage project quality</i>

		<i>BAI 11.06</i>	<i>Manage project risk</i>
		<i>BAI 11.07</i>	<i>Monitor and control project</i>
		<i>BAI 11.08</i>	<i>Manage project resource and work packages</i>
		<i>BAI 11.09</i>	<i>Close a project or iteration</i>

Table 2.5 Management Objectives Domain DSS [13].

<i>Objectives Domain</i>	<i>Descriptions</i>	<i>Processes Domain</i>	<i>Descriptions</i>
<i>DSS 01</i>	<i>Managed operations</i>	<i>DSS 01.01</i>	<i>Perform operational procedures</i>
		<i>DSS 01.02</i>	<i>Manage outsources IT service</i>
		<i>DSS 01.03</i>	<i>Monitor IT infrastructure</i>
		<i>DSS 01.04</i>	<i>Manage the environment</i>
		<i>DSS 01.05</i>	<i>Manage facilities</i>
<i>DSS 02</i>	<i>Managed incident</i>	<i>DSS 02.01</i>	<i>Define classification schemes for incidents and service request</i>
		<i>DSS 02.02</i>	<i>Record, classify and prioritize requests and incidents</i>
		<i>DSS 02.03</i>	<i>Verify, approve and fulfill service request</i>
		<i>DSS 02.04</i>	<i>Investigate, diagnose and allocate incidents</i>
		<i>DSS 02.05</i>	<i>Resolve and recover from incidents</i>
		<i>DSS 02.06</i>	<i>Close service requests and incidents</i>
		<i>DSS 02.07</i>	<i>Track status and produce report</i>
<i>DSS 03</i>	<i>Managed problems</i>	<i>DSS 03.01</i>	<i>Identify and classify problems</i>
		<i>DSS 03.02</i>	<i>Investigate and diagnose problems</i>
		<i>DSS 03.03</i>	<i>Raise known error</i>
		<i>DSS 03.04</i>	<i>Resolve and close problems</i>

		<i>DSS 03.05</i>	<i>Perform proactive problem management</i>
<i>DSS 04</i>	<i>Managed continuity</i>	<i>DSS 04.01</i>	<i>Define the business continuity policy, objectives and scope</i>
		<i>DSS 04.02</i>	<i>Maintain business resilience</i>
		<i>DSS 04.03</i>	<i>Develop and implement a business continuity plans</i>
		<i>DSS 04.04</i>	<i>Exercise, test and review the business continuity plan and disaster response plan</i>
		<i>DSS 04.05</i>	<i>Review, maintain and improve the continuity plans</i>
		<i>DSS 04.06</i>	<i>Conduct continuity plan training</i>
		<i>DSS 04.07</i>	<i>Manage backup arrangements</i>
		<i>DSS 04.08</i>	<i>Conduct post-resumption review</i>
<i>DSS 05</i>	<i>Managed security service</i>	<i>DSS 05.01</i>	<i>Protect against malicious software</i>
		<i>DSS 05.02</i>	<i>Manage network and connectivity security</i>
		<i>DSS 05.03</i>	<i>Manage endpoint security</i>
		<i>DSS 05.04</i>	<i>Manage user identify and logical access</i>
		<i>DSS 05.05</i>	<i>Manage physical access to I7T assets</i>
		<i>DSS 05.06</i>	<i>Manage sensitive documents and output device</i>
		<i>DSS 05.07</i>	<i>Manage vulnerabilities and monitor the infrastructure for security-related events</i>
<i>DSS 06</i>	<i>Managed business process controls</i>	<i>DSS 06.01</i>	<i>Align control activities embedded in business processes with enterprise objectives</i>
		<i>DSS 06.02</i>	<i>Control the processing of information</i>

		DSS 06.03	Manage roles, responsibilities, access privileges and levels of authority
		DSS 06.04	Manage errors and expectations
		DSS 06.05	Ensure traceability and accountability for information events
		DSS 06.06	Secure information assets

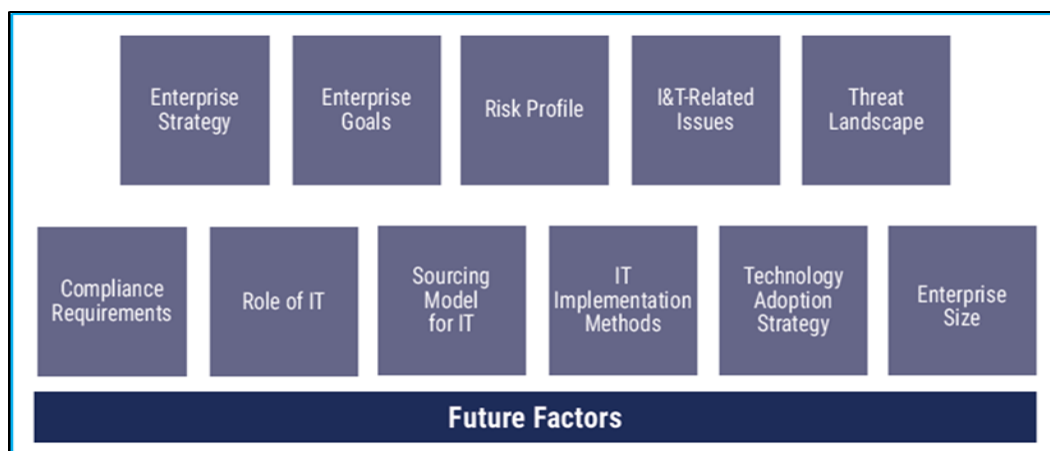
Tabel 2.6 Management Objectives Domain MEA [13].

<i>Objectives Domain</i>	<i>Descriptions</i>	<i>Processes Domain</i>	<i>Descriptions</i>
<i>MEA 01</i>	<i>Managed performance and conformance monitoring</i>	<i>MEA 01.01</i>	<i>Establish a monitoring approach</i>
		<i>MEA 01.02</i>	<i>Set performance and conformance targets</i>
		<i>MEA 01.03</i>	<i>Collect and process performance data</i>
		<i>MEA 01.04</i>	<i>Analyze and report performance</i>
		<i>MEA 01.05</i>	<i>Ensure the implementation of corrective actions</i>
<i>MEA 02</i>	<i>Managed system of internal control</i>	<i>MEA 02.01</i>	<i>Monitor internal controls</i>
		<i>MEA 02.02</i>	<i>Review effectiveness of business process control</i>
		<i>MEA 02.03</i>	<i>Perform control self-assessment</i>
		<i>MEA 02.04</i>	<i>Identify and report control deficiencies</i>
<i>MEA 03</i>	<i>Managed compliance with external requirements</i>	<i>MEA 03.01</i>	<i>Identify external compliance requirements</i>
		<i>MEA 03.02</i>	<i>Optimize response to external compliance</i>
		<i>MEA 03.03</i>	<i>Confirm external compliance</i>
		<i>MEA 03.04</i>	<i>Obtain assurance of external compliance</i>

MEA 04	Managed assurance	MEA 04.01	Ensure that assurance providers are independent and qualified
		MEA 04.02	Develop risk-based planning of assurance initiatives
		MEA 04.03	Determine the objectives of the assurance initiatives
		MEA 04.04	Define the scope of assurance initiative
		MEA 04.05	Define the work program for the assurance initiative
		MEA 04.06	Execute the assurance initiative, focusing on design effectiveness
		MEA 04.07	Execute the assurance initiative, focusing on operating effectiveness
		MEA 04.08	Report and follow up on the assurance initiative
		MEA 04.09	Follow up on recommendations and actions

Selain itu COBIT 2019 memiliki 11 *design factor* yang digunakan untuk mengetahui rancangan awal tata kelola teknologi informasi pada suatu perusahaan atau instansi.

Berikut kesebelas *design factor* pada COBIT 2019 :



Gambar 2.2 COBIT 2019 Design Factor [13].

1. Strategi perusahaan (*enterprise strategy*)
Setiap perusahaan/instansi memiliki strategi yang berbeda. Perusahaan/instansi biasanya memiliki strategi primer dan sekunder
2. Tujuan perusahaan (*enterprise goals*)
Mendukung strategi perusahaan/instansi yang direalisasikan untuk mencapai tujuan perusahaan/instansi
3. Profil risiko (*risk profile*)
profil risiko mengidentifikasi jenis risiko yang berkaitan dengan TI
4. Isu terkait (*related issues*)
Masalah terkait teknologi informasi bagi perusahaan/instansi.
5. Lanskap ancaman (*threat landscape*)
Merupakan ancaman teknologi informasi bagi perusahaan/instansi dengan *level* normal atau tinggi
6. Kepatuhan persyaratan (*compliance requirements*)
Persyaratan wajib perusahaan/instansi diklasifikasikan menjadi 3 bagian, yaitu *low compliance requirements*, *normal compliance requirements*, dan *higt compliance requirements*
7. Peran TI (*role of IT*)
Peran teknologi informasi dibagi menjadi 4, yaitu *role of support*, *role of factory*, *role of turnaround*, dan *role of strategic*
8. Model sumber TI (*sourcing model for IT*)
Model sumber teknologi mengadopsi 4 model, yaitu *outsourcing*, *cloud*, *insourced*, dan *hybrid*
9. Metode implementasi TI (*IT implementation method*)
Metode teknologi informasi dibagi menjadi 3, yaitu *agile DevOps*, *traditional*, dan *hybrid*
10. Strategi adopsi teknologi (*technology adoption strategy*)
Strategi pengadopsian teknologi informasi dibagi menjadi 3, yaitu *first mover*, *follower*, dan *slow mover*

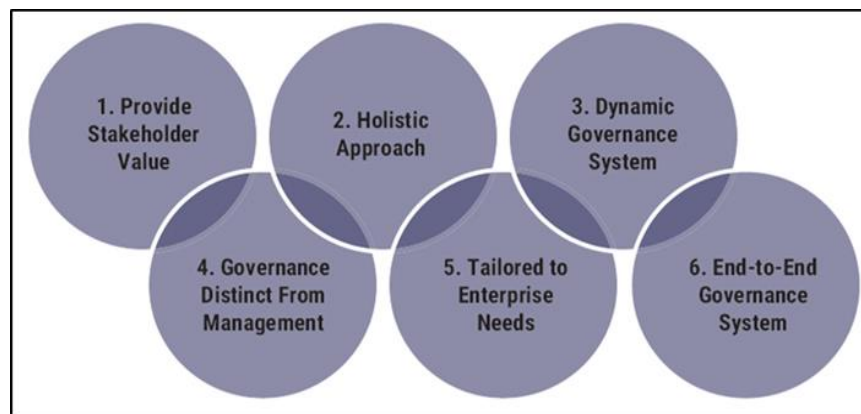
11. Ukuran perusahaan (*enterprise size*)

Ukuran perusahaan/instansi dibagi menjadi 2, ukuran kecil atau medium memiliki karyawan/tenaga kerja antara 50 sampai 250, sedangkan ukuran besar memiliki karyawan / tenaga kerja lebih dari 250 [13].

2.5 Prinsip COBIT 2019

2.5.1 Prinsip Sistem Tata Kelola

Prinsip sistem tata kelola memiliki 6 komponen. Berikut disajikan gambar dari prinsip sistem tata kelola pada COBIT 2019 :



Gambar 2.3 Prinsip Sistem Tata Kelola [13].

1. *Provide stakeholder value*

Setiap perusahaan/instansi membutuhkan sistem tata kelola untuk memenuhi kebutuhan kepentingan guna menghasilkan nilai (keseimbangan, risiko, dan sumber daya) dari penggunaan teknologi informasi

2. *Holistic approach*

Sistem tata kelola teknologi informasi perusahaan / instansi dari berbagai sejumlah jenis komponen yang dapat bekerja sama secara holistik.

3. *Dynamic governance system*

Sistem tata kelola harus dinamis, bahwa setiap satu atau lebih *design factor* berada pada perubahannya

4. *Governance distinct from management*

Sistem tata kelola harus jelas membedakan antara tata kelola dan manajemen

5. *Tailored to enterprise needs*

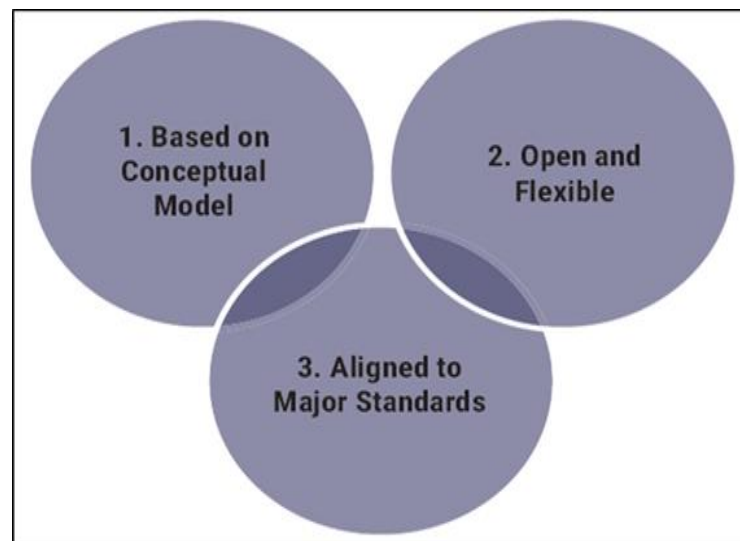
Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan/instansi, menggunakan design factor yang terpisah sebagai parameter menyesuaikan dan memprioritaskan komponen sistem tata kelola

6. *End-to-end governance system*

Sistem tata kelola harus mencakup perusahaan / instansi dari ujung ke ujung dengan fokus tidak hanya pada bagian teknologi informasi saja, tetapi pada semua aspek teknologi dan kebenaran informasi yang dilakukan perusahaan/ instansi [13].

2.5.2 Prinsip Kerangka Kerja Tata Kelola

Prinsip kerangka kerja tata kelola memiliki 3 komponen, berikut disajikan gambar dari prinsip kerangka kerja tata kelola :



Gambar 2.4 Prinsip Kerangka Kerja Tata Kelola [13].

1. *Based on conceptual model*

Kerangka kerja harus berdasarkan pada model konseptual, mengidentifikasi komponen utama dan hubungan antar komponen untuk memastikan konsistensi dan otomatisasi

2. *Open and flexible*

Kerangka tata kelola harus terbuka dan fleksibel. Mendukung penambahan konten baru dalam kemampuan untuk mengatasi masalah baru dengan cara yang fleksibel

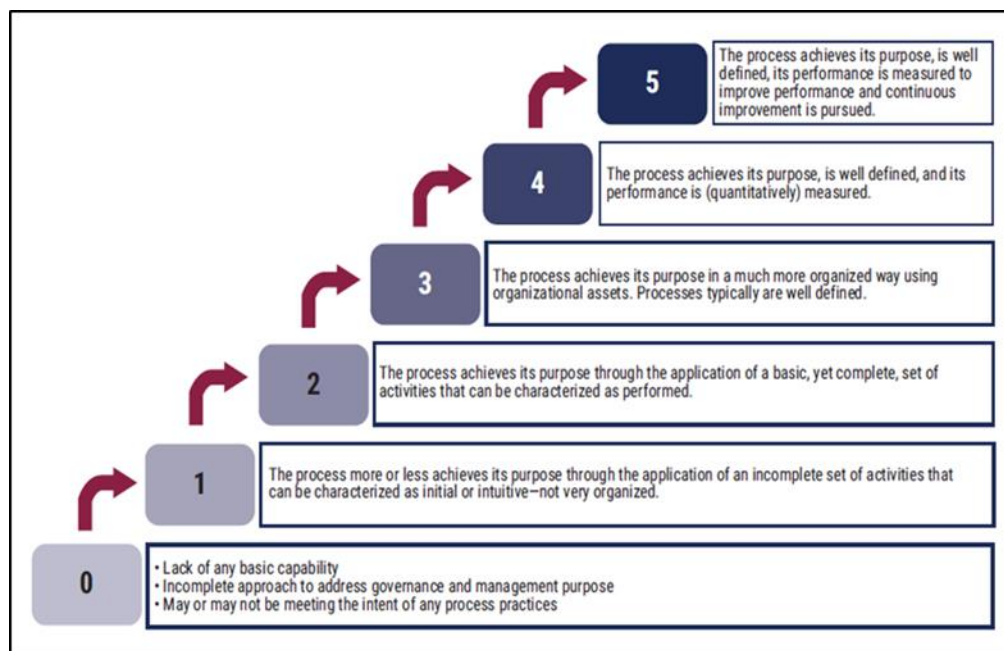
3. *Aligned to major standards*

Kerangka tata kelola harus selaras dengan kerangka kerja [13].

2.6 Tingkat Kemampuan COBIT 2019

COBIT 2019 mendukung skema kapabilitas proses berbasis *capability maturity model integration* (CMMI). Proses dalam setiap tata kelola dan tujuan manajemen dapat beroperasi pada berbagai tingkat kemampuan mulai dari 0 sampai dengan 5. Tingkat kemampuan adalah ukuran tentang proses yang telah diimplementasikan.

Berikut capability level for process pada COBIT 2019 :

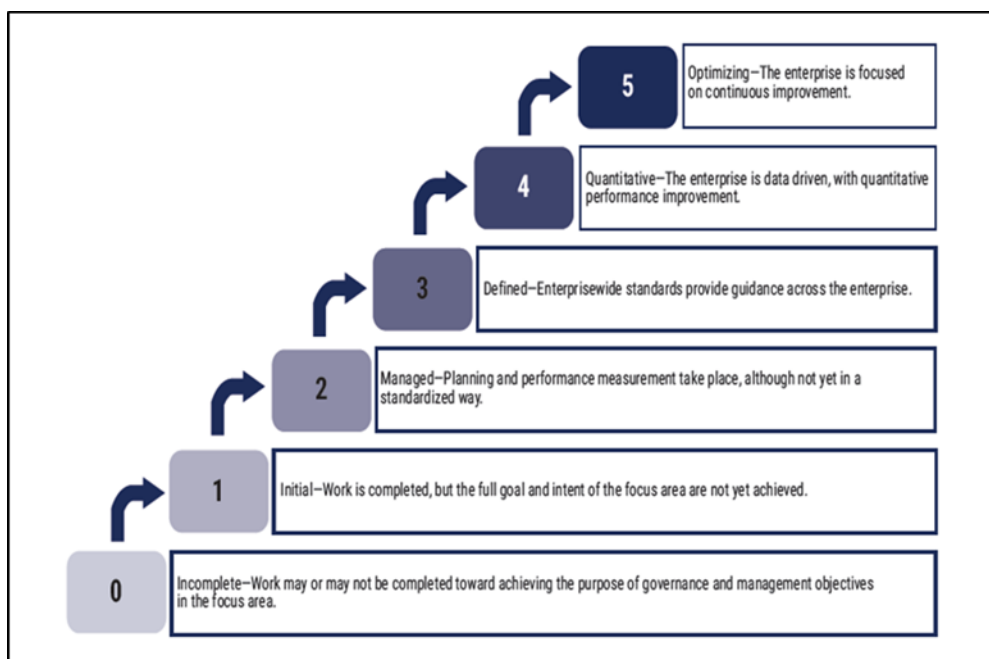


Gambar 2.5 Tingkat Kemampuan Domain Proses COBIT 2019 [13]

2.7 Tingkat Kematangan COBIT 2019

COBIT 2019 mendefinisikan *maturity level* sebagai kinerja area fokus (*focus area*) sesuai dengan domain terpilih. Setelah ditentukan domain proses COBIT 2019 yang akan dianalisis kemudian dibuat kuesioner sesuai aktivitas masing-masing domain sebagaimana yang telah disediakan COBIT 2019 dengan pilihan jawaban menggunakan rentang nilai 0-5 [14]. *Maturity level* digunakan untuk mengontrol proses-proses teknologi informasi menggunakan framework COBIT dengan informasi metode penilaian/*scoring* tujuannya adalah organisasi dapat mengetahui posisi kematangan teknologi informasi saat ini dan organisasi dapat terus menerus berusaha meningkatkan levelnya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan dengan lancar [4].

Berikut disajikan gambar tingkat kematangan area fokus (*maturity level focus area*) pada COBIT 2019:



Gambar 2.6 Tingkat Kematangan Domain Objektif COBIT 2019 [13]

2.8 Penelitian Terkait

Perancangan dan penilaian tata kelola teknologi informasi sebelumnya belum pernah dilakukan di Kantor Kementerian Agama Kabupaten Pesawaran Provinsi Lampung. Namun pada penelitian ini peneliti menggunakan penelitian lain (terdahulu) yang

dilakukan pada instansi yang berbeda sebagai referensi yang akan digunakan pada penelitian di Kantor Kementerian Agama Kabupaten Pesawaran Provinsi Lampung.

Tabel 2.7 Penelitian Terdahulu

1	Judul	Perancangan Tata Kelola TI Menggunakan COBIT 2019 Pada PT. Telekomunikasi Indonesia Regional VI Kalimantan
	Domain obyektif	Domain obyektif terpilih dengan nilai kepentingan > 50 yang terdiri dari APO 03, APO 12, APO 13, BAI 03, BAI 06, BAI 07, BAI 09, BAI 10, DSS 03, dan DSS 04.
	Keterkaitan	Keterkaitan masalah: sering terjadinya kesalahan dalam pengelolaan data Keterkaitan domain obyektif : APO 13 dan DSS 03.
2	Judul	Perancangan Tata Kelola TI Menggunakan <i>Framework</i> COBIT 2019 Pada DPMPTSP
	Domain obyektif	Domain obyektif terpilih dengan nilai kepentingan minimal 50 yang terdiri dari APO 13, BAI 02, BAI 03, BAI 05, BAI 06, BAI 07, dan BAI 10.
	Keterkaitan	Keterkaitan masalah : sering terjadinya kegagalan pada data yang dikelola. Keterkaitan domain obyektif : APO 13.
3	Judul	Analisis dan Perancangan TI Menggunakan <i>Framework</i> COBIT 2019 Pada PT. XYZ
	Domain obyektif	Domain obyektif terpilih dengan nilai kepentingan minimal 30 yang terdiri dari BAI 09, DSS 02, DSS 03, dan MEA 03.
	Keterkaitan	Keterkaitan masalah : keamanan informasi, aplikasi <i>error</i> , dan kehilangan data. Keterkaitan domain obyektif : DSS 02 dan DSS 03.
4	Judul	Penyesuaian Sistem Tata Kelola Pada Institut Teknologi Kalimantan Dengan Menggunakan COBIT 2019
	Domain obyektif	All objectives domain (belum ada pemrioritasan nilai)
	Keterkaitan	Keterkaitan masalah : kualitas data dan integritas data. Keterkaitan domain obyektif : APO 11, APO 13, DSS 02, dan DSS 03.

5	Judul	Perencanaan Audit Tata Kelola TI Laboratorium Kalibrasi Menggunakan COBIT 2019 (Studi Kasus : Laboratorium Kalibrasi BSML Regional II)
	Domain obyektif	Domain obyektif terpilih dengan nilai kepentingan minimal 85 yaitu terdiri dari EDM 03, APO 12, DSS 02, DSS 04, dan DSS 05.
	Keterkaitan	Keterkaitan masalah : sering terjadinya kehilangan data Keterkaitan domain obyektif : DSS 02