MODUL PERTEMUAN ONLINE
PROGRAM AUDIT SISTEM INFORMASI 1

A. PENDAHULUAN

Teknologi Informasi (TI) telah banyak dimanfaatkan oleh berbagai organisasi (termasuk di dalamnya institusi pemerintahan) di seluruh dunia. Pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan (*e-government*) akan meningkatkan efisiensi, efektivitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan. Hal itu, sesuai dengan tujuan pengembangan *e-government* di Indonesia berdasarkan Inpres No. 3 Tahun 2003, adalah untuk mengembangkan penyelenggaraan kepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi.

Untuk itu, agar usaha pemanfaatan TI berjalan seperti yang diharapkan tentunya diperlukan tata kelola TI yang baik. Keberhasilan *IT Governance* (tata kelola TI) sangat ditentukan oleh keselarasan penerapan TI dan tujuan organisasi. TI menjadi isu penting dalam strategi pengembangan dan peningkatan kinerja organisasi. Perubahan teknologi yang cepat menuntut keputusan TI yang tepat waktu. Evolusi lingkungan TI saat ini merupakan proses adaptasi alami menyesuaikan dengan lingkungan bisnisnya.

Berbagai *model best practices* tata kelola TI di dunia telah banyak diperkenalkan, seperti: COSO, COBIT, ITIL, IT Security, National Institute of Standards and Technology (NIST), British Standard Institution (BSI) Baselines, ISO/IEC 27002, ISO/IEC 385000, dan lain-lain. Masing-masing memiliki kelebihan dan kekurangan, beberapa model tata kelola TI tersebut dari sudut pandang strategis dan lainnya dikembangkan dari proses taktis seperti halnya manajemen proyek.

Pemerintah Indonesia telah mengeluarkan panduan tata kelola TIK Nasional bagi seluruh instansi pemerintah di Departemen atau LPND di tingkat pusat, Provinsi, dan Kabupaten/Kota melalui Permen Kominfo No. 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional. Kemudian diikuti dengan keluarnya Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik tahun 2011 yang disusun oleh Tim

Direktorat Keamanan Informasi.Kementerian Komunikasi dan Informatika RI. Pedoman yang telah ada dapat digunakan sebagai panduan umum dan dasar legalitas, namun *best practices* dunia lainnya yang telah ada tetap dapat digunakan sebagai referensi tambahan untuk melengkapi panduan lebih detail seperti dalam pengendalian dan penilaian kinerja.

Berbagai organisasi dari berbagai negara telah menetapkan beberapa penyesuaian dalam tata kelola TI, termasuk masalah audit TI. Hal tersebut dilakukan karena investasi pembangunan proyek TI untuk memenuhi tujuan dan menghasilkan nilai tambah sudah menjadi prioritas. Pengertian audit sendiri mencakup beberapa hal penting, antara lain: informasi yang dapat diukur dan kriteria yang telah ditetapkan; aktivitas mengumpulkan dan mengevaluasi bahan bukti; independensi dan kompetensi auditor; dan pelaporan hasil audit.

Pada tahun 2002, Sarbanes Oxley (SOX) mengadopsi Audit TI yang berperan dalam penjaminan keakuratan auditor keuangan OXLEY, Sarbanes-Oxley Act Of 2002, 2002. Di Eropa, Komite Basel II untuk Pengawasan Bank merekomendasikan kondisi-kondisi yang harus dipenuhi, seperti ukuran peningkatan modal, eksposur kredit, peningkatan kredit, manajemen risiko operasional dan sistem manajemen informasi melalui persyaratan yang jelas.

IT Governance adalah sebuah konsep yang dikembangkan oleh IT Governance Institute (ITGI) sebagai "bagian integral dari tata kelola perusahaan, yang terdiri dari struktur organisasi dan kepemimpinan, serta proses yang memastikan bahwa organisasi TI tersebut mendukung strategi dan tujuan organisasi

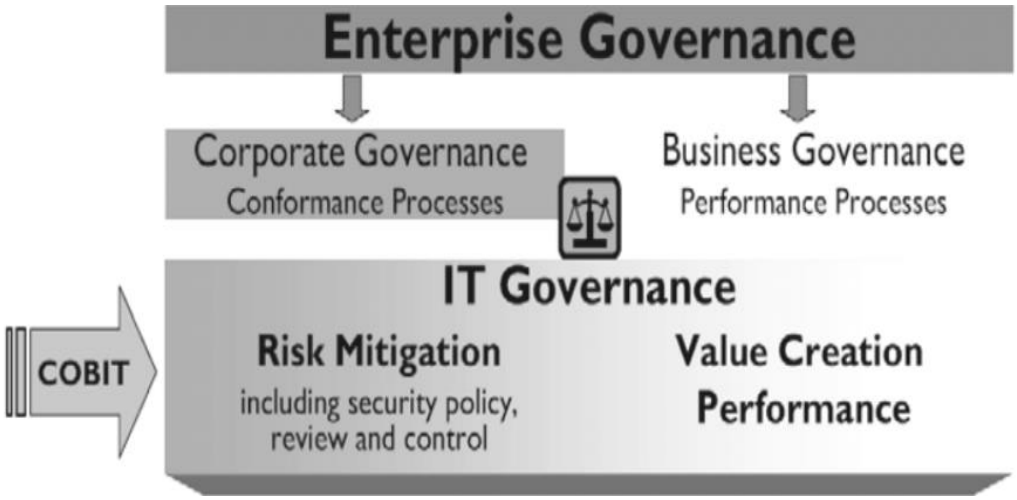
IT Governance Institute, Board Briefing on IT Governance, 2nd ed., 2003, www.itgi.org. Van Grembergen (2002) memberikan definisi IT Governance sebagai berikut: *IT Governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT*.

Weill & Ross (2004) mendefinisikan “IT Governance is defined as specifying the decision rights and accountability model to encourage desirable behavior in IT usage”.

IT Governance Institute (2007) mendefinisikan: “*IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the*

enterprise's IT sustains and extends the organisation's strategies and objectives".

Proses tata kelola dalam sebuah organisasi dapat terdiri dalam tiga kelompok, yaitu: (1) *Enterprise Governance*, (2). *Corporate Governance*, dan (3). *IT Governance* (*Institute de la Gouvernance des Systems d'Information, "The Place of IT Governance in the Enterprise Governance*" (2005) seperti tampak pada Gambar 1.



Gambar 1. Hubungan antara *Enterprise Governance, Corporate Governance*, dan *IT Governance*
(Sumber: Institute de la Gouvernance des Systems d'Information, 2005)

Enterprise Governance, digambarkan sebagai "kumpulan tanggung jawab dan praktik-praktik yang dilakukan oleh dewan dan manajemen eksekutif dengan tujuan menyediakan arah strategi, memastikan bahwa tujuan tercapai, memastikan bahwa risiko telah dikelola dengan tepat dan memverifikasi bahwa sumber daya perusahaan digunakan dengan bertanggung jawab "*IT Governance Institute, Board Briefing on IT Governance*."

Corporate Governance, didefinisikan sebagai salah satu elemen kunci dalam meningkatkan efisiensi, pertumbuhan ekonomi dan meningkatkan kepercayaan investor, dengan melibatkan hubungan antara manajemen perusahaan, dewan, pemegang saham dan stakeholders lainnya, serta menyediakan fondasi melalui tujuan perusahaan yang ditetapkan, cara mencapai tujuan tersebut dan memantau kinerja yang telah ditetapkan.

Van Grembergen menyatakan bahwa manajemen TI tetap menjadi aktor utama dalam proses tata kelola TI. Meskipun hubungan antara manajemen dan tata kelola TI merupakan dua konsep yang tetap berbeda. Manajemen TI bertanggung jawab atas layanan TI yang efektif dengan menyediakan layanan dan produk TI. Sementara tata kelola TI jauh lebih luas dan berfokus dalam memenuhi tuntutan pelanggan dan bisnis. Terdapat perbedaan dari berbagai literatur lainnya dari definisi tata kelola TI, namun tetap memiliki "benang merah" yang sama yaitu penekanan bahwa TI harus mendukung tujuan organisasi.

Dalam praktiknya, tata kelola TI harus mendukung kegiatan bisnis, memberikan nilai tambah komponen TI dan minimalisasi risiko TI. Untuk mencapai tujuan tersebut fokus tata kelola TI harus mencakup lima domain utama IT Governance Institute, *Board Briefing on IT Governance.1). IT Strategic Alignment, 2). IT Value Delivery, 3). Risk Management, 4). IT Resource Management, 5). Performance Measurement* seperti terlihat pada Gambar 2.

1) IT Strategic Alignment

   Domain tata kelola TI ini merupakan titik awal dalam merancang strategi TI sesuai dengan strategi organisasi secara menyeluruh. Dengan demikian, dimulai dengan rencana strategis organisasi, komite strategi TI harus sejalan dengan tujuan bisnis organisasi. Secara khusus, praktik tata kelola TI harus:

   - memastikan bahwa strategi TI sejalan dengan strategi bisnis
   - memastikan bahwa strategi TI memberikan peluang melalui pengukuran yang jelas
   - mengalokasikan anggaran investasi TI sesuai dengan tujuan bisnis
   - memastikan bahwa keputusan investasi teknologi selaras dengan tujuan bisnis.
   - menyediakan arah untuk menciptakan keuntungan kompetitif yang paralel dengan proses
   - mengarahkan strategi TI dengan mengatasi tingkat dan alokasi investasi, menyeimbangkan antara dukungan investasi dan pertumbuhan perusahaan, dengan pembuat keputusan sumber daya TI mana yang harus difokuskan
   - memastikan budaya keterbukaan dan kerja sama di antara bisnis, unit geografis dan fungsional perusahaan.

2) IT Value Delivery

   Tata kelola TI harus menargetkan kualitas layanan TI yang tepat dengan menggabungkan sumber daya anggaran dan faktor waktu. Praktek tata kelola TI dalam domain ini adalah:

   - memastikan bahwa rencana TI berlangsung sesuai jadwal
   - memastikan kelengkapan, kualitas dan keamanan investasi TI
   - memantau investasi TI untuk pengembalian investasi yang layak
   - memastikan manfaat layanan TI.

3) Risk Management

   Risiko pada tingkat organisasi tidak dapat dihilangkan, melainkan akan tetap ada sepanjang waktu, manajemen organisasi bertanggung jawab meminimalkan risiko ke tingkat yang wajar. Manajemen risiko harus menjadi proses berkesinambungan yang dimulai dengan menilai tingkat paparan organisasi dan mengidentifikasi insiden risiko utama. Setelah diidentifikasi, risiko harus diminimalkan dengan menggunakan prosedur pengendalian dan akhirnya risiko harus disesuaikan pada tingkat yang wajar.

   Praktik tata kelola TI untuk manajemen risiko adalah:

   - menganalisis dan menilai risiko TI
   - memantau efisiensi pengendalian internal
   - menerapkan kontrol yang diperlukan untuk meminimalkan risiko TI
   - dimasukkan ke dalam prosedur untuk memastikan transparansi risiko yang diinginkan perusahaan
   - mempertimbangkan bahwa pendekatan proaktif manajemen risiko dapat menciptakan keunggulan kompetitif
   - mendesak manajemen agar risiko dimasukkan dalam operasional perusahaan
   - memastikan bahwa manajemen telah menempatkan proses, teknologi dan jaminan untuk keamanan informasi dengan memastikan:
     - transaksi bisnis dapat dipercaya
     - layanan TI dapat digunakan, dapat
     - menolak serangan dan pulih dari kegagalan
     - menyembunyikan informasi penting dari mereka yang tidak memiliki hak akses

4) IT Resource Management

   Manajemen sumber daya berkaitan dengan manajemen sumber daya dan organisasi infrastruktur TI dalam sebuah perusahaan.

Aspek penting dari domain ini adalah masalah manajemen proyek. Manajemen proyek TI harus benar-benar diatur sebagai proyek-proyek yang memiliki dampak besar terhadap posisi keuangan dan arah strategis organisasi.

Praktek tata kelola TI untuk pengelolaan sumber daya adalah sebagai berikut:

- mengalokasikan sumber daya TI sesuai dengan prioritas bisnis
- melaksanakan pengendalian dengan memadai yang memungkinkan identifikasi infrastruktur TI lebih terpenuhi
- mempertahankan investasi yang layak dalam pengembangan staf, pengembangan pendidikan dan pelatihan operasional TI

5) Performance Measurement

Pengukuran kinerja berkaitan dengan penentuan apakah sistem TI telah mencapai tujuan yang ditetapkan oleh dewan dan manajemen senior. Untuk pengukuran kinerja TI, praktik tata kelola TI harus:

- bersama-sama manajemen menentukan dan memantau langkah-langkah untuk memastikan bahwa tujuan tercapai
- mengukur kinerja TI melalui metrik dan indikator yang memadai

Pelaksanaan kerangka kerja Tata Kelola TI apapun harus menyeimbangkan faktor internal maupun faktor eksternal yang relevan, seperti:

- fakta perkembangan teknologi: perkembangan TI yang cepat mensyaratkan bahwa keputusan terkait dengan TI dilakukan secara tepat waktu, dengan pemahaman penuh risiko terkait dengan tantangan TI.
- pengawasan fiskal: bahwa proyek TI memerlukan belanja mahal yang kadang-kadang menyebabkan keraguan dan akuntabilitas penurunan sumber daya keuangan.
- inovasi dan kontrol atas TI: dalam kasus di mana inovasi (baru proyek TI) didukung oleh TI, mungkin bertentangan dengan kontrol atas lingkungan TI.
- up to date infrastruktur: infrastruktur teknologi menjadi ketinggalan zaman dari waktu ke waktu. Menjaga agar tetap up to date adalah suatu keharusan bagi setiap departemen

Dapat dinyatakan bahwa fokus lima domain bidang tata kelola TI adalah faktor fundamental dalam proses pengambilan keputusan. Dan pada akhirnya tujuan tata kelola TI adalah tercapainya keselarasan antara investasi TI dengan tujuan bisnis, menjamin

penggunaan sumber daya TI yang bertanggung jawab, dan meyakinkan bahwa TI berada dalam batas-batas anggaran dan rencana strategis TI yang disetujui.

B. AUDIT SI

Audit Sistem Informasi memiliki beberapa fokus tujuan, salah satunya adalah pada tata kelola TI atau *IT Governance*. Tata kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada sistem teknologi informasi (TI) serta manajemen kinerja dan risikonya.

IT governance adalah istilah inklusif yang mencakup sistem informasi, teknologi, dan komunikasi, bisnis, masalah hukum dan lainnya, dan semua *stakeholder* bersangkutan, direktur, manajemen senior, pemilik proses, TI pemasok, pengguna dan auditor.

Jenis-jenis audit Sistem Informasi dikelompokkan berdasarkan Luas Pemeriksaan, Bidang Pemeriksan dan Kelompok Pelaksana Audit (Auditor).

1. Jenis-jenis audit ditinjau dari luas pemeriksaan
   a. **Pemeriksaan Umum *(General Audit)***
      Merupakan suatu pemeriksaaan umum atas laporan keuangan yang dilakukan oleh Kantor Akuntan Publik (KAP) yang indipendent dengan tujuan dapat menilai sekaligus memberikan opini mengenai kewajaran laporan keuangan.
   b. **Pemeriksaan Khusus *(Special Audit)***
      Merupakan suatu pemeriksaan yang hanya terbatas hanya pada permintaan audit yang dilakukan oleh Kantor Akuntan Publik (KAP). Dengan memberikan opini
2. Jenis-jenis audit ditinjau dari bidang pemeriksaan
   a. **Audit Laporan Keuangan (*Financial Statement Audit)***
      Berkaitan dengan kegiatan mengumpulkan dan mengevaluasi bukti tentang laporan-laporan suatu entitas dengan tujuan memberikan pendapat (opini) tentang laporan tersebut apakah sesuai dengan kriteria yang ditetapkan sesuai prinsip-prinsip akuntansi yang berlaku umum.
   b. **Audit Operasional *(Management Audit)***
      Adalah jenis pemeriksaan terhadap kegiatan operasi suatu perusahaan. meliputi kebijakan akuntansi dan kebijakan operasional manajemen yang telah ditetapkan, dengan tujuan untuk mengetahui kegiatan operasi yang dilakukan berjalan secara efektif dan efisien.

c. **Audit Ketaatan *(Compliance Audit)***

   Audit ketaatan berfungsi untuk menentukan sejauh mana perusahaan mentaati peraturan, kebijakan, peraturan pemerintah bahkan hukum yang harus dipatuhi oleh entitas yang di audit.

d. **Audit Sistem Informasi**

   Yaitu pemeriksaan yang dilakukan Kantor Akuntan Publik (KAP) terhadap perusahaan yang melakukan proses data akuntansi, umumnya menggunakan system *Elektronik Data Processing*(EDP). Auditor harus memperhatikan hal-hal berikut :

   - Perlengkapan keamanan melindungi perlengkapan computer baik program, komunikasi, atau data dari akses yang tidak sah, modifikasi bahkan penghancuran.
   - Pengembangan program yang dilakukan atas otorisasi khusus dan umum dari pihak manajemen perusahaan.
   - Pemrosesan transaksi, file, laporan dan catatan computer dengan akurat dan lengkap.
   - Data file laporan yang tersimpan di computer sangat dijaga kerahasiaanya.

e. **Audit Forensik**

   Tujuan dilakukan audit forensic adalah sebagai upaya pencegahan terjadinya kecurangan (*fraud).* Hal yang dapat dilakukan audit forensik termasuk :

   - Investigasi kriminal
   - Indikasi kecurangan dalam bisnis atau karyawan
   - Mengetahui kerugian suatu bisnis

f. **Audit Investigasi**Yang dimaksud audit investigasi adalah serangkaian kegiatan mengenali *(recorganized),*menidentifikasi *(Identify)* dan menguji *(examine)* fakta-fakta dan informasi yang ada guna mengungkap kejadian yang sebenarnya dalam rangka pembuktian demi mendukung proses hukum atas dugaan penyimpangan yang dapat merugikan keuangan suatu entitas (organisasi/perusahaan/negara/daerah).

g. **Audit Lingkungan**

   Menurut (Kep. Men. LH 42/1994) audit lingkungan adalah proses manajemen yang meliputi evaluasi secara sistematik, tercatat (terdkumentasi), serta obyektif tentang bagaimana suatu kinerja manajemen organisasi yang bertujuan memfasilitasi kendali manajemen terhadap upaya pengendalian dampak lingkungan dan pemanfaatan kebijakan usaha terhadap perundang-undangan tentang pengelolaan lingkungan.

3. Jenis-jenis audit ditinjau dari kelompok pelaksana audit (auditor)
   a. **Auditor Internal**
      Mempunyai tugas membantu manajemen puncak *(top management)* dalam mengawasi asset *(saveguard of asset)* dan mengawasi kegiatan operasional perusahaan sehari-hari. bekerja untuk perusahaan yang mereka audit, oleh karena itu tugas auditor intern adalah mengaudit manajemen perusahaan termasuk *compliance* audit.
   b. **Auditor Ekstern**
      Bekerja untuk lembaga/kantor akuntan publik (pihak ke-3) yang statusnya diluar struktur perusahaan yang mereka audit dan bekerja secara independent dan objektif. Umumnya auditor ekstern menghasilkan laporan *financial* audit.
   c. **Auditor Pajak**
      Mempunyai tugas melakukan ketaatan wajib pajak yang diaudit menurut undang-undang perpajakan yang berlaku. Di Indonesia dilaksanakan oleh Direktorat Jendral Pajak (DJP) yang berada dibawah naungan Departemen Keuangan Republik Indonesia.
   d. **Auditor Pemerintah**
      Adalah lembaga yang mempunyai tugas menilai kewajaran informasi laporan keuangan instansi pemerintah atas pelaksanaan program dan penggunaan asset milik pemerintah. Audit instansi pemerintah umumnya dilaksanakan oleh Badan Pemeriksa Keuangan (BPK) atau Badan Pemeriksa Keuangan dan Pembangunan (BPKP).

Auditor TI bertanggung jawab atas penilaian efisiensi tata kelola TI dengan tingkatan prosedur dalam pelaksanaannya. Auditor TI (dari dalam organisasi atau independen) dapat melakukan sejumlah peran kunci dalam Gary Hardy, “The Role of the IT Auditor in IT Governance” 1 (2009): 1–2 :

- memulai program tata kelola TI: menjelaskan tata kelola TI dan nilainya pada manajemen
- menilai kondisi saat ini: memberikan masukan dan membantu memberikan penilaian kondisi yang sebenarnya
- merencanakan solusi tata kelola TI
- memantau inisiatif tata kelola TI
- membantu membuat bisnis tata kelola TI, seperti : memberikan input objektif dan konstruktif, mendorong penilaian diri, dan memberikan keyakinan kepada manajemen bahwa tata kelola bekerja secara efektif.

Karakteristik audit mencakup tiga ciri dasar sebagai berikut (Pusat Pendidikan Dan Pelatihan Pengawasan Badan Pengawasan Keuangan dan Pembangunan, 2009):

- Auditing merupakan suatu proses penilaian.
- Penilaian tersebut dilakukan terhadap informasi, kondisi, operasi, dan/atau pengendalian.
- Penilaian harus dilakukan secara objektif oleh pihak yang kompeten dan independen.

Organisasi sektor publik dalam hal ini pemerintahan, mendapatkan amanah dan kepercayaan dari masyarakat untuk menggunakan sumber daya publik. Oleh karenanya, dituntut pengelolaan sumber daya tersebut secara akuntabel dan transparan. Selanjutnya untuk meningkatkan pengelolaan tersebut diperlukan audit pada sektor publik. Secara umum tidak ada perbedaan mendasar antara audit sektor publik dan privat. Namun diperlukan perhatian khusus, karena karakteristik manajemen sektor publik berkaitan erat dengan kebijakan dan pertimbangan politik serta ketentuan perundang-undangan.

Berdasarkan UU No. 15 tahun 2004 terdapat tiga jenis audit menurut tujuan pelaksanaan audit, yaitu: audit keuangan, audit kinerja dan audit dengan tujuan tertentu.

- Audit keuangan adalah untuk menentukan apakah informasi keuangan telah akurat dan dapat diandalkan (sesuai Standar Akuntansi Pemerintahan/SAP), serta untuk memberikan opini kewajaran atas penyajian laporan keuangan.
- Audit kinerja adalah pemeriksaan atas pengelolaan keuangan negara yang terdiri atas pemeriksaan aspek ekonomi dan efisiensi serta pemeriksaan aspek efektivitas. Dalam melakukan audit kinerja, auditor juga menguji kepatuhan terhadap ketentuan perundang-undangan serta pengendalian intern. Audit kinerja menghasilkan temuan, simpulan, dan rekomendasi. Menentukan: keandalan informasi kinerja, tingkat ketaatan, pemenuhan standar mutu operasi, efisiensi, ekonomis, dan efektivitas.
- Audit dengan tujuan tertentu adalah pemeriksaan yang tidak termasuk dalam pemeriksaan keuangan dan pemeriksaan kinerja/audit operasional. Sesuai dengan definisinya, jenis audit ini dapat berupa semua jenis audit, selain audit keuangan dan audit operasional. Jenis audit ini termasuk di antaranya audit ketaatan dan audit investigatif. Audit ketaatan bertujuan untuk menentukan apakah peraturan ekstern

serta kebijakan dan prosedur intern telah dipenuhi. Audit investigatif bertujuan untuk menentukan apakah kecurangan/ penyimpangan benar terjadi.

Di dalamnya, belum diatur secara khusus mengenai audit yang difokuskan pada manajemen kinerja dan risiko dalam sistem pengelolaan Teknologi Informasi (TI) di instansi pemerintah. Kemudian untuk menunjang hal tersebut, diperlukan metodologi audit yang tujuannya berbeda dengan metode pada audit keuangan, audit kinerja dan audit dengan tujuan tertentu.

Dikarenakan audit memegang peranan penting sebagai salah satu bentuk pengawasan pada instansi pemerintah, maka perlu dipertimbangkan agar pemerintah Indonesia membuat pedoman audit yang memiliki tujuan khusus dalam pemeriksaan tata kelola TI di instansi pemerintah. Tujuannya adalah melakukan penilaian atas tata kelola TI dengan tingkatan prosedur dalam pelaksanaannya, serta memberikan masukan dan solusi pada instansi pemerintah agar tata kelola TI bekerja secara efektif dan efisien. Untuk itulah diusulkan sebuah metodologi audit tata kelola TI di instansi pemerintah Indonesia, yang diharapkan dapat memberikan manfaat dan dijadikan sebagai pedoman dalam audit tata kelola TI.

Tujuan audit sistem informasi pada tata kelola TI diantaranya adalah:

1. **Meningkatkan pengamanan aset**
   Asset (aktiva) yang berhubungan dengan instalasi sistem informasi mencakup: perangkat keras, perangkat lunak, fasilitas, manusia, *file* data, dokumentasi sistem, dan peralatan pendukung lainnya. Sama halnya dngan aktiva – aktiva lainnya, maka aktiva ini juga perlu dilindungi dengan memasang pengendalian internal. Perangkat keras bisa rusak karena unsur kejahatan ataupun sebab-sebab lain. Perangkat lunak dan isi *file* data dapat dicuri. Peralatan pendukung dapat dihancurkan atau digunakan untuk tujuan yang tidak diotorisasi. Karena konsentrasi aktiva tersebut berada pada lokasi pusat sistem informasi, maka pengamanannya pun menjadi perhatian dan tujuan yang sangat penting.
2. **Menjaga integritas data**
   Integritas data merupakan konsep dasar audit sistem informasi. Integritas data berarti data memiliki atribut: kelengkapan (*completeness*), sehat dan jujur (*soundness*), kemurnian (*purity*), ketelitian (*veracity*). Tanpa menjaga integritas data, organisasi tidak

dapat memperlihatkan potret dirinya dengan benar akibatnya, keputusan maupun langkah-langkah penting di organisasi salah sasaran karena tidak didukung dengan data yang benar.

3. **Meningkatkan efektivitas system**
   Sistem informasi dikatakan efektif hanya jika sistem tersebut dapat mencapai tujuannya. Untuk menilai efektivitas sistem, auditor sistem informasi harus tahu mengenai kebutuhan pengguna sistem atau pihak-pihak pembuat keputusan yang terkait dengan layanan sistem tersebut. Selanjutnya, untuk menilai apakah sistem menghasilkan laporan / informasi yang bermanfaat bagi penggunanya, auditor perlu mengetahui karakteristik user berikut proses pengambilan keputusannya.

4. **Mengingkatkan efisiensi sumber daya**
   Suatu sistem sebagai fasilitas pemrosesan informasi dikatakan efisien jika ia menggunakan sumber daya seminimal mungkin untuk menghasilkan *output* yang dibutuhkan. Efisiensi sistem pengolahan data menjadi penting apabila tidak ada lagi kapasitas sistem yang menganggur.

Dari rumusan model risiko audit ada 4 (empat) jenis risiko audit. Masing-masing jenis risiko audit tersebut akan dijelaskan sebagai berikut:

1. **Planned Detection Risk (Risiko Penemuan yang Direncanakan)**
   Risiko bahwa bukti yang dikumpulkan dalam segmen gagal menemukan kekeliruan yang melampaui jumlah yang dapat ditolerir.

2. **Acceptable Audit Risk (Risiko Audit yang dapat diterima)**
   Ukuran atas tingkat kesediaan auditor untuk menerima kenyataan bahwa laporan keuangan mungkin masih mengandung salah saji yang material setelah audit selesai dilaksanakan serta suatu laporan audit wajar tanpa syarat telah diterbitkan.

3. **Inherent Risk (Risiko Bawaan atau Risiko Melekat)**
   Suatu ukuran yang dipergunakan oleh auditor dalam menilai adanya kemungkinan bahwa terdapat sejumlah salah saji yang material (kekeliruan atau kecurangan) dalam suatu segmen sebelum ia mempertimbangkan keefektifan dan pengendalian intern yang ada.

4. **Control Risk (Risiko Pengendalian)**
   Ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien.

Audit sistem informasi pada tata kelola TI yang sering dilakukan adalah menggunakan kerangka kerja COBIT. Contoh penerapannya dapat disimak pada paper Setia Wardani dan Mita Puspita Sari dari Fakultas Teknik Universitas PGRI Yogyakarta (UPY) tahun 2014 dengan judul *"Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT Dengan Model Maturity Level".*

C. AUDIT TATA KELOLA TI

Tata Kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada Sistem/Teknologi informasi serta manajemen Kinerja dan risikonya. Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola resiko-resiko terkait TI.

IT Governance terdiri dari struktur organisasi, kepemimpinan, dan proses yang memastikan IT dapat mendukung strategi dan tujuan organisasi. Ada 5 komponen dari IT Governance yaitu Struktur Organisasi dan Governance, Kepemimpinan dan Dukungan Eksekutif, Perencanaan strategis dan opresional, Penyampaian Service dan pengukuran, Organisasi IT dan Manajemen Resiko.

Audit *IT Governance* membutuhkan pengetahuan yang lebih dibandingkan audit Sistem Informasi biasa karena auditor TI harus mengevaluasi sejauh mana TI mendukung strategi bisnis. Audit sistem informasi umumnya digunakan untuk menjelaskan perbedaan jenis aktivitas yang terkait dengan komputer. Seperti untuk menjelaskan pengkajian ulang proses dan evaluasi pengendalian internal dalam sebuah sistem pemrosesan data elektronik. Sementara audit *IT Governance* mencakup lingkup yang lebih luas, bertujuan untuk memeriksa apakah tata kelola sumber daya TI (termasuk di dalamnya manajemen organisasi dan pimpinan) dapat mendukung dan sejalan dengan strategi bisnis.

Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia:

- mengalokasikan sumber daya TI sesuai dengan prioritas bisnis
- melaksanakan pengendalian dengan memadai yang memungkinkan identifikasi infrastruktur TI lebih terpenuhi

- mempertahankan investasi yang layak dalam pengembangan staf, pengembangan pendidikan dan pelatihan operasional TI .

DAFTAR PUSTAKA

1. Setiawan, H. & Mustofa, H. 2013. Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia. *IPTEK-KOM*, Vol. 15 No. 1 Juni 2013: 1-15
2. Indrajit, R.E. 2016. Konsep Dasar Tata Kelola Teknologi Informasi. The Preinexus Indonesia.
3. ITGI. 2005. IT Governance A Framework for Performance and Compliance: Board briefing on IT governance. www.itgi.org