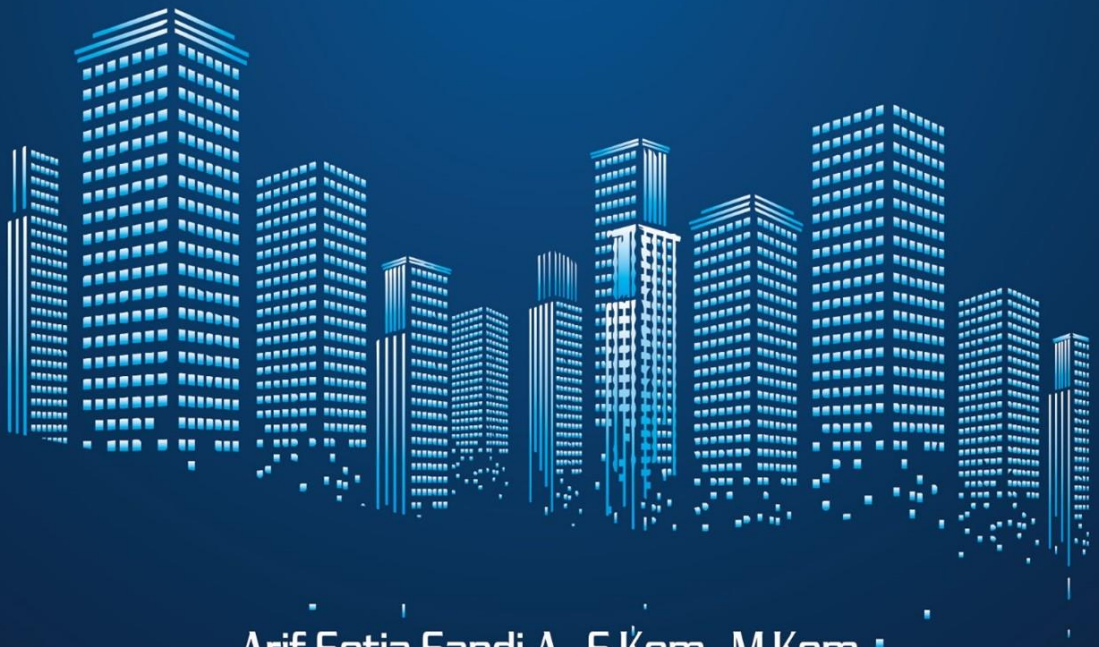
2022

MANAJEMEN RISIKO TI



Arif Setia Sandi A., S.Kom., M.Kom.

MANAJEMEN RISIKO TI

Arif Setia Sandi A., M.Kom.

Judul:
Manajemen Risiko TI

Penulis:
Arif Setia Sandi A, M. Kom.

ISBN:
978-623-99856-4-6

Editor:
Hadi Jayusman, S.Kom., M.T.

Penyunting:
Deny Nugroho Triwibowo, S.Kom., M.Kom.

Penerbit:
CV. ELVARETTA BUANA

Redaksi:
Perum Puri Sumelap Blok B6,
Kota Tasikmalaya 46196.
Tlp/Hp : +6285320608563
Email : mruhtiani@gmail.com

Kata Pengantar

Puji syukur kepada Allah SWT, Shalawat serta salam semoga tercurahkan kepada Nabi Muhammad SAW. Atas karunia dan limpahan ramhatNya, penulis masih diberikan kesempatan untuk menulis buku ini hinggai selesai.

Pada buku ini, penulis menyajikan secara kajian teori yang diambil dari berbagai sumber mengenai manajemen risiko teknologi informasi. Topik yang dibahas pada buku ini meliputi teori tentang tata kelola teknologi informasi beserta *framework* tata kelola teknologi informasi, dan konsep-konsep manajemen risiko teknologi informasi. Buku ini diharapkan dapat menjadi sumber maupun referensi belajar tambahan bagi masyarakat yang membacanya, khususnya sebagai bahan belajar bagi pelajar yang ingin mendalami topik tentang manajemen risiko TI.

Akhir kata penulis mengucapkan terima kasih kepada keluarga dan semua pihak yang telah memberi dukungan terhadap penulisan buku ini. Semoga buku ini memiliki banyak manfaat, Aamiin.

Banyumas, Agustus 2022

Penulis

Daftar Isi

BAB I TATA KELOLA TEKNOLOGI INFORMASI

1.1. Sejarah Teknologi Informasi

Informasi merupakan suatu keterangan atau pernyataan yang mendandung nilai tertentu. Sejatinya informasi sudah ada pada era awal kehidupan manusia di bumi, hanya saja metode penyampaian informasi seperti yang kita lakukan pada zaman ini tentu berbeda dengan penyampaian informasi pada zaman dahulu. Perbedaan itulah yang dapat kita sebut sebagai teknologi. Dikutip dari Kamus Besar Bahasa Indonesia bahwa teknologi merupakan salah satu ilmu pengetahuan terapan sekaligus sebagai metode ilmiah untuk mencapai berbagai macam tujuan. Tujuan yang dimaksudkan disini sebagai contoh ingin memberikan informasi tentang sebuah benda kepada orang lain, dengan cara menyampaikan informasi tersebut melalui media lisan, menyampaikan informasi melalui media tulis dan lain sebagainya.

Teknologi informasi secara terus menerus dikembangkan agar dapat membantu manusia untuk membuat sebuah berita informasi, menyimpan dan mengubah agar lebih mudah untuk disebarkan kepada manusia lain secara luas. Hingga era kehidupan sekarang, jika berbicara teknologi informasi, yang muncul dalam pikiran kita ialah penerapan dan penggabungan antara perangkat lunak atau *software* dengan perangkat keras atau *hardware.*

Hingga kini, teknologi telah bergerak dengan menyatukan komunikasi dengan komputasi untuk mempercepat penyebaran informasi melalui berbagai media visual seperti data, suara, gambar maupun video. Teknologi menjadi salah satu kebutuhan pokok masyarakat di wilayah negara berkembang maupun negara maju. Teknologi memegang peranan penting dalam kehidupan manusia era modern, teknologi bahkan telah merasuk kedalam kehidupan manusia dan menjadi sebuah alat utama yang digunakan manusia untuk menjalankan segala aktivitas sehari-hari.

Perkembangan yang begitu cepat terhadap teknologi tentunya membuat segala lini kehidupan harus menyesuaikan dan mampu beradaptasi dengan cepat untuk menghindari ketertinggalan. Tanpa disadari, hal yang terkesan sepele yang dilakukan oleh manusia, pun sudah tersentuh oleh teknologi, seperti menyampaikan kabar kepada kerabat atau rekanan, barang tentu sudah tersentuh teknologi melalui media telepon selular. Telepon selular yang kini telah berkembang menjadi telepon pintar membuat manusia semakin dipermudah dalam berkomunikasi, hingga dapat mendengarkan suara maupun tatap wajah secara virtual, dan masih banyak sisi teknologi yang mungkin belum disadari telah merubah gaya hidup penggunanya.

1.2. Tata Kelola Teknologi Informasi

Perkembangan teknologi informasi ini juga menjadikan setiap penggunanya dapat mengakses berbagai data-data dan informasi-informasi yang dibutuhkan dengan mudah dan cepat. Peningkatan penggunaan teknologi informasi dalam berbagai bidang yang terjadi saat ini sebenarnya juga diikuti dengan perubahan proses bisnisnya, seperti halnya dalam perusahaan. Pengembangan strategi bisnis selalu dikaitkan dengan pengembangan strategi teknologi informasi. Kemunculan ini

terjadi karena tidak jarang pelaksanaan strategi sistem informasi yang direncanakan tidak berjalan optimal. Disiplin tata kelola teknologi informasi merupakan bagian yang sangat penting dari proses bisnis perusahaan dalam implementasi teknologi informasi secara keseluruhan.

Keberlangsungan proses bisnis pada suatu perusahaan tentunya tidak akan terlepas dari peran tata kelola teknologi informasi pada perusahaan itu sendiri. setiap perusahaan yang sudah berjalan secara professional seharusnya telah memiliki standar dan sudah mampu menerapkan standar operasional prosedur guna mencapai tujuan perusahaan dengan target meningkatkan nilai profit bisnisnya.

Tata kelola teknologi informasi menjadi tanggung jawab sekaligus bentuk penerapan dari konsep perusahaan yang umumnya digunakan para eksekutif bisnis untuk dapat menyiapkan konsep untuk mencapai target perusahaan. Tata kelola teknologi informasi dapat digunakan oleh organisasi atau perusahaan pada level eksekutif untuk mengendalikan risiko yang kemungkinan dapat terjadi dan memastikan secara keseluruhan bentuk sumber daya perusahaan agar dapat digunakan dengan sebagaimana mestinya. Jika tata kelola perusahaan dapat dilaksanakan secara baik dan konsisten, akan mempengaruhi tingkat kepercayaan serta perlindungan investasi di masa depan yang lebih terjamin dan berujung pada meningkatknya nilai asset perusahaan.

Beberapa definisi tentang tata kelola teknologi informasi:

- Menurut Gartner, tata kelola teknologi informasi dimaknai sebagai proses yang memastikan penggunaan teknologi informasi berjalan efektif dan efisien dalam memungkinkan suatu organisasi untuk mencapai tujuannya. Tata kelola permintaan teknologi informasi adalah proses yang digunakan organisasi untuk

memastikan evaluasi, seleksi, penentuan prioritas, dan pendanaan investasi teknologi informasi yang bersaing secara efektif; awasi implementasi mereka; dan mengekstrak manfaat bisnis.

- Menurut Weill dan Ross, tata kelola teknologi informasi sebagai hak keputusan dan kerangka kerja akuntabilitas untuk mendorong perilaku yang diinginkan dalam penggunaan teknologi informasi. Ada tiga komponen tata kelola:
  1) domain keputusan TI;
  2) pola dasar tata kelola TI;
  3) mekanisme implementasi.

Tata kelola teknologi informasi terutama berkaitan dengan hubungan antara fokus bisnis perusahaan dan manajemen dan operasi perusahaan yang terkait dengan implementasi teknologi informasi. Konsep ini berfokus terhadap pentingnya hal-hal yang terkait dengan penerapan teknologi informasi dan menekankan bahwa keputusan strategis teknologi informasi harus dimiliki oleh tingkat manajemen perusahaan yang paling tinggi. Diharapkan konsep tata kelola teknologi ini telah benar-benar berjalan dari level manajemen tertinggi. Hasil dari proses ini adalah beberapa proses teknologi informasi yang sangat luar biasa yang akan mengubah banyak perusahaan guna peningkatan efisiensi dan profitabilitas perusahaan itu sendiri.

Namun tidak jarang, banyak perusahaan mengalami beberapa kegagalan dalam implementasi sistem teknologi informasi karena perencanaan yang buruk pada awal berjalannya proses bisnis, kesalahan Langkah sejak awal dapat menimbulkan kesalahan hingga target akhir dari proses bisnis tersebut. Kegagalan yang dimaksud dapat terjadi pada beberapa hal seperti pembengkakan biaya, kesalahan teknis dalam menjalankan proses bisnis, ketidaksesuaian tenaga sumber daya manusia yang dipilih

dengan bidang yang dikelola, maupun kegagalan dalam membaca situasi pasar.

Dikutip dari buku yang berjudul *Executive's Guide to IT Governance*, hampir setiap kasus, proses tata kelola berkaitan hal-hal berikut:

- Mengendalikan semua aspek pekerjaan yang bersinggungan dengan teknologi informasi
- Koordinasi antara bagian-bagian berbeda dari pekerjaan terkait teknologi informasi, seperti pengembangan sistem baru pada bidang kepegawaian, dukungan infrastruktur teknologi informasi pada divisi keuangan, dan lain-lain
- Pengukuran hasil sistem dan proses teknologi informasi.
- Kepatuhan terhadap kebijakan atau peraturan terkait teknologi informasi pada internal perusahaan.
- Justifikasi pengeluaran untuk setiap pengelolaan *resource* teknologi informasi
- Akuntabilitas dan transparansi teknologi informasi
- Membangun komunikasi yang kuat terhadap pengguna teknologi informasi

Tidak sedikit kasus dari tata kelola teknologi informasi ini menyangkut kualitas dari sistem teknologi informasi yang ditelah berjalan. Termasuk masalah implementasi teknologi yang lebih baru, sistem teknologi informasi yang masih menggunakan teknologi lama, masalah keamanan data, dokumentasi, dan banyak sisi kelamahan lain yang mungkin belum ditemukan. Untuk mengantisipasi masalah pada tata kelola teknologi informasi ini lebih utama untuk diselesaikan dahulu kepada masalah manajemen. Masalah teknologi informasi utamanya harus menjadi masalah bagi eksekutif tingkat dewan, karena beberapa masalah yang timbul dalam implementasi teknologi informasi lebih bersifat teknis, beberapa keputusan penting lebih seharusnya melibatkan dan atau diserahkan kepada tenaga professional TI. Tata kelola

teknologi informasi menyiratkan sistem di mana semua pemangku kepentingan, termasuk dewan, pelanggan internal, dan bidang terkait seperti keuangan memiliki masukan yang diperlukan ke dalam proses pengambilan keputusan.

2.2.1. Domain Tata Kelola TI

Menurut ISACA (2013) tata kelola teknologi informasi dipecah menjadi lima domain:

- **Kerangka kerja tata kelola teknologi informasi**
  Organisasi perlu menerapkan kerangka kerja tata kelola teknologi informasi yang tetap sejalan dengan tata kelola perusahaan dan pendorong utama (baik internal maupun eksternal) yang mengarahkan perencanaan, tujuan, dan sasaran strategis perusahaan. Sehingga berjalannya proses bisnis dalam perusahaan tetap dalam kontrol dan pantuan jalur yang tepat guna tercapainya tujuan perusahaan.

- **Manajemen strategis**
  Agar efektif dalam memungkinkan dan mendukung pencapaian tujuan bisnis, strategi bisnis harus menggerakkan strategi teknologi informasi. Dengan demikian, strategi bisnis dan teknologi informasi secara intrinsik terkait dan operasi bisnis dan pertumbuhan yang efektif dan efisien bergantung pada keselarasan yang tepat dari keduanya.

- **Realisasi manfaat**
  Tata kelola teknologi informasi membantu bisnis mewujudkan manfaat bisnis yang dioptimalkan melalui manajemen efektif investasi yang memungkinkan teknologi informasi. Seringkali ada kekhawatiran yang cukup tinggi pada tingkat dewan atau manajemen senior

bahwa inisiatif teknologi informasi tidak diserap kedalam manfaat bisnis.

- **Optimalisasi risiko**
  Dalam dunia digital yang semakin terintegrasi satu sama lain, identifikasi, penilaian, mitigasi, manajemen, komunikasi dan pemantauan risiko bisnis terkait teknologi informasi merupakan komponen integral dari kegiatan tata kelola perusahaan.

- **Optimalisasi sumber daya**
  Untuk meningkatkan nilai efektif dalam implementasinya, teknologi informasi membutuhkan sumber daya yang cukup, kompeten dan mampu (orang, informasi, infrastruktur dan aplikasi) untuk memenuhi tuntutan bisnis dan melaksanakan kegiatan yang diperlukan untuk memenuhi tujuan strategis dalam jangka panjang.

2.2.2. Masalah Risiko Perusahaan pada Tata Kelola Teknologi Informasi

Setiap perusahaan memiliki berbagai risiko yang terkadang berbeda-beda, permasalahan yang sering timbul diantaranya mengenai operasi bisnis perusahaan, bisnis dan faktor pasar terkait, kondisi ekonomi umum, dan permasalahan lainnya yang bervariatif. Untuk menjalankan praktik tata kelola teknologi informasi yang efektif, perusahaan perlu memiliki solusi yang tepat dan akurat untuk menyelesaikan setiap permasalahan yang berpotensi timbul dan mengelola risiko secara keseluruhan. Sebagai contoh, terdapat tenaga sumber daya manusia senior dalam satu perusahaan memiliki pengetahuan teknologi yang cukup rendah dihadapkan dengan kondisi dimana ia memiliki akses terhadap suatu sistem informasi guna menunjang

pekerjaannya dan sistem informasi tersebut memerlukan kata sandi untuk mengaksesnya.

Dalam suatu kondisi, tenaga sumber daya manusia yang tidak terlalu melek TI menghendaki sistem kata sandi yang sangat sederhana dan mudah diingat untuk mengakses sistem informasi tersebut, misalkan kata sandi yang hanya berisi beberapa karakter pendek dan ditulis berdasarkan inisial penggunanya. disisi lain, tim spesialis keamanan TI pada perusahaan tersebutyang memahami tentang perkembangan TI era sekarang akan merekomendasikan agar kata sandi yang digunakan memiliki standar tersendiri, seperti kombinasi huruf besar kecil, kombinasi dengan angka dan penambahan berbagai karakter special untuk meminimalisir kemungkinan terjadinya pencurian data kata sandi dan menjaga akses sistem agar lebih aman. Dengan diterapkannya kata sandi model kombinasi karakter pun terkadang perlu dipantau secara berkala untuk memastikan tidak adanya percobaan akses illegal pada sistem tersebut.

Buku *Executive's Guide to IT Governance* juga merangkum sejumlah masalah risiko tata kelola teknologi informasi dan merangkum beberapa strategi efektif untuk mengelola risiko tersebut.

Tabel 1. Contoh *Enterprise Risk*

Syarat Risiko Perusahaan	**Strategi Aktivasi Risiko**
Pemahaman kapasitas Risiko Perusahaan	Ketika dihadapkan dengan potensi risiko, suatu perusahaan harus memahami seberapa besar tingkat risiko yang akan diterima. Ketika manajemen bersedia menerima risiko yang lebih tinggi, perusahaan dipandang

	memiliki kemampuan yang tinggi untuk risiko menangani risiko.
Pemahaman Penerimaan Risiko	Suatu perusahaan akan menghadapi banyak risiko, tetapi harus ada pemahaman yang jelas tentang unit perusahaan apa yang akan diterima atau bertanggung jawab atas risikonya.
Memastikan keterlibatan orang	Tanggung jawab unit organisasi harus diberikan untuk semua risiko yang teridentifikasi. Sebuah unit harus menyadari bahwa itu adalah bertanggung jawab untuk mengambil tindakan yang tepat jika terjadi risiko.
Menerima Risiko Residual	Dalam perspektif akuntansi atau audit, risiko residual adalah kemungkinan bahwa auditor tidak akan menangkap suatu materi salah saji dalam laporan keuangan klien dan akan keliru memberikan pendapat yang tidak memenuhi syarat. Dalam arti yang sama, manajemen mungkin tidak mengenali implikasi dari suatu risiko dan menerima mengambil risiko atau memberikan izin
Memahami kontrol proses seleksi	Suatu perusahaan perlu memahami biaya dan

	implikasi dari berbagai kontrol yang dapat ditetapkan sebagai respons terhadap berbagai risiko yang teridentifikasi.
Memahami Biaya Remediasi Peristiwa Risiko	Suatu perusahaan akan menghadapi banyak risiko, tetapi harus memiliki kejelasan pemahaman tentang biaya untuk memperbaiki berbagai hal jika risiko yang teridentifikasi terjadi.
Menetapkan Strategi Mitigasi Risiko yang Jelas	Suatu perusahaan harus memiliki definisi yang jelas dan beralasan strategi tindakan apa yang harus diambil jika risiko terkait teknologi informasi terjadi
Pengembangan kontrol proses seleksi	Ada banyak pertimbangan jika terjadi risiko teknologi informasi. perusahaan harus mengembangkan kontrol yang sesuai yang akan perbaiki risiko ini dengan cara yang efektif.

2.2.3. Masalah Organisasi pada Tata Kelola Teknologi Informasi

Penerapan manajemen teknologi informasi juga harus memperhatikan bahwa sebaik apapun perencanaan tata Kelola teknologi informasi yang telah dirancang, tidak dapat berjalan baik untuk sebuah perusahaan apabila terdapat satu atau lebih elemen organisasi dari perusahaan tersebut yang tidak memahami proses

bisnis yang diinginkan, perlu adanya penyamaan dan pemahaman persepsi terkait ini.

Dalam lingkup organisasi ini dapat dikatakan bahwa meskipun manajemen teknologi informasi dapat mengembangkan proses dan prosedur tata kelola yang memengaruhi sistem dan operasi TI mereka sendiri, mereka harus selalu memikirkannya lebih jauh tentang keterkaitan sistem atas kelola keseluruhan perusahaan. Misalnya, terlalu mudah untuk melupakan bahwa banyak tindakan terkait tata kelola berdampak pada tanggung jawab fidusia perusahaan dan manajer utamanya, pada khususnya untuk meningkatkan nilai investasi. Jadi, untuk melakukan segala tindakan yang berkaitan dengan tata kelola perusahaan, perlu dikompromikan dengan petinggi dan pemangku kebijakan perusahaan terkait untuk melancarkan setiap proses.

2.2.4. Masalah Regulasi pada Tata Kelola Teknologi Informasi

Pesan dalam pameran ini adalah bahwa meskipun manajemen TI dapat mengembangkan proses dan prosedur tata kelola yang memengaruhi sistem dan operasi TI mereka sendiri, mereka harus selalu memikirkan mereka dalam konteks yang jauh lebih besar dari keseluruhan perusahaan. Bagi contoh, terlalu mudah untuk melupakan bahwa banyak tindakan terkait tata kelola berdampak pada tanggung jawab fidusia perusahaan dan manajer utamanya pada khususnya untuk melestarikan dan meningkatkan investasi investor di semua tingkatan. Kegagalan di sini dapat mengakibatkan perdata atau bahkan tindakan hukum terhadap petugas perusahaan. Pertimbangan terkait di sini adalah bahwa perusahaan dan operasi TI-nya tidak memiliki serangkaian sumber daya yang terbuka atau tidak terbatas untuk mengambil tindakan korektif yang sesuai. Kita harus selalu menyeimbangkan

dampak dari mengambil tindakan korektif terhadap sumber daya perusahaan secara keseluruhan

2.2.5. Masalah Keamanan pada Tata Kelola Teknologi Informasi

Implementasi teknologi informasi dalam perusahaan tentu akan terhubung baik secara internal maupun ekternal melalui jaringan internet dan berbagai akses data lainnya, masalah keamanan menjadi salah satu masalah serius dalam tata kelola teknologi informasi. Dewasa ini pengguna teknologi informasi semakin banyak yang menyadari bahwa sistem dan data mereka yang tersimpan pada server adalah rentan terhadap berbagai penyusup luar yang memiliki banyak motif, seperti mencoba-coba meretas dengan tujuan menguji kemampuan bahwa dirinya mampu mengakses sistem tersebut, ada juga motif untuk melakukan sabotase terhadap sistem dengan tujuan mengambil data-data penting, mengubah data asli dan lain sebagainya guna mendapat nilai keuntungan dar permasalahan tersebut.

Pelaku bisnis pada perusahaan yang memanfaatkan teknologi informasi sebagai salah satu alat dalam menjalankan bisnisnya harus memiliki pengetahuan dan pemahaman yang kuat terhadap risiko keamanan yang sering dialami. Buku *Executive's Guide to IT Governance* juga merangkum beberapa permasalahan keamanan dalam tata kelola teknologi informasi beserta aktivitas tata Kelola teknologi informasi yang dapat dijalankan, dapat dilihat pada tabel berikut:

Tabel 2. Contoh *Security Issues*

Permasalahan Keamanan	**Aktivitas Tata Kelola TI**
Kebijakan dan Prosedur Keamanan	Suatu perusahaan harus memiliki prosedur yang kuat

	untuk mendeteksi dan mencegah pelanggaran dan gangguan keamanan TI. Juga harus ada staf khusus dan terampil di kapal untuk memantau keamanan TI dan untuk mengambil tindakan korektif jika sesuai
Masalah Perencanaan Kelangsungan Bisnis	Proses harus ada untuk memulihkan operasi jika terjadi gangguan tak terduga dalam sistem dan operasi TI. Sistem ini harus sepenuhnya diuji dan tetap terkini untuk mencerminkan perubahan dalam operasi perusahaan
Risiko *Malware*	Manajemen harus menyadari bahwa semua sistem saat ini tunduk pada berbagai ancaman berbahaya yang terus berkembang yang memiliki kemampuan untuk menghindari deteksi dan bermutasi sendiri setelah diluncurkan.
Persyaratan untuk Deteksi Intrusi yang Efektif dan Alat Pemantauan Keamanan	Suatu perusahaan harus menginstal alat yang sesuai untuk memantau semua aspek keamanan TI, baik secara internal maupun eksternal, dan untuk mengambil tindakan perbaikan yang efektif bila diperlukan.

Risiko Klasifikasi Aset TI	Semua aset perangkat keras dan perangkat lunak TI harus diidentifikasi dengan tepat mengenai kerabat mereka kerentanan keamanan dengan tindakan korektif rencana diuji, diimplementasikan, dan di tempat.
Risiko Pemantauan Keamanan	Alat harus ada untuk memantau semua aspek keamanan TI dan untuk memulai tindakan yang sesuai ketika ada serangan atau pelanggaran keamanan Diidentifikasi
Kebijakan Enkripsi dan Risiko Manajemen	Kebijakan enkripsi yang efektif harus diinstal dan digunakan jika sesuai untuk meningkatkan praktik tata kelola TI
Risiko Keamanan Pemangku Kepentingan	Kebijakan dan alat harus ada untuk memastikan bahwa semua pemangku kepentingan perusahaan yang terlibat mengikuti prosedur keamanan TI yang sesuai.

Meskipun ada banyak jenis permasalahan yang kemungkinan timbul, setidaknya pemangku kepentingan dalam perusahan sudah memahami ancaman dan risiko yang akan dihadapi dan memiliki tim teknis pengelola teknologi informasi guna proses tata kelola teknologi informasi yang lebih efektif dan efisien.

2.2.6. Ancaman Internal dan Eksternal pada Tata Kelola TI

Selain masalah tata kelola TI yang lebih spesifik, suatu organisasi maupun perusahaan tentu akan menghadapi berbagai macam ancaman keamanan internal dan eksternal. Ancaman eksternal termasuk dari hal-hal seperti serangan teroris hingga spionase pemerintah asing hingga risiko terhadap data pada penyimpanan digital. Perusahaan skala besar maupun perusahaan yang pengelolaannya masih dalam skala kecil pasti akan menghadapi berbagai ancaman eksternal terhadap sumber daya TI dan ancaman terhadap setiap operasi bisnisnya. Eksekutif bisnis saat ini harus memastikan bahwa perusahaan telah memiliki konsep pemantauan untuk memantau berbagai jenis ancaman tersebut dan mengambil tindakan korektif yang tepat sesuai ancaman yang ditemui.

Proses ancaman internal tata kelola teknologi informasi seringkali lebih mudah dipantau dan dikendalikan dengan lebih baik. Meskipun diluar perencanaan terkadang terdapat beberapa ancaman yang datang tanpa diduga sebelumnya yang dapat menyerang sistem TI perusahaan, namun setidaknya dengan perencanaan dan upaya penyiapan strategi akan dapat mengurangi risiko ancaman internal dengan membangun kebijakan internal yang kuat beserta prosedur yang telah disusun dengan baik.

2.2.7. Masalah Regulasi Tata Kelola TI

Regulasi menjadi salah satu landasan dasar bagi perusahaan dalam merancang dan menerapkan segala kebijakan-kebijakan perusahaan. Regulasi diciptakan sesuai tren yang berlaku dan setiap wilayah tentu memiliki regulasi yang berbeda-beda. Pada era teknologi ini, bermunculan berbagai regulasi atau undang-undang yang mengatur bagaimana penggunaan teknologi.

Termasuk implementasi teknologi dalam proses operasi perusahaan, Tentu setiap undang-undang memiliki tujuan. Seperti yang terjadi di Amerika Serikat, negara besar tersebut memiliki perundang-undangan yang biasa dikenal dengan sebutan *Sarbanes-Oxley (SOx)*, peraturan ini dibuat agar setiap perusahaan publik harus membuat laporan keuangan yang lebih detail, termasuk memberikan analisa keuangan beserta risiko yang dihadapi perusahaan. Undang-undang ini tujuannya adalah untuk memperbaiki transparansi perusahaan, perbaikan secara terus menerus terhadap pengendalian internal perusahaan, serta menekankan pentingnya independensi auditor eksternal dalam menjalankan tugasnya.

Di Amerika Serikat, bahkan banyak perusahaan yang keberatan dan memutuskan untuk *delisting* atau keluar dari bursa karena adanya regulasi ini. Banyak juga perusahaan kecil yang memutuskan untuk *delisting* karena tidak sanggup dengan biaya laporan keuangan yang mahal. Banyak juga perusahaan yang nilai *credit rating*-nya harus turun karena aturan ini.

Melalui aturan yang dijalankan secara ketat ini, perusahaan dituntut untuk punya komitmen sebagai perusahaan publik untuk transparan pada laporan keuangan dan informasi perubahan neraca yang sering digunakan untuk menyembunyikan tindakan kecurangan. Sehingga perusahaan publik yang tidak bersedia untuk berkomitmen bisa dipersilahkan untuk keluar dari bursa.

Sudah seharusnya badan-badan yang bertanggung jawab untuk membentuk kebijakan mulai merancang undang-undang serupa yang disesuaikan prinsipnya dengan kondisi di Indonesia. Negara harus punya iklim pasar modal yang sehat, pasar modal yang bisa melindungi investor publik dari risiko kecurangan, sebab pasar modal yang sehat akan menghasilkan penguatan dan pertumbuhan ekonomi secara berkelanjutan.

BAB II FRAMEWORK TATA KELOLA TI

Secara umum, *framework* dapat disimpulkan sebagai suatu kerangka kerja yang digunakan sebagai panduan atau pedoman dalam melaksanakan dan mengontrol pekerjaan tertentu agar berjalan sesuai harapan, tentunya untuk mempermudah proses pekerjaan. Secara spesifik dalam tata kelola teknologi informasi, *framework* ini berfungsi sebagai panduan atau pedoman bagaimana cara merangkai dan menyusun tata kelola teknologi informasi yang sesuai dengan standar. Dalam buku ini akan membahas secara singkat beberapa contoh *framework* tata kelola teknologi informasi yang umum dikenal.

2.1. COSO Internal Controls

Committee of Sponsoring Organizations atau yang biasa disingkat COSO merupakan salah satu *framework* tata kelola teknologi informasi yang lebih berfokus terhadap aspek bisnis semisal risiko perusahaan dan pencegahan penipuan.

Pengendalian internal menjadi salah satu konsep terpenting dan mendasar yang harus dipahami oleh setiap pimpinan organisasi maupun perusahaan dan pelaku bisnis professional di semua tingkatan. Profesional bisnis membangun dan menggunakan kontrol internal, sementara auditor meninjau dan menguji operasional, teknologi informasi, sistem yang

digunakan dan proses bisnis dalam keuangan dengan tujuan mengevaluasi pengendalian internal organisasi atau perusahaan tersebut.

Dikutip dari laman resmi http://coso.org, COSO diselenggarakan pada tahun 1985 untuk mensponsori Komisi Nasional Pelaporan Keuangan Palsu, sebuah inisiatif sektor swasta independen yang mempelajari faktor-faktor penyebab yang dapat menyebabkan pelaporan keuangan yang curang. Ini juga mengembangkan rekomendasi untuk perusahaan publik dan auditor independen mereka, untuk SEC dan regulator lainnya, dan untuk lembaga pendidikan.

Komisi Nasional disponsori bersama oleh lima asosiasi profesional utama yang berkantor pusat di Amerika Serikat: *American Accounting Association* (AAA), *American Institute of Certified Public Accountants* (AICPA), *Financial Executives International* (FEI), *The Institute of Internal Auditors* (IIA), dan *National Association of Accountants* (sekarang *Institute of Management Accountants* [IMA]). Sepenuhnya independen dari masing-masing organisasi yang mensponsori, Komisi termasuk perwakilan dari industri, akuntansi publik, perusahaan investasi, dan Bursa Efek New York.

Ketua pertama Komisi Nasional adalah James C. Treadway, Jr., Wakil Presiden Eksekutif dan Penasihat Umum, *Paine Webber Incorporated* dan mantan Komisaris Komisi Sekuritas dan Bursa Amerika Serikat. Oleh karena itu, nama populer "*Treadway Commission*." Saat buku ini ditulis, Ketua COSO adalah Paul J. Sobel. Tujuan COSO adalah untuk memberikan kepemimpinan pemikiran tentang tiga subjek yang saling terkait diantaranya manajemen risiko perusahaan (ERM), pengendalian internal, dan pencegahan penipuan.

Pada tahun 2001, kedua kalinya COSO memulai inisiatif besar yang bertujuan untuk memperluas konsep pengendalian

internal untuk mengatasi atmosfer yang semakin besar pada manajemen risiko. Pada tahun ini Amerika Serikat mengalami banyak kegagalan pada perusahaan *Enron*, *Tyco, Global Crossing, Kmart, Adelphia, WorldCom, HealthSouth*, dan lainnya.

Pada tahun 2004, COSO mengeluarkan *Enterprise Risk Management - Integrated Framework*. Kerangka kerja ini diperbarui dengan rilis "Enterprise – *Integrating with Strategy and Performance*" pada tahun 2017, yang menyoroti pentingnya mempertimbangkan risiko, baik dalam proses penetapan strategi maupun dalam mendorong kinerja perusahaan, sehingga proses bisnis dan aktivitas yang dilakukan oleh perusahaan tersebut sudah dilandasi dengan pertimbangan yang matang. COSO juga telah menerbitkan beberapa makalah hasil pemikirannya yang dimulai pada tahun 2009 yang berkaitan dengan ERM. Makalah tersebut tersedia untuk diunduh gratis pada situs resmi COSO.

Era sekarang, COSO telah diterima berbagai perusahaan, khususnya di Amerika Serikat dan dianggap sebagai landasan pengendalian internal era modern dan praktik manajemen risiko perusahaan. COSO merevolusi profesi akuntansi dan auditing dengan membangun kesamaan definisi pengendalian internal, manajemen risiko perusahaan, dan konsep fundamental lainnya.

COSO Internal Controls adalah sebuah proses pengendalian internal yang dipengaruhi oleh seluruh anggota perusahaan yang dirancang untuk memberikan jaminan yang wajar mengenai pencapaian dari perusahaan itu sendiri. tujuan pengendalian internal ini antara lain:

- Efektivitas dan efisiensi operasi
- Kehandalan pelaporan keuangan
- Kepatuhan terhadap hukum dan peraturan yang berlaku

COSO Internal Controls memiliki konsep utama sebagai acuan dalam melakukan pengendalian internal, diantaranya:

- Pengendalian internal adalah suatu proses dan sarana untuk mencapai tujuan organisasi atau perusahaan yang menerapkan, bukan tujuan individu.

- Pengendalian internal dipengaruhi oleh masyarakat, tidak hanya dipengaruhi oleh anggota organisasi atau perusahaan itu sendiri.

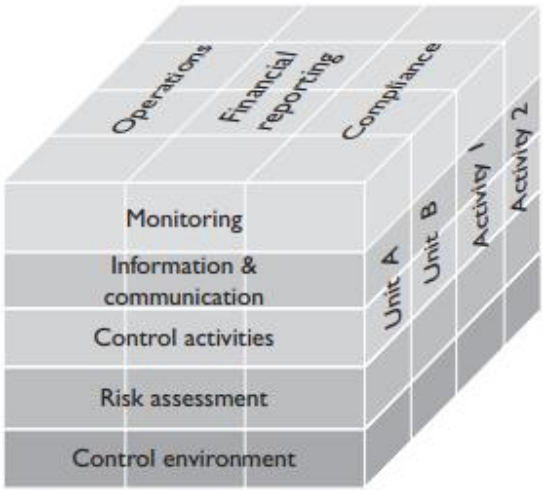
- Pengendalian internal dapat diharapkan hanya memberikan jaminan yang wajar, bukan jaminan mutlak, kepada setiap anggota organisasi atau perusahaan.

- Pengendalian internal diarahkan pada pencapaian tujuan dalam satu atau lebih kategori yang terpisah

3.3.1. *COSO Internal Controls – Integrated Framework*

Pengendalian internal merupakan aktivitas yang dijalankan atas instruksi langsung dari dewan direksi maupun manajemen organisasi perusahaan. Tujuan dilakukannya aktivitas pengendalian internal ini guna memberikan perlindungan atas semua asset yang dimiliki oleh sebuah perusahaan serta memberikan kepastian bahwa semua komponen yang ada di dalam perusahaan dapat mematuhi hukum dan peraturan yang berlaku. Penerapan pengendalian internal yang diterapkan secara efektif dan optimal dapat membantu kegiatan manajemen perusahaan serta berperan dalam mencegah penyalahgunaan asset perusahaan.

Pengendalian Internal dengan *framework* yang saling terintegrasi yang perkenalkan oleh COSO digambarkan dalam bentuk seperti gambar berikut:



Gambar 1. COSO *Cube*
(sumber: buku *IT Auditing Using Controls to Protect Information Assets – Second Edition*)

Dari gambar diatas, COSO *Internal Controls* terdiri dari lima komponen utama yang saling berhubungan:

- *Monitoring*
- *Information and communication*
- *Control activities*
- *Risk assessment*
- *Control environment*

Dalam implementasinya, pengendalian internal tidak hanya boleh dilakukan oleh organisasi atau perusahaan besar saja, melainkan dapat juga dilakukan oleh organisasi atau perusahaan yang masih kecil, penerapan pengendalian internal dapat disesuaikan dengan kapasitas perusahaan itu sendiri. Pada organisasi atau perusahaan kecil.

Monitoring

Sistem pengendalian internal akan bekerja secara efektif dengan dukungan yang tepat dari manajemen, prosedur pengendalian, dan keterkaitan informasi dan komunikasi, proses harus ada untuk memantau kegiatan ini. Pemantauan telah lama menjadi peran teknologi informasi dan auditor internal lainnya, yang melakukan peninjauan untuk menilai kepatuhan terhadap prosedur yang ditetapkan, namun, pengendalian internal COSO sekarang mengambil pandangan yang lebih luas tentang pemantauan dan mengakui bahwa prosedur kontrol dan sistem lain berubah seiring waktu. Apa yang tampaknya efektif ketika pertama kali dipasang mungkin tidak begitu efektif di masa depan karena perubahan kondisi, prosedur baru, atau faktor lainnya.

Suatu organisasi maupun perusahaan perlu menetapkan berbagai kegiatan pemantauan untuk mengukur efektivitas pengendalian internalnya melalui evaluasi terpisah serta dengan kegiatan yang sedang berlangsung untuk memantau kinerja dan mengambil tindakan korektif bila diperlukan. Banyak fungsi bisnis rutin dapat dicirikan sebagai kegiatan pemantauan, dan COSO memberikan contoh komponen penting pengendalian internal ini:

- Kegiatan manajemen berjalan normal
  Laporan ditinjau secara berkala dan tindakan korektif yang dimulai untuk setiap pengecualian yang dilaporkan.
- Komunikasi dari pihak eksternal
  Pemantauan komunikasi dengan pihak eksternal perlu dilakukan untuk mengetahu keluhan pelanggan dan kebutuhan, perusahaan perlu memantau dengan cermat dan melakukan tindakan yang sesuai.
- Struktur perusahaan dan kegiatan pengawasan
- Pimpinan ataupun manajemen tingkat tinggi harus selalu meninjau laporan ringkasan dan mengambil tindakan korektif.

- Persediaan barang secara fisik dan rekonsiliasi asset
  Memantau persediaan barang fisik secara berkala untuk dapat mengidentifikasi kebutuhan suplai barang dan dapat juga untuk mengindikasikan kehilangan barang.

COSO juga menekankan bahwa evaluasi ini dapat dilakukan oleh manajemen secara langsung melalui tinjauan penilaian mandiri. Namun, ulasan penilaian mandiri ini biasanya tidak akan selengkap audit internal pada umumnya.

Information and Communication

Menurut COSO, informasi terkait harus diidentifikasi, ditangkap, dan dikomunikasikan dalam bentuk dan kerangka waktu yang memungkinkan divisi pada organisasi atau perusahaan tersebut untuk melaksanakan tanggung jawabnya. Disini pentingya sistem informasi dalam berperan, perusahaan memerlukan sebuah sistem informasi yang diharapkan dari sistem informasi tersebut dapat menghasilkan laporan yang berisi informasi operasional, keuangan, dan terkait kepatuhan yang memungkinkan untuk menjalankan dan mengendalikan bisnis. Perusahaan juga tidak hanya membutuhkan data yang dihasilkan secara internal tetapi juga memerlukan data atau informasi tentang eksternal seperti kebutuhan, kegiatan, dan kondisi yang diperlukan untuk pengambilan keputusan bisnis yang didapat secara valid.

Komunikasi yang baik juga perlu dilakukan, tidak hanya komunikasi antar pimpinan, namun komunikasi perlu terjalin antara pimpinan dengan anggota keseluruhan, begitu sebaliknya. Seluruh anggota harus memberikan dan menerima informasi secara jelas dan detail, karena berkaitan dengan implementasi pekerjaan setiap divisi. Masing-masing juga harus memahami perannya sendiri dalam sistem pengendalian internal, serta

bagaimana kegiatan yang dilakukan oleh individu saling berhubungan dengan pekerjaan individu lain. Setiap anggota harus memiliki sarana untuk mengkomunikasikan informasi dengan pihak eksternal, seperti pelanggan, pemasok, regulator, dan pemegang saham. Informasi dan komunikasi diperlukan guna mencegah terjadinya kesalahpahaman antar pihak.

Pengendalian internal COSO juga menekankan pentingnya menjaga informasi dan sistem pendukung yang konsisten dengan kebutuhan perusahaan secara keseluruhan. Sistem informasi beradaptasi untuk mendukung perubahan di banyak tingkatan. Auditor TI, misalnya, sering ditemui kasus di mana aplikasi yang digunakan selama bertahun-tahun yang lalu masih digunakan oleh sebuah organisasi atau perusahaan untuk operasional pekerjaan mereka, sementara di sisi lain kebutuhan perusahaan era modern seperti sekarang sudah berkembang pesat, dan aplikasi yang digunakan tidak mendukung kebutuhan perusahaan yang semakin kompleks dan ini menunjukkan perlunya memahami proses manual dan teknologi yang bergerak dinamis.

Control Activities

Kegiatan pengendalian merupakan kebijakan dan prosedur yang membantu memastikan bahwa setiap instruksi dan arahan dijalankan dengan baik. Manajemen turut membantu memastikan tindakan yang diperlukan untuk diambil guna mengatasi risiko, hal ini perlu dilakukan untuk memastikan tujuan setiap divisi tercapai dengan baik. aktivitas kontrol terjadi di seluruh organisasi atau perusahaan, pada semua tingkatan dan di semua fungsi. termasuk berbagai kegiatan yang beragam sebagai persetujuan, otorisasi, verifikasi, rekonsiliasi, ulasan operasi kinerja, keamanan aset, dan pemisahan tugas.

COSO mengidentifikasi serangkaian kegiatan ini yang umumnya diklasifikasikan sebagai kontrol manual, TI, atau manajemen, dan mereka juga dijelaskan dalam hal apakah mereka preventif, kegiatan korektif, atau kontrol detektif. Sementara tidak ada semua definisi pengendalian internal itu sesuai untuk setiap situasi, pengendalian internal COSO merekomendasikan kegiatan pengendalian berikut untuk suatu perusahaan:

- *Top Level Reviews*
  Manajemen senior harus meninjau hasil kinerjanya
- *Direct functional or activity management*
  Manajemen fungsional dari berbagai divisi harus meninjau laporan operasional dari sistem kendali masing-masing
- *Information processing*
  Pengolahan informasi dilakukan dengan benar sesuai kebutuhan perusahaan, karena luaran informasi yang didapat diharapkan dapat menjadi pendukung pengambilan keputusan perusahaan
- *Physical Controls*
  perusahaan harus memiliki kontrol yang sesuai atas aset fisiknya, termasuk perlengkapan dan persediaan. Program aktif inventaris fisik berkala mewakili aktivitas kontrol utama di sini, dan TI serta audit internal dapat memainkan peran utama dalam memantau kesesuaian dengan prosedur.
- *Perfomance Indicators*
  Manajemen harus mengkaitkan berbagai data yang didapat.
- *Segregation of Duties*
  Tugas harus dibagi kepada beberapa anggota berbeda untuk mengurangi risiko kesalahan atau tindakan yang tidak pantas.

Risk Assessment

Setiap divisi akan menjumpai berbagai risiko dari sumber eksternal dan internal yang harus dinilai. Prasyarat untuk penilaian risiko adalah penetapan tujuan dari tiap divisi yang seharusnya saling terhubung satu sama lain secara konsisten antar divisi internal dan terhubung secara konsisten. Penilaian risiko adalah identifikasi dan analisis risiko yang relevan terhadap pencapaian tujuan yang membentuk dasar untuk menentukan bagaimana risiko harus dikelola. Karena ekonomi, industri, regulasi, dan kondisi operasi akan terus berubah, mekanisme diperlukan untuk mengidentifikasi dan berurusan dengan risiko khusus yang terkait dengan perubahan.

Control Environment

Lingkungan pengendalian menjadi bagian awal dari setiap komponen pengendalian internal lainnya, lingkungan pengendalian menjadi tanggung jawab manajemen tertinggi pada organisasi atau perusahaan, ini akan memberi pengaruh kuat terhadap kontrol anggotanya, integritas, nilai-nilai etika dan kompetensi anggota pada setiap divisi, konsep manajemen, model kerja dan langkah manajemen memberikan dalam memberikan otoritas, tanggung jawab, mengatur srta mengembangkan organisasi atau perusahaan dan anggotanya.

Hubungan Antar Komponen

Kelima komponen pengendalian internal yang telah dibahas sebelumnya terdapat sinergi dan keterkaitan satu sama lain, membentuk sistem terintegrasi yang bereaksi secara dinamis terhadap perubahan kondisi. Sistem pengendalian internal terkait dengan kegiatan operasi divisi dan ada karena alasan bisnis yang

mendasar. Pengendalian internal paling efektif ketika kontrol dibangun ke dalam infrastruktur divisi dan merupakan bagian dari esensi perusahaan. Pengendalian internal jika dilakukan sesuai lima konsep tersebut dapat memberikan hasil kontrol yang maksimal, sebaliknya jika salah satu dari kelima komponen tidak dilakukan, maka akan mengurahi hasil maksimal yang seharusnya bisa diperoleh dari pengendalian internal ini.

3.3.2. *Enterprise Risk Management – Integrated Framework*

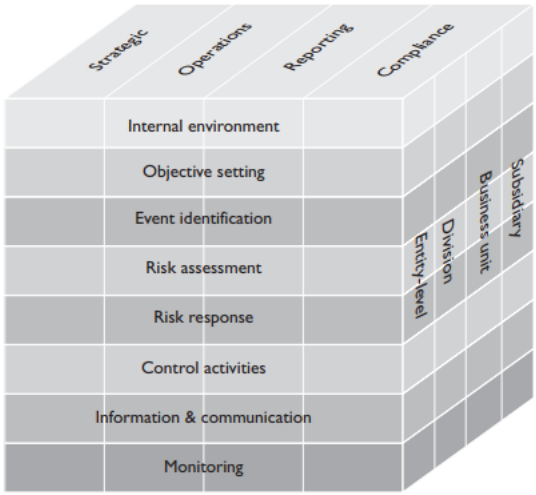
Manajemen risiko perusahaan adalah suatu proses yang dipengaruhi oleh dewan direksi, manajemen, dan anggota secara keseluruhan, yang diterapkan dalam penetapan strategi pada seluruh perusahaan dan dirancang untuk mengidentifikasi kemungkinan terjadinya hal-hal potensial yang dapat memengaruhi tiap divisi perusahaan, dan mengelola risiko untuk memberikan jaminan yang wajar mengenai pencapaian tujuan tiap divisi perusahaan.

Dikutip dalam buku yang berjudul *Executive's Guide to IT Governance*, beberapa definisi tentang manajemen risiko perusahaan dapat dilihat pada baris berikut:

- Manajemen risiko perusahaan merupakan suatu proses berkelanjutan dan mengalir melalui suatu divisi;
- Manajemen risiko dipengaruhi oleh orang-orang di setiap tingkatan organisasi atau perusahaan;
- Manajemen risiko diterapkan dalam pengaturan strategi organisasi atau perusahaan;
- Manajemen risiko diterapkan di seluruh organisasi atau perusahaan, di setiap tingkat dan unit;
- Manajemen risiko dirancang untuk mengidentifikasi peristiwa potensial yang jika terjadi akan mempengaruhi tiap divisi

- Manajemen risiko mampu memberikan jaminan yang seharusnya kepada manajemen dan dewan divisi maupun direktur;
- Manajemen risiko diarahkan untuk pencapaian tujuan organisasi atau perusahaan

Pada "*Enterprise Risk Management – Integrated Framework*", konsep COSO diperluas hingga menjadi seperti ilustrasi gambar berikut:



Gambar 2. *Expanded* COSO *Cube*
(sumber: buku *IT Auditing Using Controls to Protect Information Assets – Second Edition*)

Manajemen risiko perusahaan pada konsep ini terdiri dari delapan komponen yang saling terkait. Ini berasal dari cara manajemen menjalankan suatu perusahaan dan terintegrasi dengan proses manajemen. Delapan komponen ini antara lain:

- *Internal environment*
- *Objective setting*

- *Event identification*
- *Risk assessment*
- *Risk response*
- *Control activities*
- *Information and communication*
- *Monitoring*

Kerangka kerja manajemen risiko perusahaan ini diarahkan untuk mencapai suatu tujuan yang telah ditetapkan dalam empat kategori berikut:

- Tujuan strategis tingkat tinggi perusahaan yang selaras dengan misinya.
- Operasi penggunaan sumber daya yang efektif dan efisien
- Kehandalan pelaporan pelaporan
- Kepatuhan pepatuhan terhadap hukum dan peraturan yang berlaku

Internal Environment

Lingkungan internal mencakup instruksi pada organisasi atau perusahaan dan memberikan dasar bagaimana melihat kemungkinan timbul risiko dan cara menangani risiko oleh masing-masing divisi. Ini termasuk filosofi manajemen risiko, integritas, dan nilai-nilai etika.

Objective Setting

Organisasi atau perusahaan sudah harus memiliki tujuan dan target sebelum manajemen dapat mengidentifikasi peristiwa yang berpotensi timbul yang dapat mempengaruhi pencapaian organisasi atau perusahaan. Manajemen risiko perusahaan memastikan bahwa manajemen telah melakukan proses untuk

menetapkan tujuan dan bahwa tujuan yang dipilih mendukung dan selaras dengan misi perusahaan.

Event Identification

Peristiwa yang timbul baik pada internal maupun eksternal akan berdampak secara langsung terhadap pencapaian organisasi atau perusahaan, tujuan suatu organisasi atau perusahaan harus diidentifikasi lebih awal, membedakan antara risiko dan peluang, kemudian peluang disalurkan kembali ke strategi manajemen atau proses penetapan tujuan.

Risk Assessment

Risiko dianalisis, mempertimbangkan kemungkinan dan dampak, sebagai dasar untuk menentukan bagaimana risiko harus dikelola. Risiko dinilai berdasarkan inheren dan dasar residual.

Risk Response

Manajemen memilih respon risiko, menghindari, menerima, mengurangi, atau berbagi dan mengembangkan serangkaian tindakan untuk menyelaraskan risiko dengan toleransi risiko.

Control Activities

Kebijakan dan prosedur ditetapkan dan dilaksanakan untuk membantu memastikan bahwa respons risiko dilakukan secara efektif dan berkesinambungan.

Information and Communication

Informasi yang relevan diidentifikasi, didapatkan, dan dikomunikasikan dalam bentuk dan kerangka waktu yang memungkinkan setiap bagian untuk melakukan tanggung jawab mereka masing-masing. Komunikasi yang efektif juga terjadi dalam arti yang lebih luas, menjalin hubungan antar manajemen, pimpinan sekaligus dengan anggota dibawahnya.

Monitoring

Keseluruhan manajemen risiko perusahaan dipantau dan modifikasi dilakukan seperlunya menyesuaikan kebutuhan organisasi atau perusahaan. Pemantauan dilakukan melalui kegiatan manajemen yang sedang berlangsung, evaluasi terpisah, atau keduanya.

2.2. COBIT

Control Objectives for Information and Related Technology atau yang biasa disingkat COBIT merupakan kerangka kerja yang secara umum telah menerima praktik, *analytical tools* and *models* yang dirancang untuk tata kelola dan pengelolaan teknologi informasi di perusahaan. Berdasarkan pengalaman yang terus meluas tentang tata kelola, ISACA terus memperbarui versi dari *framework* COBIT, hingga yang terbaru sejak buku ini ditulis COBIT telah berkembang hingga versi COBIT 2019. Peningkatan versi pada COBIT tentu akan membawa peningkatan pada arsitekturnya.

Lalu apa perbedaan antara COBIT sebelumnya dengan COBIT 2019? Berikut ini perbedaan COBIT 5 versi 2019 secara garis besar:

- Pada COBIT 2019 dikenal dengan *focus area*, sedangkan pada COBIT 5 tidak ada. *Focus area* merupakan suatu topik, domain atau permasalahan utama pada sebuah tata kelola organisasi atau perusahaan.
- Pada COBIT 2019 dikenal dengan faktor desain, sedangkan pada COBIT 5 tidak ada. Faktor desain merupakan faktor penting yang diperlukan dalam mendesain sistem tata kelola untuk mewujudkan suksesnya penerapan tata kelola pada organisasi atau perusahaan tersebut.
- Penambahan pada prinsip COBIT 2019. Dimana pada COBIT 5 hanya terdapat lima prinsip utama, sedangkan pada COBIT 2019 terdapat penambahan 2 prinsip yaitu prinsip sistem tata kelola dan prinsip kerangka kerja tata kelola.
- Perubahan nama pada *enabler* di dalam COBIT 5. Jika pada COBIT 5 dinamakan 7 *enabler* sedangkan pada COBIT 2019 dinamakan komponen COBIT 2019.
- Penambahan empat buah domain proses pada domain *planning* dan *organizing, monitoring* and *evaluating* dan *manage data*.

Standar dan kerangka kerja COBIT dikeluarkan dan diperbarui secara berkala oleh *Information Technology Governance Institute* (ITGI), dan organisasi profesi yang berafiliasi sangat kuat, *Information System Audit and Control Association* (ISACA). ISACA lebih fokus pada udit TI, sedangkan penekanan ITGI adalah pada proses penelitian dan tata kelola. ISACA juga mengelola *Certified Information Technology Auditor* (CISA) serta sertifikasi lain seperti *Certified Information Systems Manager* (CISM) dan *Certified in the Governance of Enterprise Information Technology* (CGEIT).

Menurut buku yang berjudul *Executive's Guide to IT Governance*, Kerangka kerja COBIT 5 terdiri dari lima prinsip utama yang saling terhubung satu sama lain:

- ***Integrated IT Framework***
  COBIT menyerukan upaya untuk menyelaraskan operasi dan aktivitas TI dengan semua operasi perusahaan lainnya. Ini termasuk membangun keterkaitan antara operasi bisnis perusahaan dan rencana TI serta proses untuk mendefinisikan, memelihara, dan memvalidasi hubungan kualitas dan nilai.

- ***Stakeholder Value Drivers***
  Proses harus ada di tempatnya untuk memastikan bahwa TI dan unit operasi perusahaan lainnya memberikan manfaat yang dijanjikan sepanjang siklus pengiriman dan dengan strategi yang mengoptimalkan biaya sambil menekankan nilai-nilai intrinsik perusahaan TI dan kegiatan terkait.

- ***Resources Focus on a Business Context***
  Dengan penekanan pada TI, harus ada investasi dan manajemen yang tepat dari sumber daya TI, aplikasi, informasi, infrastruktur, dan sumber daya manusia. Tata kelola TI yang efektif bergantung pada optimalisasi pengetahuan dan infrastruktur ini

- ***Risk Management***
  Manajemen, di semua tingkatan, harus memiliki pemahaman yang jelas tentang risiko perusahaan dikelola, persyaratan kepatuhannya, dan dampak risiko yang signifikan. Baik TI dan operasi lainnya memiliki tanggung jawab manajemen risiko masing-masing yang dapat secara individu atau bersama-sama akan berdampak pada perusahaan itu sendiri.

- ***Performance Measurement***
  Proses harus dilakukan sesuai tujuannya guna melacak dan memantau implementasi strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses, dan pemberian layanan. Mekanisme tata kelola TI harus menerjemahkan strategi implementasi ke dalam tindakan dan pengukuran untuk mencapai tujuan-tujuannya.

Kelima prinsip dalam kerangka kerja COBIT merupakan prinsip kunci dalam suksesnya implementasi COBIT 5. Kerangka kerja COBIT adalah alat yang efektif untuk mendokumentasikan TI dan semua kontrol internal lainnya, kerangka kerja COBIT juga dapat digunakan untuk membantu dalam proses tata kelola TI manajemen, perusahaan, dan audit internal.

Kemudian pata tahun 2018 lalu, COBIT merilis versi 2019 dengan membawa beberapa perubahan, perubahan yang dimaksud terdapat pada prinsip, sistem dan komponen tata kelola. Terdapat dua klasifikasi dimana prinsip yang terdapat pada COBIT 5 ditambahkan dua tambahan prinsip, lalu disebut sebagai *governance system*. Klasifikasi baru yang ditambahkan ialah kerangka kerja tata kelola. Dengan rincian sebagai berikut:

- **Sistem Tata Kelola (*Governance System*)**
  1. Memenuhi kebutuhan para pemangku kepentingan (*stakeholder*);
  2. Mencakup organisasi secara menyeluruh
  3. Menerapkan satu framework tunggal;
  4. Memungkinkan pendekatan yang holistik;
  5. Memisahkan tata kelola dengan manajemen;
  6. Penerapan sistem tata kelola yang dinamis;
  7. Dapat disesuaikan dengan kebutuhan organisasi.

- **Kerangka Kerja Tata Kelola**
  1. Berbasis model konseptual
  2. Bersifat terbuka dan fleksibel
  3. Selaras dengan standard-standard besar lainnya

Berdasarkan situs resmi http://itgid.org, beberapa catatan penting yang perlu digaris bawahi dari COBIT 2019 diatas antara lain:

- Baik COBIT 2019 *core model* maupun COBIT 5 menggunakan pengelompokan yang sama, yaitu terdiri atas 1 domain tata kelola dan 4 domain manajemen.
- Ada perbedaan pembahasaan pada setiap item pada model COBIT 2019 dibandingkan COBIT 5. Jika pada COBIT 5 masing-masing item adalah nama proses. Sedangkan pada COBIT 2019, item-item tersebut dinamai dengan obyektif yang diharapkan jika proses tersebut dilakukan dengan baik. Misalnya pada COBIT 5, proses EDM01 itu dinamakan dengan "*Ensure Governance Framework Setting and Maintenance*". Sementara pada COBIT 2019, item EDM01 itu adalah "*Ensured Governance Framework Setting and Maintenance*".
- Setiap item obyektif tata kelola dan manajemen pada COBIT 2019 *Core Model* berkorespondensi dengan 1 proses (dengan nama yang mirip seperti contoh di atas). Hanya saja pada COBIT 2019 ini setiap obyektif tata kelola dan manajemen itu tidak hanya terkait dengan proses, tapi dapat berkaitan dengan beberapa komponen tata kelola yang lain (yang ada 7 komponen, termasuk diantaranya proses).
- Jika membandingkan COBIT 2019 *core model* dengan COBIT 5 *process reference model*, terdapat beberapa tambahan obyektif baru yang pada COBIT belum ada atau tergabung di proses lain. Sehingga secara total pada COBIT

2019 ada 40 obyektif tata kelola dan manajemen, sedangkan pada COBIT 5 hanya ada 37 proses.

2.3.1. Konsep COBIT

COBIT adalah kerangka kerja untuk tata kelola dan manajemen informasi dan teknologi, yang ditujukan untuk seluruh perusahaan. IT Perusahaan berarti semua teknologi dan pemrosesan informasi yang dilakukan perusahaan untuk mencapai tujuannya. Kerangka kerja COBIT membuat perbedaan yang jelas antara *governance* dan *management*. Kedua disiplin ilmu ini meliputi kegiatan yang berbeda, membutuhkan struktur organisasi yang berbeda dan melayani tujuan yang berbeda.

Governance memastikan bahwa kebutuhan, kondisi, dan opsi pemangku kepentingan dievaluasi untuk menentukan tujuan perusahaan yang yang sesuai dan disepakati Bersama, arah ditetapkan melalui prioritas dan pengambilan keputusan, kinerja dan kepatuhan dipantau terhadap arah dan tujuan yang disepakati Bersama. Pada sebagian besar organisasi maupun perusahaan, tata kelola merupakan bagian tanggung jawab dari dewan direksi, di bawah kepemimpinan ketua. Tanggung jawab tata kelola dapat didelegasikan secara spesifik ke struktur organisasi yang membidangi, terutama di perusahaan yang lebih besar dan kompleks dalam proses operasionalnya.

Sementara manajemen bertindak dalam merencanakan, membangun, menjalankan, dan memantau kegiatan yang selaras dengan arah yang ditetapkan oleh badan tata kelola, untuk mencapai tujuan organisasi maupun perusahaan. Pada sebagian besar organisasi maupun perusahaan, manajemen merupakan tanggung jawab manajemen eksekutif di bawah kepemimpinan kepala pejabat eksekutif (CEO).

Sebuah lembaga nonprofit, *Information Technology Governance Institute* atau yang biasa dikenal dengan ITGI merupakan Lembaga independen yang berafiliasi dengan ISACA. ITGI didirikan pada tahun 1998 untuk memajukan pemikiran dan standar internasional dalam mengarahkan dan mengendalikan IT suatu perusahaan. Selain itu, ITGI menawarkan studi riset dan studi kasus untuk membantu organisasi dan dewan direksi mereka dalam mengelola teknologi informasi secara optimal.

Di Indonesia sendiri terdapat lembaga tersebut yang dikenal dengan singkatan ITGID (*Information Technology Governance Indonesia*). Lembaga ini juga menjadi Lembaga pengembangan tata kelola teknologi informasi, risiko dan kepatuhan di Indonesia. ITGID mengumpulkan para profesional dan pakar terkait IT Governance, Risk and Compliance yang akan berkolaborasi untuk berbagi ilmu dan membantu perusahaan/organisasi dalam meningkatkan kompetensi *IT Governance, Risk and Compliance*. ITGID juga melakukan pelatihan terkait *IT Governance, Risk and Compliance* (sumber: http://itgid.org).

Agar informasi dan teknologi dapat berkontribusi pada tujuan perusahaan, sejumlah tujuan tata kelola dan manajemen harus dicapai. Konsep dasar yang berkaitan dengan tujuan tata kelola dan manajemen adalah:

- Tujuan tata kelola atau manajemen selalu berkaitan dengan satu proses (dengan nama yang identik atau mirip) dan serangkaian komponen terkait dari jenis lain untuk membantu mencapai tujuan.

- Tujuan tata kelola berkaitan dengan proses tata kelola, sedangkan tujuan manajemen berkaitan dengan proses manajemen. Dewan dan manajemen eksekutif biasanya bertanggung jawab atas proses tata kelola, sedangkan

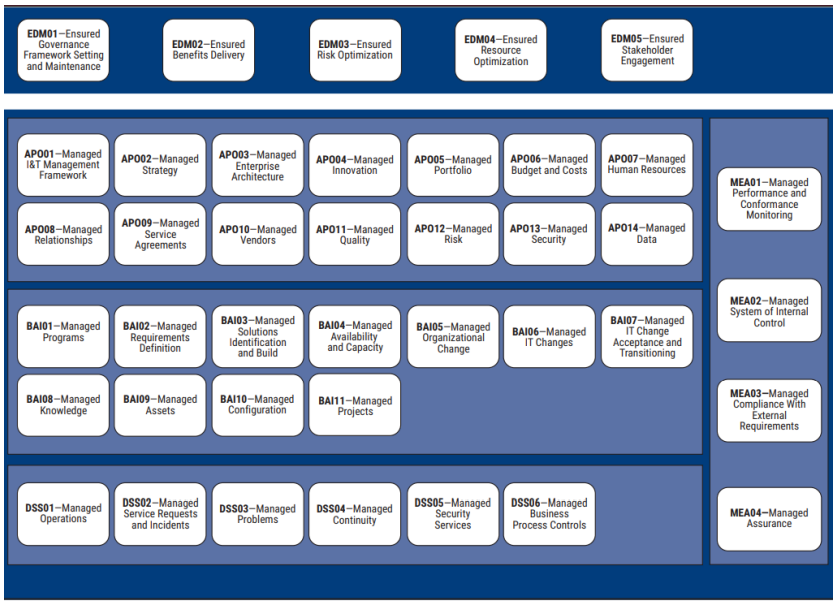
proses manajemen adalah domain manajemen senior dan menengah.

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

- Tujuan tata kelola dikelompokkan dalam domain ***Evaluate, Direct and Monitor*** **(EDM)**. Dalam domain ini, yang mengatur dalam mengevaluasi opsi strategis, mengarahkan manajemen senior pada opsi strategis yang dipilih dan memantau pencapaian dari strategi.

- Tujuan manajemen dikelompokkan dalam empat domain.
  1. ***Align, Plan and Organize*** **(APO)** membahas keseluruhan organisasi, strategi, dan kegiatan pendukung untuk IT.
  2. ***Build, Acquire and Implement*** **(BAI)** memperlakukan definisi, akuisisi, dan implementasi solusi I&T dan mereka integrasi dalam proses bisnis.
  3. ***Deliver, Service and Support*** **(DSS)** membahas pengiriman operasional dan dukungan layanan I&T, termasuk keamanan.
  4. **Monitor, Evaluate and Assess (MEA)** membahas pemantauan kinerja dan kesesuaian I&T dengan internal target kinerja, tujuan pengendalian internal dan persyaratan eksternal.

Selengkapnya terkait *core model* dari COBIT dapat dilihat pada gambar berikut:



Gambar 3. COBIT *Core Model*
(sumber: buku COBIT® 2019 *FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES*)

2.3.2. Komponen *Governance System*

Untuk memenuhi tujuan tata kelola dan manajemen, setiap perusahaan perlu membangun, menyesuaikan, dan mempertahankan sistem tata kelola yang dibangun dari sejumlah komponen, Komponen adalah faktor-faktor yang, secara individu dan kolektif, berkontribusi pada operasi yang baik dari tata kelola perusahaan sistem atas teknologi informasi. Komponen berinteraksi satu sama lain, menghasilkan sistem tata kelola holistik untuk teknologi informasi.

Komponen terdapat dari berbagai jenis, yang paling umum adalah proses. Namun tidak hanya itu, komponen sistem tata kelola juga termasuk struktur organisasi, kebijakan dan prosedur,

item informasi, budaya dan perilaku, keterampilan dan kompetensi, serta layanan, infrastruktur, dan aplikasi.

Gambar 4. Komponen COBIT *Governance System*
(sumber: buku COBIT® 2019 *FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES*)

Keterangan:

- **Proses**
  Menggambarkan serangkaian praktik dan kegiatan yang terorganisir untuk mencapai tujuan tertentu dan

menghasilkan serangkaian output yang mendukung pencapaian tujuan terkait TI secara keseluruhan.

- **Struktur organisasi**
  Entitas pembuat keputusan utama dalam suatu perusahaan.

- **Prinsip, kebijakan, dan kerangka kerja**
  Menerjemahkan perilaku yang diinginkan ke dalam panduan praktis untuk manajemen sehari-hari.

- **Informasi**
  Informasi tersebar luas di seluruh organisasi mana pun dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. COBIT berfokus pada informasi yang diperlukan untuk berfungsinya sistem tata kelola sistem tata kelola yang efektif usaha.

- **Budaya, etika dan perilaku**
  Budaya, etika dan perilaku Individu dan perusahaan sering diremehkan sebagai faktor dalam keberhasilan kegiatan tata kelola dan manajemen.

- **Kepegawaian, keterampilan, dan kompetensi**
  Tiga komponen ini diperlukan untuk keputusan yang baik, pelaksanaan tindakan korektif dan keberhasilan penyelesaian semua kegiatan.

- **Layanan, infrastruktur, dan aplikasi**
  Komponen ini meliputi infrastruktur, teknologi, dan aplikasi yang menyediakan perusahaan dengan sistem tata kelola untuk pemrosesan teknologi informasi.

Setiap tujuan tata kelola atau manajemen tentu untuk mendukung pencapaian tujuan penyelarasan yang terkait dengan perusahaan. Tujuan-tujuan penyelarasan yang dimaksud dapat dilihat pada poin berikut:

- AG01: Kepatuhan IT dan dukungan untuk kepatuhan bisnis terhadap hukum dan peraturan eksternal
- AG02: Risiko terkait IT terkelola
- AG03: Manfaat yang direalisasikan dari investasi yang didukung IT dan portofolio layanan
- AG04: Kualitas informasi keuangan terkait teknologi
- AG05: Pengiriman layanan IT sesuai dengan kebutuhan bisnis
- AG06: Kelincahan untuk mengubah persyaratan bisnis menjadi solusi operasional
- AG07: Keamanan informasi, infrastruktur dan aplikasi pemrosesan, dan privasi
- AG08: Memungkinkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi
- AG09: Memberikan program tepat waktu, sesuai anggaran dan memenuhi persyaratan dan standar kualitas
- AG10: Kualitas informasi manajemen IT
- AG11: Kepatuhan IT terhadap kebijakan internal
- AG12: Staf yang kompeten dan termotivasi dengan saling pengertian tentang teknologi dan bisnis
- AG13: Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis

Setelah mengetahui tujuan penyelarasan, ada pula perusahaan perlu menyiapkan target atau tujuang yang ingin dicapai, tentu berdasarkan penyelarasan pada poin diatas. Target perusahaan yang dimaksud antara lain:

- EG01: Portofolio produk dan layanan yang kompetitif
- EG02: Risiko bisnis yang dikelola

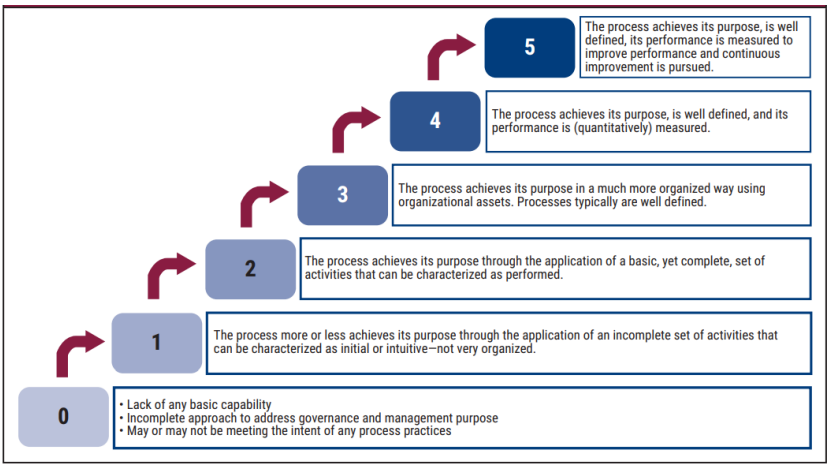
- EG03: Kepatuhan hukum dan peraturan eksternal
- EG04: Kualitas informasi keuangan
- EG05: Budaya layanan yang berorientasi pada pelanggan
- EG06: Kontinuitas dan ketersediaan layanan bisnis
- EG07: Kualitas informasi manajemen
- EG08: Optimalisasi fungsionalitas proses bisnis
- EG09: Optimalisasi biaya proses bisnis
- EG10: Keterampilan staf, motivasi dan produktivitas
- EG11: Kepatuhan terhadap kebijakan internal
- EG12: Program transformasi digital terkelola
- EG13: Inovasi produk dan bisnis

2.3.3. Struktur COBIT

Komponen: Proses

Setiap tujuan tata kelola dan manajemen mencakup beberapa praktik proses. Setiap proses memiliki satu atau lebih kegiatan. Sejumlah contoh matriks beserta setiap praktik proses, untuk mengukur pencapaian praktik dan kontribusi terhadap pencapaian tujuan secara keseluruhan.

Tingkat kemampuan ditetapkan untuk semua aktivitas proses, memungkinkan definisi proses yang jelas pada tingkat kemampuan yang berbeda. Suatu proses mencapai tingkat kemampuan tertentu segera setelah semua aktivitas tingkat itu dilakukan dengan sukses. COBIT® 2019 mendukung skema kemampuan proses berbasis *Capability Maturity Model Integration*® (CMMI), mulai dari 0 hingga 5. Tingkat kemampuan adalah ukuran seberapa baik suatu proses diimplementasikan dan dilakukan.



Gambar 5. Tingkat Kemampuan Proses
(sumber: buku COBIT® 2019 *FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES*)

Komponen: Struktur Organisasi

Komponen tata kelola bagian struktur organisasi dapat dijadikan acuan untuk mengetahui tingkat tanggung jawab dan akuntabilitas bagi setiap pemegang posisi atau jabatan dalam organisasi maupun perusahaan, baik dari bisnis maupun TI.

Posisi dan struktur organisasi berikut telah didefinisikan dalam konteks COBIT 2019:

- Dewan Direksi
- Komite Eksekuti
- Direktur Eksekutif
- Direktur Keuangan
- Direktur Operasi
- Kepala Petugas Risiko
- Kepala Petugas Informasi
- Direktur Teknologi

- Direktur Digital
- Dewan Tata Kelola IT
- Dewan Arsitektur
- Komite Risiko Perusahaan
- Kepala Petugas Keamanan Informasi
- Pemilik Proses Bisnis
- Manajer Portofolio
- Komite Pengarah (Program/Proyek)
- Manajer Program
- Manajer Proyek
- Kantor Manajemen Proyek
- Fungsi Manajemen Data
- Kepala Sumber Daya Manusia
- Manajer Humas
- Kepala Arsitek
- Kepala Pengembangan
- Kepala Operasi TI
- Kepala Administrasi TI
- Manajer Layanan
- Manajer Keamanan Informasi
- Manajer Kelangsungan Bisnis
- Petugas Privasi
- Penasihat Hukum dan Legal
- Audit

Komponen: Item dan Arus Informasi

Komponen tata kelola ini akan memberikan panduan tentang arus informasi dan item yang terkait dengan praktik proses. Setiap praktik meliputi *input* dan *output*, dengan indikasi asal dan tujuan.

Komponen: Kepegawaian, Keterampilan dan Kompetensi

Komponen tata kelola kepegawaian, keterampilan dan kompetensi mengidentifikasi sumber daya manusia dan keterampilan yang diperlukan untuk mencapai tujuan tata kelola atau manajemen.

Komponen: Kebijakan dan Prosedur

Komponen ini memberikan panduan terperinci tentang kebijakan dan prosedur yang relevan untuk tata kelola atau manajemen secara obyektif. Kebijakan dan prosedur yang relevan disertakan, dengan deskripsi tujuan dan isi dari kebijakan itu sendiri. Tentu antara tujuan yang diinginkan organisasi maupun perusahaan diharuskan memenuhi prosedur dan kebijakan yang berlaku pada suatu wilayah, inilah pentingnya memahami kebijakan dan prosedur guna menghindari ketidakpatuhan.

Komponen: Budaya, Etika dan Perilaku

Komponen tata kelola budaya, etika, dan perilaku memberikan panduan terperinci tentang elemen budaya yang diinginkan di dalam organisasi yang mendukung pencapaian tujuan tata kelola atau manajemen. Jika relevan, referensi ke standar lain dan panduan tambahan disertakan. Budaya, etika dan perilaku tentu akan berkaitan dengan hal-hal yang umum dilakukan dalam lingkungan organisasi maupun perusahaan. Memahami hal ini menjadi bagian penting dalam tata kelola.

Komponen: Layanan, Infrastruktur dan Aplikasi

Komponen layanan, infrastruktur, dan tata kelola aplikasi memberikan panduan terperinci tentang layanan pihak ketiga, jenis infrastruktur dan kategori aplikasi yang dapat diterapkan untuk mendukung pencapaian suatu tata kelola atau tujuan manajemen. Panduan bersifat umum, dengan tujuan untuk menghindari penamaan vendor atau produk tertentu, namun. Komponen ini juga perlu dipahami dalam proses tata kelola teknologi informasi. Selain memanfaatkan pihak ketiga, sebenarnya perusahaan juga dapat mengembangkan layanan, infrastruktur maupun aplikasi oleh tim perusahaan itu sendiri.

2.3.4. COBIT *Core Model*

COBIT Core Model merupakan konsep dasar yang djadikan sebagai tujuan tata kelola dan manajemen, dengan aktivitas yang saling berkaitan.

***Evaluate, Direct and Monitor* (EDM)**

Dalam domain ini memastikan pengaturan dan pemeliharaan kerangka tata kelola yang pasti, manfaat tata kelola dapat tersampaikan dengan baik, menjamin optimalisasi risiko, menjamin optimalisasi sumber daya, dan memastikan keterlibatan pemangku kepentingan

Kemampuan teknologi informasi yang digunakan dapat memadai dalam mendukung tujuan perusahaan yang lebih efektif dalam hal pembiayaan. Menempatkan dan melakukan perawatan pada komponen tata kelola dengan kejelasan otoritas beserta tanggung jawab untuk mencapai tujuan, dan sasaran perusahaan. Hal ini dimaksudkan untuk emberikan pendekatan yang konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola

perusahaan. Keputusan terkait teknologi informasi dibuat sejalan dengan strategi perusahaan, tujuan serta target capaian yang diinginkan diwujudkan. Untuk dapat merealisasikan hal tersebut, perlu adanya kepastian bahwa proses terkait teknologi dipantau secara efektif dan terbuka, tertib terhadap persyaratan hukum, perjanjian kerja dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan terpenuhi.

Optimalisasi nilai untuk bisnis dari investasi bidang layanan teknologi, dan aset teknologi informasi juga perlu diupayakan untuk mengamankan nilai bisnis pada titik optimal, pemberian solusi dan layanan yang hemat biaya, dan analisa biaya yang akurat untuk menunjang kebutuhan kebutuhan bisnis agar didukung secara efektif dan efisien.

Memastikan bahwa sumber daya terkait bisnis dan teknologi yang memadai dan memadai (orang, proses, dan teknologi) tersedia untuk mendukung perusahaan tujuan secara efektif dan, dengan biaya optimal untuk emastikan bahwa kebutuhan sumber daya perusahaan terpenuhi secara optimal, biaya teknologi dioptimalkan, dan ada peningkatan kemungkinan realisasi manfaat dan kesiapan untuk perubahan di masa depan.

Pada domain ini juga perlu menyiapkan pendekatan terstruktur untuk memastikan rekrutmen, perencanaan, evaluasi dan pengembangan sumber daya manusia yang optimal, baik internal dan eksternal, dengan tujuan untuk mengoptimalkan kemampuan sumber daya manusia untuk memenuhi tujuan perusahaan.

Kemudian perlu memastikan bahwa pemangku kepentingan diidentifikasi dan terlibat dalam sistem tata kelola IT dan bahwa pengukuran, pelaporan kinerja dan kesesuaian IT perusahaan transparan, dengan pemangku kepentingan menyetujui tujuan serta menyiapkan tindakan perbaikan yang diperlukan. Untuk memastikan bahwa pemangku kepentingan

mendukung strategi dan peta jalan teknologi informasi, komunikasi kepada pemangku kepentingan efektif dan tepat waktu, dan dasar untuk pelaporan dibuat untuk meningkatkan kinerja. Identifikasi area untuk perbaikan, dan konfirmasikan bahwa tujuan dan strategi terkait teknologi informasi sejalan dengan strategi perusahaan.

Align, Plan and Organized (APO)

Dalam domain ini memastikan bahwa kerangka manajemen IT, strategi, arsitektur perusahaan, inovasi, portofolio, anggaran dan pembiayaan, sumber daya manusia, relasi, kualitas, risiko, keamanan, dan data terkelola dengan baik.

Merancang sistem manajemen untuk IT perusahaan berdasarkan tujuan perusahaan dan faktor lainnya dan mulai menerapkan semua komponen yang diperlukan dari sistem manajemen. Ini dimaksudkan untuk menerapkan pendekatan manajemen yang konsisten untuk memenuhi persyaratan tata kelola perusahaan, yang mencakup komponen tata kelola seperti proses manajemen, struktur organisasi, peran dan tanggung jawab, kegiatan yang andal dan berulang, item informasi, kebijakan dan prosedur, keterampilan dan kompetensi, budaya dan perilaku, serta layanan, infrastruktur, dan aplikasi.

Pengelolaan strategi juga perlu memberikan pandangan holistik tentang bisnis saat ini dan lingkungan IT, arah masa depan, dan inisiatif yang diperlukan untuk bermigrasi ke lingkungan masa depan yang diinginkan. Pastikan bahwa tingkat digitalisasi yang diinginkan merupakan bagian integral dari arah masa depan dan strategi IT. Menilai kematangan digital organisasi saat ini dan mengembangkan peta jalan untuk menutup kesenjangan. Dengan bisnis, pikirkan kembali operasi internal serta kegiatan yang berhadapan dengan pelanggan. Pastikan fokus pada perjalanan

transformasi di seluruh organisasi. Manfaatkan blok bangunan arsitektur perusahaan, komponen tata kelola, dan ekosistem organisasi, termasuk layanan yang disediakan secara eksternal dan kemampuan terkait, untuk memungkinkan respons yang andal namun gesit dan efisien terhadap tujuan strategis. Hal ini dimaksudkan untuk mendukung strategi transformasi digital organisasi dan memberikan nilai yang diinginkan melalui peta jalan perubahan inkremental. Gunakan pendekatan TI holistik, memastikan bahwa setiap inisiatif jelas terhubung dengan strategi menyeluruh. Memungkinkan perubahan dalam semua aspek organisasi yang berbeda, dari saluran dan proses hingga data, budaya, keterampilan, model operasi, dan insentif.

Membangun arsitektur yang terdiri dari proses bisnis, informasi, data, aplikasi dan lapisan arsitektur teknologi. Tentukan persyaratan untuk standar, pedoman, maupun prosedur Meningkatkan keselarasan, meningkatkan kualitas informasi dan menghasilkan potensi penghematan biaya.

Dalam pengelolaan inovasi juga perlu untuk mempertahankan kesadaran akan IT dan tren layanan terkait dan pantau tren teknologi yang muncul. Secara proaktif mengidentifikasi peluang inovasi dan merencanakan bagaimana mendapatkan manfaat dari inovasi dalam kaitannya dengan kebutuhan bisnis dan strategi IT yang ditentukan. Menganalisis peluang apa untuk inovasi atau peningkatan bisnis yang dapat diciptakan oleh teknologi, layanan, atau inovasi bisnis berkemampuan IT yang sedang berkembang; melalui teknologi mapan yang ada; dan dengan inovasi proses bisnis dan TI. Mempengaruhi perencanaan strategis dan keputusan arsitektur perusahaan. Hal ini penting karena untuk mencapai keunggulan kompetitif, inovasi bisnis, peningkatan pengalaman pelanggan, dan peningkatan efektivitas dan efisiensi operasional dengan memanfaatkan perkembangan IT dan teknologi yang muncul.

Mengelola kegiatan keuangan terkait IT yang mencakup anggaran, manajemen biaya dan manfaat serta prioritas pengeluaran melalui penggunaan dan pengalokasian biaya yang adil dan merata bagi perusahaan. Konsultasikan dengan pemangku kepentingan untuk mengidentifikasi dan mengontrol total biaya dan manfaat dalam konteks rencana strategis dan taktis IT. Ini akan mendorong kemitraan antara pemangku kepentingan TI dan perusahaan untuk memungkinkan penggunaan sumber daya terkait IT yang efektif dan efisien serta menyediakan transparansi , akuntabilitas biaya dan layanan. Memungkinkan perusahaan untuk membuat keputusan yang tepat mengenai penggunaan solusi dan layanan IT.

Melaksanakan arah strategis yang ditetapkan untuk investasi sejalan dengan visi arsitektur perusahaan dan peta jalan IT. Pertimbangkan berbagai kategori investasi dan sumber daya serta kendala pendanaan. Mengevaluasi, memprioritaskan, dan menyeimbangkan program dan layanan, mengelola permintaan dalam kendala sumber daya dan pendanaan, berdasarkan keselarasannya dengan tujuan strategis, nilai dan risiko perusahaan. Pindahkan program yang dipilih ke dalam portofolio produk atau layanan aktif untuk dieksekusi. Memantau kinerja keseluruhan portofolio produk dan layanan dan program, mengusulkan penyesuaian seperlunya dalam menanggapi kinerja program, produk atau layanan atau mengubah prioritas perusahaan. Hal ini guna mengoptimalkan kinerja portofolio program secara keseluruhan sebagai tanggapan terhadap program individu, kinerja produk dan layanan serta perubahan prioritas dan permintaan perusahaan.

Build, Acquire and Implement (BAI)

Domain ini memastikan bahwa setiap program, definisi persyaratan, identifikasi dan pembuatan solusi, ketersediaan,

perubahan organisasi, penerimaan dan transisi Perubahan TI, pengetahuan, aset, proyek dapat terkelola dengan baik.

Kelola semua program dari portofolio investasi yang selaras dengan strategi perusahaan dan secara terkoordinasi, berdasarkan pendekatan manajemen program standar. Memulai, merencanakan, mengontrol, dan menjalankan program, dan memantau nilai yang diharapkan dari program. Hal ini dimaksudkan untuk mewujudkan nilai bisnis yang diinginkan dan kurangi risiko keterlambatan, biaya, dan erosi nilai yang tidak terduga. Untuk melakukannya, meningkatkan komunikasi dan keterlibatan bisnis dan pengguna akhir, memastikan nilai dan kualitas hasil program dan tindak lanjut proyek dalam program, dan memaksimalkan kontribusi program terhadap portofolio investasi.

Identifikasi solusi dan analisis persyaratan sebelum akuisisi atau pembuatan untuk memastikan bahwa mereka selaras dengan persyaratan strategis perusahaan meliputi proses bisnis, aplikasi, informasi atau data, infrastruktur dan layanan. Koordinasikan peninjauan opsi yang layak dengan yang terpengaruh pemangku kepentingan, termasuk biaya dan manfaat relatif, analisis risiko, dan persetujuan persyaratan dan solusi yang diusulkan. Hal ini dimaksudkan guna menciptakan solusi optimal yang memenuhi kebutuhan perusahaan sambil meminimalkan risiko.

Menetapkan dan memelihara produk dan layanan yang teridentifikasi (teknologi, proses bisnis, dan alur kerja) sesuai dengan persyaratan perusahaan yang mencakup desain, pengembangan, pengadaan/pengadaan, dan bermitra dengan vendor. Mengelola konfigurasi, persiapan pengujian, pengujian, manajemen persyaratan, dan pemeliharaan proses bisnis, aplikasi, informasi atau data, infrastruktur, dan layanan. Hal ini dimaksudkan untuk memastikan pengiriman produk dan layanan

digital yang gesit dan dapat diskalakan. Membangun solusi yang tepat waktu dan hemat biaya (teknologi, proses bisnis dan alur kerja) yang mampu mendukung tujuan strategis dan operasional perusahaan.

Pengelolaan ketersediaan perlu dipertimbangkan untuk dibangun, seimbangkan kebutuhan saat ini dan masa depan untuk ketersediaan, kinerja, dan kapasitas dengan penyediaan layanan yang hemat biaya. Termasuk penilaian kemampuan saat ini, peramalan kebutuhan masa depan berdasarkan persyaratan bisnis, analisis dampak bisnis, dan penilaian risiko untuk merencanakan dan menerapkan tindakan untuk memenuhi persyaratan yang diidentifikasi, hal ini perlu diupayakan karena untuk menjaga ketersediaan layanan, manajemen sumber daya yang efisien, dan optimalisasi kinerja sistem melalui prediksi kinerja dan persyaratan kapasitas di masa depan.

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

Domain ini memastikan bahwa setiap proses operasi, permintaan dan insiden layanan, masalah, kontinuitaslayanan keamanan, kontrol proses bisnis terkelola dengan baik.

Mengoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang diperlukan untuk memberikan layanan internal IT dan *outsourcing*. Termasuk pelaksanaan prosedur operasi standar yang telah ditentukan dan kegiatan pemantauan yang diperlukan. Hal ini bertujuan untuk memberikan hasil produk dan layanan operasional IT sesuai rencana.

Memberikan respons yang tepat waktu dan efektif terhadap permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal, merekam dan memenuhi pengguna permintaan, dan mencatat, menyelidiki, mendiagnosis, meningkatkan, dan menyelesaikan insiden. Dini dimaksudkan

untuk mencapai peningkatan produktivitas dan meminimalkan gangguan melalui resolusi cepat kueri dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Atasi permintaan pengguna dan pulihkan layanan sebagai respons atas insiden.

Dalam mengelola permasalahan, perlu dilakukan identifikasi dan klasifikasikan masalah beserta akar penyebabnya. Berikan resolusi tepat waktu untuk mencegah insiden berulang. Memberikan rekomendasi untuk perbaikan. Ini dimaksudkan guna meningkatkan ketersediaan, meningkatkan tingkat layanan, mengurangi biaya, meningkatkan kenyamanan dan kepuasan pelanggan dengan mengurangi jumlah masalah operasional, dan mengidentifikasi akar penyebab sebagai bagian dari penyelesaian masalah.

Tidak boleh dilupakan ialah mempersiapkan untuk melakukan reformasi pada perusahaan dengan memaksimalkan sumber daya yang ada, ataupun dengan melakukan proses rekrutmen jika memang dibutuhkan. Ini perlu dilakukan untuk mengantisipasi apabila terjadi keterlambatan pencapaian target ataupun kemungkinan terjadi kegagalan pencapaian tujuan perusahaan. Sehingga apabila ini terjadi, perusahaan sudah siap dengan situasi tersebut dengan melakukan pergantian maupun rotasi.

Monitor, Evaluate and Assess (MEA)

Dalam domain ini memastikan perihal pemantauan kinerja dan kesesuaian, sistem pengendalian internal, tata tertib, asuransi terkelola dengan baik.

Kumpulkan, validasi, dan evaluasi tujuan perusahaan beserta penyelarasannya. Memantau bahwa proses dan praktik berkinerja terhadap yang disepakati tujuan dan metrik kinerja dan

kesesuaian. Berikan pelaporan yang sistematis dan tepat waktu. Hal ini dilakukan dalam upaya memberikan transparansi kinerja dan kesesuaian serta mendorong pencapaian tujuan.

Dalam mengelola sistem pengendalian internal, perlu dilakukan peemantauan dan evaluasi pengendalian lingkungan secara rutin, termasuk penilaian diri dan kesadaran diri. Memungkinkan manajemen untuk mengidentifikasi kekurangan dan inefisiensi kontrol dan untuk memulai tindakan perbaikan. Merencanakan, mengatur, dan memelihara standar penilaian pengendalian internal dan efektivitas pengendalian proses. Guna memperoleh transparansi bagi pemangku kepentingan utama tentang kecukupan sistem pengendalian internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan pada pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

Perlu juga melakukan evaluasi terhadap proses IT dan proses bisnis yang didukung IT sesuai dengan hukum, peraturan, dan perjanjian kontrak dengan pihak eksternal mupun internal. Memperoleh jaminan bahwa perjanjian telah diidentifikasi dan dipenuhi, mengintegrasikan kepatuhan TI dengan kepatuhan perusahaan secara keseluruhan. Ini dilakukan guna memastikan bahwa perusahaan mematuhi semua persyaratan yang berlaku.

2.3. I.T.I.L.

Information Technology Infrastructure Library merupakan sebuah kerangka kerja dalam manajemen layanan teknologi informasi yang menguraikan secara *best practices* untuk memberikan layanan teknologi informasi. Salah satu tujuan utama diterapkannya *IT Infrastructure Library* ini untuk memastikan bahwa layanan teknologi informasi yang digunakan selaras dengan tujuan bisnis, bahkan ketika tujuan bisnis itu berubah.

Information Technology Infrastructure Library telah berkontribusi dan dirasakan manfaatnya oleh banyak perusahaan di dunia yang telah menerapkan *Information Technology Infrastructure Library* ini. Beberapa manfaat yang telah dirasakan diantaranya:

- Peningkatan kepuasan pengguna dan pelanggan dengan layanan teknologi informasi yang diberikan.
- Peningkatan ketersediaan layanan, yang secara langsung mengarah pada potensi peningkatan bisnis keuntungan dan pendapatan.
- Penghematan finansial dari pengurangan pengerjaan yang dilakukan berulang-ulang, menghemat waktu, manajemen sumber daya yang lebih baik dan optimal kinerjanya.
- Peningkatan untuk aspek TI dari produk dan layanan baru.
- Pengambilan keputusan yang lebih baik dan risiko yang dioptimalkan untuk semua proses terkait teknologi informasi.

Salah satu bagian terpenting dari *IT Infrastructure Library* adalah *Configuration Management Database* (CMDB), yang menyediakan otoritas pusat untuk semua komponen, termasuk layanan, perangkat lunak, komponen teknologi informasi, dokumen, pengguna, dan perangkat keras yang harus dikelola untuk memberikan layanan teknologi informasi. CMDB ini melacak lokasi, dan perubahan pada, semua aset dan proses ini, bersama dengan atribut dan hubungannya satu sama lain.

2.3.1. Konsep *IT Infrastructure Library*

IT Infrastructure Library menyediakan serangkaian referensi dan standar khusus untuk manajemen infrastruktur dan layanan yang dapat disesuaikan secara virtual untuk organisasi mana pun. Fungsi dukungan layanan seperti ini akan membantu

mengatasi masalah seperti manajemen masalah, manajemen insiden, layanan, manajemen perubahan, manajemen rilis, dan manajemen konfigurasi. Fungsi pemberian layanan mencakup manajemen kapasitas, manajemen ketersediaan, manajemen keuangan, manajemen kontinuitas, dan tingkat layanan.

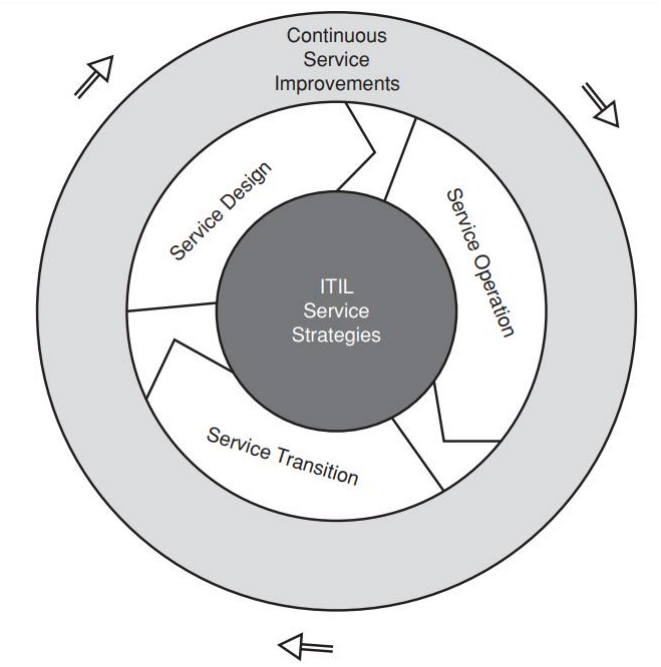
IT Infrastructure Library berkembang karena meningkatnya ketergantungan bisnis pada teknologi informasi dan telah mendapat pengakuan secara global. Sebelumnya, definisi *best practices* dalam layanan teknologi informasi telah bergantung pada individu dan penilaian subjektif tentang apa yang menurut manajer TI paling baik. Pertumbuhan telah dilengkapi dengan menjamurnya konsultasi profesional dan sertifikasi manajer yang mendorong perusahaan untuk semakin meningkatkan keahlian professional sumber daya manusianya dalam melakukan perencanaan, pengaturan, dan penerapan standar organisasi maupun perusahaan.

Konsep *best practices* yang ditawarkan oleh *IT Infrastructure Library* mencakup apa yang sering disebut infrastruktur teknologi informasi, proses pendukung yang memungkinkan aplikasi TI berfungsi dengan baik dan memberikan hasilnya kepada pengguna sistem. Manajemen perusahaan telah memusatkan perhatiannya pada sisi pengembangan aplikasi dari proses teknologi informasi.

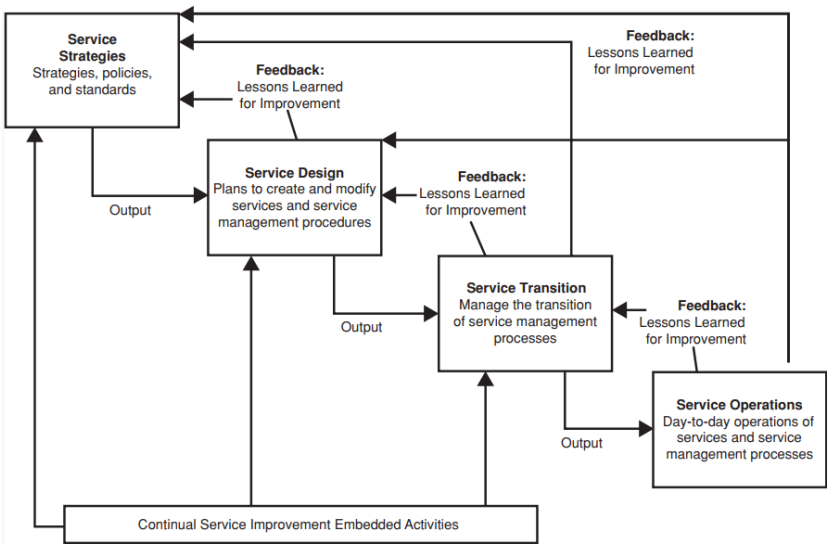
Perusahaan dapat menyiapkan konsep yang lebih luas dalam upaya mengembangkan perusahaan melalui berbagai upaya seperti membangun dan menerapkan sistem prediksi anggaran untuk periode-periode kedepan, untuk dapat menerapkan sistem ini tentu perusahaan sudah harus menerapkan tata kelola yang baik seperti manajemen masalah dan insiden, untuk memungkinkan tingkat konsistensi dari penggunaan sistem prediksi anggaran ini dan tidak menyulitkan sistem dalam "berpikir". Juga diperlukan kapasitas dan proses ketersediaan

yang baik untuk memungkinkan aplikasi baru berjalan seperti yang diharapkan. Proses ini adalah bagian dari infrastruktur teknologi informasi, dan aplikasi yang dirancang dengan baik dan terkontrol dengan baik dan memiliki manfaat yang banyak bagi perusahaan.

Strategi pemberian layanan dapat diilustrasikan sebagai siklus aktivitas berkelanjutan *IT Infrastructure Library*, yang ditunjukkan pada gambar dibawah ini.



Gambar 6. Siklus *Feedback* Berkelanjutan I.T.I.L
(sumber: buku *Executive's Guide to IT Governance*)



Gambar 7. Proses Feedback Layanan I.T.I.L
(sumber: buku *Executive's Guide to IT Governance*)

Proses *IT Infratructure Library* secara tradisional telah dibagi antara yang mencakup dukungan layanan dan yang mencakup pemberian layanan. Proses dukungan layanan membantu membuat aplikasi teknologi informasi beroperasi dengan lebih efisien dan memuaskan pelanggan, sementara proses pemberian layanan meningkatkan efisiensi dan kinerja elemen infrastruktur teknologi informasi.

Ada beberapa proses *best practices* dukungan layanan, mulai dari apa yang disebut manajemen rilis, untuk menempatkan komponen teknologi informasi ke dalam produksi, hingga manajemen insiden guna keperluan pelaporan masalah atau peristiwa pada teknologi informasi secara tertib. Proses dukungan layanan mencakup praktik yang baik untuk setiap perusahaan teknologi informasi, *best practices* yang ditawarkan pada konsep *IT Infrastructure Library* ini menyarankan pendekatan operasi

teknologi informasi, misalnya mempromosikan model operasi yang efisien dan memberikan layanan berkualitas kepada pengguna utama atau pelanggan dari layanan ini. Ini akan sangat berguna untuk melakukan penilaian dan membuat rekomendasi di area operasi teknologi informasi.

2.3.2. Komponen Strategi Layanan *IT Infrastructure Library*

Sebagai *best practices* pada layanan tata kelola teknologi informasi, *IT Infrastructure Libray* menyarankan bahwa manajemen pada teknologi informasi harus terlebih dahulu menilai strategi layanan mereka dengan bertanya pada diri sendiri tentang kualitas dan fungsi layanan TI mereka, diantaranya:

- Ciri khas layanan apa yang kami tawarkan?
- Manakah dari layanan kami yang paling menguntungkan bagi perusahaan secara keseluruhan?
- Manakah dari pelanggan dan pemangku kepentingan kami yang paling puas?
- Area atau layanan mana yang merupakan titik masalah potensial atau area mana yang memiliki tingkat kepuasan paling rendah?
- Manakah dari kegiatan kami yang paling berbeda dan efektif?

Diatas merupakan beberapa pertanyaan penting yang harus dipertimbangkan oleh manajemen pada teknologi informasi ketika akan menilai strategi layanan teknologinya. Diharapkan ini dapat digunakan untuk mendorong fungsi teknologi informasi perusahaan menjadi lebih dari sekadar sumber daya yang mempertahankan proses teknologi informasi, melainkan sumber daya yang menyediakan layanan yang berharga dan hemat biaya

bagi perusahaan secara keseluruhan dan meningkatkan kemampuan penerapan teknologinya.

Infrastruktur teknologi informasi ini akan sangat berbeda di masing-masing perusahaan besar maupun perusahaan skala kecil, karena ukuran operasi maupun sifat bisnis masing-masing perusahaan akan berbeda. Ini dapat terjadi kemungkinan dikarenakan banyak variasi yang mungkin terjadi dalam jenis, ukuran sistem, fasilitas teknologi informasi yang dibutuhkan. Dalam implementasi infrastruktur, tidak ada yang bisa dipermasalahkan antara perusahaan besar maupun kecil, namun setidaknya setiap perusahaan harus menetapkan dan menerapkan infrastruktur sesuai tujuannya.

Saat ini, pertimbangan penganggaran untuk implementasi layanan teknologi informasi harus menjadi focus utama yang jauh lebih penting. Fungsi teknologi informasi yang dikelola dengan baik harus lebih banyak beroperasi, dan manajemen keuangan adalah proses yang penting dan utama untuk membantu mengelola kontrol keuangan bisnisnya.

Tujuan dari strategi manajemen keuangan layanan tentunya untuk menyiapkan panduan guna pengelolaan aset dan sumber daya yang digunakan dalam penyediaan layanan teknologi informasi menjadi yang lebih hemat. Teknologi informasi harus dapat memperhitungkan keseluruhan pengeluarannya untuk layanan teknologi dan untuk mengaitkan biaya layanan yang diberikan kepada pelanggan perusahaan. Terdapat tiga bagian penting dalam pengelolaan keuangan pada *IT Infrastructure Libray*, yang akan dibahas pada paragraf berikutnya.

IT Budgeting

IT budgeting sangat penting untuk melacak dan mengendalikan pengeluaran teknologi informasi perusahaan, juga

untuk menyusun strategi cara mengoptimalkan dan menghemat uang seoptimal mungkin. Hal ini berfungsi sebagai membantu mengalokasikan sumber daya yang diperlukan untuk rencana bisnis kedepan.

IT Budgeting membantu menyediakan anggaran yang diperlukan untuk menjaga perusahaan tetap berjalan. Ini akan bermanfaat bagi perusahaan dalam mengidentifikasi dan menerapkan peningkatan teknologi yang berguna bagi perusahaan. *IT Budgeting* dapat dilihat sebagai investasi dalam sumber daya teknologi informasi yang tidak hanya membantu meningkatkan efisiensi bisnis tetapi juga mendorong pertumbuhan dan keuntungan dalam jangka panjang.

Penganggaran untuk teknologi informasi tentu dapat meningkatkan produktivitas bisnis perusahaan dan memastikan bahwa perusahaan membuat keputusan bisnis yang menguntungkan. Ini dapat membantu perusahaan untuk fokus pada pembaruan teknologi kedepan dan menarik lebih banyak pelanggan. Sering diasumsikan bahwa penganggaran untuk teknologi informasi hanya diperlukan untuk mendapatkan pemahaman tentang biaya yang terlibat dalam membeli teknologi atau peralatan baru dan mencari tahu cara melakukan pembayaran. Namun tidak hanya pada sebatas itu, era modern seperti ini, penganggaran teknologi informasi juga membantu memastikan bahwa perusahaan akan dapat memanfaatkan sumber daya secara optimal dan efisien.

IT Accounting

IT Accounting merupakan serangkaian proses yang memungkinkan teknologi informasi dapat memperhitungkan secara keseluruhan tentang pengelolaan anggaran untuk keperluan perbelanjaan. Fungsi teknologi informasi saat ini tidak

selalu melakukan pekerjaan dengan baik di bidang ini. Mereka memiliki berbagai macam biaya eksternal, termasuk perangkat lunak, sewa peralatan, biaya telekomunikasi, instalasi jaringan internet dan lainnya, tetapi biaya ini seringkali tidak dikelola atau dilaporkan dengan baik. Mereka memiliki data yang cukup untuk membayar tagihan dan mengevaluasi beberapa biaya area tertentu, tetapi fungsi teknologi informasi seringkali tidak memiliki tingkat akuntansi yang lebih rinci seperti akuntansi biaya atau model akuntansi berbasis aktivitas yang ditemukan di perusahaan manufaktur besar.

Charging

Charging merupakan proses yang menyediakan penetapan harga dan penagihan untuk layanan teknologi informasi. Ini membutuhkan akuntansi teknologi informasi yang baik, dan perlu dilakukan dengan cara yang sederhana, adil, dan terkontrol dengan baik. Proses *charging* ini terkadang tidak diterapkan dengan baik, karena laporan penagihan layanan teknologi informasi terlalu rumit atau teknis untuk dipahami banyak pelanggan. Teknologi informasi perlu menghasilkan laporan yang jelas dan dapat dimengerti tentang layanan teknologi informasi yang digunakan sedemikian dengan rupa sehingga pelanggan memahami dengan jelas.

Dalam mendukung proses strategi peningkatan layanan, manajemen keuangan harus memahami prosedur penetapan biaya, penetapan harga, dan *charge* yang ditentukan ini. Meskipun umumnya tidak dijadikan sebagai pusat laba perusahaan, proses manajemen keuangan memungkinkan teknologi informasi dan pelanggannya untuk lebih memikirkan operasi layanan teknologi informasi dalam hal bisnis. Proses manajemen keuangan dapat memungkinkan teknologi informasi dan manajemen secara keseluruhan untuk membuat keputusan dan tindakan.

2.3.3. Desain Layanan *IT Infrastructure Library*

Dalam pembelajaran ini, terdapat lima aspek dalam desain layanan *IT Infrastructure Library*:

- Desain setiap layanan teknologi informasi yang ditawarkan diantaranya termasuk persyaratan fungsionalnya, kebutuhan sumber daya, dan kemampuan yang diantisipasi.
- Desain sistem dan alat manajemen layanan sering disajikan melalui portofolio formal, untuk manajemen dan kontrol layanan ini melalui siklus operasi mereka.
- Desain arsitektur teknologi informasi dan sistem manajemen yang diperlukan untuk menyediakan layanan.
- Desain proses yang diperlukan untuk menginstal, mengoperasikan, dan meningkatkan proses layanan secara keseluruhan.
- Desain metode pengukuran dan metrik proses layanan dan arsitektur komponennya.

Untuk mendukung pemberian layanan yang lebih optimal dan efisien, *IT Infrastructure Libray* telah menentukan serangkaian proses. Seperti proses manajemen kontinuitas, *Service Level Agreement* (SLA) yang mendefinisikan kinerja dan harapan antara teknologi informasi dan hal ini tidak selalu dipahami atau diimplementasikan dengan baik.

Manajemen kapasitas pada *IT Infrastructure Library* memastikan kapasitas infrastruktur teknologi informasi yang diterapkan selaras dengan kebutuhan bisnis untuk mempertahankan tingkat pemberian layanan yang diperlukan dengan biaya yang dapat diterima melalui tingkat kapasitas yang sesuai. Melalui pengumpulan data kapasitas bisnis dan teknis, proses ini harus menghasilkan rencana kapasitas untuk

memberikan persyaratan kapasitas teknologi informasi guna penyesuaian dengan anggaran biaya untuk perusahaan. Selain tujuan utama untuk memahami persyaratan kapasitas teknologi informasi perusahaan dan untuk memenuhinya, kapasitas manajemen juga bertanggung jawab untuk menilai potensi keunggulan teknologi baru bisa memiliki untuk perusahaan.

Implementasi proses manajemen kapasitas yang efektif akan membantu merencanakan pengelolaan kapasitas yang baik dan menghasilkan manfaat yang baik juga. Manajemen kapasitas yang efektif harus dapat memperkirakan dampak aplikasi atau modifikasi baru serta memberikan penghematan biaya yang selaras dengan persyaratan operasi perusahaan. Perencanaan kapasitas yang tepat dapat secara signifikan mengurangi biaya keseluruhan kepemilikan sistem teknologi informasi.

Manajemen ketersediaan pengiriman layanan di era sekarang benar-benar menjadi konsep yang memanjakan kebutuhan konsumen. Perusahaan saat ini semakin bergantung pada layanan teknologi informasi yang dapat berjalan pada setiap waktu. Dalam banyak kasus ketika layanan teknologi informasi tersebut tidak tersedia atau bahkan tidak berfungsi, maka proses bisnis juga akan berhenti. Ini menjadi sangat penting bahwa fungsi teknologi informasi mengelola dan mengontrol ketersediaan layanannya. Ini dapat dicapai dengan mendefinisikan persyaratan dari bisnis mengenai ketersediaan layanan teknologi informasi dan kemudian mencocokkannya dengan kemampuan perusahaan dalam menggunakan teknologi informasinya.

Best practices yang ditawarkan dalam konsep manajemen ketersediaan pada IT Infrastructure Library bergantung terhadap beberapa inputan, diantaranya mengenai ketersediaan bisnis, pemeliharaan dan pemulihan, layanan, informasi antar proses yang ada, manajemen masalah, serta target layanan yang ingin dicapai. Tujuan dari proses manajemen ketersediaan antara lain:

- Menghasilkan dan memelihara rencana ketersediaan yang sesuai dan terkini yang mengacu pada kebutuhan perusahaan saat ini dan masa depan.
- Memberikan layanan dan panduan kepada semua bidang perusahaan lainnya tentang masalah terkait ketersediaan teknologi informasi.
- Pastikan bahwa pencapaian ketersediaan layanan memenuhi atau melampaui target, dengan mengelola kinerja ketersediaan terkait layanan dan sumber daya.
- Membantu diagnosis, penyelesaian insiden dan masalah terkait ketersediaan.
- Menilai dampak semua perubahan pada rencana ketersediaan, kinerja, kapasitas semua layanan dan sumber daya.
- Memastikan setiap kebutuhan yang ada beserta proses-proses didalamnya mendapat pendanaan yang cukup.

Setiap perusahaan, apalagi yang sudah berjalan secara profesional perlu menyiapkan rancangan infrastruktur pemulihan sedemikian rupa sehingga jika terdapat gangguan sewaktu-waktu, dapat dilakukan pemulihan kondisi dalam waktu yang singkat. Merancang pemulihan ini merupakan bagian dari manajemen ketersediaan. Bagaimanapun, ketidakbaikan dalam manajemen ketersediaan ini dapat menjadi salah satu penyebab terhentinya proses operasional perusahaan, misalnya manajemen ketersediaan bahan baku tidak diatur dengan baik, saat proses operasional terjadi, bahan baku mengalami kekurangan, secara otomatis ini akan mengakibatkan proses operasi terhenti.

Tren dunia era modern terhadap ketergantungan yang tinggi pada dukungan dan layanan teknologi informasi ini semakin terlihat jelas, bahkan kemungkinan akan terus berlanjut dan semakin mempengaruhi bisnis yang berkaitan dengan pelanggan langsung, manajer, maupun pembuat keputusan. Menguatkan strategi yang tepat untuk dikembangkan dan digunakan dalam

jangka yang lama demi mengoptimalkan peran teknologi informasi dalam pekerjaan bisnis perlu dipikirkan oleh pemangku kepentingan, organisasi teknologi informasi perusahaan harus menerapkan serangkaian keberlanjutan layanan yang lebih efektif.

Meningkatnya ketergantungan ini perlu diimbangi dengan penyiapan keamanan teknologi informasi. Manajemen keamanan informasi dalam implementasi tata kelola berperan penting dalam menyiapkan langkah strategis untuk keamanan informasi dan data perusahaan, tentu ini akan berkaitan dengan tujuan yang ingin dicapai perusahaan, keamanan informasi lebih dari sekedar masalah, melainkan juga menjadi perlindungan atas kepentingan perusahaan. Keamanan informasi perlu direncanakan guna mencapai tujuan-tujuan seperti berikut:

- **Tujuan ketersediaan**
  Informasi tersedia dan dapat digunakan bila diperlukan, dan sistem yang menyediakannya dapat dengan tepat untuk menahan serangan dan pemulihan.
- **Tujuan kerahasiaan**
  Informasi diamati atau diungkapkan hanya kepada mereka yang memiliki hak untuk mengetahui.
- **Tujuan integritas dan Non-Repudiasi**
  Informasi lengkap, akurat, dan terlindungi dari manipulasi data dan memastikan bahwa tidak ada pihak yang dapat menolakk bahwa pesan dikirim dan diterima melalui enkripsi.

2.3.4. Manajemen Transisi Layanan

Sebagai manajer dan atau professional bidang teknologi informasi, operasi teknologi informasinya hampir selalu mengalami perubahan baik dari sisi perangkat keras maupun perangkat lunak, selama teknologi digunakan, perubahan ini akan selalu rutin berlangsung karena efek perubahan teknologi yang

begitu cepat. Hal ini memungkinkan perusahaan untuk mulai menyusun perencanaan transisi yang tepat untuk antisipasi persiapan penggunaan komponen baru, pengujian komponennya beserta validasi sebelum masuk pada tahap rilis atau penggunaan. Inilah yang disebut sebagai manajemen transisi, suatu lingkup pengelolaan yang berkaitan dengan proses operasi teknologi informasi.

Manajemen Perubahan Transisi Layanan

Tujuan dari manajemen perubahan transisi layanan adalah untuk memanfaatkan metode dan prosedur standar dalam penanganan yang lebih efisien dan cepat dari semua perubahan tansisi layanan, tentu juga untuk meminimalkan dampak yang akan ditimbulkan terhadap kualitas layanan dan operasi sehari-hari. Proses manajemen perubahan ini meliputi:

- Perubahan *hardware* dan *software* sistem
- Peralatan dan perangkat komunikasi.
- Semua perangkat lunak aplikasi yang digunakan.
- Semua dokumentasi dan prosedur yang terkait dengan eksekusi, dukungan, dan pemeliharaan sistem.

Dari keempat poin diatas mempunyai peran penting yang tidak dapat disampingkan, dimana *hardware* dan *software* akan terus berkembang sesuai kebutuhan penggunanya, jika salah satu dari hardware tetap menggunakan komponen lama sementara spesifikasi *software* yang digunakan sudah menuntut spesifikasi baru, maka *software* tidak dapat digunakan secara maksimal, begitu pula sebaliknya jika *software* yang masih digunakan menggunakan infrastruktur lama, sementara tuntutan fitur sistem perusahaan lebih kompleks, maka ini tidak akan berperan maksimal.

Dokumentasi juga memiliki peran penting, setiap perubahan komponen perlu membutuhkan dokumentasi untuk memudahkan pengguna sistem atau pengguna komponen dapat mengetahui teknologi atau perubahan apa yang diterapkan, langkah-langkah dalam menggunakan fitur baru, dan lain sebagainya.

Dalam melakukan perubahan setiap komponen TI, baik itu perubahan *software*, *hardware*, maupun dokumentasi, yang perlu dipertimbangkan adalah terkait sistem yang diterapkan oleh perusahaan, karena ini akan menimbulkan pengaruh juga terhadap implementasi teknologi secara keseluruhan. Sehingga dalam melakukan perubahan komponen perlu didiskusikan secara internal oleh tim TI terkait, misal akan terjadi perubahan peningkatan spesifikasi perangkat keras perlu koordinasi dengan tim penanganan perangkat lunak juga.

Untuk menciptakan proses manajemen perubahan yang efektif, diperlukan infrastruktur teknologi informasi yang tepat. Infrastruktur yang dipilih juga harus melalui penyusunan rencana yang matang dan menyesuaikan dengan kebutuhan agar infrastruktur teknologi digunakan secara efektif, dan harus mencakup hal-hal berikut:

- Penyelarasan layanan teknologi informasi yang lebih baik dengan kebutuhan bisnis.
- Peningkatan visibilitas dan komunikasi perubahan pada bisnis dan layanan pendukung.
- Penilaian risiko yang lebih baik.
- Berkurangnya dampak buruk dari perubahan pada kualitas layanan.
- Penilaian yang lebih baik atas biaya perubahan yang diusulkan sebelum dikeluarkan.
- Peningkatan produktivitas dengan adanya peningkatan pada teknologi informasi.

- Kemampuan TI lebih maksimal

Proses manajemen perubahan pada *IT Infrastructure Library* adalah komponen penting dari pengendalian infrastruktur pada teknologi informasi dan harus selaras erat dengan konfigurasi, kapasitas, dan proses dalam infrastruktur teknologi informasi.

Manajemen Konfigurasi Transisi Layanan

Fungsi dari operasi teknologi informasi cukup kompleks, dengan berbagai jenis dan versi komponen perangkat keras dan perangkat lunak dan komponen lainnya yang mana komponen tersebut harus bekerja sama secara teratur dan terkelola dengan baik. Fungsi dari manajemen konfigurasi adalah sebagai proses pemberian layanan yang mendukung identifikasi, pencatatan, dan pelaporan komponen teknologi informasi, versi, komponen penyusunnya, dan hubungan antar komponen. Manajemen konfigurasi juga menjaga hubungan antar aset, yang biasanya tidak dilakukan pada manajemen aset. Beberapa perusahaan mulai dengan manajemen aset dan kemudian beralih ke manajemen konfigurasi.

BAB III MANAJEMEN RISIKO TI

3.1. Tinjauan

Manajemen risiko teknologi informasi merupakan implementasi dari prinsip-prinisip manajemen risiko terhadap perusahaan yang memanfaatkan teknologi informasi sebagai alat bantu untuk menjalankan proses bisnisnya dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan.

Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan operasional dan biaya ekonomi dari tindakan perlindungan dan mencapai keuntungan perusahaan, dengan proses melakukan perlindungan terhadap Sistem dan data TI yang terkait perusahaan tersebut. Contoh kasus yang dapat diambil dalam pembelajaran ini adalah kasus keamanan data misalnya. Banyak perusahaan memutuskan untuk menginstal sistem keamanan data perusahaan dan mengeluarkan banyak uang untuk membayar jasa penyedia layanan agar sistem ini tetap dalam pengamanan berkala guna memastikan data perusahaan aman. Dalam hal ini seharusnya pemilik perusahaan telah mempertimbangkan dan menghitung kemungkinan biaya yang dikeluarkan untuk melakukan pengamanan data perusahaan, biaya yang dikeluarkan diharapkan sebanding dengan profit yang didapat perusahaan itu sendiri. Sehingga tidak timbul kerugian

atas kasus diatas. Tentu risiko keamanan data akan diimbangi dengan seberapa tinggi nilai dari perusahaan tersebut, tidak berbanding jika perusahaan tersebut hanya memiliki data yang bersifat tidak rahasia, namun pihak perusahaan membayar mahal hanya untuk menjaga keamanan data tersebut. Ini akan menjadi sebuah kerugian yang cukup signifikan.

Beberapa risiko yang dapat mengakibatkan hambatan atas berjalannya teknologi antara lain:

- Kerusakan pada perangkat keras dan perangkat lunak
- *Malware*
- Virus komputer
- *Spam, scams, and phishing*
- *Human error*

Hambatan-hambatan diatas dapat terjadi berasal dari kemungkinan tindakan seperti:

- *Hacking*, yaitu tindakan dari seseorang yang secara illegal menerobos ke dalam sistem computer melalui berbagai cara.
- *Fraud*, yaitu penggunaan komputer yang berdampak kepada manipulasi data untuk kepentingan yang melanggar hukum.
- *Denial-of-service*, yaitu serangan *online* yang mengakibatkan sebuah situs tidak dapat diakses.
- *Staff dishonesty*, yaitu pencurian data atau informasi penting oleh pegawai internal perusahaan.

Pimpinan organisasi atau perusahaan setidaknya harus memastikan bahwa organisasi memiliki kemampuan yang dibutuhkan untuk mencapai misinya. Ini akan berkaitan dengan kemampuan keamanan sistem yang diperlukan organisasi atau perusahaan. Sebagian besar organisasi memiliki anggaran yang ketat untuk keamanan teknologi informasinya, oleh karena itu,

keamanan teknologi informasi harus ditinjau secara menyeluruh seperti keputusan manajemen lainnya. Risiko yang terstruktur dengan baik dapat berjalan secara efektif, dapat membantu manajemen mengidentifikasi secara tepat pengendalian meningkatkan kemampuan keamanan demi tercapainya tujuan perusahaan.

Apalagi di era *big data* seperti sekarang ini, beberapa perusahaan besar berlomba-lomba mengumpulkan data dari konsumen guna melakukan pemetaan minat konsumen, sehingga produk maupun jasa yang diciptakan perusahaan akan tepat sasaran sesuai kebutuhan konsumennya. Hal ini tentu membuat banyak oknum yang tidak bertanggungjawab berupaya menciptakan berbagai varian *malware* yang didistribusikan kedalam sistem-sistem perusahaan tertentu demi mendapatkan data-data pentingnya. Inilah yang menjadikan proses audit teknologi informasi pada organisasi atau perusahaan menjadi aktivitas yang harus dilakukan oleh perusahaan, baik audit secara internal maupun audit oleh pihak eksternal, khususnya audit terhadap implementasi teknologi informasinya.

3.2. Perspektif Manajemen Risiko TI

Risiko dapat diatasi dengan tiga cara yaitu menerimanya, menguranginya, atau mentransfernya. Yang sesuai metode sepenuhnya tergantung pada nilai keuangan risiko dengan investasi diperlukan untuk menguranginya ke tingkat yang dapat diterima atau mentransfernya ke pihak ketiga. Selain kontrol preskriptif, peraturan mengharuskan organisasi menilai risiko terhadap informasi yang dilindungi dan menerapkan kontrol yang wajar untuk mengurangi risiko ke tingkat yang dapat diterima.

Manajemen risiko teknologi informasi menjadi konsep maupun prinsip-prinisip manajemen risiko terhadap perusahaan

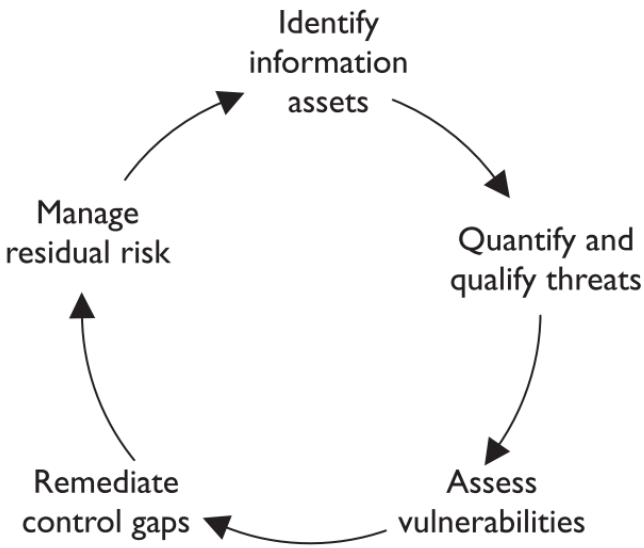
yang memanfaatkan teknologi informasi dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan.

Dalam perusahaan, yang bertanggung jawab dalam manajemen risiko disebut sebagai *risk management officer*. Sementara tugas dan tanggung jawab seorang manajemen risiko berdasarkan situs roberthalf, antara lain:

- Merancang dan menerapkan proses manajemen risiko
- Melakukan penilaian risiko
- Melakukan evaluasi risiko
- Menetapkan tingkat risiko yang diambil perusahaan
- Mempersiapkan manajemen risiko dan anggaran asuransi
- Pelaporan risiko disesuaikan dengan audiens yang relevan
- Menjelaskan risiko eksternal yang ditimbulkan oleh tata kelola perusahaan kepada pemangku kepentingan
- Membuat rencana kesinambungan bisnis untuk membatasi risiko
- Menerapkan langkah-langkah kesehatan dan keselamatan, dan membeli asuransi
- Melakukan audit kebijakan dan kepatuhan
- Memelihara catatan polis dan klaim asuransi
- Meninjau kontrak besar atau proposal bisnis internal
- Membangun kesadaran risiko di antara staf dengan memberikan dukungan dan pelatihan di dalam perusahaan

3.3. Siklus Manajemen Risiko TI

Seperti metodologi pada umumnya, manajemen risiko memiliki karakteristik yang tertuang dalam beberapa fase yang dapat dilihat pada gambar berikut:



Gambar 8. Siklus Manajemen Risiko

3.3.1. Fase 1: *Identify Information Assets*

Fase pertama dalam siklus manajemen risiko teknologi informasi adalah dengan melakukan identifikasi atas aset informasi organisasi. Untuk melakukan ini, perlu melakukan penyelesaian pada beberapa tugas berikut:

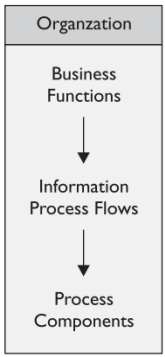
- Tentukan nilai kekritisan informasi.
- Identifikasi fungsi bisnis.
- Memetakan proses informasi.
- Mengidentifikasi aset informasi.
- Menetapkan nilai kekritisan untuk aset informasi

Tujuan dari fase ini adalah untuk mengidentifikasi semua aset informasi dan menetapkan setiap aset informasi memiliki tingkat kerahasiaan, integritas dan persyaratan ketersediaan dengan nilai tinggi, sedang, atau rendah. Contoh kasus, dari sebuah perusahaan perbelanjaan dapat mengidentifikasi informasi pelanggannya secara detail. Aset informasi ini memiliki nilai yang berharga bagi pencuri jika disebarluaskan ke publik dengan cara yang tidak baik. Perusahaan juga menyadari jika data pelanggan tersebut diubah bahkan dihapus, ini akan mengakibatkan kehilangan data konsumen. Dari kasus ini maka perusahaan akan menetapkan bahwa nilai untuk asset informasi data konsumen ini kedalam nilai yang memiliki kerahasiaan tinggi sebagai bentuk kepercayaan dan integritas data konsumen pada perusahaan ini.

Cara terbaik untuk mengidentifikasi aset informasi adalah dengan mengambil pendekatan *top-down* yang dimulai dengan fungsi organisasi, mengidentifikasi proses yang mendukung fungsi bisnis tersebut, dan menelusuri ke aset informasi yang diproses oleh sistem yang mendukung setiap fungsi bisnis.

Mendefinisikan Nilai Kekritisan Informasi

Sebelum kita mulai mengidentifikasi aset informasi, alangkah baiknya mengamati gambar berikut:



Gambar 9. Uraian Fungsi Bisnis

Langkah pertama dalam proses ini adalah untuk mendefinisikan setiap nilai dalam hal seberapa parah dampaknya jika terjadi pelanggaran aset dengan nilai tertentu. Agar berhasil, ini perlu mendapatkan konsensus dari pemangku kepentingan organisasi utama mengenai definisi dan untuk melakukan dokumentasi definisi-definisi tersebut. Proses ini perlu memerlukan tingkatan level yang dapat ditetapkan dengan pimpinan organisasi atau perusahaan ini untuk mendapatkan persetujuan mereka pada satu Definisi.

Mengidentifikasi Fungsi Bisnis

Mengidentifikasi dimana informasi asset tertentu berada dan melakukan pemetaan asset mana yang paling penting bagi bisnis, ini menjadi salah satu bagian yang paling sulit dari manajemen risiko. Untungnya, sebagian besar bisnis diatur berdasarkan fungsi. Akibatnya, fungsi bisnis yang penting dapat diidentifikasi menggunakan bagan organisasi. Tentu hal ini tidak dapat dibiarkan, tetap harus dilakukan verifikasi bahwa semua fungsi bisnis diwakili secara tepat dan akurat.

Setelah fungsi bisnis dapat diidentifikasi dengan benar, kita dapat melakukan penetapan nilai kekritisan untuk masing-masing fungsi. Sebagai contoh, sebuah perusahaan dapat menentukan bahwa fungsi bisnis operasi pusat perbelanjaan memerlukan tingkat kerahasiaan yang tinggi karena penggunaan informasi data konsumen. ini perlu tingkat integritas informasi yang tinggi karena transaksi bersifat finansial.

Pemetaan Proses Informasi

Karena dalam hal ini teknologi informasi bertindak sebagai alat bantu memproses informasi, risiko TI memiliki kompleksitas tambahan untuk menyentuh beberapa titik dalam suatu proses untuk mendapat hasil yang akurat. Melakukan pemetaan proses informasi menjadi sangat penting karena beberapa hal yang perlu diperhatikan:

- Pemetaan proses informasi membantu organisasi ataupun perusahaan dalam mengidentifikasi aset informasi mana yang digunakan oleh setiap proses.
- Pemetaan proses informasi membantu organisasi ataupun perusahaan dalam menemukan titik proses identitas (langkah-langkah) yang memerlukan input manual (yang cenderung lebih rentan dari pada proses otomatis).
- Pemetaan proses informasi membantu organisasi ataupun perusahaan dalam memahami sistem informasi mana yang membutuhkan perlindungan

Setelah organisasi ataupun perusahaan berhasil mengidentifikasi fungsi bisnis, kini dapat mulai mengidentifikasi proses yang mendukung fungsi bisnis tersebut dan aset informasi yang berada melalui proses. Penting untuk diperhatikan bahwa pimpinan organisasi ataupun perusahaan tidak memikirkan secara detail dengan teknologi yang digunakan untuk memproses

informasi, melainkan lebih memperhatikan proses dan hasil akhir yang didapatkan.

Menetapkan Nilai Kekritisan Informasi untuk Aset Informasi

Pada studi kasus sebelumnya telah kita coba identifikasi fungsi bisnis operasi pada pusat perbelanjaan, bahwa fungsi bisnis operasi pusat perbelanjaan tersebut bertanggung jawab untuk memproses transaksi yang menggunakan data konsumennya yang mana dari proses tersebut akan menghasilkan proses transaksi Dengan demikian, dapat diidentifikasi asset informasi tersebut dan dapat ditetapkan nilai kekritisannya. Saat meninjau suatu proses, kita perlu mempertimbangkan semua aset potensial yang berada pada setiap proses tersebut. Jenis aset informasi data pelanggan ini seringkali diabaikan dan dianggap sesuai yang biasa, tetapi setelah dilakukan pemetaan dan penelusuran, nilai data tersebut memiliki tingkat kritis yang tinggi terhadap perusahaan dan menjadi data penting proses penting.

Saat menetapkan nilai kekritisan, kita perlu mempertimbangkan persyaratan aset untuk kategori kerahasiaan, integritas, dan ketersediaan. Hubungan ini terwakili dengan baik menggunakan matriks kekritisan informasi yang awalnya dikembangkan oleh Badan Keamanan Nasional untuk Metodologi Penilaian (*NSA INFOSEC - National Security Agency*). Seperti contoh yang dapat dilihat pada tabel berikut:

Tabel 3. Matriks Kekritisan Informasi

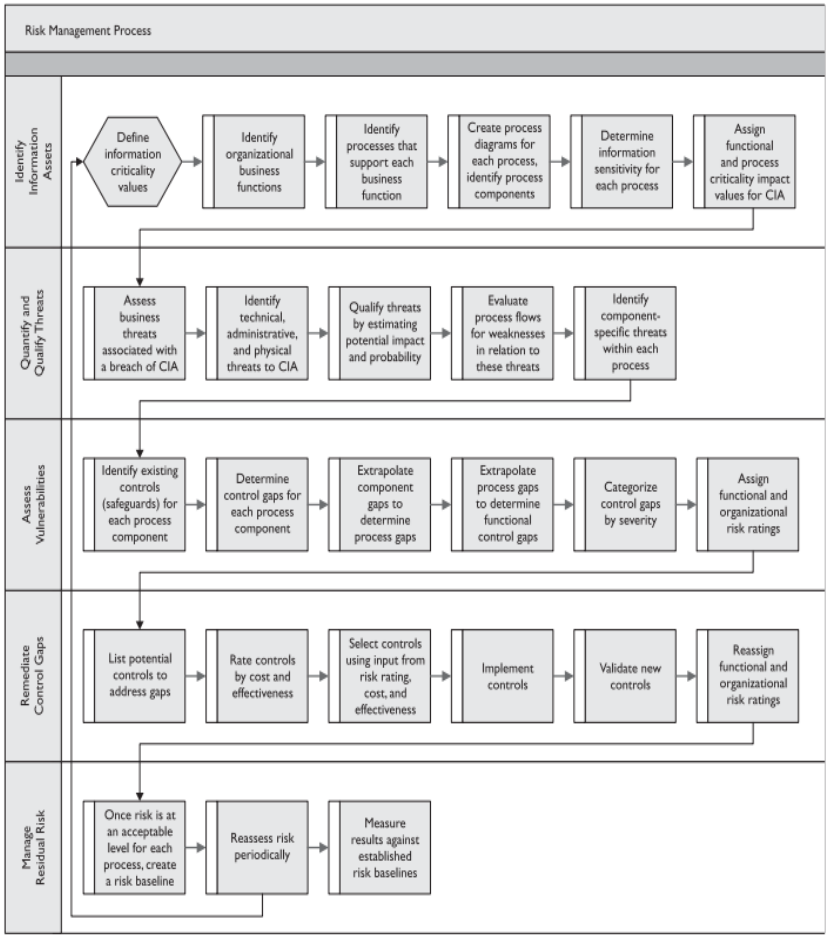
Asset Informasi	Kerahasiaan	Integritas	Ketersediaan
Data Pelanggan	Tinggi	Tinggi	Tinggi

Konfigurasi Sistem	Medium	Tinggi	Medium
Informasi pemantauan sistem	Rendah	Tinggi	Tinggi

3.3.2. Fase 2: *Quantify and Qualify Threats*

Ancaman informasi berdampak pada nama baik organisasi maupun perusahaan dan daya minat konsumen berisiko berkurang, hilang sumber daya, biaya pemulihan, dan tindakan hukum beserta peraturan. Ketika ancaman tersebut terjadi, terkadang beberapa perusahaan tidak mempertimbangkan dana darurat guna mengatasi permasalahan tersebut. Biaya-biaya ini seringkali tidak diperhitungkan karena tidak diidentifikasi dengan benar. Sebagai contoh, katakanlah organisasi atau perusahaan tertentu diserang oleh pihak tak bertanggungjawab yang mengakibatkan hilangnya banyak data, dan memerlukan waktu yang lama untuk pemulihan data tersebut, lama atau tidaknya proses pemulihan data tentu berdasarkan banyaknya data yang hilang. Biaya ini dapat dihitung dengan mengukur waktu yang diperlukan untuk pemulihan dan estimasi kerugian yang terkait dengan penundaan pemrosesan data yang seharusnya berjalan jika tidak terjadi masalah ini.

Langkah selanjutnya dalam siklus manajemen risiko adalah mengukur dan memenuhi syarat ancaman. Dalam pembelajaran ini juga dapat diambil pendekatan top-down saat mulai mengidentifikasi ancaman, dimulai dengan ancaman bisnis dan beralih ke ancaman teknis yang dapat ditimbulkan dan teridentifikasi sebagai ancaman bisnis.



Gambar 10. Proses Manajemen Risiko
(sumber: buku *IT Auditing Using Controls to Protect Information Assets – Second Edition*)

Setidaknya dalam penerapannya, fase siklus manajemen risiko ini memerlukan langkah-langkah berikut:

- Menilai ancaman bisnis.
- Mengidentifikasi ancaman teknis, fisik, dan administratif.
- Mengukur dampak dan probabilitas ancaman.
- Mengevaluasi alur proses untuk kelemahan.
- Identifikasi ancaman komponen proses

Menilai Ancaman Bisnis

Ancaman bisnis tentu menjadi salah satu kemungkinan yang tidak dapat dihindari oleh setiap organisasi maupun perusahaan, baik yang sudah berskala besar ataupun organisasi dan perusahaan yang masih dalam skala kecil. Ancaman dalam setiap bisnis sebenarnya dapat dipertanggungjawabkan melalui berbagai upaya, ancaman bisnis terhadap informasi dapat dibagi menjadi tiga kategori: ancaman finansial, ancaman hukum, dan ancaman peraturan. Dari kategori ancaman ini merupakan bagian dari setiap langkah strategis yang diambil keputusannya oleh pimpinan perusahaan.

Ancaman Finansial

Untuk mendefinisikan ancaman peraturan dan hukum. Namun secara garis besar, ancaman keuangan didefinisikan sebagai ancaman yang jika terjadi suatu ancaman akan menyebabkan hilangnya dana aktual, reputasi, efektivitas operasional, atau persaingan antar perusahaan, yang pada akhirnya menghasilkan dampak perubahan pada penggunaan finansial perusahaan.

Ancaman Hukum

Setelah dilakukan proses identifikasi dari beberapa ancaman keuangan, berikutnya harus mempertimbangkan potensi adanya hukum yang terkait dengan realisasi ancaman. Era modern saat ini telah muncul undang-undang terkait privasi, jika informasi pribadi seseorang seperti nama, alamat dan data selengkapnya disebarluaskan untuk kepentingan yang tidak baik, maka dapat berdampak pada kemungkinan berbenturan dengan peraturan dan hukum terkait. Selain itu, jika tingkat layanan terpengaruh atau informasi rahasia organisasi maupun perusahaan lain disebarluaskan, pelanggaran kontrak dapat terjadi. Maka dapat disimpulkan bahwa pemangku kebijakan maupun pimpinan organisasi dan perusahaan wajib mengetahui hukum yang berlaku dimana organisasi atau perusahaan itu berdomisili, setidaknya ini menjadi penting untuk dapat dikaji dalam upaya menghindari ancaman hukum.

Ancaman Regulasi

Seiring dengan ancaman finansial dan hukum, penting juga untuk mempertimbangkan ancaman peraturan. Pelanggaran peraturan yang diakibatkan oleh insiden keamanan informasi dapat menyebabkan denda atau hukuman lain, serta penghentian sementara atau permanen operasi perusahaan. Lembaga keuangan umumnya mengambil undang-undang yang mengatur operasi, konsekuensi yang didapat juga cukup serius apabila terdapat tidakpatuhan perusahaan pada regulasi setempat. Maka bagi pemangku kebijakan ataupun pimpinan perusahaan wajib mengetahui regulasi yang berlaku pada wilayah tersebut untuk menghindari ancaman regulasi.

Mengidentifikasi ancaman teknis, fisik, dan administratif

Setelah semua ancaman bisnis yang berkaitan dengan aset informasi dapat diidentifikasi, selanjutnya dapat mulai mengidentifikasi ancaman teknis, fisik, dan administratif. Ancaman ini jika disadari, akan memunculkan salah satu ancaman bisnis yang telah diidentifikasi sebelumnya. Misalnya kerusakan sistem terkait proses produksi akan menimbulkan hilangnya produktivitas organisasi maupun perusahaan, apalagi jika organisasi atau perusahaan tersebut tidak memiliki *backup* sistem untuk melanjutkan proses produksi tersebut, otomatis proses produksi dapat terhenti.

Ancaman teknis umumnya berkaitan dengan sistem yang memiliki pengaruh langsung terhadap informasi yang disimpan atau ditransmisikan secara elektronik. Mengingat contoh pemrosesan data pelanggan sebelumnya pada pusat perbelanjaan, salah satu ancaman teknis adalah intrusi sistem. Ancaman ini kemudian dapat menimbulkan pencurian informasi kepemilikan, peraturan atau ancaman bisnis hukum. Berikut adalah beberapa contoh ancaman teknis:

- Intrusi sistem
- *Worm, virus, spyware*, dan *malware* lainnya
- Kegagalan sistem
- Kegagalan kontrol akses

Ancaman fisik biasanya terkait fasilitas sarana dan seringkali dapat terkait dengan peristiwa alam atau kerusakan mekanis. Walaupun bersifat fisik, justru model ancaman ini dapat menyebabkan hilangnya informasi yang cukup signifikan. Sehingga rencana kelangsungan bisnis dan pemulihan bencana maupun kontrol server data harus dilakukan guna bertujuan untuk mengatasi ancaman ini.

Mengukur Ancaman

Setelah berbagai ancaman teridentifikasi dengan detail, selanjutnya perlu dipahami bahwa potensi dampak dan probabilitas dari ancaman-ancaman tersebut bisa saja lekas terjadi, namun bisa saja dapat dikurangi. Setidaknya terdapat dua faktor yang berperan dalam memperkirakan tingkat keparahan ancaman:

- Tingkat kerugian asset
- Kemungkinan terjadinya

3.3.3. Fase 3: *Assess Vulnerabilities*

Setelah melakukan proses identifikasi aset informasi dan ancaman terhadap setiap aset, selanjutnya dilakukan proses penilaian terhadap kerentanan. Dalam memeriksa ancaman, dalam hal ini yang dimaksud adalah aset informasi, karena setiap ancaman terkait dengan aset informasi. Pertama yang perlu dilakukan adalah mengidentifikasi kerentanan komponen proses dan kemudian menggabungkannya untuk menentukan kerentanan proses. Kerentanan proses kemudian akan digabungkan untuk menentukan kerentanan fungsi bisnis. Langkah yang perlu dilalui untuk menganalisis tingkat kerentanan dapat dilihat pada poin berikut:

- Identifikasi kontrol yang berkaitan dengan ancaman.
- Tentukan kesenjangan antar kontrol komponen proses.
- Gabungkan kesenjangan kontrol ke dalam proses dan kemudian fungsi bisnis.
- Kategorikan kesenjangan kontrol berdasarkan tingkat keparahan.
- Tetapkan peringkat risiko.

Mengidentifikasi Kontrol yang Ada

Selanjutnya yang perlu dilakukan dalam memeriksa kerentanan adalah dengan cara meninjau ancaman dan pengendalian inventaris yang ada guna mengurangi setiap ancaman. Dalam contoh pemrosesan data pelanggan, telah teridentifikasi ancaman kegagalan pada alat penyimpanan data yaitu *harddisk*, dan juga dapat menentukan bahwa sistem mencadangkan informasi pada *disk* utama setiap setiap kurun waktu yang telah ditentukan. Untuk mendapatkan pemahaman yang akurat tentang risiko organisasi, kita perlu mengidentifikasi semua kontrol yang telah diterapkan. Seperti ancaman, kontrol dapat bersifat teknis, fisik, atau bersifat administratif

Menggabungkan Kesenjangan Kontrol

Setelah dapat mengidentifikasi semua celah kontrol untuk komponen proses, kita dapat menggabungkannya untuk mulai menganalisis kemungkinan risiko untuk proses informasi. Kita kemudian dapat menggabungkan proses yang mendukung setiap fungsi bisnis untuk mulai melihat risiko untuk masing-masing dari fungsi bisnis.

Menentukan Kesenjangan Kontrol Komponen Proses

Setelah teridentifikasi kontrol yang ada yang telah digunakan, kita dapat mulai untuk melihat area di mana kontrol tidak efektif.

Mengkategorikan Kesenjangan Kontrol berdasarkan Tingkat Keparahan

Dengan memiliki analisis yang baik tentang risiko organisasi, kita dapat mengetahui lebih kritis dan tanggap bahwa

kemungkinan beberapa risiko mulai muncul dapat kita deteksi sejak dini, karena hal ini akan mempengaruhi terhadap berharga atau tidaknya aset informasi yang dimiliki. Pada titik ini, kita harus dapat menetapkan fungsi bisnis, proses informasi, dan komponen proses peringkat risiko kualitatif tinggi, sedang, atau rendah.

3.3.4. Fase 4: *Remediate Control Gaps*

Pada titik ini, risiko harus dikategorikan kedalam nilai tinggi, sedang, atau rendah. Tahap awal ini berfokus pada mitigasi risiko yang paling parah, karena kemungkinan besar kita akan condong untuk melakukan pemulihan pada bagian yang memiliki nilai investasi tertinggi. Intinya, kita dapat mengurangi lebih banyak risiko dengan lebih sedikit uang. disini akan menggunakan langkah-langkah berikut dalam remediasi celah pengendalian:

- Pilih kontrol.
- Terapkan kontrol.
- Validasi kontrol baru.
- Hitung ulang peringkat risiko.

3.3.5. Fase 5: *Manage Residual Risk*

Risiko secara inheren bersifat dinamis, terutama komponen ancaman risiko. Akibatnya, kita perlu mengukur risiko secara terus-menerus dan berinvestasi dalam kontrol baru untuk dapat merespon setiap ancaman yang muncul. Fase ini terdiri dari dua langkah:

- Buat garis besar risiko
- Menilai kembali risiko

BAB IV ANALISIS RISIKO

4.1. Tinjauan

Analisis risiko merupakan cara organisasi maupun perusahaan dalam mengukur dan mengidentifikasi kemungkinan-kemungkinan yang berisiko mengancam atau menghambat keberlangsungan proses organisasi maupun perusahaan dalam mencapai tujuan bisnisnya. Analisis risiko juga dapat dijadikan sebagai alat bantu untuk menentukan tindakan antisipasi untuk meminimalisir kemungkinan-kemungkinan yang dapat terjadi dikemudian hari. Analisis risiko memberikan saran atas proses evaluasi risiko dan memberikan saran dalam pengambilan keputusan terhadap suatu risiko yang terjadi. Analisis risiko merupakan bagian dari tahap penilaian risiko dalam proses manajemen risiko dan dilakukan terhadap risiko-risiko yang telah diidentifikasi dalam proses identifikasi risiko.

Untuk melakukan analisis risiko setidaknya memerlukan beberapa tahapan diantaranya mengidentifikasi kemungkinan kondisi, kejadian, atau situasi negatif baik secara eksternal maupun internal, penentuan hubungan sebab-akibat antara peluang kejadian, skalanya, dan kemungkinan dampaknya, evaluasi berbagai dampak di bawah asumsi dan probabilitas yang berbeda, penerapan teknik kualitatif dan kuantitatif untuk mengurangi ketidakpastian dari dampak dan biaya, kewajiban, atau kerugian. Identifikasi risiko merupakan proses penemuan, pengenalan dan pencatatan dalam proses manajemen risiko,

identifikasi risiko merupakan bagian yang dilakukan paling terdahulu dalam proses assessmen risiko.

Risiko dapat dianalisis menggunakan dua cara yaitu secara kuantitatif dan kualitatif. Seperti halnya metode analisis yang umum digunakan banyak orang, masing-masing cara tersebut memiliki kelebihan dan kekurangan. Dimana pendekatan kuantitatif lebih condong menganalisis dari sudut objektif, namun proses ini akan memakan lebih banyak waktu analisis. Pendekatan kualitatif lebih cocok untuk menyajikan pandangan risiko yang bertingkat, tetapi bisa lebih subjektif dan karenanya sulit untuk dibuktikan. Metode analisis resiko ini dapat difungsikan sebagai pencegah segala alasan, faktor dan variabel yang dapat menghalangi sebuah tindakan guna mencapai tujuan yang diinginkan oleh individu, organisasi maupun perusahaan. Analisis risiko juga dapat diimplementasikan baik dalam lingkup perusahaan kecil atau perusahaan skala besar sekalipun.

4.2. Analisis Risiko Kualitatif

Menurut Santosa (2009) analisis kualitatif merupakan proses menilai *impact* dan kemungkinan dari risiko yang sudah teridentifikasi. Risiko disusun berdasarkan efeknya terhadap tujuan dari proyek. Analisis risiko kualitatif digunakan untuk menentukan risiko-risiko tertentu dan merespon apa yang harus diberikan untuk mengurangi terjadinya risiko. Setidaknya terdapat tujuh hal yang perlu diperhatikan dalam analisis ini:

- *Risk management plan*
- Risiko yang sudah diidentifikasi
- Status proyek
- Tipe proyek
- Data
- Skala probabilitas dan *impact*

Seperti yang telah dibahas sebelumnya bahwa metode analisis risiko kualitatif ini lebih cocok dipakai untuk menganalisis berdasarkan pandangan risiko yang bertingkatdan cenderung dapat lebih subjektif, maka dari itu analisis ini sulit untuk dibuktikan. Organisasi maupun perusahaan dengan program manajemen risiko yang lebih sukses cenderung bergantung lebih banyak pada analisis risiko kualitatif untuk mengidentifikasi area fokus dan kemudian menggunakan teknik analisis risiko kuantitatif untuk membenarkan pengeluaran mitigasi risiko. Metode analisis risiko kualitatif akan fokus pada nilai-nilai seperti tinggi, sedang, rendah atau warna seperti hijau, biru, dan kuning untuk mengevaluasi risikonya.

Seperti yang telah disinggung pada pembahasan sebelumnya, bahwa pendekatan kualitatif dan kuantitatif saling melengkapi. Sebagian besar organisasi mendasarkan metodologi manajemen risiko mereka pada metode kualitatif, menggunakan rumus kuantitatif untuk membangun kasus bisnis untuk investasi mitigasi risiko.

4.3. Analisis Risiko Kuantitatif

Menurut Santosa (2009) analisis risiko kuantitatif merupakan salah satu metode analisis risiko yang digunakan untuk mengidentifikasi kemungkinan kerusakan atau kegagalan sistem dan memprediksi besar kecilnya kerugian. Dengan beberapa pengecualian, baik yang terkait dengan finansial, fisik, atau teknologi, berbagai jenis risiko dapat dihitung menggunakan rumus universal yang sama.

4.3.1. Elemen Risiko

Seperti yang dipelajari dalam pembahasan sebelumnya, bahwa risiko terdiri dari tiga elemen: nilai aset, ancaman, dan kerentanan. Memperkirakan elemen-elemen ini dengan benar sangat penting untuk menilai risiko secara akurat.

Asset

Umumnya asset diasumsikan sebagai sesuatu yang nilai finansial, aset dapat didefinisikan sebagai apa pun yang bernilai bagi organisasi maupun perusahaan dan memiliki sifat yang dapat dirusak ataupun hilang, entah akibat kesalahan manusia atau kesalahan sistem, baik disengaja maupun tidak disengaja. Pada kenyataannya, tidak jarang bahwa nilai aset merupakan nilai yang tinggi dan penting bagi organisasi atau perusahaan, jika terjadi kehilangan nilai aset merupakan kehilangan yang cukup fatal dan membutuhkan biaya penggantian yang tidak sedikit. Oleh karena itu, untuk mendapatkan ukuran risiko yang akurat, suatu aset harus dinilai dengan mempertimbangkan biaya *bottom-line* dari nilai kompromінya. Misalnya, pelanggaran informasi pribadi mungkin tidak menyebabkan kerugian fatal, tetapi jika

pelanggaran tersebut berlangsung berkali-kali dalam jumlah banyak, kemungkinan akan mengakibatkan tindakan hukum, kerusakan reputasi perusahaan, dan hukuman peraturan. Konsekuensi ini berpotensi akan menyebabkan kerugian finansial yang signifikan, mengakibatkan organisasi maupun perusahaan kehilangan anggota maupun pelanggannya. Dalam hal ini, bagian nilai aset dari persamaan akan mewakili informasi pribadi.

Ancaman

Ancaman dapat didefinisikan sebagai peristiwa potensial yang jika terjadi, akan menyebabkan dampak yang tidak diinginkan. Dampak yang tidak diinginkan bisa datang dalam berbagai bentuk, tetapi tidak jarang akan dapat mengakibatkan kerugian finansial.

Kerentanan

Kerentanan dapat didefinisikan sebagai lemahnya pengendalian atau kontrol secara kumulatif yang melindungi asset tertentu milik organisasi atau perusahaan. Kerentanan diperkirakan sebagai persentase berdasarkan tingkat kelemahan pengendalian aset.

4.3.2. Penyebab Umum Ketidakakuratan Analisis

Dalam melakukan analisis data, baik menggunakan analisis model kuantitatif maupun kualitatif, salah satu hal yang menjadikan kekhawatiran adalah ketidakakuratan hasil analisis yang didapat. Kesalahan analisis atau prediksi akan berdampak pada kelangsungan hidup organisasi maupun perusahaan untuk jangka pendek maupun jangka panjang, apalagi jika sesuatu yang dianalisis merupakan hal yang sangat penting bagi organisasi atau

perusahaan. Misalnya hasil analisis tentang pemetaan potensi produk yang paling diminati oleh konsumen, data yang diperoleh bukan data asli hasil survey dari konsumen, maupun ketika dalam proses analisis terdapat kekeliruan perhitungan, maka akan menghasilkan hasil analisis yang tidak sesuai dengan harapan. Jika organisasi atau perusahaan mengambil begitu saja dari hasil analisis tadi, maka ini akan berakibat fatal. Justru hal yang tidak diinginkan dapat ditimbulkan, mulai dari kerugian materi ataupun non materi.

Kegagalan identifikasi asset, ancaman dan kerentanan

Contoh diatas hanyalah gambaran umum dari salah satu kasus yang kemungkinan dijumpai. Namun secara garis besar penyebab ketidakakuratan dalam analisis disebabkan karena kegagalan identifikasi asset, ancaman dan kerentanan. Hal ini sebagian besar disebabkan oleh fakta bahwa sebagian besar organisasi tidak menggunakan proses manajemen risiko secara nyata formal dan sumber daya manusia yang dipercaya belum dibekali kemampuan untuk menganalisis risiko. Akan menjadi semakin sulit untuk mengidentifikasi ancaman dan kerentanan karena bersifat dinamis. Apalagi dalam perkembangan dunia teknologi informasi, hampir setiap waktu teknologi mendapat pembaharuan yang disertai juga dengan bertambahnya berbagai varian virus atau malware. Tentu hal ini dapat diantisipasi jauh sebelum terjadi hal yang tidak diinginkan jika organisasi maupun perusahaan menerapkan rencana dan menyiapkan scenario atas kemungkinan risiko yang dapat terjadi.

Meskipun mengidentifikasi ancaman dan kerentanan dapat menjadi hal yang sulit, kita dapat memanfaatkan layanan pihak ketgia untuk membantu berbagai kasus yang dialami oleh organisasi maupun perusahaan, beberapa layanan seperti peringatan keamanan informasi dari CERT, Bugtraq, dan layanan

pemberitahuan kerentanan keamanan gratis maupun jika ingin menggunakan layanan berbayar. Auditor TI juga dapat memeriksa insiden keamanan ketika dipublikasikan untuk mempelajari setiap pelanggaran yang terjadi.

Ketidakakuratan Estimasi

Seperti contoh kasus diatas mengenai ketidakakuratan dalam menganalisis data dan salah mengambil data konsumen, informasi mengenai asset organisasi maupun perusahaan juga merupakan bagian terpenting yang harus dipastikan akurasinya. Asset berkaitan dengan kepemilikan organisasi maupun perusahaan, semisal mengenai persediaan bahan, memastikan penjadwalan pemasokan bahan baku. Hal tersebut perlu diperhitungkan secara detail dan pasti, karena ini akan berdampak pada banyak hal seperti keterlambatan proses produksi yang diakibatkan karena keterlambatan mendatangkan bahan baku baru. Meskipun diperhitungkan dengan detail, terkadang organisasi atau perusahaan perlu mempersiapkan skenario apabila terjadi permintaan produk yang cukup tinggi sehingga mengharuskan perusahaan memasok bahan baku lebih cepat dari yang telah dijadwalkan, ataupun sebaliknya bahwa perusahaan mempersiapkan skenario jika terjadi penurunan jumlah produksi maka secara otomatis perlu mengatur ulang jadwal pemasokan bahan baku agar tidak terjadi penumpukan bahan baku di gudang. Ini hanyalah contoh salah satu kasus dari berbagai kasus tentang ketidakakuratan estimasi asset.

Selain ketidakakuratan estimasi asset, perkiraan tentang kemungkinan ancaman yang dapat timbul dari berbagai pihak juga perlu diperhatikan dengan baik, mengingat hal ini juga akan berdampak terhadap nilai profit perusahaan. Ambil contoh ketika analisis risiko mengenai kemungkinan bermunculannya perusahaan dengan jenis yang sama. Seorang pakar analitik data

melalui berbagai metode perhitungannya memprediksikan bahwa sepuluh tahun kedepan perusahaan dengan jenis usaha warung sembako tidak mengalami persaingan ketat dikarenakan wilayah tempat warung sembako tersebut berdomisili tidak memiliki jumlah penduduk yang banyak. Alasan tersebut terlintas memang masuk akal, namun jika kita perhatikan lebih jauh, peningkatan jumlah penduduk pada wilayah tersebut yang cukup pesat akan berdampak pada meningkatnya kebutuhan pokok penduduk tersebut, jika hal ini terjadi tentu dalam jangka beberapa waktu kedepan potensi persaingan jenis usaha warung sembako berpotensi menjamur. Dari simulasi kasus ini dapat kita simpulkan bahwa kesalahan menganalisis lingkungan akan mengancam organisasi atau perusahaan itu sendiri, baik ancaman menurunnya profit, berkurangnya konsumen, timbul persaingan baru, ataupun ancaman-ancaman lain yang dapat ditimbulkan.

Kerentanan terhadap berbagai sisi pada organisasi maupun perusahaan juga sering terjadi karena lemahnya atau tidak adanya kontrol. Kerentanan dapat dihindari jika kontrol pada setiap proses dapat dijalankan, sehingga setiap proses yang dilalui sudah melalui tahapan pengendalian yang sesuai.

BAB V PENILAIAN RISIKO

5.1. Tinjauan

Penilaian risiko merupakan proses untuk menentukan sejauh mana potensi ancaman dan risiko yang terkait dengan penerapan sistem teknologi informasi sistem pada tiap siklus prosesnya. Luaran yang dihasilkan dari proses ini diharapkan dapat membantu mengidentifikasi pengendalian yang sesuai untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko. Secara garis besar, penilaian risiko juga memiliki tujuan, diantaranya dapat digunakan untuk menetapkan kemunginan terjadinya dan dampak suatu kejadian yang menghambat pencapaian tujuan dan sasaran organisasi maupun perusahaan agar dapat dilakukan penanganan risiko secara tepat sesuai dengan kejadian yang ditemui.

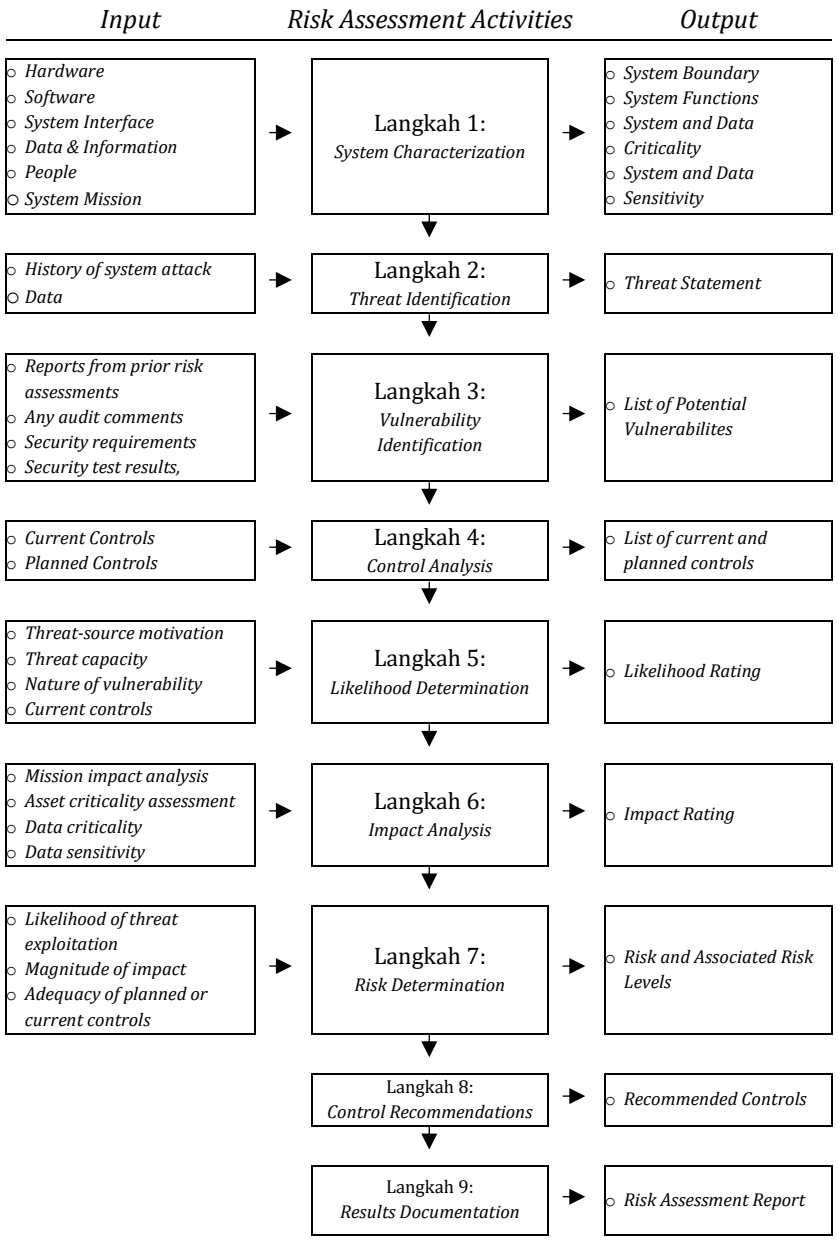
Penilaian risiko dilakukan untuk menjaga kesinambungan pelayanan kepada para *stakeholder* terkait, penilaian risiko akan berdampak pada peningkatan pelayanan secara efektif dan efisien jika hasil dari penilaian risiko tersebut benar-benar diterapkan sebagaimana mestinya, penilaian risiko juga menjadi dasar penyusunan rencana strategis organisasi atau perusahaan untuk jangka panjang dan menghindari terjadinya pemborosan, karena jika risiko tidak dilakukan penilaian, organisasi atau perusahaan tidak akan pernah tahu potensi kelemahan yang dimiliki.

Prasyarat untuk melakukan penilaian risiko ialah dengan melakukan penetapan tujuan, baik tujuan organisasi atau perusahaan secara umum, amaupun tujuan dari setiap bagian-bagian dari perusahaan, dan setiap bagian-bagian perusahaan tersebut tentu seharusnya harus saling terhubung satu sama lain yang mengarah pada satu tujuan yang sama. Penilaian risiko adalah identifikasi dan analisis risiko yang relevan terhadap pencapaian tujuan yang membentuk dasar untuk menentukan bagaimana risiko harus dikelola. Karena ekonomi, industri, regulasi, dan kondisi operasi akan terus berubah mengikuti perkembangan dan potensi pasar, hal tersebut akan mengakibatkan risiko juga akan terus berubah menyesuaikan proses bisnis yang berjalan pada organisasi maupun perusahaan itu sendiri.

Menurut buku yang berjudul "*Risk Management Guide for Information Technology Systems*", metodologi penilaian risiko terbagi dalam sembilan langkah:

- Langkah 1 : *System Characterization*
- Langkah 2 : *Threat Identification*
- Langkah 3 : *Vulnerability Identification*
- Langkah 4 : *Control Analysis*
- Langkah 5 : *Likelihood Determination*
- Langkah 6 : *Impact Analysis*
- Langkah 7 : *Risk Determination*
- Langkah 8 : *Control Recommendations*
- Langkah 9 : *Results Documentation*

Diagram alir dari metodologi penilaian risiko dapat dilihat pada gambar pada halaman selanjutnya.



Gambar 11. Diagram Alir Penilaian Risiko

5.2. Langkah Penilaian Risiko

Pada bagian ini kita akan mencoba memahami lebih detail mengenai tahapan pada metodologi penilaian risiko yang sudah disinggung pada poin sebelumnya.

5.2.1. Langkah 1: *System Characterization*

Dalam menilai risiko untuk suatu sistem berbasis teknologi informasi, langkah pertama yang perlu dilakukan ialah menentukan ruang lingkup. Pada langkah ini, batas-batas sistem teknologi informasi dapat diidentifikasi dengan baik, bersama dengan sumber daya dan informasi yang membentuk sistem. Melakukan karakterisasi sistem teknologi informasi, menetapkan ruang lingkup upaya penilaian risiko, menggambarkan batas-batas otorisasi operasional, dan memberikan informasi yang penting seperti perangkat keras, perangkat lunak, konektivitas sistem, dan divisi atau personel pendukung yang bertanggungjawab.

Untuk mengidentifikasi informasi terkait sistem membutuhkan pemahaman yang tajam tentang lingkungan pemrosesan sistem tersebut. Oleh karena itu, pelaku atau orang yang melakukan penilaian risiko harus terlebih dahulu mengumpulkan informasi terkait sistem, informasi yang dimaksud diantaranya:

- Perangkat keras
- Perangkat lunak
- Antarmuka sistem
- Data dan informasi
- Orang yang mendukung dan menggunakan sistem
- Misi sistem (proses yang dilakukan oleh sistem)
- Kekritisan sistem dan data (seperti nilai atau kepentingan sistem bagi suatu organisasi)
- Sensitivitas sistem dan data.

Untuk mendapatkan data diatas memerlukan teknik pengumpulan data, berikut ini beberapa Teknik pengumpulan data yang dapat dijadikan pilihan:

- **Kuisioner**: Untuk mengumpulkan informasi yang relevan dan lebih akurat, pelaku penilai risiko dapat mengembangkan kuesioner mengenai manajemen dan kontrol operasional yang direncanakan atau digunakan untuk sistem teknologi informasi yang berjalan. Kuesioner ini diberikan kepada personal yang terlibat dan memiliki kaitan dengan data yang dibutuhkan, seperti tenaga manajemen teknis dan nonteknis yang merancang atau mendukung sistem TI.

- **Wawancara**: melakukan wawancara dengan tenaga manajemen teknis dan nonteknis yang terlibat langsung juga dapat dijadikan pilihan sebagai teknik dalam mengumpulkan data. Selain itu, wawancara juga dapat dikombinasikan dengan kuisioner, guna melakukan validasi kebenaran atas data dan informasi yang telah diberikan melalui kuisioner. Dengan metode wawancara ini penilai risiko akan dapat mengetahui secara jelas bagaimana gambaran informasi yang didapat, karena dapat melihat langsung pembuktian dari informasi tersebut.
- **Dokumen**: melalui dokumentasi-dokumentasi yang tersedia pada organisasi atau perusahaan yang terkait dengan sistem TI juga dapat dijadikan sebagai sumber data. Seperti dokumentasi tentang spesifikasi dari sistem yang digunakan, dokumentasi petunjuk manual penggunaan sistem, dokumentasi tentang syarat minimum yang diperlukan sebelum menggunakan sistem tersebut, dokumentasi tentang infrastruktur dari sistem TI yang digunakan, dan lain sebagainya. Tentu dokumen-dokumen

yang dimaksudkan ini sudah seharusnya tersedia pada organisasi ataupun perusahaan yang sudah berjalan secara professional, namun terkadang dokumen tersebut belum dimiliki.

- **Menggunakan Pemindai Alat Otomatis**: Metode teknis ini dapat digunakan sebagai pilihan tambahan untuk mengumpulkan informasi sistem secara efisien. Misalnya, mendeteksi kecepatan koneksi internet yang digunakan untuk menjalankan sistem tersebut dapat menggunakan situs pemindai kecepatan jaringan.

5.2.2. Langkah 2: *Threat Identification*

Langkah kedua dalam penilaian risiko adalah perlu mengetahui ancaman-ancaman yang memungkinkan untuk terjadi. Ancaman perlu diidentifikasi karena akan berkaitan terhadap kelangsungan organisasi atau perusahaan di waktu mendatang. Sebenarnya ancaman tidak selalu merugikan atau membahayakan, ancaman terkadang dapat berbalik mendatangkan peluang baru yang belum dipikirkan sebelumnya. Maka dari itu diperlukan identifikasi ancaman untuk mengetahui apakah ada celah peluang yang bisa diambil dari ancaman tersebut atau tidak.

Untuk mengetahui ancaman, yang perlu dilakukan pertama kali ialah mengidentifikasi sumber dari kemungkinan ancaman tersebut. Tujuan dari langkah ini adalah untuk mengidentifikasi potensi sumber ancaman dan Menyusun daftar ancaman yang memiliki potensi mengancam sistem TI yang sedang dievaluasi. Sumber ancaman didefinisikan sebagai setiap keadaan atau peristiwa yang berpotensi menyebabkan kerusakan pada IT sistem. Sumber ancaman secara umum dapat berupa alam, manusia, atau lingkungan.

Setelah itu perlu juga dicari motif dan tindakan dari setiap ancaman. Pada tabel berikut terdapat beberapa contoh jenis ancaman beserta kemungkinan motif dari tindakan ancaman itu sendiri:

Tabel 4. Contoh Motivasi Ancaman

Sumber Ancaman	**Motivasi**	**Tindakan Ancaman**
Hacker, Cracker	Menguji kemampuan diri pelaku, ketidaksukaan pelaku atas organisasi tersebut, mengambil data penting	Meretas sistem, memanipulasi data asli, menyebarluaskan data secara illegal
Terrorist	Pemerasan, penghancuran, eksploitasi, ketidaksukaan pelaku terhadap pemilik organisasi	Bom, serangan sistem (DDoS)

5.2.3. Langkah 3: *Vulnerability Identification*

Analisis ancaman terhadap sistem TI harus mencakup analisis kerentanan yang terkait dengan lingkungan sistem itu sendiri. Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem (kekurangan atau kelemahan) yang mungkin dieksploitasi oleh sumber ancaman yang memiliki potensi tinggi. Kerentanan yang dimaksud disini dapat berupa cacat atau kelemahan dalam sistem prosedur keamanan, desain, implementasi, atau pengendalian internal yang dapat dilakukan (dipicu secara tidak sengaja atau sengaja dieksploitasi) dan mengakibatkan pelanggaran keamanan atau pelanggaran terhadap kebijakan keamanan sistem.

Berikut disajikan tabel yang berisi contoh kerenatan yang dapat terjadi:

Tabel 5. Tabel kerentanan ancaman

Kerentanan	Sumber ancaman	Tindakan ancaman
Pemberhentian karyawan IT yang mengelola sistem, tapi data karyawan tersebut belum dihapus dari sistem, sehingga masih memiliki akses masuk	Karyawan yang diberhentikan	Menelepon ke perusahaan jaringan dan mengakses data kepemilikan perusahaan
Terbakarnya ruang tempat penyimpanan data (server) perusahaan	Api, kerusakan alat	Alat penyiraman air disediakan pada ruangan

5.2.4. Langkah 4: *Control Analysis*

Tujuan dari langkah ini adalah untuk menganalisis pengendalian yang telah dilaksanakan, atau direncanakan untuk implementasi, oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan ancaman kerentanan sistem.

Kontrol keamanan mencakup penggunaan metode teknis dan nonteknis. Kontrol teknis adalah perlindungan yang dimasukkan ke dalam perangkat keras, perangkat lunak, atau *firmware* komputer seperti metode enkripsi, perangkat lunak pendeteksi penyusupan. Pengendalian nonteknis adalah pengendalian manajemen dan operasional, seperti kebijakan keamanan, prosedur operasional, personel, fisik, dan lingkungan keamanan.

5.2.5. Langkah 5: *Likelihood Determination*

Untuk memperoleh keseluruhan yang menunjukkan kemungkinan bahwa kerentanan potensial dapat dilakukan dalam konstruksi lingkungan ancaman terkait, perlu mempertimbangkan hal berikut:

- Motivasi dan kemampuan sumber ancaman
- Sifat kerentanan
- Keberadaan dan efektivitas pengendalian saat ini

Kemungkinan bahwa kerentanan potensial dapat dilakukan oleh sumber ancaman tertentu dapat digambarkan dengan tinggi, sedang, atau rendah.

Tabel 6. Definisi Level Kemungkinan

Level kemungkinan	**Definisi**
Tinggi	Sumber ancaman tinggi dan pengendalian pencegahan kerentanan dilakukan tidak efektif.
Sedang	Sumber ancaman cukup tinggi, tetapi ada pengendalian yang mungkin menghambat keberhasilan pelaksanaan kerentanan.
Rendah	Sumber ancaman rendah, namun ada pengendalian untuk mencegah, atau paling tidak secara signifikan menghambat kerentanan untuk dilaksanakan.

5.2.6. Langkah 6: *Impact Analysis*

Langkah berikutnya dalam mengukur tingkat risiko adalah menentukan dampak yang dihasilkan dari percobaan ancaman yang dilakukan. Dalam menganalisis dampak, perlu disiapkan informasi mengenai tujuan dari sistem dijalankan, tingkat kekritisan sistem dan data-datanya, tingkat sensivitas sistem dan datanya.

5.2.7. Langkah 7: *Risk Determination*

Tujuan dari langkah ini adalah untuk menilai tingkat risiko terhadap sistem TI. Penentuan risiko untuk pasangan ancaman/kerentanan tertentu dapat dinyatakan sebagai fungsi dari kemungkinan sumber ancaman mencoba menggunakan kerentanan tertentu, besarnya dampak jika sumber ancaman berhasil menerapkan kerentanan, kecukupan kontrol keamanan yang direncanakan atau yang ada untuk mengurangi atau menghilangkan risiko.

5.2.8. Langkah 8: *Control Recommendations*

Tujuan dari langkah ini adalah untuk mengurangi tingkat risiko terhadap sistem TI dan datanya ke tingkat yang dapat diterima. Faktor-faktor berikut harus dipertimbangkan dalam merekomendasikan pengendalian beserta solusi alternatif untuk meminimalkan atau menghilangkan risiko yang teridentifikasi:

- Efektivitas Pilihan yang direkomendasikan (misalnya, kompatibilitas sistem)
- Perundang-undangan dan regulasi
- Kebijakan organisasi
- Dampak operasional
- Keamanan dan keandalan.

5.2.9. Langkah 9: *Results Documentation*

Setelah penilaian risiko selesai (sumber ancaman dan kerentanan diidentifikasi, risiko dinilai, dan pengendalian yang direkomendasikan disediakan), hasilnya harus didokumentasikan dalam laporan.

BAB VI MITIGASI RISIKO

6.1. Tinjauan

Mitigasi risiko merupakan konsep terstruktur yang digunakan oleh pimpinan organisasi atau perusahaan atau manajemen senior untuk mengurangi risiko dari tujuan-tujuan organisasi maupun perusahaan. Mitigasi risiko melibatkan penentuan prioritas, evaluasi, dan menerapkan pengendalian pengurangan risiko yang sesuai yang direkomendasikan dari proses penilaian risiko.

Mitigasi Risiko merupakan tindakan terencana dan berkelanjutan yang dilakukan oleh pemilik risiko agar bisa mengurangi dampak dari suatu kejadian yang berpotensi atau telah merugikan atau membahayakan pemilik risiko tersebut. (sumber: http://djkn.kemenkeu.go.id)

Mitigasi risiko dapat dicapai melalui salah satu pilihan mitigasi risiko berikut:

- ***Risk Asumption***
  Untuk menerima potensi risiko dan terus mengoperasikan sistem TI atau untuk menerapkan pengendalian untuk menurunkan risiko ke tingkat yang dapat diterima.

- ***Risk Avoidance***
  Untuk menghindari risiko dengan menghilangkan penyebab dan/atau konsekuensi risiko (misalnya,

mengabaikan fungsi tertentu dari sistem atau mematikan sistem ketika ada risiko yang teridentifikasi).

- ***Risk Limitation***
  Untuk membatasi risiko dengan menerapkan kontrol yang dapat meminimalkan dampak buruk dari ancaman (misalnya, penggunaan dukungan, pencegahan, kontrol detektif).

- ***Risk Planning***:
  Untuk mengelola risiko dengan mengembangkan rencana mitigasi risiko yang memprioritaskan, mengimplementasikan, dan memelihara pengendalian.

- ***Research and Acknowledgment***
  Untuk menurunkan risiko kerugian dengan mengakui kerentanan atau cacat dan meneliti pengendalian untuk memperbaiki kerentanan.

- ***Risk Transference***
  Untuk mentransfer risiko dengan menggunakan pilihan lain untuk mengkompensasi kerugian, seperti membeli asuransi.

6.2. Strategi Mitigasi Risiko

Strategi mitigasi risiko merupakan langkah yang perlu disiapkan secara terstruktur untuk menghadapi berbagai kemungkinan dan potensi masalah. Tentu masalah yang dimaksud dapat berdampak pada kerugian organisasi maupun perusahaan di masa mendatang yang dapat muncul tanpa dipastikan waktunya. Strategi mitigasi risiko disimulasikan dalam aturan praktis

berikut, yang memberikan panduan tentang tindakan untuk mengurangi risiko dari ancaman manusia yang disengaja:

- Ketika terdapat kerentanan (cacat, kelemahan), terapkan teknik jaminan untuk mengurangi kemungkinan terjadinya kerentanan.
- Ketika kerentanan dapat dilakukan, terapkan perlindungan berlapis, arsitektural desain, dan kontrol administratif untuk meminimalkan risiko atau mencegah hal ini terjadi kembali.
- Ketika kemungkinan biaya yang dikeluarkan kurang dari potensi keuntungan, terapkan perlindungan untuk mengurangi motif tindak penyerangan seperti penggunaan sistem pengendalian, membatasi apa yang dapat diakses dan dilakukan oleh pengguna sistem.
- Ketika potensi kerugian terlalu besar, terapkan prinsip-prinsip desain, desain arsitektur, dan teknis dan perlindungan nonteknis untuk membatasi tingkat serangan, sehingga mengurangi potensi kerugian

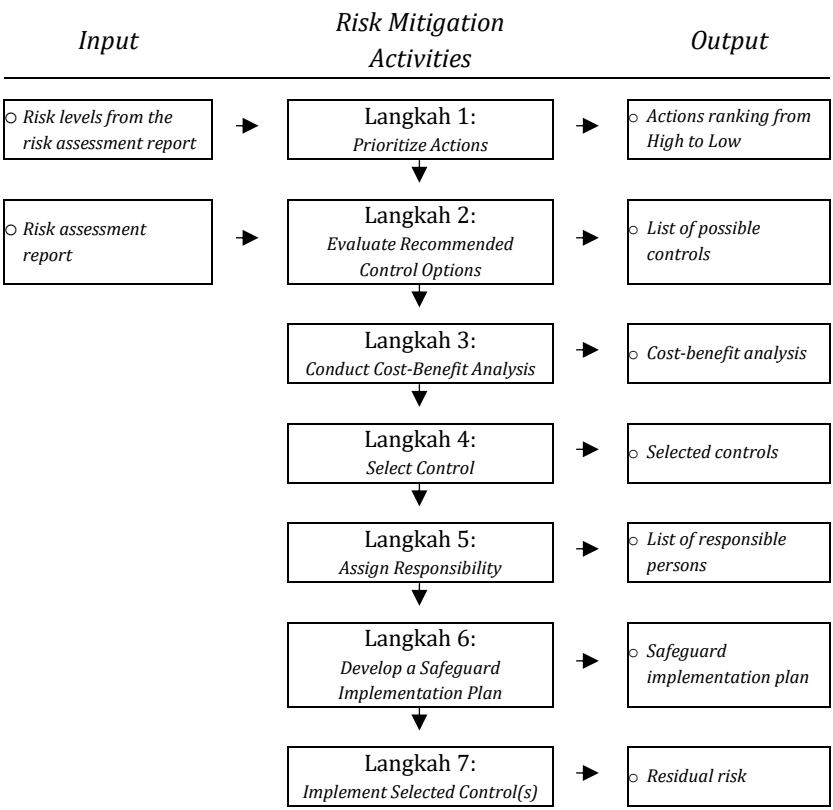
6.3. Implementasi Pengendalian

Pengendalian merupakan salah satu upaya untuk memastikan bahwa jalannya pengelolaan organisasi maupun perusahaan berjalan sesuai dengan tujuan awal. Pengendalian ini mencakup proses, strategi, program, penganggaran dan akuntabilitas sebuah organisasi atau perusahaan. Tentu bagian-bagian tersebut memiliki keterkaitan satu sama lain.

Ketika tindakan pengendalian harus dilakukan, maka perlu ditekankan bahwa proses implementasi pengendalian lebih dahulu berfokus untuk mengatasi risiko terbesar dan upayakan mitigasi risiko yang memadai dengan biaya terendah, dengan minimal.

Untuk melakukan implementasi pengendalian, dapat mengikuti langkah-langkah yang tertuang pada poin berikut:

- Langkah 1 : *Prioritize Actions*
- Langkah 2 : *Evaluate Recommended Control Options*
- Langkah 3 : *Conduct Cost-Benefit Analysis*
- Langkah 4 : *Select Control*
- Langkah 5 : *Assign Responsibility*
- Langkah 6 : *Develop a Safeguard Implementation Plan*
- Langkah 7 : *Implement Selected Control(s)*



Gambar 12. Diagram Alir Mitigasi Risiko

Ketujuh Langkah diatas merupakan proses terstruktur yang dapat dilakukan ketika sudah dilakukan penilaian risiko. Penjelasan diagram alir dari ketujuh langkah tersebut dapat dilihat pada pembahasan berikut.

6.4.1. Langkah 1: *Prioritize Actions*

Berdasarkan tingkat risiko yang disajikan dalam laporan penilaian risiko, perlu dilakukan pemetaan untuk menentukan skala prioritas atas tindakan implementasi. Dalam mengalokasikan sumber daya, prioritas utama harus diberikan pada risiko item dengan peringkat risiko tingkat tinggi. Kerentanan atau ancaman ini membutuhkan tindakan lebih utama karena ini berkaitan dengan perlindungan terhadap kepentingan dan tujuan organisasi. Dengan pemetaan ini akan memudahkan pengambil keputusan untuk mengambil langkah yang lebih tepat. Hasil luaran dari langkah ini akan menghasilkan urutan prioritas tindakan dari prioritas paling tinggi hingga prioritas terendah.

6.4.2. Langkah 2: *Evaluate Recommended Control Options*

Kontrol yang direkomendasikan dalam proses penilaian risiko mungkin tidak banyak pilihan yang sesuai dan layak untuk organisasi dan sistem TI tertentu. Selama langkah ini, kelayakan (seperti kompatibilitas, penerimaan pengguna) dan efektivitas (seperti tingkat perlindungan dan tingkat mitigasi risiko) dari pilihan pengendalian yang direkomendasikan dianalisis. Tujuannya adalah untuk memilih pengendalian yang paling tepat untuk meminimalkan risiko. Luaran dari tahapan ini akan menghasilkan daftar pengendalian yang layak.

6.4.3. Langkah 3: *Conduct Cost-Benefit Analysis*

Analisis biaya menjadi hal yang tidak bisa dilewatkan begitu saja, hal ini karena analisis biaya akan membantu manajemen dalam pengambilan keputusan dan untuk mengidentifikasi pengendalian keuntungan maupun kerugian yang dialami organisasi atau perusahaan. Luaran dari Langkah ini akan menghasilkan analisis biaya yang berkaitan dengan penerapan pengendalian.

6.4.4. Langkah 4: *Select Control*

Berdasarkan evaluasi dari hasil analisis *cost-benefit*, manajemen menentukan pengendalian yang paling hemat biaya untuk mengurangi risiko terhadap misi organisasi. Pengendalian yang dipilih harus menggabungkan elemen kontrol teknis, operasional, dan manajemen untuk memastikan keamanan yang memadai untuk sistem TI dan organisasi. Luaran dari Langkah ini akan menghasilkan keputusan dari Teknik pengendalian yang telah dipilih.

6.4.5. Langkah 5: *Assign Responsibility*

Berikutnya diperlukan untuk memasukkan tenaga (personel internal atau staf kontraktor eksternal) yang memiliki keahlian profesional dan keahlian yang sesuai untuk mengimplementasikan pengendalian yang telah dipilih dan memiliki rasa tanggungjawab yang bai katas pekerjaan yang dipercaya kepadanya. Luaran dari Langkah ini menghasilkan daftar tenaga personel yang sesuai.

6.4.6. Langkah 6: *Develop a Safeguard Implementation Plan*

Pada Langkah ini, lebih difokuskan terhadap rencana implementasi pengamanan atau rencana aksi untuk lebih dikembangkan. Setidaknya rencana yang dikembangkan harus memuat hal-hal berikut:

- Risiko dan tingkat risiko terkait (hasil dari laporan penilaian risiko)
- Kontrol yang disarankan (hasil dari laporan penilaian risiko)
- Tindakan yang diprioritaskan (prioritas diberikan pada item dengan risiko tingkat tinggi)
- Pengendalian terencana yang dipilih (ditentukan berdasarkan kelayakan, efektivitas, manfaat bagi organisasi, dan biaya)
- Sumber daya yang diperlukan untuk menerapkan rencana pengendalian yang dipilih
- Daftar tim dan staf yang bertanggungjawab pada kegiatan pengembangaan rencana
- Tanggal mulai untuk implementasi
- Target tanggal penyelesaian untuk implementasi
- Persyaratan pemeliharaan

Rencana implementasi pengamanan memprioritaskan tindakan implementasi dan memproyeksikan tanggal mulai dan penyelesaian target. Rencana ini digunakan untuk mentukan tindakan yang tepat yang akan membantu dan mempercepat proses mitigasi. Luaran dari Langkah ini akan menghasilkan rencana implementasi pengamanan dan pengembangan rencana.

6.4.7. Langkah 7: *Implement Selected Control(s)*

Pada tahap ini pengendalian yang telah dipilih mulai diterapkan. Implementasi pengendalian bergantung pada situasi individu, pengendalian yang diterapkan dapat menurunkan risiko level, namun tidak menghilangkan kemugkinan risiko. Hasil dari Langkah ini adalah implementasi dari pengendalian yang telah dipilih, sehingga akan menyisakan risiko-risiko kecil yang seharusnya dapat ditangani lebih mudah.

6.4. Kategori Pengendalian

Dalam melaksanakan pengendalian yang direkomendasikan untuk mengurangi risiko, organisasi atau perusahaan tersebut harus mempertimbangkan pengendalian keamanan teknis, manajemen, dan operasional, atau kombinasi dari pengendalian tersebut, ini perlu dilakukan guna memaksimalkan efektivitas pengendalian untuk sistem dan organisasi teknologi informasinya. Pengendalian keamanan bila digunakan dengan tepat dapat membatasi, atau mencegah terjadinya ancaman dalam setiap proses yang berjalan pada Lembaga tersebut.

6.4.1. Teknik Pengendalian Keamanan

Teknik pengendalian keamanan dalam proses mitigasi risiko dapat diatur untuk melindungi dari berbagai jenis tertentu. Pengendalian ini dapat dilakukan mulai dari tindakan sederhana hingga kompleks dan biasanya melibatkan sistem arsitektur, disiplin ilmu teknis dan paket keamanan dengan campuran perangkat keras, perangkat lunak, dan *firmware*. Semua bagian tersebut harus saling bekerja sama untuk mengamankan data, informasi, dan fungsi sistem TI yang penting dan sensitif.

pengendalian teknis dapat dikelompokkan ke dalam kategori utama berikut:

- **Dukungan**
  pengendalian pendukung bersifat umum dan menjadi dasar kemampuan dalam menangani bagian keamanan teknologi informasi. Yang termasuk pengendalian pendukung diantaranya.
- **Pencegahan**
  pengendalian preventif berfokus pada pencegahan pelanggaran keamanan sejak awal.
- **Deteksi dan Pemulihan**
  pengendalian ini berfokus pada proses mendeteksi dan pemulihan data dari pelanggaran keamanan.

6.4.2. Pengendalian Keamanan Manajemen

Pengendalian keamanan manajemen, bersama dengan pengendalian teknis dan operasional merupakan tindakan dan upaya dalam mengelola dan mengurangi risiko kerugian dan untuk melindungi misi organisasi. pengendalian manajemen berfokus pada penetapan kebijakan, pedoman, dan perlindungan informasi standar, yang dilakukan melalui prosedur operasional untuk memenuhi tujuan organisasi. Pengendalian keamanan ini meliputi pengendalian keamanan manajemen preventif, pengendalian keamanan manajemen deteksi, pengendalian keamanan manajemen pemulihan.

6.4.3. Pengendalian Keamanan Operasional

Standar keamanan organisasi ataupun perusahaan harus menetapkan serangkaian pengendalian dan pedoman untuk memastikan bahwa prosedur keamanan yang mengatur penggunaan aset dan sumber daya TI organisasi dapat ditegakkan

dan dilaksanakan dengan benar sesuai dengan tujuan organisasi. Manajemen menjalankan peran penting dalam mengawasi implementasi kebijakan dan dalam memastikan pembentukan pengendalian operasional yang sesuai.

Daftar Pustaka

Airlangga, G. (2018). Mengukur Tingkat Keselarasan Information Technology dan Bisnis (Studi Kasus Perusahaan Start-up Digital Wilayah Jawa). Jurnal Buana Informatika, 53-60.

COSO. (2004). Enterprise Risk Management – Integrated Framework (Application Technique). New York: COSO

Davis, C., Schiller, M., Wheeler, K. *IT Auditing: Using Controls to Protect Information Assets (Second Edition)*. United State: The McGrawHill

ISACA. (2018). *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution.* USA: ISACA.

ISACA. (2018). *COBIT 2019 Framework: Governance and Management Objectives*. USA: ISACA

ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. USA: ISACA.

Moeller, R.R. (2013). *Executive's Guide to IT Governance. mproving Systems Processes with Service Management, COBIT, and ITIL*. John Wiley & Sons Inc.