MODUL PERTEMUAN ONLINE
MODEL DAN STRATEGI TATA KELOLA TI

A. PENDAHULUAN

Tata kelola teknologi informasi merupakan suatu struktur dan proses yang saling berhubungan serta mengarahkan dan mengendalikan perusahaan dalam pencapaian tujuan perusahaan melalui nilai tambah dan penyeimbang antara risiko dan manfaat dari teknolgi informasi serta prosesnya.Tata kelola teknologi informasi menyediakan struktur yang menghubungkan proses teknologi (TI), sumberdaya TI dan informasI bagi strategi dan tujuan perusahaan/instansi tidak terkecuali Koperasi.Tata kelola TI menggabungkan cara terbaik dari perencanaan dan pengorganisasian TI, pembangunan dan pengimplementasian, dukungan dan pelayanan, serta memantau kinerja TI untuk memastikan informasi perusahaan/instansi dan teknologi informasi berhubungan dengan tujuan perusahaan/instansi. Seperti yang pada umumnya dipahami, peranan teknologi informasi diperlukan untuk mendapatkan informasi yang cepat dan akurat.

IT Governance adalah upaya menjamin pengelolaan TI agar mendukung bahkan selaras dengan strategi bisnis suatu enterprise yang dilakukan oleh dewan direksi, manajemen eksekutif, dan juga oleh manajemen TI. *IT Governance* adalah suatu struktur hubungan dan proses untuk mengatur dan mengontrol perusahaan yang bertujuan untuk mencapai tujuan perusahaan yang telah ditetapkan dengan pertambahan nilai dengan tetap menyeimbangkan resiko-resiko dengan nilai yang didapatkan dari penerapan TI dan proses-prosesnya.

IT Governance bukan bidang yang terpisah dari pengelolaan perusahan, melainkan merupakan komponen pengelolaan perusahaan secara keseluruhan, dengan tanggung jawab utama sebagai berikut:

a. Memastikan kepentingan *stakeholder* diikutsertakan dalam penyusunan strategi perusahaan.
b. Memberikan arahan kepada proses-proses yang menerapkan strategi perusahaan.
c. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur.
d. Memastikan adanya informasi mengenai hasil yang diperoleh dan mengukurnya.

e. Memastikan keluaran yang dihasilkan sesuai dengan yang diharapkan.

IT Governance merefleksikan adanya penerapan prinsip-prinsip organisasi dengan memfokuskan pada kegiatan manajemen dan penggunaan TI untuk pencapaian tujuan organisasi. *IT Governance* pada intinya mencakup pembuatan keputusan, akuntabilitas pelaksanaan kegiatan penggunaan TI, siapa yang mengambil keputusan dan memanajemen proses pembuatan dan pengimplementasian keputusan-keputusan yang berkaitan dengan TI.

Suatu IT Governance yang efektif berarti penggunaan TI pada organisasi tersebut mampu meningkatkan dan mensinergiskan antara penggunaan TI dengan visi, misi, tujuan dan nilai organisasi yang bersangkutan.

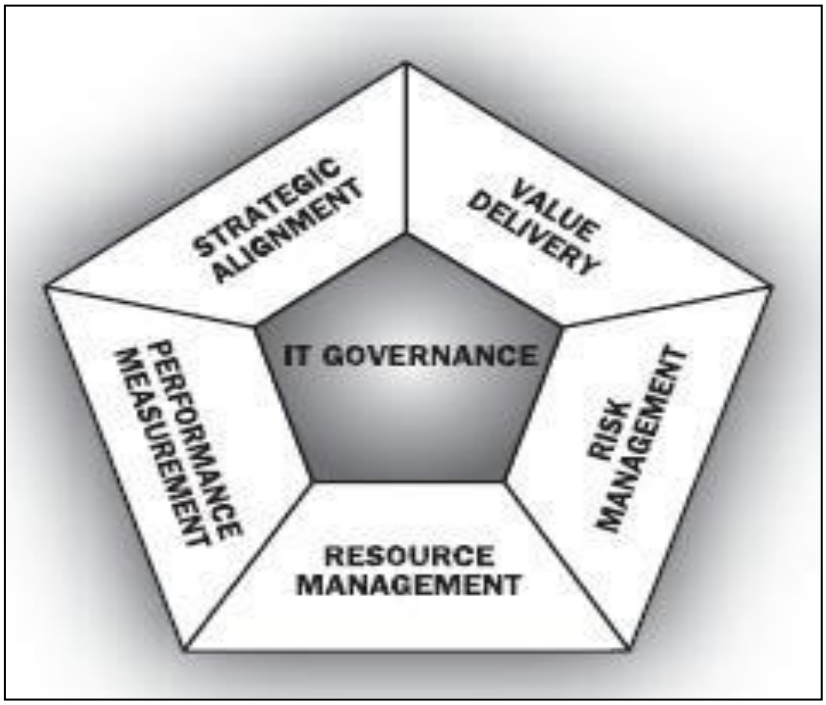
B. STRATEGI DALAM TATA KELOLA TI

Tata kelola Teknologi Informasi adalah sebuah kerangka kebijakan, prosedur dan kumpulan proses-proses yang bertujuan untuk mengarahkan dan mengendalikan perusahaan untuk pencapaian tujuan perusahaan dengan memberikan tambahan nilai bisnis, melalui penyeimbangan keuntungan dan resiko TI beserta proses-proses yang ada di dalamnya. Mereka bertanggung jawab terhadap arah strategi organisasi, memastikan tujuan organisasi dapat tercapai dan sumber daya organisasi telah dimanfaatkan dengan tepat. Tata kelola TI juga membutuhkan pengaturan yang tepat untuk menggabungkan strategi TI dan pemanfaatan sumber daya TI untuk memberikan keuntungan yang kompetitif bagi organisasi. Secara tidak langsung, tata kelola TI menggunakan prinsip-prinsip tata kelola organisasi terhadap unit TI.

Jadi definisi dari Tata Kelola TI adalah suatu tanggung jawab yang akan di laksanakan oleh direksi yang semuanya melibatkan pimpinan, struktur organisasi, dan proses untuk memastikan bahwa TI menjadi pendukung dalam realisasi strategi suatu perusahaan. Selain itu dalam tatakelola bidang IT terdapat lima bidang utama dalam Tata Kelola TI, yaitu:

Tata kelola TI mencakup area sebagaimana ditunjukan pada gambar 3 dari kelima fokus area tata kelola TI dua diantaranya: value delivery and risk management merupakan outcome, sedang tiga lainnya merupakan driver (pendorong) : strategic alignment, resource management dan performace measurement: kelima hal ini semuanya digerakkan oleh stakeholder value.

a. Penyesuaian strategis (Strategic Allignment), penerapan TI harus mendukung pencapaian misi perusahaan. Strategi TI harus benar-benar mendukung strategi bisnis perusahaan.
b. Penambahan nilai (Value Delivery), penerapan TI harus memberikan nilai tambah bagi pencapaian misi perusahaan.
c. Pengelolaan resiko (Risk Management), penerapan TI harus disertai dengan identifikasi terhadap resiko-resiko TI, sehingga dapat mengatasi dampak yang ditimbulkan olehnya. Resiko penerapan TI dapat berupa virus, penyalahgunaan hak akses, kesalahan/kerusakan sistem, kerusakan sistem pendukung dan lain-lain.
d. Pengelolaan sumber daya (Resource Management), penerapan TI harus didukung sumber daya yang memadai dan penggunaan sumber daya yang optimal.
e. Pengukuran kinerja (Performance Measurement), penerapan TI harus diukur dan dievaluasi secara berkala, untuk memastikan bahwa investasi dan kinerja TI sesuai dengan kebutuhan bisnis perusahaan.



Gambar 3 Fokus Area tata kelola TI [ITGI, 2005]

Dengan Perencanaan TI dapat memberikan kontribusi dan mempertajam strategi organisasi dalam mencapai tujuannya. Adapun macam-macam strategi tata kelola TI diantaranya adalah:

1. **IT Strategic Alignment**

   Strategi TI dapat mengartikulasi niat dari suatu perusahaan untuk menggunakan TI dari berbagai area yang berdasarkan dari kebutuhan bisnis. Hal yang harus dipertimbangkan dalam merumuskan strategi TI adalah

   a. *Business objectives and the competitive environment*
   b. *Current and future technologies and the costs, risks and benefits they can bring to the business*
   c. *The capability of the IT organisation and technology to deliver current and future levels of service to the business, and the extent of change and investment this might imply for the whole enterprise*
   d. *Cost of current IT and whether this provides sufficient value to the business*
   e. *The lessons learned from past failures and successes*

2. **Strategic Plan**

   Strategic plan menjelaskan bagaimana sebuah perusahaan mengeksekusi strategi yang dipilih. Strategic plan merupakan sebuah alat untuk membantu organisasi dalam melakukan pekerjaan yang lebih memfokoskan pada energy, sumberdaya dan waktu dari setiap orang dalam organisasi.

3. **Element of strategic plan**

   Terdiri dari tiga elemen yaitu:

   a. *Where are we now*

      Untuk melihat posisi strategis apa yang terjadi secara internal dan eksternal dalam menentukan perlu atau tidaknya suatu perubahan. Elemen dasarnya adalah Mission Statement, Value and/or guiding principles, and SWOT.

   b. *Where are we going*

      Untuk melihat arah dan tujuan serta bentuk organisasi di masa yang akan dating. Elemen dasar yang menentukan adalah Sustainable competitive advantage dan Vision Statement.

   c. *How are we going to get there*

      Untuk mengetahui apa yang harus dilakukan dalam mencapai sasaran strategi yang di tetapkan. Hal-hal yang dapat membantu dalam mencapai sasaran strategis adalah:

- Strategic objective
- Strategy
- Short-term goals /priorities/initiatives
- Action Items
- Scorecard
- Execution

C. MODEL DALAM TATA KELOLA TI

1. The Infrastructure IT Library

a. Definisi

The Infrastructure IT Library Merupakan framework pengelolaan layanan TI (IT Service Management) yang sudah di adopsi sebagai standar industry perangkat lunak. Kerangka kerja digunakan untuk mendefinisikan pengelolan layanan yang terintegrasi, berbasiskan proses dan praktik-praktik yang terbaik dalam organisasi.

ITIL atau (Information Technology Infrastructure Library) adalah suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan serta operasi teknologi informasi (TI). Nama ITIL diterbitkan dalam suatu rangakaian buku yang masing-masing membahas suatu topic pengelolaan TI. Nama ITIL dan TI Infrastructure Library merupakan merek dagang terdaftar dari Office of Government Commerce (OGC) Britania Raya.

ITIL memberikan deskripsi detail tentang beberapa praktek TI penting dengan daftar cek, tugas, serta prosedur yang menyeluruh yang dapat di sesuaikan dengan segala jenis organisasi TI.

b. Sejarah

Pada tanggal 30 Juni 2007, OGC menerbitkan ITIL versi 3 yang terdiri dari lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi. Kelima bagian tersebut adalah :

1) *Service Strategy* : Memberikan panduan kepada pengimplementasi ITSM pada bagaimana memandang konsep ITSM bukan hanya sebagai sebuah kemampuan organisasi. Proses –proses yang dicakup dalam Service Strategy :
   - Service Protofolio Management
   - Financial Management
   - Demand Management

2) *Service Design* : Berisikan prinsip-prinsip dan metode desain untuk mengkonversi tujuan strategis organisasi TI dan bisnis menjadi portofolio/koleksi layanan TI serta aset-aset layanan, seperti server,storage dan sebagainya. Proses-proses yang dicakup dalam Service Design, yaitu :
   - Service Catalog Management
   - Service Level Management
   - Supplier Management
   - Capacity Management
   - Availability Management
   - IT Service Continuity Management
   - Information Security Management
3) *Service Transition* : Menyediakan panduan kepada organisasi TI untuk dapat mengembangkan serta kemampuan untuk mengubah hasil desain layanan TI baik yang baru maupun layanan TI yang dirubah spesifikasinya kedalam lingkungan operasional.
4) *Service Operation* : Merupakan tahapan lifecycle yang mencakup kegiatan operasional harian pengelolaan layanan-layanan TI. Di dalamnya terdapat panduan bagaimana mengelola layanan TI secara efektif dan efisien. Proses-proses yang dicakup kedalam Service Operation :
   - Event Management
   - Incident Management
   - Problem Management
   - Request Fulfillment
   - Access Management
5) *Continual Service Improvement* : Memberikan panduan penting dalam menyusun serta memelihara kualitas layanan dari proses desain, transisi dan pengoprasiannya. CSI mengkombinasikan berbagai prinsip dan metode dari manajemen kualitas. Penerapan ini merupakan pendahuluan dari Continual Service Inprovement (CSI) berdasarkan ISO/IEC 20000, yang merupakan :
   - Mendefinisikan pemeriksaan yang dibutuhkan dalam melakukan eksekusi pada tahapan pemeriksaan.
   - Mengidentifikasikan komparisasi tampilan berdasarkan CSI serta lifecycle yang lainnya.
   - Mengidentifikasikan proses aktivitas yang membutuhkan pengenalan.
   - Mengidentifikasikan kewajiban dan wewenang dari manajemen.

- Mencari tools yang dibutuhkan untuk mendukung dan mempros dokumen.

Kelima bagian tersebut akan dikemas dalam bentuk buku atau biasa disebut *Core Guidance Publications*. Setiap buku nya berisikan :

1) Practice fundamentals : Menjelaskan latar belakang tahapan lifecycle serta kontribusi terhadap pengelolaan layanan TI secara keseluruhan.
2) Practice principles : Menjelaskan konsep-konsep kebijakan serta tata kelola tahanan lifestyle yang menjadi acuan setiap proses terkait dalam tahapan ini.
3) Lifecycle processes and activies : Menjelaskan berbagai proses maupun aktivitas yang menjadi kegiatan utama tahapan lifecycle. Misalnya proses financial management dalam tahapan Service Strategy.
4) Examples and templates : berisi tamplate maupun contoh-contoh pengaplikasian proses.
5) Supporting organization structure and roles : Proses ITIL tidak akaan dapat berjalan dengan baik tanpa definisi roles dan responsibilities. Bagian ini menjelaskan kesiapan model dan struktur organisasi
6) Practice Implementation : Berisi acuan atau panduan bagi organisasi TI yang ingin mengimplementasikan atau yang ingin meningkatkan proses ITIL

Pada awalnya ITIL adalah serangkaian buku pedoman tentang pengelolaan layanan IT yang terdiri dari modul. Perpustakaan besar pertama ini juga dikenal sebgai ITIL 1.0. Antara 2000 dan 2004 disebabkan oleh peningkatan pelayanan yang berkesinambungan dan adaptasi terhadap situasi saat ini dalam lingkungan (IT) modern ITIL 1.0 dirilis besar dan digabungkan menjadi delapan inti manual : ITIL 2.0 Pada awal musim panas 2007 ITIL 3.0 diterbitkan. Ini didirikan struktur yang sama sekali baru, yang terdiri dari tiga bidang utama, yaitu:

- ITIL Core Publikasi
- ITIL Pelengkap Bimbingan
- ITIL Web Support Services

Disamping buku-buku dalam *core guidance publications*, ada juga complementary guidance. Dimana buku-buku dalam kategori nantinya dimasukkan untuk memberikan model, acuan dan panduan bagi penerapan ITIL pada sektor-sektor tertentu seperti jenis industri tertentu, tipe organisasi serta arsitektur teknologi. Dengan demikian, ITIL akan dapat lebih diterima serta diadaptasi sesuai dengan lingkungan serta behaviour dari setiap organisasi TI.

c. Perkembangan

Dalam perkembangannya, ITIL telah mengalami perkembangan seiring dengan berkembangnya teknologi informasi. Pada awal perkembangannya, dokumentasi ITIL teridiri dari kurang lebih 40 publikasi yang terbagi kedalam modul-modul terpisah, setelah itu untuk simplifikasi serta kemudahan implementasu ITIL dibagi kedalam 7 domain yang masing-masing saling berhubungan dan dapat berdiri sendiri.

Dalam perkembangan fase ini atau sekarang disebut juga dengan ITIL versi 2, domain Service Support dan Service Delivery dijadikan sebagai CORE dalam tata kelola layanan teknologi informasi atau IT Service Management. Versi terakhir dari ITIL adalah versi 3

Framework ITIL dikembangkan sejak 1980-an oleh Office of Government Commerce (Departemen Perdagangan) Inggris sebagai guidance bagi organisasi/perusahaan disana. Pada pertengahan 1990, ITIL diakui dunia menjadi standar de facto di bidang service management. ITIL menyediakan sekumpulan best practice yang lengkap dan konsisten untuk ITSM, serta mempromosikan pendekatan kualitas untuk mencapai efektivitas dan efisiensi organisasi dalam penggunaan sistem informasi.

Walaupun dikembangkan sejak dasawarsa 1980-an, penggunaan ITIL baru meluas pada pertengahan 1990 dengan spesifikasi versi kedualnya (ITIL v-2) yang paling dikenal dengan dua set bukunya yang berubungan dengan ITSM (IT Service Management), yaitu Service Delivery (antar layanan) dan Service Support (dunkungan layanan).

2. ISO 17799

a. Isi ISO 1799

Berikut adalah isi dari ISO-17799 :

1) Security Policy (kebijakan keamanan)

Mengarahkan visi dan misi manajemen agar kontinuitas bisnis dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan informasi-informasi krusial yang dimiliki oleh perusahaan. Security Policy sangat diperlukan mengingat banyak ditemuinya masalah-masalah non teknis salah satunya penggunaan password oleh lebih dari satu orang. Hal ini menunjukan tidak adanya kepatuhan dalam menerapkan sistem keamanan informasi. Harus dilakukan inventarisasi data-data perusahaan. Selanjutnya dibuat peraturan yang melibatkan semua departemen sehingga peraturan yang dibuat dapat diterima oleh semua pihak. Setelah itu rancangan

peraturan tersebut diajukan ke pihak direksi. Setelah disetujui, peraturan tersebut dapat diterapkan.

Security Policy meliputi berbagai aspek, yaitu :

a) Information security infrastructure
b) Information security policy

2) System Access Control

Mengendalikan/membatasi akses user terhadap informasi-informasi yang telah diatur kewenangannya, termasuk pengendalian secara mobile-computing ataupun tele-networking. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada meliputi berbagai aspek, yaitu :

a) Access control.
b) User Access Management.
c) User Responsibilities.
d) Network Access Control
e) Operation System access Control
f) Application Access Control.
g) Monitor system Access and use.
h) Mobile Computing and Telenetworking.

3) Communication and Operations

Menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu :

a) Operational procedures and reponsibilities.
b) System Planning and acceptance.
c) Protection against malicious software.
d) Housekeeping
e) Network Management.
f) Media handling and security.
g) Exchange of Information and software.

4) Management

Management (manajemen komunikasi dan operasi), menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional.

Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu :

a) Operational procedures and reponsibilities.
b) System Planning and acceptance.
c) Protection against malicious software.
d) Housekeeping
e) Network Management.
f) Media handling and security.
g) Exchange of Information and software.

5) Management

System Development and Maintenance (pengembangan sistem dan pemeliharaan), memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi/validasi terlebih dahulu sebelum diluncurkan ke live environment.

Penelitian untuk pengembangan dan perawatan sistem yang ada meliputi berbagai aspek, yaitu :

a) Security requirements of system.
b) Security in application system.
c) Cryptographic control
d) Security of system files
e) Security in development and support process.

6) Physical And Environmental Security

Physical and Environmental Security (keamanan fisik dan lingkungan), membahas keamanan dari segi fisik dan lingkungan jaringan, untuk mencegah kehilangan/ kerusakan data yang diakibatkan oleh lingkungan, termasuk bencana alam dan pencurian data dalam media penyimpanan atau fasilitas informasi yang lain. Aspek yang dibahas antara lain:

a) Secure Areas
b) Equipment security
c) General Control

7) Compliance

Compliance (penyesuaian), memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk persyaratan kontraktual melalui audit sistem secara berkala. Kepatuhan yang mengarah kepada pembentukan prosedur dan aturan – aturan sesuai dengan hukum yang berlaku meliputi berbagai aspek, yaitu :

a) Compliance with legal requirements

b) Reviews of security policy and technical comliance.

a. System audit and consideration

8) Personel Security

Personnel Security (keamanan perorangan), mengatur tentang pengurangan resiko dari penyalahgunaan fungsi penggunaan atau wewenang akibat kesalahan manusia (human error), sehingga mampu mengurangi human error dan manipulasi data dalam pengoperasian sistem serta aplikasi oleh user, melalui pelatihan-pelatihan mengenai security awareness agar setiap user mampu menjaga keamanan informasi dan data dalam lingkup kerja masing-masing.

Personnel Security meliputi berbagai aspek, yaitu :

a) Security in Job Definition and Resourcing.
b) User Training.
c) Responding to Security Incidens and Malfunction.

9) Security Organization

Security Organization (organisasi keamanan), mengatur tentang keamanan secara global pada suatu organisasi atau instansi, mengatur dan menjaga integritas sistem informasi internal terhadap keperluan pihak eksternal termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (outsourcing). Aspek yang terlingkupi, yaitu :

a) Security of third party access
b) Outsourcing

10) Asset Classification Ana Control

Asset Classification and Control (klasifikasi dan kontrol aset), memberikan perlindungan terhadap aset perusahaan dan aset informasi berdasarkan level proteksi yang ditentukan. Membahas tentang penjagaan aset yang ada meliputi berbagai aspek, diantaranya :

a) Accountability for Assets.
b) Information Classification.

11) Bussiness Continiity

Business Continuity Management (manajemen kelanjutan usaha), siap menghadapi resiko yang akan ditemui didalam aktivitas lingkungan bisnis yang bisa mengakibatkan ”major failure” atau resiko kegagalan yang utama ataupun ”disaster” atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan manajemen untuk kelangsungan proses bisnis, dengan mempertimbangkan:

a) Aspects of business continuity management

Membangun dan menjaga keamanan sistem manajemen informasi akan terasa jauh lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang lebih nyata bagi organisasi bila didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

36 objek pengamatan/pengawasan keamanan merupakan uraian dari aspek 10 control clouse tersebut.

b. Sejarah

ISO 17799 diterbitkan oleh International Organization for Standardization (ISO) pada tahun 2000. ISO 17799 adalah standar internasional yang menyediakan petunjuk dan kontrol untuk mengatur keamanan informasi (Information Security Management Standard/ISMS). ISO 17799 berasal dari standar yang dikembangkan Department of Trade and Industry (DIT) tahun 1993. British Standards Institute (BSI) kemudian mengambil alih dan memperbaikinya kemudian disebut BS 7799 pada Februari tahun 1995, dan kemudian direvisi pada Mei 1999 dan diterbitkan dalam dua bagian:

1) Part I : Code Of Practice For Information Security Management
2) Part II : Specification For Information Security Management Systems

ISO hanya mengadopsi Part I dari BS 7799, sehingga Part I sekarang disebut sebagai “ISO/IEC 17799:2000” atau “ISO 17799”, sedangkan Part II tetap disebut “BS 7799-2”. Edisi pertama ISO 17799 diterbitkan pada tahun 2000, dan edisi keduanya terbit pada tahun 2005. Sejak edisi kedua tersebut ISO 17799 menjadi standar resmi ISO yang berdampak diperlukannya revisi dan pemutakhiran setiap tiga hingga lima tahun sekali.

ISO/IEC 17799:2005 tidak memfokuskan pada *effectiveness* dan *efficiency* serta hanya memberikan sedikit perhatian pada *reliability*. Sedangkan pada pengelolaan sumber daya TI dalam ISO/IEC 17799:2005 tidak terlalu memfokuskan pada *infrastructure*.

Membangun dan menjaga keamanan system manajemen informasi akan lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

3. COSO

a. Definisi

COSO merupakan *framework* untuk mengevaluasi efektifitas control internal suatu perusahaan. Lima komponen control yang dapat membantu mencapai sasaran kontrol internal adalah monitoring, communication, control activities, information, control environment dan risk assessment. Kemudian sasaran control internal dibagi menjadi beberapa area yaitu operations, financial reporting dan compliance.

b. Sejarah

COSO Framework merupakan kepanjangan dari *Committee of Sponsoring Organizations of the Treadway Commission* yang merupakan lembaga yang dibuat oleh sektor swasta untuk menghindari tindak korupsi yang sering terjadi di Amerika pada tahun 1970an. Padahal sebelumnya sudah ada FCPA (Foreign Corrupt Practises Act) yaitu suatu aturan yang dibuat tahun 1977 atas inisiatif dari eksekutif--legislatif kongres Amerika tentang peraturan anti penyuapan dan korupsi bagi perusahaan atau warga Amerika Serikat terhadap pegawai atau pejabat asing. Sektor swasta ini membentuk "National Commission on Fraudulent Financial Reporting" atau dikenal juga dengan "The Treadway Commission" di tahun 1985. Komisi ini disponsori oleh 2 professional association. Kelima organisasi tersebut terdiri dari American Accounting Associaton (AAA), American Institute of Certified Public Accountant (AICPA), Financial Executive International (FEI), The Association of Accountant and Financial Professionals in Business (IMA), dan The Institute of Internal Auditor (IIA).

Produk yang telah dihasilkan oleh COSO antara lain Internal Control–Integrated Framework (1992) dan Enterprise Risk Management–Integrated Framework (1994). Indonesia mengadopsi Internal Control–Integrated Framework (1992) dalam Peraturan Pemerintah Nomor 60 Tahun 2008 mengenai Sistem Pengendalian Intern Pemerintah. Dalam perkembangannya COSO telah mengeluarkan kerangka IC terbaru yaitu Internal Control–Integrated Framework (2013) untuk menggantikan kerangka IC yang lama.

COSO mendefinisikan IC adalah process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. Definisi ini sengaja dibuat secara luas agar dapat menangkap konsep yang penting mengenai bagaimana suatu organisasi merancang, mengimplementasikan, melaksanakan IC, dan menilai efektivitas dari sistem pengendalian internal, serta memberikan dasar dalam pengaplikasiannya di berbagai tipe organisasi. Selain itu definisi ini juga mengakomodasi bagian-bagian dari IC.

Tujuan dari IC terdiri dari operations, reporting, dan compliance dapat dijelaskan sebagai berikut:

1) *Operations Objectives:* Tujuan operasional terkait dengan pencapaian visi, misi, dan tujuan didirikannya entitas. Tujuan ini terkait dengan peningkatan *financial performance,* produktivitas, kualitas, *enviromental practices, return of assets,* dan likuiditas. Salah satu tujuan yang terkait dengan tujuan operasional adalah Pengamanan Aset. Entitas dapat menentukan tujuan yang terkait dengan pencegahan kehilangan aset serta secara periodik mendeteksi dan melaporkan kehilangan aset.
2) *Reporting Objectives:* Tujuan pelaporan berkaitan dengan penyusunan laporan untuk digunakan oleh organisasi dan stakeholders dalam hubungannya dengan pelaporan finansial/non-finansial serta pelaporan eksternal/internal. Karakteristik dari pelaporan finansial/non-finansial eksternal adalah disesuaikan dengan aturan dan kebutuhan eksternal, dipersiapkan sesuai dengan standar eksternal, dan mungkin diharuskan menurut regulator, kontrak, dan perjanjian. Sedangkan karakteristik pelaporan finansial/non-finansial internal adalah digunakan dalam pengambilan keputusan dan pengelolaan bisnis serta ditetapkan oleh manajemen dan board.
3) *Compliance Objectives:* Aturan dan hukum merupakan standar minimal dari perilaku organisasi. Organisasi diharapkan akan menggabungkan standar tersebut ke dalam tujuan dari entitas, bahkan organisasi dapat menetapkan standar yang lebih tinggi daripada yang ditetapkan oleh hukum dan peraturan. Satu tujuan dan tujuan lainnya dapat saling tumpang tindih atau saling membantu. Misalnya dalam hal pelaporan keuangan, dapat menjadi dasar bagi manajemen dalam melakukan review dalam kinerja operasionalnya serta kepatuhannya terhadap aturan. Selain itu, pengamanan aset yang merupakan salah satu contoh tujuan operasional juga berpengaruh terhadap ketepatan jumlah aset dalam pelaporan. Sehingga dapat disimpulkan bahwa penetapan tujuan-tujuan ini tetap saling berkesinambungkan, tapi tetap bergantung dengan situasi yang ada.

4. COBIT

a. Definisi

Kerangka kerja COBIT (Control Objectivea for Information related Technology) telah menjadi standar yang diterima secara global untuk tata kelola TI. COBIT 5 adalah perbaikan strategis utama dan *Information System Audit and Control Association* (ISACA) yang memberikan generasi panduan berikutnya mengenai tata kelola TI

perusahaan. COBIT 5 dirancang untuk memenuhi kebutuhan para pemangku kepentingan saat ini dan menyelaraskan dengan pola pemikiran tata kelola secara *enterprise* dan Teknik manajemen TI

b. Sejarah

Control Objectivies for Informastion and Related Technology (COBIT) muncul pertama kali pada tahun 1996, yaitu COBIT versi 1 yang menekankan pada bidang audit, COBIT versi 2 pada taun 1998 yang menekankan pada tahap control, COBIT veRsi 3 pada tahun 2000 yang berorientasi kepada manajemen COBIT versi 4 yang lebih mengarah pada *IT Governance*, dan yang terakhir dirilis adalah COBIT versi 5 pada tahun 2012 yang mengarah pada tata kelola dan manajemen untuk aset-aset perusahaan/institusi IT. COBIT adalah kerangka kerja tata kelola TI dan kumpulan perangkat yang mendukung dan memungkinkan para manager untuk menjembatani jarak (*gap*) yang ada antara kebutuhan yang dikendalikan (*control requirement*), masalah teknis (*technical issues*), dan risiko bisnis (*business risk)*.

COBIT 5 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan dalam mencapai tujuan untuk tata kelola dan manajemen perusahaan IT. Secara sederhana, hal ini membantu perusahaan/institusi menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan tingkat risiko dan penggunaan sumber daya. COBIT 5 memungkinkan TI untuk diatur dan dikelola secara holistic untuk seluruh perusahaan, melakukan pendekatan dengan bisnis secara *end-to-end* bidang fungsional IT serta tanggungjawabnya, dan mengingat kepentingan terkait pemangku kepentingan TI internal dan eksternal. COBIT 5 bersifat generic dan berguuna untuk perusahaan dari semua ukuran, komersial, monprofit atau di sector public.

5. VAL IT

Val IT, adalah salah satu metoda yang dapat digunakan untuk memberikan gambaran yang jelas akan manfaat investasi TI pada organisasi. Val IT merupakan konsep baru yang diluncurkan oleh Information Technology Governance Institute (ITGI) sebagai sebuah kerangka kerja standar untuk melengkapi kerangka kerja tata kelola TI yang sudah lama dirilis dan dipergunakan secara luas yaitu COBIT. Karena Val IT merupakan pelengkap COBIT, maka dalam beberapa hal, asumsi yang digunakan serta cara pendeskripsian kerangka kerjanya sangat mirip dan sangat erat kaitannya dengan COBIT. Val IT terdiri atas sekumpulan prinsip dasar dan 3 proses utama untuk mengukur nilai TI. Masing-masing proses

kemudian dirinci lagi menjadi beberapa item manajemen praktis seperti halnya pada COBIT.

IT Governance Institute (ITGI), lembaga yang mengeluarkan kerangka kerja tatakelola TI, sekitar bulan April 2006 mengeluarkan kerangka kerja pelengkap yang dapat digunakan untuk mengukur nilai TI yang disebut dengan Val IT. Saat ini, Val IT berfokus pada investasi TI baru dan selanjutnya akan dikembangkan hingga meliputi semua layanan dan asset TI. Tujuan inisiatif Val IT meliputi riset, publikasi dan dukungan layanan untuk membantu manajemen memahami nilai investasi TI dan menjamin bahwa organisasi dapat memperoleh nilai optimal atas investasi TI dalam konteks biaya dan resiko yang dapat diterima.

Val IT terdiri atas pedoman, proses dan beberapa saran praktis untuk membantu pihak manajemen dan eksekutif untuk memahami dan menjalankan perannya dalam investasi TI. Beberapa manfaat yang dapat diperoleh dari implementasi Val IT adalah sebagai berikut:

1. Meningkatkan pemahaman dan transparansi atas biaya, resiko, dan manfaat yang dihasilkan dari keputusan manajamen yang dilandasi oleh informasi yang memadai.
2. Meningkatkan kemampuan memilih investasi yang memiliki potensial pengembalian manfaat terbesar.
3. Meningkatkan kecenderungan keberhasilan dalam menjalankan investasi yang dipilih sehingga investasi tersebut dapat menghasilkan manfaat sesuai yang diharapkan.
4. Mengurangi biaya dengan hanya mengerjakan apa yang seharusnya dikerjakan dan segera mengambil tindakan korektif atau menghentikan investasi yang tidak menghasilkan potensi manfaat yang diharapkan.
5. Mengurangi resiko kegagalan, khususnya kegagalan yang beresiko tinggi.
6. Mengurangi ‘kejutan’ yang berhubungan dengan biaya dan delivery TI, sehingga dapat meningkatkan nilai bisnis, mengurangi biaya yang tidak perlu dan meningkatkan kepercayaan terhadap IT secara keseluruhan.

DAFTAR PUSTAKA

1. COSO. 2019. COSO Internal Control – Integrated Framework. An Implementation Guide for the Healthcare Provider Industry. www.coso.org
2. Indrajit, R.E. 2016. Konsep Dasar Tata Kelola Teknologi Informasi. The Preinexus Indonesia.
3. INVESTMENTS, O. 2008. ENTERPRISE VALUE: GOVERNANCE OF IT INVESTMENTS. http://www.accelerosblog.com/wp-content/uploads/2011/05/TheValITFramework_v2.0.pdf
4. ISO. 2015. ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management. www.iso.org
5. ITGI. 2005. IT Governance A Framework for Performance and Compliance: Board briefing on IT governance. www.itgi.org
6. Rouse, Margaret. 2018 ITIL (Information Technology Infrastructure Library). https://searchdatacenter.techtarget.com/definition/ITIL