BAB II
TINJAUAN PUSTAKA

2.1 Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) adalah seperangkat kebijakan dan prosedur untuk mengelola data sensitif organisasi secara sistematis. Tujuan dari SMKI adalah untuk meminimalkan resiko dan memastikan kelangsungan bisnis dengan secara proaktif membatasi dampak pelanggaran keamanan. SMKI biasanya membahas perilaku dan proses karyawan serta data dan teknologi. Ini dapat ditargetkan pada tipe data tertentu, seperti data pelanggan atau dapat diimplementasikan secara komprehensif yang menjadi bagian dari budaya perusahaan

SMKI adalah sistem manajemen keamanan informasi, sebuah metodologi yang memastikan tingkat keamanan informasi yang tinggi melalui proses yang ditetapkan dan praktek terbaik. Dalam konteks ISO, dapat dianggap SMKI sebagai standar untuk praktek keamanan yang bertanggung jawab

2.2 COBIT 5

2.2.1 Pengertian COBIT 5

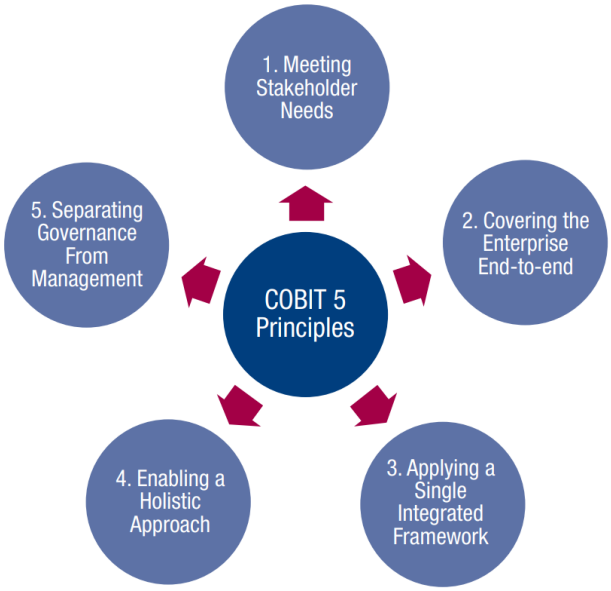
Control Objectives for Information and Related Technology atau yang biasa disebut dengan COBIT merupakan kerangka kerja yang berisi kumpulan dokumentasi dan panduan yang dikembangkan oleh *Information System Audit and Control Association* (ISACA). COBIT lebih mengarah pada Tata Kelola TI dan Manajemen IT yang dapat membantu pengguna, manajemen, dan auditor untuk menjembatani *gap* antara resiko bisnis, kebutuhan kontrol, dan masalah - masalah teknis IT (Sa'diyah & Manuputty, 2018).

Sampai saat ini COBIT telah melewati beberapa generasi. COBIT 5 merupakan salah satu generasi terbaru dari COBIT yang berhasil dikembangkan pada tahun 2012. COBIT 5 merupakan *framework* yang dirancang untuk mengukur kualitas sebuah tata kelola TI yang membantu agar lebih fokus pada *IT strategic value* dan memastikan penerapan TI dapat

mendukung tercapainya visi dan misi perusahaan atau institusi(Darmawan & Harto, 2019). Dalam *COBIT 5 Process Reference Model* terdapat 5 domain utama dengan 37 proses atau sub-domain yang selanjutnya pada penelitian ini akan disebut dengan sub-domain.

2.2.2 Prinsip COBIT 5

COBIT 5 memiliki lima prinsip yang memungkinkan tata kelola TI suatu perusahaan secara keseluruhan dengan mempertimbangkan kepentingan *stakeholder*. COBIT 5 bersifat generik dan dapat digunakan oleh berbagai skala perusahaan, baik komersial sampai dengan sektor publik (ISACA. & Lainhart, 2012). Berikut merupakan lima prinsip COBIT 5 yang digambarkan oleh Gambar 1 (ISACA, 2012).



Gambar 1. Lima Prinsip COBIT 5

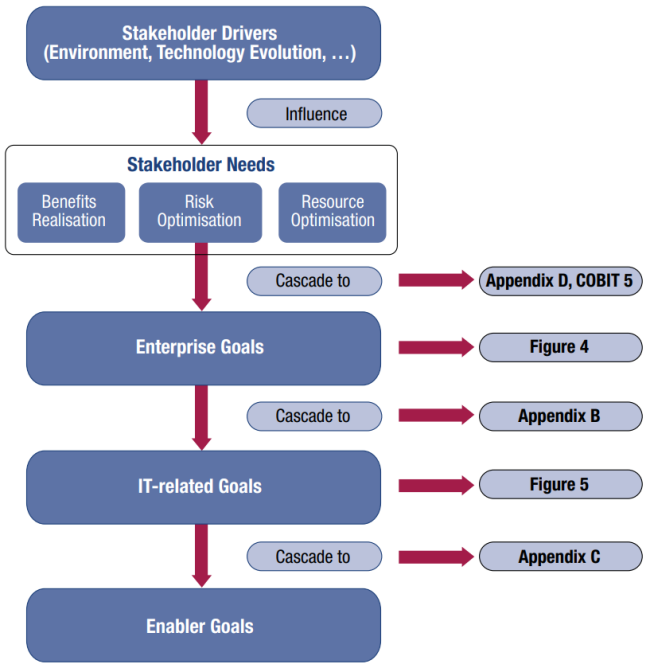
1. Prinsip 1: Memenuhi kebutuhan stakeholder

   Pada COBIT 5 tersedia semua proses yang dibutuhkan untuk mendukung penciptaan nilai bisnis melalui penggunaan TI. Penggunaan COBIT 5 dapat dikustomisasi agar selaras dengan konteks perusahaan melalui *goal cascade* (pengaliran tujuan). Pada *goal*

cascade akan diterjemahkan tujuan utama dari perusahaan menjadi tujuan yang dapat diatur, spesifik, dan berhubungan dengan TI.

Kemudian hasil terjemahan tersebut dipetakan menjadi beberapa proses dan praktek yang spesifik. Tata kelola juga berkaitan dengan negosiasi di antar stakeholder. Sistem tata kelola yang dibangun sebaiknya dapat mempertimbangkan seluruh stakeholder ketika membuat keputusan mengenai keuntungan, risiko, dan penugasan sumber daya. Kebutuhan dari stakeholder selanjutnya ditransformasikan ke dalam suatu strategi tindakan perusahaan.

Dapat disimpulkan, *Goal Cascade* COBIT 5 adalah mekanisme untuk menerjemahkan kebutuhan stakeholder menjadi beberapa tujuan spesifik pada setiap tingkatan dan area dalam mendukung tujuan utama perusahaan, memenuhi kebutuhan stakeholder, dan secara efektif mendukung keselarasan antara kebutuhan perusahaan dengan solusi dan layanan TI(ISACA, 2012). Berikut merupakan tahapan *Goals Cascading* yang dapat dilihat pada Gambar 2.



Gambar 2. Alur Tujuan dalam COBIT 5

a. Langkah 1. Penggerak stakeholder mempengaruhi kebutuhan stakeholder

   Jumlah dari penggerak stakeholder akan mempengaruhi kebutuhan stakeholder misalnya seperti perubahan strategi, lingkungan bisnis, dan teknologi baru.

b. Langkah 2. Kebutuhan stakeholder diturunkan menjadi tujuan perusahaan

   Pada kebutuhan stakeholder juga berhubungan dengan beberapa tujuan perusahaan. Tujuan perusahaan dikembangkan menggunakan dimensi BSC (*Balanced Scorecard*) kemudian hasilnya akan merepresentasikan sebuah daftar tujuan umum digunakan.

c. Langkah 3. Tujuan perusahaan diturunkan menjadi tujuan yang berhubungan dengan TI.

   Tujuan- tujuan yang berhubungan dengan TI, disusun dalam IT BSC. Gambar 3 merupakan 17 tujuan yang berhubungan dengan TI yang didefinisikan pada COBIT 5.

d. Langkah 4. Tujuan TI diturunkan menjadi *enabler goal* (pemicu tujuan)

   Dalam mencapai tujuan TI dibutuhkan beberapa penerapan yang sukses dan penggunaan sejumlah pemicu. Pemicu dapat meliputi proses, struktur organisasi, dan informasi.

IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Gambar 3. Tabel Tujuan Perusahaan dan tujuan *IT-Related* dalam COBIT 5 (ISACA, 2012)

2. Prinsip 2: Melingkup seluruh perusahaan

   Pada COBIT 5 terdapat suatu pandangan menyeluruh dan sistemik pada tata kelola dan manajemen TI perusahaan, berdasarkan beberapa pemicu/*enabler*. *Enabler* tersebut telah melingkupi seluruh perusahaan dari ujung ke ujung. Pendekatan yang digunakan dalam tata kelola adalah sebagai berikut :

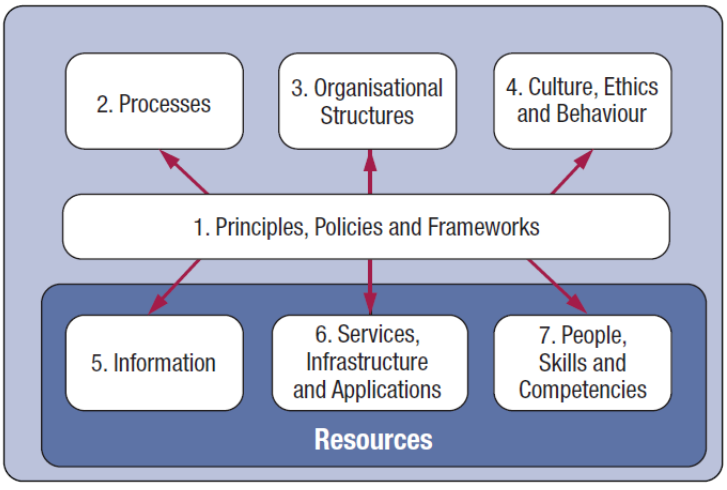
   a. Pemicu Tata Kelola
   b. Ruang Lingkup Tata Kelola
   c. Peran, Aktivitas, dan Hubungan

3. Prinsip 3: Menerapkan suatu kerangka tunggal yang terintegrasi

   Ada beberapa standar dan *best practices* yang berhubungan dengan TI, masing-masing daripada itu terdapat beberapa panduan dalam sebuah bagian dari aktivitas TI.

4. Prinsip 4: Menggunakan sebuah pendekatan yang menyeluruh

   Tata kelola dan manajemen TI perusahaan akan efektif dan efisien jika pendekatan diterapkan secara menyeluruh dan melibatkan beberapa komponen untuk saling bekerja sama. Tujuh kategori pemicu, ditunjukkan pada Gambar 4.



Gambar 4. Tujuh Kategori *Enablers* dalam COBIT 5 (ISACA, 2012)

Hubungan satu pemicu dengan lainnya harus dipertimbangkan secara matang oleh perusahaan. Setiap pemicu memerlukan masukan dari pemicu yang lain untuk dapat berfungsi secara efektif. Setiap pemicu juga akan memberikan keluaran yang bermanfaat bagi pemicu yang lain.

5. Prinsip 5: Pemisahan tata kelola dari manajemen

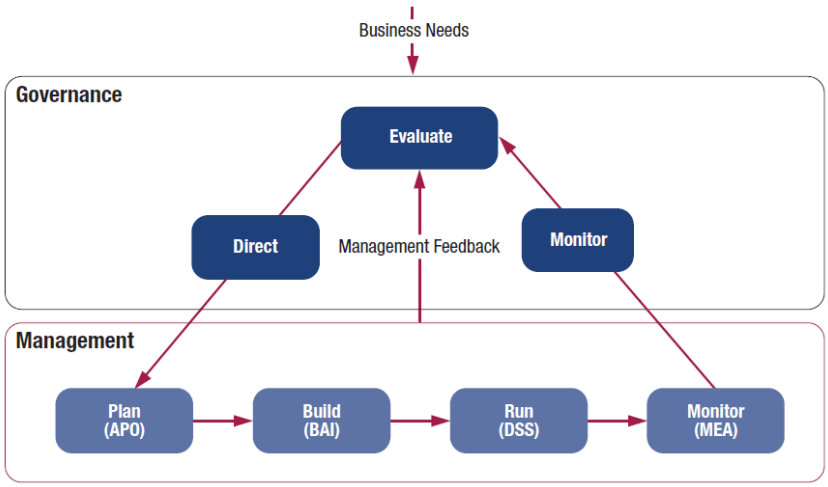
   Pada susunan kerangka COBIT 5 digambarkan suatu perbedaan yang jelas antara tata kelola dan manajemen. Aktivitas pada kedua disiplin juga berbeda. Masing- masing memerlukan struktur organisasi yang berbeda sekaligus melayani tujuan yang berbeda. Kunci perbedaan antara tata kelola dan manajemen adalah :

   a. Tata kelola

      Pada tata kelola akan menjamin beberapa kebutuhan stakeholder, kondisi, dan pilihan. Hal tersebut dilakukan melalui evaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati, menentukan arah dan pengambilan keputusan melalui penentuan prioritas, dan memantau pemenuhan kinerja terhadap tujuan dan arah.

   b. Manajemen

      Pada manajemen dilakukan perencanaan, pembangunan, pelaksanaan dan pemantauan aktivitas- aktivitas untuk menyelaraskan arah perusahaan yang telah ditentukan oleh badan pengelola dalam mencapai tujuan.



Gambar 5. Area Kunci Tata kelola dan Manajemen dalam COBIT 5 (ISACA, 2012)

Tata kelola dan manajemen memiliki tanggung jawab yang berbeda. Gambar 5 menjelaskan bahwa berdasarkan peranan tata kelola memerlukan suatu interaksi dengan manajemen untuk menghasilkan sistem tata kelola yang efektif dan efisien. Pada COBIT 5 terdapat model referensi proses yang menjelaskan secara detail mengenai proses tata kelola dan proses manajemen. Model referensi proses telah tersebut mewakili semua proses yang biasa ditemukan dalam perusahaan terkait aktivitas TI, serta menyajikan pemahaman yang mudah dalam operasional TI dan oleh manajer bisnis.

Model referensi proses dapat dilihat pada Gambar 6. Dimana model referensi proses terbagi menjadi dua domain proses utama yaitu:

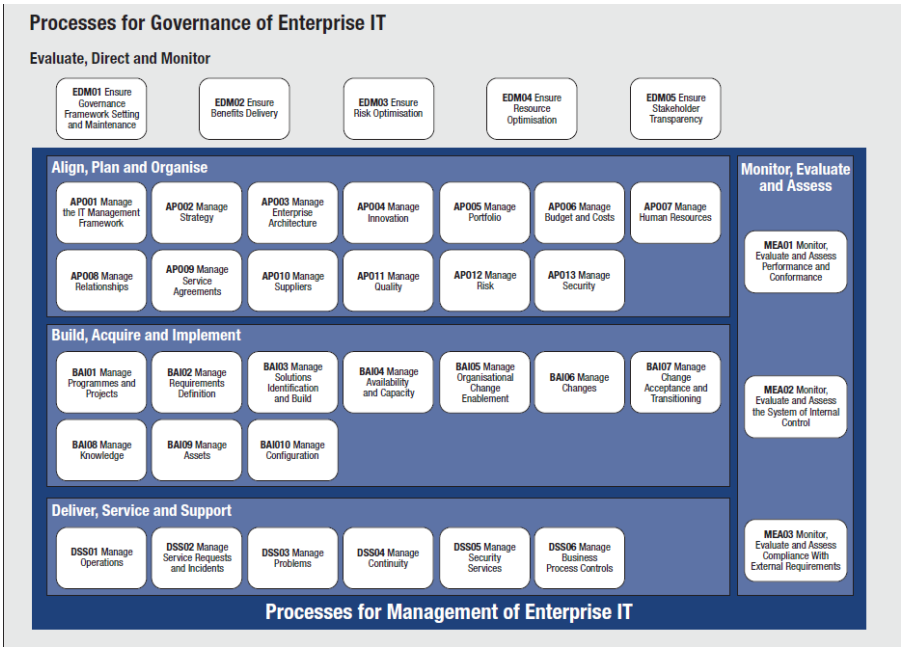
1. Tata Kelola

   Dalam tata kelola terdapat lima proses yang akan menentukan praktek- praktek dalam setiap proses *Evaluate*, *Direct*, dan *Monitor* (EDM).

2. Manajemen

   Pada manajemen terdapat empat domain yang sejajar dengan area tanggung jawab dari *Plan, Build, Run, and Monitor* (PBRM), serta berhubungan dengan ruang lingkup TI yang menyeluruh dari ujung ke ujung. Domain ini adalah perkembangan dari domain dan struktur proses pada COBIT 4.1. Domain tersebut diantar

a. *Align, Plan, and Organize* (APO) – Penyelarasan, Perencanaan, dan Pengaturan
b. *Build, Acquire, and Implement* (BAI) – Membangun, Memperoleh, dan Mengimplementasikan
c. *Deliver, Service and Support* (DSS) – Mengirimkan, Layanan, dan Dukungan
d. *Monitor, Evaluate, and Assess* (MEA) – Pengawasan, Evaluasi, dan Penilaian



Gambar 6. Model Referensi Proses dalam COBIT 5(ISACA, 2012)

2.2.3 *Process* APO13

Align, Plan and Organise atau yang sering kali disingkat dengan APO merupakan salah satu domain yang terdapat pada Cobit 5. Domain ini menjelaskan tentang penyelarasan tujuan TI dan bisnis serta perencanaan dan pengorganisasian sumber daya TI(Sa'diyah & Manuputty, 2018). Domain APO sendiri memiliki 13 sub-domain dan pada studi kasus ini akan digunakan sub-domain APO13 dengan fokus pada pengelolaan keamanan. APO13 memiliki tiga *Management Practices* dengan rincian sebagai berikut (ISACA, 2012):

- APO13.01 Membangun dan memelihara *Information Security Management System* (ISMS)
- APO13.02 Mendefinisikan dan mengelola rencana perawatan risiko keamanan informasi
- APO13.03 Memantau dan mengulas *Information Security Management System* (ISMS)

2.3 Tingkat Kapabilitas

Tingkat kapabilitas atau *capability level* merupakan kapabilitas dari hasil penilaian tiap proses yang dinyatakan dengan nilai 0 sampai dengan 5. *Process capability levels* yang digunakan pada Cobit 5 merupakan adaptasi dari ISO/IEC 15504 dimana setiap tingkat kapabilitas berbanding lurus dengan situasi proses saat ini(Isaca et al., 2013). Berikut merupakan rincian tingkat dan kapabilitas dari *process capability levels* (Kristanto et al., 2016):

1) Level 0 - *Incomplete Process* :
   Proses yang belum atau gagal diimplementasikan.
2) Level 1 - *Performed Process* :
   Proses yang menentukan tercapainya tujuan.
3) Level 2 - *Managed Process* :
   Proses yang mencakup perencanaan, monitor, dan penyesuaian.
4) Level 3 - *Established Process*:
   Proses yang sudah dibangun kemudian diimplementasikan untuk mencapai hasil dari proses.
5) Level 4 - *Predictable Process*:
   Proses yang sudah dibangun kemudian dioperasikan dengan batasan batasan yang mampu meraih harapan dari proses.
6) Level 5 - *Optimizing Process*:
   Proses yang diprediksi secara terus-menerus ditingkatkan untuk memenuhi tujuan bisnis dan tujuan perusahaan.

Pada setiap level memiliki skala kematangan yang dapat dilihat pada Tabel 1 berikut :

Tabel 1. Skala Kematangan(Kristanto et al., 2016)

Skala kematangan	Level	Kapabilitas
0,00 - 0,50	Level 0	*Incomplete Process*
0,51 - 1,50	Level 1	*Performed Process*
1,51 - 2,50	Level 2	*Managed Process*
2,51 - 3,50	Level 3	*Established Process*
3,51 - 4,50	Level 4	*Predictable Process*
4,51 - 5,00	Level 5	*Optimizing Process*

Base Practice (BP) adalah proses penyediaan definisi tugas dan kegiatan yang bertujuan untuk menyelesaikan tujuan proses dan memenuhi outcome dari proses tersebut. setiap BP secara eksplisit berhubungan dengan sebuah *outcomes* (Sa'diyah & Manuputty, 2018). Persentase *outcome* didapatkan dari persentase dilakukannya *management practice*. Atau mengikuti Persamaan (1), Persamaan (2) dan Persamaan (3).

$$management\_practice = \frac{\sum aktivitas}{\sum total\_aktivitas} \times 100\% \quad (1)$$

$$outcome = \frac{\sum persentase\_BP}{\sum total\_BP} \times 100\% \quad (2)$$

$$IT\_process = \frac{\sum persentase\_outcome}{\sum total\_outcome} \times 100\% \quad (3)$$

Dalam menentukan kategori dari tiap hasil penilaian level menggunakan bentuk N-P-L-F dimana *process* akan dinyatakan lulus jika meraih kategori *Fully Achieved* (F) dengan ketentuan nilai yang diperoleh sebesar 85% s/d 100%. Apabila *process* meraih nilai dengan range >85% sehingga masuk kedalam kategori N-P-L maka penilaian tingkat kapabilitas tidak dapat dilanjutkan ke tingkat selanjutnya. Perusahaan/instansi diharuskan untuk

memenuhi *process* tersebut hingga mendapatkan kategori *Fully Achieve*d (F) untuk dapat melanjutkan ke tingkat kapabilitas selanjutnya(Hidayat, 2015).

N- 0%-15%	**P-** 15%-50%	**L-** 50%-85%	**F-** 85%-100%

(4)

Keterangan :

N : Not Achieved

P : *Partially Achieved*

L : *Largely Achieved*

F : *Fully Achieved*

2.4 Analisis Kesenjangan

Analisis kesenjangan atau *Gap Analysis* adalah suatu alat yang digunakan dalam evaluasi kinerja pengelolaan manajemen internal perusahaan. *Gap* digunakan sebagai alat bantu mengukur kualitas perusahaan. Dalam bidang bisnis dan manajemen *gap analysis* diartikan sebagai tolak ukur kinerja aktual dengan yang ditingkatkan. Semakin rendah hasil *gap analysis*, semakin baik kualitas kinerja perusahaan atau instansi tersebut (Tri, 2016). Berikut manfaat penerapan analisis kesenjangan:

1. Menilai kesenjangan aktual dengan yang diharapkan
2. Mengetahui peningkatan kinerja untuk menutup kesenjangan
3. Dasar pengambilan keputusan untuk memenuhi standar.

Untuk mengetahui nilai *gap*, terlebih dahulu mengetahui tingkat kematangan saat ini dan mengetahui tingkat kematangan yang diharapkan. Sehingga dapat dituliskan dengan rumus :

Gap = Nilai Ekspektasi - Nilai Realita (5)