# BAB II

# TINJAUAN PUSTAKA

## 2.1. Risiko

### 2.1.1. Definisi Risiko

Risiko berhubungan dengan ketidakpastian, ini terjadi oleh karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi. Sesuatu yang tidak pasti *(uncertain)* dapat berakibat menguntungkan atau merugikan. Menurut Wideman, ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang *(opportunity)*, sedangkan ketidakpastian yang menimbulkan akibat yang merugikan dikenal dengan istilah risiko *(risk)*. Secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan.

Vaughan (1997:18) mengemukakan beberapa definisi risiko sebagai berikut :

1. *Risk is the chance of loss* (risiko adalah kans kerugian)

   *Chance of Loss* dipergunakan untuk menunjukkan suatu keadaan dimana terdapat suatu keterbukaan terhadap kerugian atau suatu kemungkinan kerugian. Sebaliknya jika disesuaikan dengan istilah yang dipakai dalam statistik, maka *chance* sering dipergunakan untuk menunjukkan tingkat probabilitas akan munculnya situasi tertentu.

2. *Risk is the possibility of loss* (risiko adalah kemungkinan kerugian)

Istilah *possibility* berarti bahwa probabilitas sesuatu peristiwa berada di antara nol dan satu. Definisi ini sangat mendekati dengan pengertian risiko yang dipakai sehari-hari, kurang cocok dipakai dalam analisis secara kuantitatif.

3. *Risk is uncertainty* (risiko adalah ketidakpastian)

   Risiko selalu berhubungan dengan ketidakpastian.

## 2.2. Manajemen Risiko

### 2.2.1. Definisi Manajemen Risiko

Manajemen risiko adalah suatu pendekatan terstruktur atau metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman dan merupakan suatu rangkaian aktifitas manusia termasuk : penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan sumberdaya. Strategi yang dapat diambil antara lain adalah memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau semua konsekuensi risiko tertentu. Manajemen risiko tradisional terfokus pada risiko-risiko yang timbul oleh penyebab fisik atau legal seperti bencana alam atau kebakaran, kematian, serta tuntutan hukum.

Sasaran dari pelaksanaan manajemen risiko adalah untuk mengurangi risiko yang berbeda-beda yang berkaitan dengan bidang yang telah dipilih pada tingkat yang dapat diterima oleh masyarakat. Hal ini dapat berupa berbagai jenis ancaman yang disebabkan oleh lingkungan, teknologi, manusia, organisasi dan

politik. Di sisi lain pelaksanaan manajemen risiko melibatkan segala cara yang tersedia bagi manusia, khususnya, bagi entitas manajemen risiko (manusia, staff, dan organisasi).

Pengertian manajemen risiko menurut beberapa ahli sebagai berikut :

1. Manajemen risiko sebagai suatu pendekatan yang komprehensif untuk menangani semua kejadian yang menimbulkan kerugian *(Clough and Sears, 1994).*
2. Manajemen risiko juga merupakan suatu aplikasi dari manajemen umum yang mencoba untuk mengidentifikasi, mengukur, dan menangani sebab dan akibat dari ketidakpastian pada sebuah organisasi *(William, et.al., 1995, p.27).*

## 2.3. Teknologi Informasi

### 2.3.1. Definisi Teknologi Informasi

Teknologi Informasi (TI) adalah istilah umum untuk teknologi apa pun yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan atau menyebarkan informasi. TI menyatukan komputasi dan komunikasi berkecepatan tinggi untuk data, suara, dan video. Contoh dari Teknologi Informasi bukan hanya berupa komputer pribadi, tetapi juga telepon, TV, peralatan rumah tangga elektronik, dan piranti genggam modern.

Pengertian teknologi informasi menurut beberapa ahli teknologi informasi :

1. Teknologi Informasi adalah studi atau peralatan elektronika, terutama komputer, untuk menyimpan, menganalisa, dan mendistribusikan informasi apa saja, termasuk kata-kata, bilangan, dan gambar *(kamus Oxford, 1995)***.**
2. Teknologi Informasi adalah seperangkat alat yang membantu anda bekerja dengan informasi dan melaksanakan tugas-tugas yang berhubungan dengan pemrosesan informasi *(Haag & Keen, 1996).*
3. Teknologi Informasi tidak hanya terbatas pada teknologi komputer (*software* & *hardware*) yang digunakan untuk memproses atau menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi *(Martin, 1999).*

4. Teknologi Informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronis *(Lucas, 2000).*
5. Teknologi Informasi adalah teknologi yang menggabungkan komputasi (komputer) dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan video *(William & Sawyer, 2003).*

Dalam konteks bisnis, *Information Technology Association of America* menjelaskan pengolahan, penyimpanan dan penyebaran vokal, informasi bergambar, teks dan numerik oleh mikro elektronika berbasis kombinasi komputasi dan telekomunikasi. Istilah dalam pengertian modern pertama kali muncul dalam sebuah artikel 1958 yang diterbitkan dalam *Harvard Business Review*, di mana penulis Leavitt dan Whisler berkomentar bahwa "Teknologi baru belum memiliki nama tunggal yang didirikan. Kita akan menyebutnya teknologi informasi (TI)". Beberapa bidang modern dan muncul teknologi informasi adalah generasi berikutnya teknologi *web*, bioinformatika, *cloud computing*, sistem informasi global, skala besar basis pengetahuan dan lain-lain.

## 2.4. *Control Objective for Information and related Technology* (COBIT)

### 2.4.1. COBIT *Overview*

*Control Objective for Information and related Technology* atau yang lebih dikenal sebagai COBIT dirilis dan disusun oleh *IT Governance Institute* (ITGI) yang merupakan bagian dari ISACA *(Information Systems Audit and Control Association)* pada tahun 1996. COBIT versi pertama diterbitkan pada tahun 1996,

versi kedua tahun 1998, versi 3.0 di tahun 2000, versi 4.0 pada tahun 2005 dan COBIT 4.1 dirilis pada tahun 2007 serta versi terakhir yang baru saja dirilis tahun 2011 adalah COBIT versi 5.

### 2.4.2. COBIT Versi 5

COBIT 5 menggabungkan COBIT 4.1, Val IT 2.0 dan Risiko TI serta konsep-konsep dari Model Bisnis Informasi untuk kerangka kerja yang rinci bagi tata kelola dan manajemen yang efektif dari TI yang mengaktifkan bisnis. COBIT 4.1 memastikan bahwa TI bekerja seefektif mungkin untuk memaksimalkan keuntungan dari investasi teknologi, Val IT membantu perusahaan membuat keputusan yang lebih baik tentang di mana untuk berinvestasi, memastikan bahwa investasinya konsisten dengan strategi bisnis. COBIT 4.1 menyediakan satu set kontrol untuk mengurangi risiko TI dalam proses TI sementara RiskIT menyediakan kerangka kerja bagi perusahaan untuk mengidentifikasi, mengatur dan mengelola risiko yang berhubungan dengan TI.

COBIT 5 adalah kerangka *end-to-end* yang menggabungkan banyak kerangka kerja serta dirancang untuk memenuhi kebutuhan *stakeholder* saat ini. COBIT 5 fokus pada tata kelola dan manajemen informasi perusahaan. COBIT 5 mengadopsi pandangan ISO 38500 mengenai perlunya tata kelola TI dan manajemen TI dan menggunakan model *Evaluate, Direct and Monitor* ISO 38500. COBIT 5 mengarahkan TI dan bidang fungsional bisnis di seluruh perusahaan serta mempertimbangkan kepentingan TI yang berhubungan dari semua *stakeholder*. Ini membantu organisasi untuk menciptakan nilai bagi

investasi IT dengan menjaga keseimbangan antara pengoptimalan tingkat risiko dan menyadari manfaat.

### 2.4.2.1. Prinsip dalam COBIT 5

COBIT 5 dibangun di atas 5 prinsip utama untuk tata kelola dan manajemen teknologi informasi perusahaan. Berikut ini pemaparan mengenai prinsip-prinsip COBIT 5 :




**Gambar 2.2.** Prinsip-Prinsip COBIT 5 (COBIT 5, 2012)

1. **Prinsip 1 : Memenuhi Kebutuhan *Stakeholder***

   Perusahaan ada untuk menciptakan nilai bagi para *stakeholder* mereka, sehingga penciptaan nilai merupakan tujuan tata kelola semua perusahaan. Penciptaan nilai berarti menyadari manfaat dengan mengoptimalkan biaya sumber daya, sementara disisi lain mengoptimalkan risiko.




**Gambar 2.3.** Objektif Tata Kelola : Penciptaan Nilai (COBIT 5, 2012)

2. **Prinsip 2 : Meliputi *End-to-End* Perusahaan**

   COBIT 5 mengintegrasikan tata kelola TI perusahaan dalam tata kelola perusahaan, karena meliputi organisasi secara keseluruhan (fokus tidak hanya pada fungsi TI). Hal ini juga mencakup semua hal yang berhubungan dengan TI sehingga memberikan dasar untuk mengintegrasikan kerangka kerja lainnya, standar dan praktek yang digunakan.

3. **Prinsip 3 : Menerapkan Kerangka Tunggal yang Terintegrasi**

   Kebanyakan standar TI terkait dan praktik terbaik hanya mengatasi bagian tertentu dari kegiatan TI, COBIT sejalan dengan standar lain yang relevan dan kerangka kerja pada tingkat tinggi sehingga membuat kerangka kerja menyeluruh untuk tata kelola dan manajemen perusahaan TI.

4. **Prinsip 4 : Mengaktifkan Pendekatan Holistik**

Tata kelola yang efektif dan manajemen TI perusahaan membutuhkan pendekatan TI secara menyeluruh, COBIT 5 mengimplementasikan tata kelola yang komprehensif dan manajemen perusahaan TI melalui *enabler*. *Enabler* adalah hal-hal yang memungkinkan perusahaan untuk mencapai tujuannya. COBIT 5 mendefinisikan 7 kategori *enabler,* yaitu :

1. Prinsip, kebijakan dan kerangka kerja : merupakan alat untuk menyampaikan tata cara yang diingikan melalui panduan praktik untuk manajemen sehari-hari.
2. Proses : mendeskripsikan praktik dan aktifitas yang dikelola untuk mencapai tujuan dan menghasilkan *output* dalam mendukung tujuan terkait TI.
3. Struktur organisasi : entitas pengambilan keputusan penting dalam organisasi.
4. Budaya, etika dan perilaku : hal ini baik bagi individu maupun organisasi, merupakan salah satu faktor kesuksesan tata kelola dan manajemen yang seringkali diremehkan.
5. Informasi : informasi menyebar di seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. Informasi dibutuhkan agar organisasi tetap berjalan dan dikelola dengan baik. Pada level operasional, informasi merupakan produk kunci dari *enterprise* itu sendiri.

6. Layanan, infrastruktur dan aplikasi : termasuk infrastruktur, teknologi dan aplikasi yang memberikan layanan dan proses TI bagi *enterprise.*
7. Manusia, keterampilan dan kompetensi : berhubungan dengan manusia dan dibutuhkan untuk kesuksesan segala aktifitas, serta untuk pengambilan tindakan dan keputusan yang tepat.

**5. Prinsip 5 : Memisahkan Tata Kelola dari Manajemen**

Kerangka kerja COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua disiplin ini secara fundamental melayani tujuan yang berbeda, masing-masing meliputi berbagai jenis kegiatan dan memerlukan struktur organisasi yang berbeda. Tata kelola memastikan kebutuhan stakeholder, kondisi dan pilihan dievaluasi untuk menentukan keseimbangan, sepakat pada tujuan perusahaan yang ingin dicapai, menetapkan arah melalui prioritas dan pengambilan keputusan, pemantauan kinerja dan kepatuhan terhadap arah dan tujuan yang disepakati. Sedangkan manajemen disini merencanakan, membangun, menjalankan dan memantau kegiatan yang sejalan dengan arah yang ditetapkan oleh tata kelola untuk mencapai tujuan perusahaan.

#### 2.4.2.2. Domain dan Proses COBIT 5

COBIT 5 memiliki 5 domain yang terbagi kedalam domain tata kelola dan domain manajemen, setiap domain memiliki proses yang memungkinkan untuk mencapai tujuannya. Satu domain tertuju pada tata kelola dan empat domain lainnya mencakup manajemen.

#### 2.4.2.3. *Governance of Enterprise IT* (GEIT)

Domain tata kelola TI perusahaan berisi lima proses, dimana didalam setiap proses berisi tentang *evaluate, direct* dan *monitoring practice* (EDM) yang telah ditetapkan. Tabel dibawah ini berisi tingkat tinggi proses TI untuk domain EDM.

**Tabel 2.1.** Proses TI untuk Domain EDM

| | |
|---|---|
| **EDM01** | Memastikan Pengaturan Kerangka Kerja Tata Kelola dan Pemeliharaan |
| **EDM02** | Memastikan Penyampaian Manfaat |
| **EDM03** | Memastikan Optimasi Risiko |
| **EDM04** | Memastikan Optimasi Sumber Daya |
| **EDM05** | Memastikan Transparansi *Stakeholder* |

#### 2.4.2.4. *Management of Enterprise IT*

Domain manajemen TI perusahaan sejalan dengan bidang tanggung jawabnya yaitu *plan, build, run* dan *monitor* (PBRM). Berikut ini adalah keempat domain manajemen :

1. *Align, Plan and Organize (APO),* 13 proses.
2. *Build, Acquire and Implement (BAI),*10 proses.
3. *Deliver, Service and Support (DSS),* 6 proses.
4. *Monitor, Evaluate and Assess (MEA),* 3 proses.

##### 2.4.2.4.1. *Align, Plan and Organize* (APO)

Domain *Align, Plan and Organize* mencakup penggunaan informasi dan teknologi dan bagaimana cara terbaik penggunaan informasi dan teknologi dalam sebuah organisasi untuk membantu mencapai tujuan dan sasaran organisasi. Domain ini juga melihat bentuk organisasi dan infrastruktur TI dalam rangka untuk mencapai hasil yang optimal dan menghasilkan manfaat paling dari penggunaan TI. Tabel berikut berisi proses TI tingkat tinggi untuk domain APO.

**Tabel 2.2.** Proses TI untuk Domain APO

| Proses | Keterangan |
|---|---|
| **APO01** | Mengelola Kerangka Kerja Manajemen TI |
| **APO02** | Mengelola Strategi |
| **APO03** | Mengelola Enterprise Architecture |
| **APO04** | Mengelola Inovasi |
| **APO05** | Mengelola Portofolio |
| **APO06** | Mengelola Anggaran dan Biaya |
| **APO07** | Mengelola Hubungan Manusia |
| **APO08** | Mengelola Hubungan |
| **APO09** | Mengelola Perjanjian Layanan |
| **APO10** | Mengelola Pemasok |
| **APO11** | Mengelola Kualitas |
| **APO12** | Mengelola Risiko |
| **APO13** | Mengelola Keamanan |

#### 2.4.2.4.2. *Build, Acquire and Implement* (BAI)

Domain *Build, Acquire and Implement* meliputi identifikasi kebutuhan TI, penguasaan teknologi, dan pengimplementasiannya dalam proses bisnis perusahaan saat ini. Tabel berikut berisi daftar tujuan pengendalian tingkat tinggi untuk domain BAI.

**Tabel 2.3.** Proses TI untuk Domain BAI

| Proses | Keterangan |
|---|---|
| **BAI01** | Mengelola Program dan Proyek |
| **BAI02** | Manage Definisi Persyaratan |
| **BAI03** | Mengelola Identifikasi Solusi dan Membangun |
| **BAI04** | Mengelola Ketersediaan dan Kapasitas |
| **BAI05** | Mengelola Pemberdayaan Perubahan Organisasi |
| **BAI06** | Mengelola Perubahan |
| **BAI07** | Mengelola Penerimaan Perubahan dan Transisi |
| **BAI08** | Mengelola Pengetahuan |
| **BAI09** | Mengelola Aset |
| **BAI10** | Mengelola Konfigurasi |

#### 2.4.2.4.3. *Deliver, Service and Support* (DSS)

Domain *Deliver, Service and Support* berfokus pada aspek penyampaian teknologi informasi. Ini mencakup bidang-bidang seperti eksekusi aplikasi di dalam sistem TI dan hasil-hasilnya, serta proses pendukung yang memungkinkan pelaksanaan sistem TI yang efektif dan efisien. Tabel berikut berisi daftar tujuan pengendalian tingkat tinggi untuk domain DSS.

**Tabel 2.4.** Proses TI untuk Domain DSS

| Proses | Keterangan |
|---|---|
| **DSS01** | Mengelola Operasi |
| **DSS02** | Mengelola Layanan Permintaan dan Insiden |
| **DSS03** | Mengelola Masalah |
| **DSS04** | Mengelola Keberlangsungan |
| **DSS05** | Mengelola Layanan Keamanan |
| **DSS06** | Mengelola Pengendalian Proses Bisnis |

#### 2.4.2.4.4. *Monitor, Evaluate and Assess* (MEA)

Domain *Monitor, Evaluate and Assess* berhubungan dengan strategi perusahaan dalam menilai kebutuhan perusahaan dan menilai apakah sistem TI saat ini masih memenuhi tujuan yang sudah dirancang dan pengendalian yang diperlukan untuk memenuhi regulasi persyaratan. Pemantauan juga mencakup masalah penilaian independen terhadap kemampuan efektivitas sistem TI untuk memenuhi tujuan bisnis dan proses-proses pengendalian perusahaan oleh auditor internal dan eksternal. Tabel berikut berisi daftar tujuan pengendalian tingkat tinggi untuk domain MEA.

**Tabel 2.5.** Proses TI untuk Domain MEA

| Proses | Keterangan |
|---|---|
| **MEA01** | Monitor, Evaluasi dan Menilai Kinerja dan Kesesuaian |

| | |
|---|---|
| **MEA02** | Monitor, Evaluasi dan Menilai Sistem Pengendalian Internal |
| **MEA03** | Mengevaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal |

### 2.4.2.5. *Process Capability Model*

COBIT 5 meliputi *process capability model* berdasarkan ISO/IEC 15504 yang diakui secara internasional. Model ini akan mencapai tujuan keseluruhan penilaian proses dan mendukung proses perbaikan, yaitu akan menyediakan sarana untuk mengukur kinerja dari setiap proses tata kelola (berbasis EDM) atau manajemen proses (berbasis PBRM), dan akan memungkinkan area perbaikan dapat teridentifikasi. Skala Peringkat dari *process capability model* ini melibatkan enam tingkat kemampuan, yaitu :

1. **Level 0, *Incomplete Process*** : Proses ini tidak dilaksanakan atau gagal untuk mencapai tujuan prosesnya. Pada tingkat ini, ada sedikit bukti atau bahkan tidak ada bukti setiap pencapaian sistematis dari tujuan proses.
2. **Level 1, *Performed Process (one attribute)*** : Proses dilaksanakan dan mencapai tujuan prosesnya.
3. **Level 2, *Managed process (two attributes)*** : Proses yang dilakukan sekarang diimplementasikan, dikelola (direncanakan, dimonitor dan disesuaikan) dan produk kerja yang tepat ditetapkan, dikendalikan dan dipelihara.
4. **Level 3, *Established Process (two attributes)*** : Proses yang dikelola kini diterapkan menggunakan proses yang telah ditetapkan yang mampu mencapai hasil prosesnya.

5. **Level 4, *Predictable Process (two attributes)*** : Proses yang ditetapkan sekarang beroperasi dalam batas yang telah ditetapkan untuk mencapai hasil prosesnya.
6. **Level 5, *Optimizing process (two attributes)*** : Proses diprediksi untuk terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan tujunan bisnis masa datang.

*Process capability model* menggunakan skala peringkat ISO/IEC 15504 untuk menetapkan peringkat masing-masing tujuan tercapai. Peringkat ini seperti dijelaskan pada tabel 2.6 dibawah ini :

**Tabel 2.6. Persentase Peringkat (COBIT 5, 2012)**

| ***Abbreviation*** | ***Description*** | ***%Achieved*** |
|---|---|---|
| ***N*** | *Not achieved* | *0 to 15% achievement* |
| ***P*** | *Partially achieved* | *>15% to 50% achievement* |
| ***L*** | *Largely achieved* | *>50% to 85% achievement* |
| ***F*** | *Fully achieved* | *>85% to 100% achievement* |

1. ***Not achieved***. Terdapat sedikit bukti atau bahkan tidak ada bukti dari pencapaian atribut yang ditetapkan pada proses yang dinilai.
2. ***Partially achieved***. Terdapat beberapa bukti dan beberapa pencapaian dari atribut yang ditetapkan pada proses yang dinilai. Beberapa aspek pencapaian atribut mungkin tidak dapat diprediksi.

3. ***Largely achieved***. Terdapat bukti pendekatan sistematis untuk proses yang dinilai dan terdapat pencapaian yang signifikan. Beberapa kelemahan terkait dengan atribut ini mungkin ada dalam proses yang dinilai.
4. ***Fully achieved***. Terdapat bukti dari pendekatan yang lengkap dan sistematis dari atribut yang ditetapkan dalam proses yang dinilai. Terdapat bukti dari pendekatan yang lengkap dan sistematis terhadap pencapaian keseluruhan. Tidak ada kelemahan signifikan yang berhubungan dengan atribut ini ada dalam proses dinilai.

Dalam melakukan proses penilaian *capability* level proses COBIT, masing-masing proses dicek secara bertahap apakah proses tersebut telah memenuhi persyaratan-persyaratan yang harus dipenuhi pada masing-masing level, mulai dari level 1 hingga level 5. Selain itu, terdapat ketentuan kategori dari hasil penilaian ditiap levelnya, yaitu suatu proses cukup meraih kategori *Largely achieved* (L) dengan range nilai berkisar 50-85% atau *Fully achieved* (F) dengan range nilai berkisar 85%-100% untuk dapat dinyatakan bahwa proses tersebut telah meraih suatu level kapabilitas tersebut, namun proses tersebut harus meraih kategori *Fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas berikutnya. Template ringkasan pencapaian *capability level* ditunjukkan pada tabel di bawah ini :

**Tabel 2.6.** Template Ringkasan Pencapaian *Capability* Level

| Tujuan | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Proses | Level 0 | Level 1 | Level 2 | | Level 3 | | Level 4 | | Level 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| Rating | | | | | | | | | | |

### 2.4.2.6. Menghitung *Process Capability Level*

Untuk menghitung pencapaian danri *process capability level*, dilakukan dengan cara perhitungan seperti berikut ini :

$$\textit{Capability Level} = \frac{(0*y_0) + (1*y_1) + \ldots + (5*y_5)}{z}$$

Keterangan :

$y_n$ ($y_{0...}y_5$) = jumlah proses yang berada dilevel n

z = jumlah proses yang dievaluasi