AUDIT SISTEM INFORMASI BERBASIS KOMPUTER

KONSEP PENGENDALIAN BERDASARKAN COSO, COBIT, SOA, ISO 17799 & BASEL II

PENDAHULUAN

Pengendalian (controlling) merupakan salah satu fungsi manajemen dalam mencapai tujuan organisasi, yang merupakan manifestasi dari usaha manajemen untuk mengurangi resiko kerugian dan penyimpangan dalam suatu organisasi. Pengendalian Internal yang efektif merupakan salah satu faktor kunci dalam kesuksesan sebuah organisasi. Dalam pengendalian intern yang efektif, manajemen dan segenap anggota organisasi yang lain akan memiliki tingkat keyakinan yang memadai dalam mencapai tujuan dan sasaran suatu organisasi. Dimana dengan adanya sistem pengendalian intern yang efektif, dapat membantu dalam mencapai tujuan organisasi yang antara lain dalam hal efisiensi, mengurangi resiko kerugian, dan menghasilkan suatu laporan keuangan yang andal dan sesuai dengan hukum dan peraturan yang berlaku.

Dengan semakin dominannya penggunaan komputer dalam membantu kegiatan operasional diberbagai perusahaan, maka diperlukan standar-standar yang tepat sebagai alat pengendali internal untuk menjamin bahwa data elektronik yang diproses adalah benar. Sehingga data elektronik tersebut menghasilkan pelaporan keuangan perusahaan yang dapat dipertanggungjawabkan.

Dalam perkembangannya terdapat banyak standar-standar control yang muncul akibat berbagai latar belakang yang berbeda. Oleh karena itu, dalam paper ini akan diuraikan beberapa jenis standar kontrol EDP yaitu *Committee of the Sponsoring Organizations* (COSO), COBIT, SARBOX, ISO 17799, dan BASEL II. Selanjutnya akan dibahas beberapa perbedaan diantara kelima standar tersebut mencakup tujuan pembentukan standar dimaksud, *stakeholders* siapa yang diuntungkan dan siapa yang terbebani atas penerapan standar, pengaturan yang diterapkan dalam masing-masing standar, konsep pengendalian yang diatur dalam standard dan aspek-aspek dari standar yang paling cocok untuk diterapkan pada pengendalian EDP di Indonesia, khususnya untuk diimplementasikan oleh Badan Usaha Milik Negara.

COSO

The Comitte of Sponsoring Organizations of the treadway commission's (COSO) dibentuk pada tahun 1985 sebagai alinasi dari 5 (lima) organisasi professional. Organisasi tersebut terdiri dari American Accounting Association, American Instititue of Certified Public Accountants, Financial Executives International, Instititute of Management Accountants, dan The Institute of Internal Auditors. Koalisi ini didirikan untuk menyatukan pandangan dalam komunitas bisnis berkaitan dengan isu-isu seputar pelaporan keuangan yang mengandung fraud.

Pada tahun 1992, COSO menyusun dan menerbitkan *internal control integrated framework* yang berisi rumusan definisi pengendalian intern, pedoman penilaian, serta perbaikan terhadap sistem pengendalian intern. Kerangka ini diterima sebagai acuan umum pengendalian intern, yang penggunaannya mencakup penentuan tujuan pengendalian pelaporan keuangan dan proses operasional dalam konteks organisasional, sehingga perbaikan dan kontrol dapat dilakukan secara menyeluruh. Struktur pengendalian intern menurut COSO mencakup aktivitas pengendalian terkait pengendalian dengan pemrosesan informasi yaitu pengendalian umum dan pengendalian aplikasi.

Pada tahun 2004, COSO mengembangkan *internal control integrated framework* dengan menambahkan cakupan tentang manajemen dan strategi risiko yang selanjutnya dikenal dengan pendekatan *enterprise risk management* (ERM). Menurut kerangka tersebut, pengendalian intern merupakan bagian integral dari manajemen risiko.

Tujuan Pembentukan

COSO mendefinisikan pengendalian intern sebagai, "sebuah proses yang dipengaruhi oleh dewan komisaris, manajemen dan pegawai perusahaan lainnya yang dibentuk untuk menyediakan keyakinan yang memadai/wajar berkaitan dengan pencapaian tujuan dalam kategori berikut:

- Efektifitas dan efisiensi aktivitas operasi

Kendali ini dimaksudkan untuk mendorong penggunaan yang efektif dan efisien atas sumber daya organisasi, hal ini mencakup personil untuk mengotimalkan sasaran perusahaan. Bagian penting dari kendali ini adalah informasi yang akurat untuk pengambilan keputusan internal.

- Kehandalan pelaporan keuangan
  Secara legal dan profesional manajemen bertanggungjawab untuk menyiapkan laporan keuangan bagi investor, kreditur, dan para pemakai lainnya. Dalam rangka memenuhi tanggung jawab tersebut maka diperlukan adanya kendali untuk memastikan bahwa informasi tersebut disiapkan secara wajar menurut prinsip akuntansi yang berlaku secara umum (PAYBU).
- Ketaatan terhadap hukum dan peraturan yang berlaku
  Konsekuensi logis dari pendirian suatu organisasi yang berorientasi publik adalah kewajiban legal, organisasi diwajibkan untuk mematuhi aturan hukum dan berbagai peraturan yang berlaku (misal, UU Pajak dan peraturan Bursa Efek). Kendali ini memiliki nilai penting dalam rangka memastikan bahwa oraganisasi dalam kelangsungan telah mematuhi dan taat terhadap hukum dan peraturan tersebut.
- Pengamanan aset entitas
  Terkait dengan tujuan pelaporan publik manajemen, ditambahkan kategori baru yaitu pengamanan aset entitas. Nilai penting dari kendali ini adalah mencegah terjadinya akuisisi, penggunaan atau pemindahan aset yang tidak terotorisasi yang dapat memiliki efek material terhadap laporan keuangan.

Stakeholder

Setiap personel berperan dalam implementasi pengendalian internal perusahaan, tetapi tanggung jawab penyedia dan pelaksana pengendalian internal adalah manajemen senior, dalam hal ini CEO dan CFO. CEO berperan sebagai “pemberi warna” dan juga memberikan contoh kepada anggota lain. Sedangkan CFO dan manajemen senior lainnya berperan dalam proses desain, implementasi dan monitoring sistem pelaporan keuangan perusahaan.

Dewan komisaris dan komite audit menyediakan, panduan dan pengawasan. Anggota dewan komisaris dan komite audit harus objektif, mampu, dan kritis. Mereka juga harus menitikberatkan pada peran pengawasan, selain itu

mereka juga harus mengetahui lingkungan bisnis perusahaan, aktifitas pelaporan dan sistem pengendalian internal.

Secara garis besar stakeholder atas COSO yaitu Entitas; regulator; penyusun standar; organisasi profesi; intitusi pendidikan. Namun, pihak yang bertanggung jawab dan terbebani yaitu Dewan Komisaris, manajemen dan pegawai lainnya, sedangkan pihak yang diuntungkan adalah entitas dan pengguna informasi.

Overview COSO

Secara garis besar, COSO menghadirkan suatu kerangka kerja yang integral terkait dengan definisi pengendalian intern, komponen-komponennya, dan kriteria pengendalian intern yang dapat dievaluasi.

Pengendalian internal terdiri dari 5 komponen yang saling berhubungan. Komponen-komponen tersebut memberikan kerangka kerja yang efektif untuk menjelaskan dan menganalisa sistem pengendalian internal yang diimplementasikan dalam suatu organisasi. Komponen-komponen tersebut, adalah sebagai berikut:

1. Lingkungan pengendalian
2. Penilaian resiko
3. Aktifitas pengendalian
4. Informasi dan komunikasi
5. Pemantauan

I.Lingkungan Pengendalian

Lingkungan pengendalian menempatkan kualitas dalam organisasi, mempengaruhi kesadaran pengendalian terhadap pegawainya. Hal ini juga merupakan dasar bagi komponen pengendalian internal yang lain, menyiapkan disiplin dan struktur. Faktor lingkungan pengendalian meliputi integritas, nilai etis, gaya operasi manajemen, sistem pelimpahan wewenang, serta proses untuk mengatur dan mengembangkan sumber daya manusia dalam organisasi.

1. Integritas dan Nilai etika
   a) Ada dan diterapkannya kode etik
   b) Bekerjasama dengan karyawan, pemasok dan lain-lain dengan integritas yang tinggi
   c) Tekanan mencapai target yang tidak realistis dan target ini dipakai sebagai ukuran kinerja
2. Komitmen atas kompetensi
   a) Deskripsi pekerjaan formal atau informal

b) Analisis mengenai kompetensi dalam mengisi formasi pegawai

3. Dewan Komisaris/Komite Audit
   a) Independen dari manajemen
   b) Frekuensi dan ketepatan pertemuan dengan CFO, internal auditor maupun eksternal auditor
   c) Penyediaan informasi yang penting dan tepat waktu untuk memungkinkan pemantauan atas tujuan dan strategi manajemen, performa keuangan perusahaan dan syarat-syarat atas perjanjian penting
4. Filosofi Manajemen dan Gaya Operasi
   a) Resiko bisnis yang diterima, ini bisa berbentuk risk adverse atau risk taker
   b) Frekuensi pertemuan manajemen puncak dan manajemen operasi, terutama ketika beroperasi dalam wilayah geografis yang berbeda
   c) Sikap dan tindakan berkaitan dengan pelaporan keuangan termasuk juga mengenai perbedaan pendapat atas perlakuan akuntansi yang diterima.
5. Struktur organisasi
   a) Kelayakan struktur organisasi dan tersedianya jalur informasi yang layak
   b) Kecukupan pembagian tanggung jawab diantara manajer
   c) Kemampuan dan pengalaman manajer dalam memenuhi tanggung jawabnya
6. Kewenangan dan Tanggung Jawab
   a) Pendelegasian wewenang dan tanggung jawab disesuaikan dengan keperluan pencapaian tujuan perusahaan, peraturan yang berlaku, atau tujuan operasional
   b) Kecukupan standar dan prosedur yang berkaitan dengan pengendalian, termasuk juga deskripsi pekerjaan
   c) Kecukupan kuantitas dan kualitas pegawai dalam bidang akuntansi dan pemrosesan data disesuaikan dengan kompleksitas, sifat dan ukuran entitas
7. Kebijakan dan praktek berkaitan dengan manajemen SDM
   a) Adanya kebijakan dan prosedur berkaitan dengan penerimaan, pelatihan dan promosi pegawai
   b) Untuk kasus yang tidak sesuai dengan kebijakan yang berlaku, maka prosedurnya harus diulang
   c) Kecukupan pengecekan mengenai latar belakang pegawai
   d) Kecukupan kriteria promosi dan teknik-teknik pengumpulan informasi berkaitan dengan kode etik pegawai

II.Penilaian Risiko

Setiap organisasi dalam mencapai tujuannya menghadapi berbagai macam risiko baik eksternal maupun internal. Resiko ini bermacam-macam dilihat dari dampak ataupun tingkat keseringan terjadinya, misalkan resiko kebakaran tentu berbeda dengan resiko pencurian dana kas di cash register tentu berbeda dampak dan frekuensi terjadinya. Penilaian risiko merupakan tindakan yang penting untuk menentukan pengelolaan risiko.

Aspek-aspek penilaian resiko adalah sebagai beikut:

1. Tujuan

Tujuan entitas dapat bersifat eksplisit atau implisit, biasanya tercermin dalam misi atau nilai entitas. Lebih spesifik lagi, tujuan terdapat dalam rencana strategis perusahaan yang merupakan tujuan tingkat entitas. Tujuan ini kemudian dikaitkan dengan tujuan tingkat aktifitas. Kategori tujuan terdiri dari :

a) Tujuan operasi, memasukkan unsur efektif dan efisien termasuk juga tujuan kinerja dan tujuan laba dan pengamanan terhadap sumber daya
b) Tujuan pelaporan keuangan, yang menitikberatkan pada penyusunan laporan keuangan yang andal sesuai dengan standar
c) Tujuan Kepatuhan, yang menitikberatkan pada ketaatan kepada hukum dan peraturan yang berlaku

2. Identifikasi dan analisa resiko

Identifikasi dan analisa resiko harus bisa mencakup semua resiko yang signifikan dalam pencapaian tujuan. Proses identifikasi dan analisa resiko biasanya berulang-ulang dan terintegrasi dalam proses perencanaan.

a. Resiko tingkat entitas

   Resiko ini bersumber dari internal dan eksternal perusahaan, entitas harus bisa mendeteksi resiko semacam ini, berikut resiko-resiko entitas baik internal maupun eksternal :

b. Resiko tingkat aktifitas

   Semua aktifitas yang signifikan harus diidentifikasikan resiko yang mungkin timbul. Resiko aktifitas sendiri mungkin signifikan atau tidak, relevan atau tidak. Dalam identifikasi dan analisis resiko penting untuk memperhatikan dampak yang ditimbulkan resiko dan frekuensi resiko terjadi.

3. Manajemen perubahan

Setiap entitas harus mempunyai sebuah prosedur, baik formal atau informal, untuk mengidentifikasikan kondisi-kondisi yang menghalangi kemampuan perusahaan dalam mencapai tujuannya. Mekanisme ini harus mampu

mengantisipasi perubahan yang signifikan untuk dapat menghindari masalah atau memanfaatkan peluang yang muncul dari perubahan itu.

III.Aktivitas Pengendalian

Aktivitas pengendalian adalah kebijakan dan prosedur yang memastikan arahan manajemen dilaksanakan. Aktivitas pengendalian terjadi di seluruh bagian organisasi, baik pada berbagai tingkatan maupun berbagai fungsi yang meliputi otorisasi, verifikasi, rekonsiliasi, review kinerja operasi, keamanan aset, pemisahan wewenang dan tanggung jawab. Aktifitas pengendalian dapat bersifat preventif atau detektif, manual atau otomatis, atau review manajemen.

Aspek-aspek aktifitas pengendalian:

A. Prosedur dan Kebijakan

Kebijakan berfungsi menetapkan apa yang harus dilakukan sedangkan prosedur adalah tindakan personel untuk menjalankan kebijakan. Keduanya membantu memastikan bahwa arahan manajemen mengenai resiko dijalankan. Kebijakan dan prosedur dapat dibagi menjadi 3 kategori yaitu operasi, pelaporan keuangan dan ketaatan.

Berbagai jenis pengendalian dapat diterapkan untuk memastikan bahwa tujuan akan terpenuhi. Aktifitas pengendalian dapat diklasifikasikan menjadi :

1. Pengendalian preventif
2. Pengendalian detektif
3. Pengendalian manual
4. Pengendalian otomatis
5. Pengendalian manajemen

B. Sistem pengendalian Informasi

Terdiri dari 2 macam pengendalian yaitu : pengendalian umum dan pengendalian khusus. Pengendalian ini berlaku baik bagi mainframe ataupun komputer pengguna.

1. Pengendalian umum
   a. Operasi pusat data, meliputi tindakan backup, pengesetan dan pengecekan komputer, dan tindakan-tindakan kontijensi ketika terjadi bencana atas pusat data
   b. Software sistem, pengendalian atas perolehan, penggunaan dan perawatan software baik sistem operasi maupun software pendukung lainnya termasuk software keamanan, basis data dan yang lain.

c. Keamanan akses, semua akses ke sistem harus diotorisasi yang dapat berupa id khusus dengan password atau nomor-nomor tertentu
d. Metodologi pengembangan sistem, mencakup desain sistem dan implementasi sistem, fase-fase pengembangan, dokumentasi yang diharuskan, pengesahan dan pengujian untuk menekan biaya pengembangan sistem

2. Pengendalian aplikasi

Pengendalian aplikasi didesain untuk memastikan kelengkapan dan akurasi pemrosesan transaksi, otorisasi dan validasi. Dalam banyak kasus, pengecekan komputer dapat mencegah terjadinya kesalahan dan mendeteksi serta mengkoreksi kesalahan.

Pengendalian umum diperlukan untuk mendukung pelaksanaan pengendalian aplikasi, sedangkan pengendalian aplikasi diperlukan untuk memastikan pemrosesan transaksi yang akurat dan lengkap.

C. Pengendalian entitas khusus

Karena masing-masing entitas memiliki tujuan dan strategi masing-masing, maka aktifitas pengendalian mungkin akan berbeda satu sama lain. Faktor-faktor yang mempengaruhi desain pengendalian internal adalah : kemampuan dan penilaian manajemen, lingkungan dan industri beroperasinya, kompleksitas dan sifat organisasi, penyebaran asset dan karyawan serta tingkat kerumitan operasi dan pemrosesan informasi.

IV.Informasi dan Komunikasi

Sistem informasi berperan dalam sistem pengendalian internal sebagai penghasil laporan, termasuk operasional, finansial, dan ketaatan, sehingga memungkinkan karyawan untuk melakukan aktifitas pengendalian dan juga untuk memperoleh informasi serta mengkomunikasikannya secara tepat waktu maupun tepat bentuknya. Ini akan memudahkan manajemen untuk melakukan dan mengendalikan bisnis dengan efektif.

V.Pemantauan

Pemantauan (monitoring) merupakan suatu proses yang menilai kualitas dari kinerja suatu sistem dalam suatu waktu. Sistem pengendalian internal harus dimonitor untuk mengetahui kualitas sistem pengendalian internal dari waktu ke waktu. Ketika monitoring diatur dengan baik perusahaan cenderung diuntungkan karena perusahaan akan dapat :

a) Mengidentifikasikan dan memperbaiki pengendalian internal pada waktu yang tepat
b) Menyediakan informasi yang lebih akurat dan dapat diandalkan untuk pengambilan keputusan
c) Menyediakan laporan keuangan yang akurat dan tepat waktu
d) Berada dalam posisi kesiapan menyatakan pendapat mengenai kemampuan pengendalian internal

Konsep Pengendalian

Beberapa konsep utama/dasar terkait dengan pengendalian intern adalah:

Tanggung jawab manajemen – Manajemen yang bertanggung jawab dalam rangka mempersiapkan dan menyajikan laporan keuangan. Oleh karena itu manajemen yang bertanggung jawab dalam menentukan dan memelihara adanya pengendalian intern yang efektif dan handal.

Proses yang berkesinambungan– Internal control bukanlah suatu kejadian tunggal, tetapi merupakan serangkaian tindakan dan kegiatan yang meliputi operasi organisasi. Tindakan-tindakan ini melekat dalam metode yang digunakan manajemen untuk melaksanakan operasi sehari-hari. Internal control jangan dipandang sebagai sesuatu yang terpisah atau suatu sistem tersendiri dalam suatu bagian, tetapi lebih merupakan suatu bagian yang terpadu dari proses bisnis yang dikelola oleh manajemen untuk mencapai tujuan organisasi. Suatu sistem internal control yang efektif ditandai dengan pengendalian “melekat” pada infrastruktur suatu bagian dan bukan pengendalian yang ditambahkan “di atas” infrastruktur.

Bergantung pada faktor manusia – Manusia yang membuat internal control berjalan. Pimpinan pada akhirnya bertanggung jawab untuk memelihara struktur internal control yang efektif, meskipun manajemen mencapainya melalui pendelegasian dan kinerja dari pertanggungjawaban oleh semua pegawai dalam organisasi. Dengan demikian para pegawai dengan jelas harus memahami tanggung jawab dan batas wewenangnya serta pengaruhnya terhadap pencapaian efektifitas dari struktur internal control. Faktor manusialah yang mendefinisikan tujuan-tujuan bisnis yang terukur, mengawali mekanisme internal control dan kegiatan, dan memantau seberapa bagus pengendalian membantu dalam pencapaian tujuan-tujuan yang telah ditetapkan.

Keyakinan Yang Memadai bukan mutlak – Walaupun internal control dibuat dan dilaksanakan dengan sebaik-baiknya, internal control tidak dapat

memberikan keyakian mutlak. Manajemen harus merancang dan mengimplementasikan internal control berdasarkan perkiraan manfaat dan biaya. Pada dasarnya, internal control hanya memberikan keyakinan yang memadai dalam mencapai tujuan. Kesalahan dalam memberikan penilaian, kapasitas manajemen untuk menolak pengendalian, dan tindakan kolusi untuk mengelak dari pengendalian dapat menghambat pencapaian tujuan. Namun, struktur internal control yang efektif dapat memberikan keyakinan terbaik bahwa kejadian yang tidak diharapkan dapat diminimalkan serta tercapainya tujuan organisasi.

Pengendalian intern beroperasi pada level efektivitas yang berbeda-beda. Pengendalian Internal dapat dinilai apakah efektif atau tidak berdasarkan 3 kriteria dimana baik dewan komisaris maupun manajemen mempunyai jaminan yang wajar bahwa tujuan organisasi diupayakan dalam bentuk:

a. Laporan keuangan yang dipublikasikan bersifat handal
b. Hukum dan peraturan yang berlaku ditaati

Ketika pengendalian internal adalah sebuah proses, maka tingkat keefektifannya adalah keadaan pada satu saat tertentu (bervariasi dari waktu ke waktu).

Implementasi pada BUMN

Dalam rangka meningkatkan keberhasilan usaha dan akuntabilitas perusahaan/BUMN (corporate governance) guna mewujudkan nilai pemegang saham dalam jangka panjang dengan tetap memperhatikan kepentingan stakeholder lainnya, berlandaskan peraturan perundangan dan nilai-nilai etika maka pemerintah Republik Indonesia telah menerbitkan Keputusan Menteri Negara BUMN Nomor Kep-117/M-MBU/2002 tentang Penerapan Praktek Good Corporate Governance pada Badan Usaha Milik Negara (BUMN).

Salah satu bagian penting yang diatur dalam keputusan tersebut adalah sistem pengendalian internal dari BUMN. Pada pasal 22 KEP-117/M-MBU/2002 tersebut dinyatakan hal-hal sebagai berikut:

Ayat (1)

Direksi harus menetapkan suatu Sistem Pengendalian Internal yang efektif untuk mengamankan investasi dan aset BUMN.

Ayat (2)

Sistem Pengendalian Internal sebagaimana dimaksud dalam ayat (1), antara lain mencakup hal-hal sebagai berikut:

a. Lingkungan pengendalian internal dalam perusahaan yang disiplin dan terstruktur, yang terdiri dari :
    1. integritas, nilai etika dan kompetensi karyawan;
    2. filosofi dan gaya manajemen;
    3. cara yang ditempuh manajemen dalam melaksanakan kewenangan dan tanggung jawabnya;
    4. pengorganisasian dan pengembangan sumber daya manusia; dan
    5. perhatian dan arahan yang dilakukan oleh Direksi.
b. pengkajian dan pengelolaan resiko usaha yaitu suatu proses untuk mengidentifikasi, menganalisis, menilai dan mengelola resiko usaha relevan.
c. aktivitas pengendalian yaitu tindakan-tindakan yang dilakukan dalam suatu proses pengendalian terhadap kegiatan perusahaan pada setiap tingkat dan unit dalam struktur organisasi BUMN, antara lain mengenai kewenangan, otorisasi, verifikasi, rekonsiliasi, penilaian atas prestasi kerja, pembagian tugas dan keamanan terhadap aset perusahaan.
d. sistem informasi dan komunikasi yaitu suatu proses penyajian laporan mengenai kegiatan operasional, financial, dan ketaatan atas ketentuan dan peraturan yang berlaku pada BUMN.
e. monitoring yaitu proses penilaian terhadap kualitas sistem pengendalian internal termasuk fungsi internal audit pada setiap tingkat dan unit struktur organisasi BUMN, sehingga dapat dilaksanakan secara optimal, dengan ketentuan bahwa penyimpangan yang terjadi dilaporkan kepada Direksi dan tembusannya disampaikan kepada Komite Audit.

Berdasarkan ketentuan tersebut maka penyaji dapat memastikan bahwa kerangka kerja pengendalian intern COSO tidak hanya aplikatif pada BUMN Indonesia, namun juga telah memiliki basis legal yang memastikan bahwa BUMN Indonesia memiliki kewajiban baik secara professional maupun legal untuk mengadopsi dan mengaplikasikan pengendalian intern COSO.

COBIT

Control Objectives for Information and Related Technology (COBIT) dapat definisikan sebagai alat pengendalian untuk informasi dan teknologi terkait dan merupakan standar terbuka untuk pengendalian terhadap teknologi informasi yang dikembangkan oleh *Information System Audit and Control Association* (ISACA) melalui lembaga yang dibentuknya yaitu *Information and Technology Governance Institute* (ITGI) pada tahun 1992.

COBIT yang pertama kali diluncurkan pada tahun 1996, mengalami perubahan berupa perhatian lebih kepada dokumen sumber, revisi pada tingkat lebih lanjut serta tujuan pengendalian rinci dan tambahan seperangkat alat implementasi *(implementation tool set)* pada edisi keduanya yang dipublikasikan pada tahun 1998. COBIT pada edisi ketiga ditandai dengan masuknya penerbit utama baru COBIT yaitu ITGI. COBIT edisi keempat merupakan versi terakhir dari tujuan pengendalian untuk informasi dan teknologi terkait.

Tujuan Pembentukan

Tujuan diluncurkan COBIT adalah untuk mengembangkan, melakukan riset dan mempublikasikan suatu standar teknologi informasi yang diterima umum dan selalu *up to date* untuk digunakan dalam kegiatan bisnis sehari-hari.

Dengan bahasa lain, COBIT dapat pula dikatakan sebagai sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, manajemen and pengguna (user) untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan permasalahan-permasalahan teknis melalui pengendalian terhadap masing-masing dari 34 proses IT, meningkatkan tingkatan kemapanan proses dalam IT dan memenuhi ekspektasi bisnis dari IT. COBIT mampu menyediakan bahasa yang umum sehingga dapat dipahami oleh semua pihak. Adopsi yang cepat dari COBIT di seluruh dunia dapat dikaitkan dengan semakin besarnya perhatian yang diberikan terhadap *corporate governance* dan kebutuhan perusahaan agar mampu berbuat lebih dengan sumber daya yang sedikit meskipun ketika terjadi kondisi ekonomi yang sulit.

Fokus utama COBIT adalah harapan bahwa melalui adopsi COBIT ini perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi resiko-resiko *inheren* yang teridentifikasi didalamnya.

Stakeholder

COBIT dirancang untuk digunakan oleh tiga pengguna berbeda yaitu :

- Manajemen

  Dengan penerapan COBIT, manajemen dapat terbantu dalam proses penyeimbangan resiko dan pengendalian investasi dalam lingkungan IT yang tidak dapat diprediksi.
- User

  Pengguna dapat menggunakan COBIT untuk memperoleh keyakinan atas layanan keamanan dan pengendalian IT yang disediakan oleh pihak internal atau pihak ketiga.
- Auditor

  Dengan penerapan COBIT, auditor dapat memperoleh dukungan dalam opini yang dihasilkan dan/atau untuk memberikan saran kepada manajemen atas pengendalian internal yang ada.

Overview COBIT

Secara singkat dapat COBIT memiliki kerangka kerja yang terdiri atas beberapa arahan (*guidelines*), yakni :

I. Control Objectives

COBIT terdiri atas 4 tujuan pengendalian tingkat-tinggi (*high-level control objectives*), yaitu :

1. Planning and Organization

Mencakup strategi, taktik dan perhatian atas identifikasi bagaimana IT secara maksimal dapat berkontribusi dalam pencapaian tujuan bisnis. Selain itu, realisasi dari visi strategis perlu direncanakan, dikomunikasikan, dan dikelola untuk berbagai perspektif yang berbeda. Terakhir, sebuah pengorganisasian yang baik serta infrastruktur teknologi harus di tempatkan di tempat yang semestinya.

Proses dalam domain ini adalah :

- Menetapkan rencana stratejik TI
- Menetapkan susunan informasi
- Menetapkan kebijakan teknologi
- Menetapkan hubungan dan organisasi TI
- Mengelola investasi IT
- Mengkomunikasikan arah dan tujuan manajemen
- Mengelola sumberdaya manusia
- Memastikan pemenuhan keperluan pihak eksternal
- Menaksir risiko
- Mengelola proyek
- Mengelola kualitas

2. Acquisition and Implementation

Untuk merealisasikan strategi IT, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan, dan terintegrasi ke dalam proses bisnis. Selain itu, perubahan serta pemeliharaan sistem yang ada harus di cakup dalam domain ini untuk memastikan bahwa siklus hidup akan terus berlangsung untuk sistem-sistem ini. Langkah-langkah domain ini adalah :

- Mengidentifikasi solusi terotomatisasi
- Mendapatkan dan memelihara software aplikasi
- Mendapatkan dan memelihara infrastruktur teknologi
- Mengembangkan dan memelihara prosedur
- Memasang dan mengakui sistem
- Mengelola perubahan

3. Delivery and Support

Domain ini berfokus utama pada aspek penyampaian/pengiriman dari IT. Domain ini mencakup area-area seperti pengoperasian aplikasi-aplikasi dalam sistem IT dan hasilnya, dan juga, proses dukungan yang memungkinkan pengoperasian sistem IT tersebut dengan efektif dan

efisien. Proses dukungan ini termasuk isu/masalah keamanan dan juga pelatihan.

Proses dalam domain ini adalah :

- Menetapkan dan mengelola tingkat pelayanan
- Mengelola pelayanan kepada pihak lain
- Mengelola kinerja dan kapasitas
- Memastikan pelayanan yang kontinyu
- Memastikan keamanan sistem
- Melakukan identifikasi terhadap atribut biaya
- Memberi pelatihan kepada user
- Melayani konsumen IT
- Mengelola konfigurasi/susunan
- Mengelola masalah dan kecelakaan
- Mengelola data
- Mengelola fasilitas
- Mengelola operasi

4. Monitoring

Semua proses IT perlu dinilai secara teratur sepanjang waktu untuk menjaga kualitas dan pemenuhan atas syarat pengendalian. Domain ini menunjuk pada perlunya pengawasan manajemen atas proses pengendalian dalam organisasi serta penilaian independen yang dilakukan baik auditor internal maupun eksternal atau diperoleh dari sumber-sumber anternatif lainnya. Proses dalam domai ini sebagai berikut :

- Memonitor proses.
- Menaksir kecukupan pengendalian internal.
- Mendapatkan kepastian yang independen.

II. **Audit Guidelines COBIT**

*B*erisi sebanyak 318 tujuan-tujuan pengendalian yang bersifat rinci (*detailed control objectives*) untuk membantu para auditor dalam memberikan *management assurance* dan/atau saran perbaikan.

III. **Management Guidelines COBIT**

Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan-pertanyaan berikut :

- Sejauh mana TI harus bergerak, dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkannya?
- Apa saja indikator untuk suatu kinerja yang bagus?
- Apa saja faktor atau kondisi yang harus diciptakan agar dapat mencapai sukses?
- Apa saja risiko-risiko yang timbul apabila kita tidak mencapai sasaran yang ditentukan?
- Apa yang dilakukan perusahaan lain?
- Bagaimana mengukur keberhasilan dan bagaimana pula membandingkannya?

Kerangka kerja COBIT juga memasukkan juga hal-hal berikut ini :

1. *Maturity Models* – Untuk memetakan status maturity proses-proses TI (dalam skala 0 - 5) dibandingkan dengan *"the best in the class in the Industry"* dan juga *International best practices*.
2. *Critical Success Factors* (CSFs) – Arahan implementasi bagi manajemen agar dapat melakukan kontrol atas proses TI.
3. *Key Goal Indicators* (KGIs) – Kinerja proses-proses TI sehubungan dengan *business requirements.*
4. *Key Performance Indicators* (KPIs) – Kinerja proses-proses TI sehubungan dengan *process goal.*

Konsep Pengendalian

COBIT mengadopsi definisi pengendalian dari COSO yaitu : "Kebijakan, prosedur, dan praktik, dan struktur organisasi yang dirancang untuk memberikan keyakinan yang wajar bahwa tujuan organisasi dapat dicapai dan hal-hal yang tidak diinginkan dapat dicegah atau dideteksi dan diperbaiki".

Sedangkan dalam tujuan pengendalian, COBIT mendefinisikannya sebagai : “Suatu pernyataan atas hasil yang diinginkan atau tujuan yang ingin dicapai dengan mengimplementasikan prosedur pengendalian dalam aktivitas IT tertentu”.

COBIT melihat pengendalian dalam tiga dimensi berbeda yaitu Sumber IT, Proses IT, dan Kriteria Informasi IT.

Dimensi pertama mencakup semua asset IT suatu perusahaan, yang dapat diidentifikasikan sebagai berikut :

a. Data
b. Sistem aplikasi
c. Teknologi
d. Fasilitas
e. Manusia

Proses IT sebagai dimensi kedua dari COBIT terdiri dari tiga segmen, yaitu : domains, proses, dan aktivitas. Sedangkan dalam dimensi ketiganya COBIT menetapkan kriteria informasi yang berguna dalam mendukung tercapainya tujuan organisasi dengan merujuk pada kebutuhan informasi di organisasi atau perusahaan. COBIT mengkombinasikan beberapa prinsip penyusunan informasi berdasarkan model-model yang sudah ada, dan merumuskannya kedalam tiga kategori utama, yaitu : *quality, fiduciary responsibility* dan *security*. Tiga kategori ini kemudian diuraikan lebih lanjut dalam kriteria-kriteria sebagai berikut :

- Efektifitas
- Efisiensi
- Kerahasiaan
- Integritas
- Ketersediaan
- Kepatuhan
- Keandalan

Implementasi pada BUMN

Dipandang dari cukup luasnya cakupan COBIT dalam pengendalian IT perusahaan, maka dapat disimpulkan bahwa BUMN dapat (bahkan seharusnya) mengadopsi guidelines COBIT dalam pengelolaan dan pengendalian IT-nya.

Sebelum uraian lebih lanjut mengenai aspek-aspek COBIT yang sesuai untuk BUMN, terlebih dahulu akan diuraikan mengenai keunggulan-keunggulan COBIT dalam pengendalian internal terhadap manajemen sistem dan informasi sebagai berikut :

- Akseptansi secara internasional, karena didasarkan atas pengalaman praktik dan profesionalitas para ahli di seluruh dunia.
- Memenuhi standar ISO17799, COSO I dan II, dan standar-standar terkait lainnya.
- COBIT menjadi jembatan komunikasi antara fungsi IT, bisnis dan auditor dengan menyediakan suatu pendekatan umum yang dapat dimengerti oleh semuanya pihak.
- COBIT berorientasi kepada manajemen, dapat diaplikasikan, dan mudah digunakan.
- COBIT menyediakan dukungan yang kuat untuk audit IT, meminimalisasi biaya resiko audit, dan dapat meningkatkan kualitas audit dan opini audit.
- COBIT dapat menghemat waktu dalam mengimplementasikan praktek-praktek yang efektif.
- COBIT bersifat fleksibel dan mudah beradaptasi untuk menyesuaikan dengan ukuran dan budaya organisasi, serta kebutuhan khusus lainnya.
- COBIT adalah sebuah konsep yang lengkap dan terintegrasi, dan dikelola oleh organisasi non profit yang sudah memiliki reputasi, yakni ISACA.

Selain berbagai keunggulan-keunggulan yang disebutkan diatas, terdapat beberapa alasan lain mengapa sebuah perusahaan mengadopsi COBIT yaitu :

- COBIT memberikan perhatian kepada tata kelola IT yang baik (Good IT Governance).
- Untuk menguji akuntabilitas manajemen terhadap sumber daya teknologi informasi.
- Adanya kebutuhan khusus untuk pengendalian sumber daya TI.
- Sebuah solusi yang berorientasi bisnis, karena COBIT mengedepankan penggunaan sumber daya TI yang efektif dan efisien.
- COBIT menyediakan kerangka untuk penilaian resiko atas IT.
- Berbasis otorisasi.
- Meningkatkan komunikasi antara manajemen, pengguna (users), dan auditor.

Dari keuntungan diatas, dapat disimpulkan bahwa penerapan COBIT dalam pengelolaan IT BUMN adalah sebuah keharusan. Keseluruhan aspek dalam kerangka kerja COBIT dapat diadopsi, uraian singkat berikut akan memberikan penjelasan lebih lanjut :

- Manajemen dapat mengadopsi *control objectives* COBIT dalam perancangan model pengelolaan dan pengendalian IT perusahaan. Proses perancangan tersebut dapat diadopsi dari langkah-langkah/proses yang ada dalam domain-domain COBIT.
- Manajemen dapat mengadopsi *management guideline* COBIT sebagai *tools* dalam perumusan kebijakan management baik kebijakan mengenai IT maupun kebijakan lainnya yang berhubungan dengan kinerja perusahaan.
- Pengawas internal (auditor) dapat menggunakan *audit guideline* COBIT sebagai standar dalam perancangan dan pelaksanaan audit atas sistem informasi perusahaan. Secara rinci, auditor menggunakannya dalam :

  perencanaan audit dan pengembangan program audit.

  validasi kontrol-kontrol IT

evaluasi resiko-resiko IT

Mudahnya adopsi COBIT dalam pengelolaan IT pada dasarnya disebabkan oleh mudahnya modifikasi *guidelines* COBIT sesuai dengan kondisi industri dan kondisi IT perusahaan atau organisasi.

SARBANES-OXLEY ACT

Sarbanes-Oxley Act (Sarbox) merupakan peraturan yang ditandatangani Presiden George W. Bush pada tanggal 30 Juli 2002 untuk mereformasi dunia pasar modal Amerika Serikat yang sempat terguncang oleh skandal akuntansi yang menimpa Enron dan WorldCom.

Seperti yang dinyatakan pada bagian awalnya ***"To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes",*** undang-undang ini diharapkan dapat memberikan kepastian atas realibilitas Laporan Keuangan yang dipublikasikan dan meningkatkan kepercayaan diri pasar modal Amerika Serikat dengan memaksa perusahaan terbuka untuk memperbaiki pengungkapan laporan keuangannya.

TUJUAN PEMBENTUKAN

Beberapa tujuan dari Sarbox adalah :

1. Meningkatkan akuntabilitas manajemen dengan memastikan bahwa manajemen, akuntan dan pengacara memiliki tanggung jawab atas informasi keuangan yang menjadi tanggung jawab mereka.

2. Meningkatkan pengungkapan dengan berusaha untuk menyatakan bahwa beberapa kejadian kunci dan transaksi luar biasa tidak mendapatkan pengawasan hanya karena tidak disyaratkan untuk diungkap ke publik.
3. Meningkatkan pengawasan rutin yang lebih intensif oleh SEC. Hal ini berdasarkan pengalaman bahwa kurangnya review pada laporan Enron di masa lalu menyebabkan kebangkrutan dan kerugian bagi investor.
4. Meningkatkan akuntabilitas akuntan. Sarbox ingin membersihkan konflik kepentingan, opini sub-standar dan hal-hal lain yang membahayakan investor ketika mempercayai laporan keuangan yang bersertifikasi.

STAKEHOLDERS

Penggagas Sarbox adalah senator Paul Sarbanes dan salah seorang anggota *house of representative*, Michael Oxley. Entitas yang terpengaruh dengan adanya undang-undang ini antara lain:

1. Perusahaan penerbit laporan keuangan (dewan komisaris, komite audit, dan manajemen)
   - ✔ Sarbox berlaku untuk seluruh perusahaan publik di Amerika dan perusahaan asing yang listing di pasar modal Amerika.
   - ✔ Manajemen perusahaan harus menerbitkan laporan tahunan mengenai pengendalian intern perusahaan.
   - ✔ CEO dan CFO harus melakukan sertifikasi terhadap laporan keuangan yang diterbitkannya.
   - ✔ Perusahaan diharuskan memiliki komite audit yang independen dan tidak menerima gaji dari perusahaan atas keanggotaannya dalam komite tersebut.
2. Kantor Akuntan Publik (auditor eksternal)
   - ✔ Sarbox berlaku untuk seluruh auditor eksternal yang mengaudit perusahaan publik di Amerika dan perusahaan asing yang listing di pasar modal Amerika.
   - ✔ Untuk menghindari konflik kepentingan sesuai dengan tujuannya, maka KAP yang melakukan audit yang tidak diperbolehkan memberikan jasa non-audit tertentu kepada klien yang diauditnya. Jika audit dilakukan dua tahun berturut-turut atau lebih maka diharuskan ada rotasi tim audit.
   - ✔ Auditor eksternal diharuskan membuktikan kebenaran (atestasi) atas laporan pengendalian intern yang dikeluarkan manajemen perusahaan.

- ✔ Auditor eksternal akan lebih mudah memahami sistem pengendalian intern perusahaan sekaligus meningkatkan keterandalan laporan audit.

3. Securities Exchange Comission

   Sarbox mengharuskan SEC melakukan review kepada perusahaan-perusahaan secara lebih teratur dan intensif.

4. Public Company Accounting Oversight Board (PCAOB)

   Pada Title 1 Sarbox diatur mengenai pendirian dewan baru, yaitu PCAOB. PCAOB merupakan dewan independen pengawas akuntansi bagi perusahaan publik di Amerika. Tugas dari PCAOB ini menetapkan standar audit bagi auditor untuk perusahaan publik dan juga melakukan audit terhadap para auditor tersebut.

5. Investor

   Investor lebih akan lebih diuntungkan karena informasi laporan keuangan yang disajikan perusahaan lebih valid sebagai dasar pengambilan keputusan berikutnya.

OVERVIEW SARBOX

Sarbanes-Oxley Act terdiri atas 11 bagian (*title*) dengan gambaran sebagai berikut:

Bagian I- *Public Company Accounting Oversight Board*

Dalam bagian ini terdapat sembilan pasal dimana fokusnya adalah mengubah cara kerja auditor sebelumnya dengan kerangka kerja baru dengan mendirikan *Public Company Accounting Oversight Board* (PCAOB). PCAOB menetapkan standar audit bagi auditor untuk perusahaan publik dan juga melakukan audit terhadap para auditor tersebut. Hal lain yang juga diatur dalam bagian ini adalah aturan yang menetapkan keharusan untuk menetapkan kertas kerja, menyediakan 2 partner untuk mengaudit, dan juga evaluasi akan pengendalian intern oleh auditor.

Bagian II-Independensi Auditor

Sembilan pasal dalam bagian ini memfokuskan diri untuk membuat batasan untuk menghindari *conflict of interest* yang terjadi akibat hubungan yang terlalu dekat antara auditor dan perusahaan. Hal ini dilakukan dengan melarang auditor melakukan jasa non-audit tertentu

kepada perusahaan yang diauditnya. KAP juga diharuskan melakukan rotasi atas tim audit apabila audit dilakukan dua tahun berturut-turut atau lebih.

Bagian III-Tanggung-Jawab Perusahaan

Bagian ini mengatur mengenai tanggung jawab perusahaan akan isi dari laporan keuangan yang disampaikan. Dalam hal ini perusahaan yang diatur oleh Sarbox diharuskan memiliki komite audit yang independen dimana walaupun dia merupakan bagian dewan direksi namun dia tidak menerima gaji lainnya dari perusahaan.

Selain itu, bagian ini juga mengatur bahwa perusahaan harus memberikan sertifikasi bahwa:

a. Laporan keuangan periodik yang disampaikan tidak mengandung isi yang tidak benar maupun *material omissions*.
b. CFO dan CEO bertanggung jawab terhadap pengendalian intern yang dirancang untuk memastikan manajemen menerima informasi yang bersifat material terkait dengan perusahaan
c. Bahwa pengendalian intern telah di *review* dalam jangka waktu 90 hari sebelum laporan
d. Melaporkan apabila telah terjadi perubahan signifikan dalam pengendalian intern.

Bagian IV-Pengungkapan Laporan Keuangan yang lebih baik

Hal-hal yang penting mengenai pengungkapan yang diatur di pasal ini temasuk

a. Pengungkapan transaksi maupun penyesuaian yang *off-balance sheet.*
b. Pelarangan untuk memperpanjang pinjaman pribadi terhadap eksekutif perusahaan
c. Pengungkapan akan perubahan kepemilikan *inside stock*
d. Sertifikasi pengendalian intern
e. Kode Etik
f. *Review* dari SEC secara teratur

Bagian V- Analisa *Conflict of Interest*

Bagian ini memfokuskan diri pada pencegahan terjadinya berbagai macam konflik kepentingan yang mungkin terjadi.

Bagian VI- Sumber Komisi dan Kewenangan

Bagian ini memberikan kewenangan kepada SEC beserta dananya untuk merekrut 200 profesional untuk mengawasi auditor dan kantor audit. Dimana SEC juga berhak untuk memberi larangan bagi auditor tertentu untuk melakukan jasa audit terkait dengan tindakan tidak etis dan profesional yang dilakukan auditor tersebut

Bagian VII- Studi dan Laporan

Dalam bagian ini SOX memberikan dana dan kewenangan untuk melakukan studi mengenai beberapa hal termasuk peran agensi *credit rating* dalam pasar sekuritas, bank investasi, tindakan penegakan hukum, dll.

Bagian VIII- *Corporate and Criminal Fraud Accountability*

Bagian ini memberikan hukuman (maksimal 10 tahun penjara) apabila diketahui menghancurkan, menyembunyikan, mengubah, ataupun memalsukan catatan dengan maksud menggangu atau pun mempengaruhi penyelidikan terkait dengan masalah kebangkrutan. Selain itu bagian ini juga memberikan perlindungan kepada *whistle-blower* dengan melarang perusahaan untuk melakukan balas dendam kepada pegawai yang melakukan pengaduan terhadap adanya kecurangan didalam perusahaan.

Bagian IX- Peningkatan Hukuman Bagi Kejahatan *Kerah-Putih*

Bagian ini meningkatkan tingkat hukuman bagi kejahatan yang dilakukan oleh pekerja kerah-putih seperti kegagalan untuk mensertifikasi laporan tertentu, ataupun mengetahui bahwa suatu laporan salah atau tetap mensertifikasi walaupun kaporan tersebut salah.

Bagian X- Restitusi Pajak perusahaan

Bagian ini mengatur mengenai restitusi pajak yang dilakukan oleh perusahaan, dimana salah satunya mengatur bahwa CEO wajib menandatangani dokumen terkait.

Bagian XI- Kecurangan Perusahaan dan Akuntabilitas Perusahaan

Bagian ini meningkatkan hukuman atas pelanggaran terhadap peraturan yang belum diatur oleh bagian SOX lainnya, dan pemberian wewenang kepada SEC untuk me-*freeze extraordinary payment* kepada suatu perusahaan maupun individu yang sedang diinvestigasi untuk pelanggaran peraturan sekuritas. Selain itu bagian ini juga menetapkan *black list* yaitu apabila seseorang seseorang dihukum karena melakukan pelanggaran terhadap hukum negara bagian maupun federal terkait

dengan manipulasi, penipuan maupun kecurangan untuk bekerja sebagai direktur ataupun *officer* pada perusahaan publik.

KONSEP PENGENDALIAN INTERN

Sarbaness-Oxley Act diterbitkan untuk memproteksi kepentingan investor dengan cara menciptakan tata kelola perusahaan yang baik (*good corporate governance*), *full disclosure*, dan akuntabilitas dalam perusahaan. Untuk mewujudkan hal tersebut, Sarbox mengatur mengenai pengendalian intern perusahaan secara lebih intensif. Konsep pengendalian intern dalam Sarbanes-Oxley Act terdapat pada section 302 dan 404.

1. Section 302

Ringkasan section 302 Sarbanes-Oxley Act adalah sebagai berikut:

> *Section 302: Corporate Responsibility For Financial Reports.*
> *The CEO and CFO of each issuer shall prepare a statement to accompany the audit report to certify the "appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respects, the operations and financial condition of the issuer." A violation of this section must be knowing and intentional to give rise to liability.*

Peraturan ini mewajibkan Direktur Utama dan Direktur Keuangan perusahaan yang mencatatkan sahamnya di bursa Amerika Serikat untuk memberikan sertifikasi mengenai efektivitas rancangan dan pelaksanaan pengendalian intern dan pengungkapan kekurangan yang signifikan atas pengendalian intern dalam rangka pelaporan. Dari ringkasan tersebut dapat diidentifikasikan bahwa section 302 pada undang-undang ini menuntut *Chief Executive Officer* (CEO) dan *Chief Financial Officer* (CFO) untuk memberikan sertifikasi yang mendampingi laporan keuangan tahunan maupun triwulanan yang menyatakan bahwa:

a. CEO dan CFO telah mereview laporan keuangan tersebut,
b. berdasarkan pengetahuan CEO dan CFO, laporan keuangan tersebut tidak mengandung pernyataan yang tidak benar mengenai fakta-fakta material atau lalai dalam menyampaikan fakta-fakta material yang menyebabkan laporan keuangan menyesatkan,
c. berdasarkan pengetahuan CEO dan CFO, laporan keuangan tersebut dan informasi keuangan lainnya telah disajikan secara wajar atas semua hal yang material dari operasi dan kondisi keuangan perusahaan.

Sertifikasi ini juga harus menyatakan bahwa CEO dan CFO:

a. bertanggung jawab atas penyelenggaraan dan pemeliharaan pengendalian intern perusahaan,
b. telah merancang pengendalian intern untuk meyakinkan bahwa informasi yang berhubungan dengan perusahaan dan anak perusahaandiketahui oleh seluruh personel dalam perusahaan,
c. telah mengevaluasi efektivitas pengendalian intern dalam tempo 90 hari sebelum tanggal penyampaian laporan,
d. telah menyampaikan laporan kesimpulan mengenai efektivitas pengendalian intern tersebut berdasarkan evaluasi yang telah dilakukan.

Lebih lanjut, pejabat terkait harus memberikan sertifikasi bahwa mereka telah mengungkapkan kepada auditor dan komite audit semua kekurangan yang signifikan pada desain atau operasi pengendalian intern, termasuk setiap kelemahan material, dan setiap *fraud* (baik yang material maupun tidak), yang melibatkan manajemen atau pegawai lainnya yang mempunyai peran signifikan pada pengendalian intern perusahaan.

Berikut ini adalah contoh pernyataan manajemen:

> *"Kami sudah merancang internal kontrol atas laporan keungan perusahaan kami, dan kami sudah memantau pelaksanaan internal kontrol tersebut, dengan tujuan untuk menyediakan jaminan kepada pihak luar atas keandalan laporan keuangan perusahaan kami, dan memberikan jaminan lebih lanjut bahwa laporan keuangan perusahaan kami sudah sesuai dengan prinsip akuntansi berlaku umum di Amerika Serikat".*

2. Section 404

Ringkasan section 404 Sarbanes-Oxley Act adalah sebagai berikut:

> *Section 404: Management Assessment Of Internal Controls.*
>
> *Requires each annual report of an issuer to contain an "internal control report," which shall:*
>
> *(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and*
>
> *(2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.*
>
> *Each issuer's auditor shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this section shall be in accordance with standards for attestation engagements issued*

or adopted by the Board. An attestation engagement shall not be the subject of a separate engagement.

*The language in the report of the Committee which accompanies the bill to explain the legislative intent states, "**---** the Committee does not intend that the auditor's evaluation be the subject of a separate engagement or the basis for increased charges or fees."*

Directs the SEC to require each issuer to disclose whether it has adopted a code of ethics for its senior financial officers and the contents of that code.

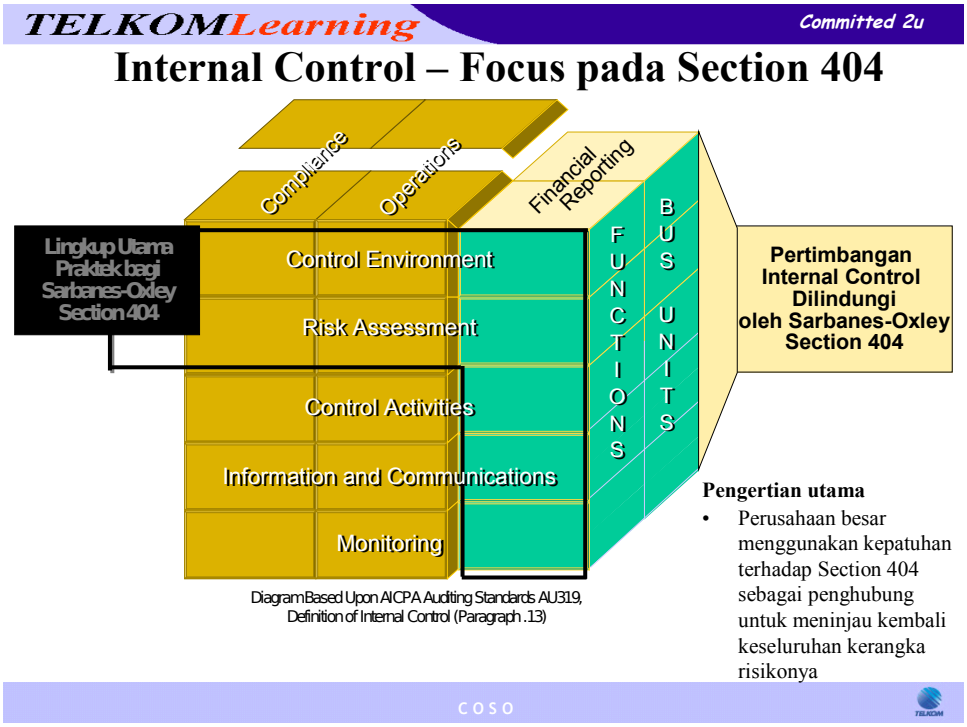
Directs the SEC to revise its regulations concerning prompt disclosure on Form 8-K to require immediate disclosure "of any change in, or waiver of," an issuer's code of ethics.

Peraturan ini mewajibkan perusahaan yang mencatatkan sahamnya di bursa Amerika Serikat untuk mendokumentasikan, mengevaluasi dan melaporkan hasil evaluasi atas efektivitas pengendalian intern laporan keuangannya. Auditor eksternal dituntut untuk melakukan penegasan dan melaporkan hasil evaluasi atas penilaian pengendalian intern perusahaan yang diauditnya tersebut. Dari ringkasan section 404 ini, dapat diidentifikasi bahwa undang-undang ini menuntut tanggung jawab baik dari manajemen perusahaan maupun dari auditor. Manajemen perusahaan diwajibkan untuk membuat laporan pengendalian intern tahunan yang berisi:

a. pernyataan tanggung jawab manajemen untuk membuat dan memelihara struktur dan prosedur pengendalian intern yang memadai untuk laporan keuangan, dan
b. penilaian pada akhir tahun pajak tentang efektivitas struktur dan prosedur pengendalian intern laporan keuangan issuer.

Jika manajemen perusahaan diharuskan untuk menyajikan suatu asersi tertulis mengenai efektivitas pengendalian intern dari perusahaan yang bersangkutan dan melengkapi evaluasinya dengan bukti-bukti yang memadai, maka auditor berkewajiban untuk membuktikan sekaligus melaporkan penilaian manajemen tersebut.

Diagram Mengenai Fokus Sarbox Section 404 Pada Pengendalian Intern Telkom



IMPLEMENTASI PADA BUMN DI INDONESIA

BUMN di Indonesia yang telah menerapkan Sarbanes-Oxley Act adalah BUMN yang telah melakukan listing di New York Stock Exchange, yaitu PT Telekomunikasi Indonesia, Tbk (Telkom) dan PT Indosat, Tbk (Indosat).

Telkom mulai menerapkan Sarbox dalam perjalanannya bergabung dengan bursa efek di Amerika Serikat. Ketika itu Telkom mengalami beberapa hambatan, antara lain Securities and Exchange Commissions (SEC) menolak Laporan Keuangan Telkom Tahun 2002 yang telah diaudit. Masalah tersebut timbul karena Kantor Akuntan Publik (KAP) yang melakukan audit atas laporan keuangan tersebut tidak terdaftar pada SEC serta adanya permasalahan komunikasi dengan auditor pendukung lainnya. Kasus ini menyebabkan Laporan Keuangan Telkom Tahun 2002 perlu diaudit ulang (reaudit) oleh KAP yang terdaftar pada SEC. Dalam proses audit ulang tersebut Telkom juga diarahkan agar mengikuti aturan yang tercantum dalam Sarbanes-Oxley Act.

Masalah dengan SEC yang dialami Telkom pada tahun 2002 menjadikan Telkom lebih waspada dalam menjalankan perusahaan dan berusaha untuk memperbaiki kesalahannya dan mematuhi peraturan dalam Sarbanes-Oxley Act, diantaranya mengenai pengendalian intern perusahaan pada section 302 dan section 404. Menghadapi kedua tuntutan mengenai pengendalian intern ini, Telkom segera melakukan beberapa tindakan, antara lain menerbitkan Keputusan Direksi

Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor: KD. 49/PW000/KUG-10/2004 tentang Kebijakan Pengendalian Intern dalam Rangka Penyajian Laporan Keuangan yang Sesuai dengan Sarbanes-Oxley Act Section 302 dan 404 dan menerbitkan Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor: KD. 53/PS150/CTG-10/2004 tentang Pembentukan Organisasi Proyek Integrasi *Internal Control* Perusahaan.

Nilai tambah yang diperoleh Telkom setelah menerapkan Sarbanes Oxley Act melakukan *Good Corporate Governance* dengan lebih baik sehingga kinerja perusahaan meningkat yang berpengaruh pada meningkatnya pendapatan dan laba perusahaan. Selain itu setelah menerapkan Sarbox, Telkom mampu mengelola anak cabang perusahaan dan melakukan ekspansi perusahaan dengan lebih baik. Hal tersebut dapat dibuktikan dengan beberapa penghargaan yang diraih Telkom antara lain:

1. The Asset Asian Award untuk *Good Governance Corporation* Terbaik di Indonesia dari The Asset Magazine, berdasarkan atas survey yang dilakukan oleh The Asset Benchmark Research,
2. Untuk kedua kalinya, TELKOM menerima Indonesia’s Most Admired Company Award sebagai *The Best in Building Corporate Image* dari Majalah Business Week, berdasarkan penilaian yang dilakukan oleh Frontier bekerja sama dengan Majalah Business Week,
3. Asia’s Top 100 IT Users: TELKOM menduduki peringkat ke-4 dari 100 perusahaan di Asia yang mendapat penghargaan Asia’s Top 100 IT Users oleh Majalah Management Information System (MIS),
4. Brand perusahaan terkemuka dari lembaga Superbrands International.

Penerapan Sarbox oleh Telkom memang memberikan pengaruh positif. Namun bukan Telkom merasa nyaman dalam menerapkannya. Setelah dapat melakukan listing di NYSE, pada pertengahan 2009 ini Telkom mempunyai wacana untuk melakukan delisting seperti halnya yang pernah terjadi pada tahun 2005. Wacana ini muncul karena untuk mematuhi aturan Sarbox diperlukan biaya audit yang cukup tinggi, yaitu mencapai Rp 100 miliar. Selain mahal, audit terkait Sarbox ini memerlukan waktu yang cukup lama, yaitu 6 bulan. Kedua hal ini menyebabkan ketidakefisienan perusahaan.

Selain Telkom, Indosat yang juga listing di NYSE sedang mengkaji kebijakan untuk melakukan delisting dari bursa saham Amerika itu dengan alasan yang kurang lebih sama. Jika Telkom lebih menekankan masalah biaya, maka Indosat lebih menekankan pada teknis pelaporan keuangan yang harus memakan waktu

lama karena menyesuaikan audit untuk dua bursa saham yang berbeda yaitu NYSE dan Bursa Efek Indonesia.

ISO 17799

TUJUAN PEMBENTUKAN

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting).

Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekseposnya data ke pihak eksternal yang tidak diinginkan.

Bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspose, merupakan tujuan disusunnya ISO 17799, yaitu menghadirka sebuat standar untuk sistem manajemen keamanan informasi. Kebutuhan ISO 17799 standard meliputi: dokumen kebijakan keamanan informasi, alokasi keamanan informasi tanggung-jawab, menyediakan semua para pemakai dengan pendidikan dan pelatihan di dalam keamanan informasi, mengembangkan suatu sistem untuk pelaporan peristiwa keamanan, memperkenalkan virus kendali, mengembangkan suatu rencana kesinambungan bisnis, mengendalikan pengkopian perangkat lunak kepemilikan, surat pengantar arsip organisatoris, mengikuti kebutuhan untuk perlindungan data, dan menetapkan prosedur untuk mentaati kebijakan keamanan.

Penyusunan standar ini berawal pada tahun 1995, dimana sekelompok perusahaan besar seperti BOC, BT, Marks & Spencer, Midland

Bank, Nationwide Building Society, Shell dan Unilever bekerja sama untuk membuat suatu standar yang dinamakan BS (British Standard) 7799.

BS 7799 Part 1: the Code of Practice for Information Security Management. Februari 1998 BS 7799 Part 2: The Specification for Information Security Management Systems (ISMS) menyusul diterbitkan. Desember 2000 ISO (International Organization of Standardization) dan IEC (International Electro-Technical Commission) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799:2000 yang diakui secara internasional.

STAKEHOLDER

Sebuah keamanan informasi yang lebih terjamin tentunya menhuntungkan semua pihak yang terkait dalam bisnis entitas, yaitu manajer bisnis, mitra usaha, auditor ,karena adanaya manajemen informasi yang efektif untuk memastikan informasi yang menjamin kesinambungan bisnis dan meminimise kerusakan bisnis dengan pencegahan dan memimise dampak peristiwa keamanan.

Pihak yang diuntungkan adalah perusahaan sebagai sebuah entitas, dan para pemakai informasi dari system informasi perusahaan termasuk pihak manajemen.

Pihak yang terbebani adalah bidang IT yang bertanggungjawab menyelenggarakan keamanan informasi termasuk juga pihak manajemen.

OVERVIEW ISO 17799

Secara umum standar tersebut mengatur struktur dan rekomendasi pedoman yang diakui secara internasional untuk keamanan informasi yang dapat diusahakan atau di implementasikan bagi perusahaan agar memperoleh manfaat keamanan yang diinginkan.

Isi ISO 17799, meliputi :

- 10 control clauses (10 pasal pengamatan)
- 36 control objectives (36 objek/sasaran pengamanan)
- 127 controls securiy (127 pengawasan keamanan)

Kesepuluh control causes merupakan konsep pengendalian didalam standar ISO 17799, adapun 36 control objectives tersebut yaitu:

- Control Objectives
- Information security policy
- Information security infrastructure
- Security of third party access
- Outsourcing
- Accountability for assets
- Information classifications
- Security in job definition and resourcing
- User training
- Responding to security incidents and malfunctions
- Secure areas
- Equipment security
- General controls
- Operational procedures and responsibilities
- System planning and acceptance
- Protection against malicious software
- Housekeeping
- Network management
- Media handling and security
- Exchanges of information and software
- Access Control
- Use access management
- User responsibilities
- Network access control
- Operating system access control
- Application access control
- Monitoring system access and use
- Mobile computing and teleworking
- Security requirements of systems
- Security in application system
- Cryptographic controls
- Security of systems files
- Security in development and support process

- Aspects of business continuity management
- Compliance with legal requirements
- Review of security policy & technical compliance

KONSEP PENGENDALIAN

Konsep pengendalian di dalam ISO 17799 berdasar pada 10 control clauses yang menjadi fokus pengamatannya, yaitu:

1. Kebijakan Pengamanan *(Security Policy)*, mengarahkan visi dan misi manajemen agar kelangsungan organisasi dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan data/informasi penting yang dimiliki oleh perusahaan.

Kebijakan pengamanan sangat diperlukan mengingat banyaknya masalah-masalah non teknis seperti penggunaan *password* oleh lebih dari satu orang yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi. Kebijakan pengamanan ini meliputi aspek infratruktur dan regulasi keamanan informasi.

Hal pertama dalam pembuatan kebijakan keamanan adalah dengan melakukan inventarisasi data-data perusahaan. Selanjutnya dibuat regulasi yang melibatkan semua departemen, sehingga peraturan yang akan dibuat tersebut dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi untuk mendapatkan persetujuan dan dukungan agar dapat diterapkan dengan baik.

2. Pengendalian Akses Sistem (*System Access Control*), mengendalikan/membatasi akses *user* terhadap informasi-informasi dengan cara mengatur kewenangannya, termasuk pengendalian secara *mobile-computing* ataupun *tele-networking*. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada yang meliputi berbagai aspek seperti :

a. Persyaratan bisnis untuk kendali akses; b. Pengelolaan akses user (*User Access Management*); c. Kesadaran keamanan informasi (*User Responsibilities*); d. Kendali akses ke jaringan (*Network Access Control*); e. Kendali akses terhadap sistem operasi (*Operating System Access Control*); f. Pengelolaan akses terhadap aplikasi (*Application Access Management*); g. Pengawasan dan penggunaan akses sistem (*Monitoring System Access and Use*); dan h. *Mobile Computing* dan *Telenetworking.*

3. Pengelolaan Komunikasi dan Kegiatan (Communication and Operations Management), 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. Prosedur dan tanggung jawab operasional; b. Perencanaan dan penerimaan sistem; c. Perlindungan terhadap software jahat (*malicious software*); d. *Housekeeping*; e. Pengelolaan Network; f. Pengamanan dan Pemeliharaan Media; dan g. Pertukaran informasi dan software.

4. Pengembangan dan Pemeliharaan Sistem (*System Development and Maintenance*), memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi dan validasi.

Penelitian untuk pengembangan dan pemeliharaan sistem meliputi berbagai aspek, seperti : Persyaratan pengamanan sistem; Pengamanan sistem aplikasi; Penerapan Kriptografi; Pengamanan file sistem; dan Pengamanan pengembangan dan proses pendukungnya.

5. Pengamanan Fisik dan Lingkungan (*Physical and Environmental Security*), mencegah kehilangan dan/atau kerusakan data yang diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau dalam fasilitas penyimpan informasi yang lain.

Pengamanan fisik dan lingkungan ini meliputi aspek : Pengamanan area tempat informasi disimpan; Pengamanan alat dan peralatan yang berhubungan dengan informasi yang akan dilindungi; dan Pengendalian secara umum terhadap lingkungan dan hardware informasi.

6. Penyesuaian (*Compliance*), memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk perjanjian kontrak melalui audit sistem secara berkala. Aspek-aspek yang diperlukan untuk membentuk prosedur dan peraturan, yaitu : Penyesuaian dengan persyaratan legal; Peninjauan kembali kebijakan pengamanan dan penyesuaian secara teknis; serta Pertimbangan dan audit sistem.

7. Keamanan personel/sumber daya manusia (*Personnel Security*), upaya pengurangan resiko dari penyalahgunaan fungsi dan/atau wewenang akibat kesalahan manusia (*human error*), manipulasi data dalam pengoperasian sistem serta aplikasi oleh *user*. Kegiatan yang dilakukan diantaranya adalah pelatihan-pelatihan mengenai kesadaran informasi (*security awareness*) agar setiap *user*

mampu menjaga keamanan data dan informasi dalam lingkup kerja masing-masing.

Personnel Security meliputi berbagai aspek, *yaitu : Security in Job Definition and Resourcing*; Pelatihan-pelatihan dan *Responding to Security Incidens and Malfunction.*

8. Organisasi Keamanan (*Security Organization*), memelihara keamanan informasi secara global pada suatu organisasi atau instansi, memelihara dan menjaga keutuhan sistem informasi internal terhadap ancaman pihak eksternal, termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (*outsourcing*). Aspek yang terlingkupi, yaitu : keamanan dan pengendalian akses pihak ketiga dan *Outsourcing*

9. Klasifikasi dan pengendalian aset (*Asset Classification and Control*), memberikan perlindungan terhadap aset perusahaan yang berupa aset informasi berdasarkan tingkat perlindungan yang telah ditentukan. Perlindungan *aset ini meliputi accountability for Asset* dan klasifikasi informasi.

10. Pengelolaan Kelangsungan Usaha (*Business Continuity Management*), siaga terhadap resiko yang mungkin timbul didalam aktivitas lingkungan bisnis yang bisa mengakibatkan "*major failure*" atau resiko kegagalan sistem utama ataupun "*disaster*" atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan pengelolaan untuk kelangsungan proses bisnis, dengan mempertimbangkan semua aspek dari *business continuity management.*

IMPLEMENTASI PADA BUMN INDONESIA

Secara umum semua aspek keamanan informasi yang diatur dalam standar ini cocok untuk diterapkan oleh BUMN di Indonesia.Suatu organisasi yang menerapkan ISO 17799 akan mempunyai suatu alat untuk mengukur, mengatur dan mengendalikan informasi yang penting bagi operasional sistem mereka. Pada gilirannya ini dapat mendorong ke arah kepercayaan masyarakat, efisiensi dan efektifitas.

Basel II

Tujuan Pembentukan

Basel II dibentuk untuk menyempurnakan Basel I. Basel I (the 1988 Accord) dibentuk oleh BIS mengingat pentingnya permodalan pada perbankan. Basel I dirancang oleh komite Basel sebagai standar yang sederhana. Sistem ini dibuat sebagai penerapan kerangka pengukuran bagi risiko kredit, dengan mensyaratkan standar modal minimum adalah 8%. Sistem ini mensyaratkan bank-bank untuk memisahkan eksposurnya ke dalam kelas yang lebih luas, yang menggambarkan kesamaan tipe debitur.

Sebagaimana kita tahu, produk-produk perbankan semakin berkembang saat ini. Basel II dibentuk sebagai penyempurnaan Basel I. Basel II dibuat dengan kerangka perhitungan yang sama dengan Basel I, namun lebih *risk sensitive* serta memberikan insentif terhadap peningkatan kualitas penerapan manajemen risiko di bank.

Basel II dibentuk dengan tujuan memberikan kerangka perhitungan modal yang bersifat lebih sensitif terhadap risiko serta memberikan insentif terhadap peningkatan kualitas penerapan manajemen risiko bank. Tujuan ini sejalan dengan semakin berkembangnya produk-produk yang ada di dunia perbankan sehingga bank, kreditur, dan debitur dianggap memerlukan perlindungan dari sisi permodalan bank yang lebih kuat.

Stakeholder

Basel II digagas oleh BIS dalam Komite Basel. Di Indonesia implementasi Basel II diatur oleh BI dengan Peraturan Bank Indonesia (PBI) No. 5/8/PBI/2003 yang diperbarui dengan PBI No. 11/25/PBI/2009 tentang Penerapan Manajemen Risiko bagi Bnk Umum.

Pihak yang diuntungkan oleh Basel II secara tidak langsung adalah nasabah karena simpanan mereka lebih terjamin dengan modal perbankan yang lebih baik. Pihak yang merasa terbebani adalah perbankan. Perbankan menganggap situasi saat ini tidak normal, sehingga pemberlakuan Basel II dirasa menyulitkan. Direktur Utama BNI Gatot Suwondo mengatakan "Basel II aturannya ketat, sekarang situasi yang kita hadapi kan abnormal," pada Kamis 2 Juli 2009. Dalam kondisi tak menentu, pengetatan aturan akan membuat bank sulit untuk bergerak. Selain itu, pemberlakuan Basel II juga membutuhkan tambahan biaya baru bagi bank.

OVERVIEW BASEL II

Dalam Basel II, bank wajib menerapkan manajemen risiko secara efektif, baik untuk bank secara individual maupun bank secara konsolidasi dengan anak perusahaan.

Bank umum konvensional wajib menerapkan manajemen risiko untuk seluruh risiko. Dalam ketentuan ini ada 8 risiko yang merupakan prinsip Basel II. Sementara bank umum syariah wajib menerapkan manajemen risiko sekurang-kurangnya 4 jenis risiko, yaitu risiko kredit, risiko pasar, risiko likuiditas, dan risiko operasional.

Dijelaskan, untuk mempermudah integrasi antara Manajemen Risiko dan Tingkat Kesehatan bank, peringkat risiko dikategorikan menjadi 5 peringkat, yaitu 1 (Low), 2 (Low to Moderate), 3 (Moderate), 4 (Moderate to High), dan 5 (High). Bagi Bank Umum Syariah, peringkat risiko dikategorikan menjadi 3 peringkat, yaitu 1 (Low), 2 (Moderate), dan 3 (High).Untuk itu bank sentral memberlakukan masa transisi. Pertama, penerapan Manajemen Risiko bagi Bank Umum Konvensional untuk seluruh Risiko (8 risiko) dan penetapan penilaian peringkat Risiko yang dikategorikan dalam 5 peringkat berlaku sejak tanggal 1 Juli 2010.

Kedua, penerapan Manajemen Risiko bagi Bank Umum Konvensional untuk seluruh Risiko (8 risiko) dan penetapan penilaian peringkat Risiko yang dikategorikan dalam 3 peringkat sebagaimana diatur dalam PBI No.5/8/PBI/2003 tentang Penerapan Manajemen Risiko Bagi Bank Umum tetap berlaku sampai dengan tanggal 30 Juni 2010.

Konsep Pengendalian

Basel II bertujuan meningkatkan keamanan dan kesehatan sistem keuangan, dengan menitikberatkan pada perhitungan permodalan yang berbasis

risiko, supervisory review process, dan market discipline. Framework Basel II disusun berdasarkan forward-looking approach yang memungkinkan untuk dilakukan penyempurnaan dan penyesuaian dari waktu ke waktu. Hal ini untuk memastikan bahwa framework Basel II dapat mengikuti perubahan yang terjadi di pasar maupun perkembangan-perkembangan dalam manajemen risiko.

Basel II menghitung kebutuhan modal yang sesuai dengan profil risiko bank, serta memberikan insentif bagi peningkatan kualitas dalam praktek manajemen risiko di perbankan. Menggunakan berbagai alternatif pendekatan (approaches) dalam mengukur risiko kredit (credit risk), risiko pasar (market risk) dan risiko operasional (operational risk), maka hasilnya adalah perhitungan modal bank yang lebih sensitif terhadap risiko (risk sensitive capital allocation). Dalam Basel II, perhitungan modal bank ini dimuat dalam Pilar-1 Minimum Capital Requirement. Dalam berbagai alternatif pendekatan di atas pada dasarnya dapat dikelompokkan menjadi 2 (dua) kelompok besar yaitu pendekatan standar berlaku untuk seluruh bank (standardised model) dan model yang dikembangkan secara internal sesuai dengan karakteristik kegiatan usaha dan profil risiko individual bank (internal model) sehingga lebih sophisticated.

IMPLEMENTASI PADA BUMN INDONESIA

Penerapan Basel II telah dituangkan dalam PBI sehingga berlaku bagi seluruh bank termasuk bank dengan status BUMN. Penerapan Basel II cocok untuk BUMN mengingat perbankan kita pernah jatuh pada waktu krisis 1998. Dengan penerapan Basel II ini perbankan akan lebih kuat dari sisi permodalan sehingga akan lebih tahan terhadap gejolak ekonomi.