

## **Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia**

### ***Audit Method for Information Technology Governance in Indonesian Government Agencies***

**Herri Setiawan<sup>1\*</sup> dan Khabib Mustofa<sup>2</sup>**

<sup>1</sup>Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri Palembang  
Jl. Jenderal Sudirman No. 629 Palembang, *e-mail*: herri.setiawan@mail.ugm.ac.id

\*Alamat Korespondensi Penulis

<sup>2</sup>Jurusan Ilmu Komputer dan Elektronika, Fakultas MIPA, Universitas Gadjah Mada Yogyakarta  
Sekip Utara Yogyakarta, 55281, *e-mail*: khabib@ugm.ac.id

Naskah diterima: 03 Maret 2013, direvisi: 05 April 2013, disetujui: 24 Mei 2013

#### **Abstrak**

Dalam rangka menciptakan nilai tambah dan meminimalkan risiko Teknologi Informasi (TI) dibutuhkan manajemen pengelolaan semua sumber daya TI yang efisien dan efektif, antara lain melalui *IT Governance* (Tata Kelola TI). Berdasarkan tujuannya, audit Tata kelola TI memiliki tujuan yang berbeda dengan tiga jenis audit berdasarkan UU No. 15 tahun 2004, karena audit ini bertujuan khusus untuk memeriksa pengelolaan seluruh sumber daya TI (termasuk di dalamnya manajemen organisasi dan pimpinan), apakah dapat mendukung dan sejalan dengan strategi bisnis. Dibandingkan audit di sektor privat, audit di sektor publik dalam hal ini di instansi pemerintah, memerlukan perhatian khusus, karena karakteristik manajemen sektor publik berkaitan erat dengan kebijakan dan pertimbangan politik serta ketentuan perundang-undangan. Penelitian ini mengusulkan sebuah metode audit tata kelola TI di instansi pemerintah. Metode yang dihasilkan dapat dijadikan sebagai salah satu acuan auditor pemerintah dalam mengevaluasi risiko yang terkait dengan Tata Kelola TI di instansi pemerintah.

**Kata kunci:** Teknologi Informasi, tata kelola, instansi pemerintah, audit

#### **Abstract**

*In order to create added value and minimize Information Technology (TI) risk, it requires supervision management of all IT resources efficiently and effectively, for example through IT Governance (IT Governance). By design, IT governance audit has different goals with three types of audits in accordance with Law no. 15 of 2004, because the aim of audit is specifically to examine the management of all IT resources (including management and leadership organizational) whether they can support and align with business strategies. Compared with private sector audit, public sector audit in government agencies, need a special attention, due to the characteristics of public sector management is closely related to policy and political considerations, and the provisions of legislation. This study proposes an audit method of IT governance in government agencies. The result of this study can be used as a reference by government auditors in evaluating the risks associated with IT Governance in government agencies.*

**Keywords:** Information Technology, governance, government agencies, audit

## 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 pemerintahan 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 mengoptimalkan 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 (Arens et. al., 2006).

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.

Menurut Iliescu (2010), 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.

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 eksternal 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.

*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 terse-

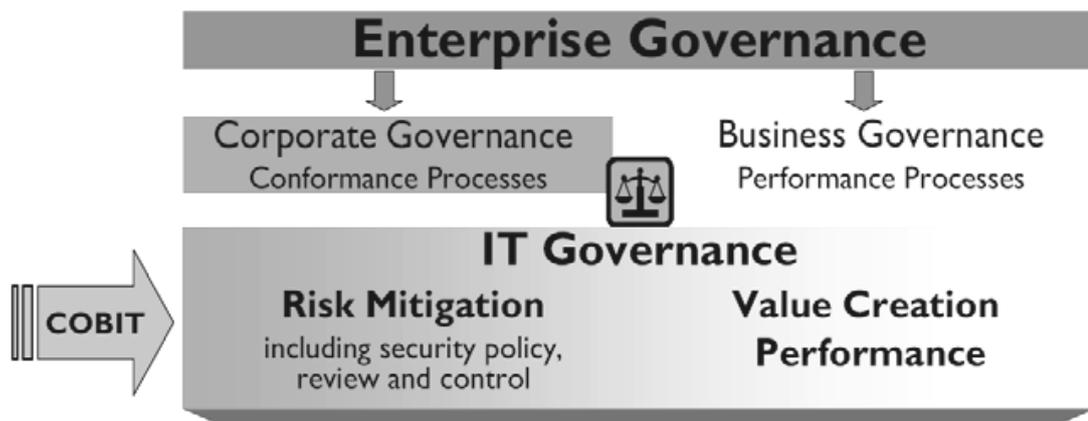
but mendukung strategi dan tujuan organisasi *IT Governance Institute, Board Briefing on IT Governance, 2nd ed., 2003, www.itgi.org..*

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 (Organisation For Economic Co-Operation And Development, 2004).

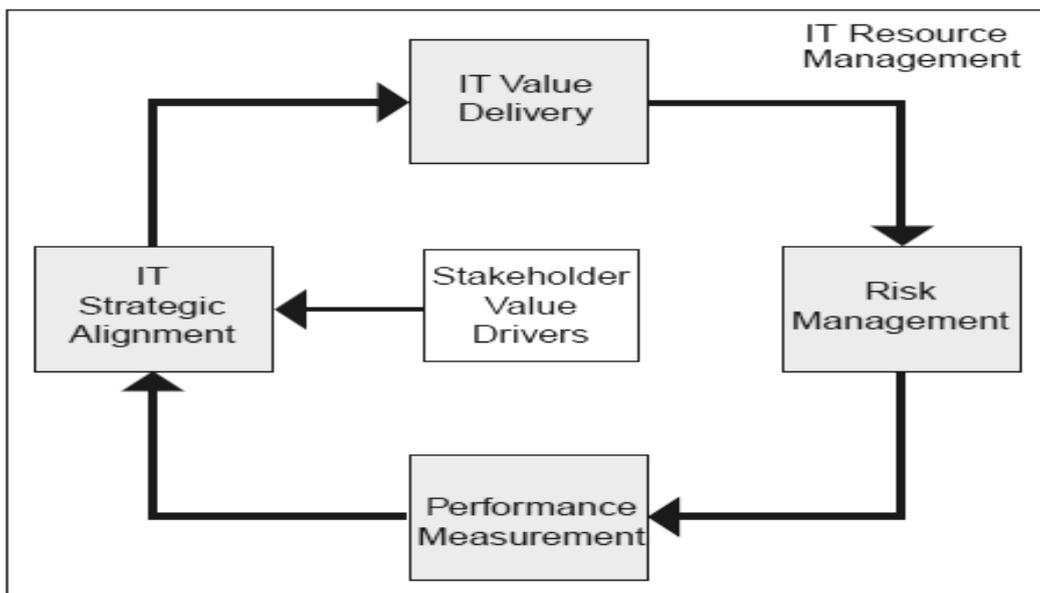
Van Grembergen (Haes & Grembergen, 2004) menyatakan bahwa manajemen TI tetap menjadi aktor utama dalam proses tata kelola TI. Meskipun hubungan antara manajemen dan tata kelola TI merupakan dua konsep yang tetap berbeda. Manajemen TI bertanggung

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:



**Gambar 2. Fokus Tata Kelola TI**  
(Sumber : *IT Governance Institute*, 2003)

- 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

kasi 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.

Berbagai pendapat para ahli telah mendefinisikan istilah “audit”. Salah satunya menurut Arens et al (2006) mendefinisikan: *Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person.* Definisi tersebut dapat diartikan bahwa *auditing* adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang dimaksud. Auditing seharusnya dilakukan oleh orang yang berkompeten dan independen.

Menurut Kutsikos (2007), dalam audit diperlukan kerangka kerja yang menyediakan standar sebagai sumber perencanaan audit. Melalui analisis *best practice* dalam bidang TI (seperti ITIL, COBIT, ISO27001), diusulkan metode pelaksanaan audit TI berdasarkan langkah-langkah sebagai berikut (Amancei and Surcel, 2010): 1). toleransi organisasi terhadap ketersediaan sistem TI, 2). identifikasi area dan subarea yang akan diaudit, 3). faktor risiko dan bobot yang terkait, 4). tingkat, total skor dan peringkat risiko yang signifikan, 5). melakukan prosedur audit berdasarkan kuesioner dan pengujian, 6). penilaian terhadap sisa risiko gabungan.

Tujuan dari pedoman *IT Governance* adalah memberikan informasi bagaimana SI auditor harus melakukan pendekatan audit *IT Governance*. Mencakup posisi auditor TI yang tepat di dalam organisasi, hal yang perlu

dipertimbangkan ketika merencanakan audit, dan bukti untuk menelaah saat melakukan audit (Cilli, 2003). Audit *IT Governance* membutuhkan pengetahuan yang lebih dibandingkan audit Sistem Informasi biasa (IS Auditor), karena auditor harus mengevaluasi TI yang memungkinkan strategi bisnis berjalan sesuai harapan (Iliescu, 2010). Dalam penelitiannya diusulkan penggunaan *Val IT Framework* sebagai *best practice* dalam menentukan tolok ukur temuan. Seperti yang didefinisikan dalam *Val IT Framework*, tiga domain berikut merupakan bagian yang akan dievaluasi dalam audit *IT Governance*, yaitu: evaluasi nilai *governance*, evaluasi manajemen portofolio, dan evaluasi manajemen investasi.

Dalam penelitian Radovanovic et al., (2010) dijelaskan konsep audit sistem informasi dan metode yang digunakan. Metode yang diterapkan adalah: metode analisis, metode abstraksi, metode spesialisasi dan metode deduksi. Organisasi dapat mempertimbangkan untuk menggunakan beberapa metode dan standar seperti: COBIT, ITIL, COSO, ISO 27002 (ex ISO 17799) dan ISO 9000.

Penelitian yang dilakukan oleh Lusiani (2009), tata kelola TI belum sesuai dengan kebutuhan pemerintah daerah di Indonesia sehingga perlu suatu standar nasional dalam tata kelola IT. Penyusunan standar tersebut dapat dilakukan dengan mengadopsi standar yang ada dan disesuaikan dengan aturan, hukum dan dengan mempertimbangkan proses bisnis dan risiko yang ada di Indonesia. Secara garis besar audit dengan menggunakan COBIT memiliki prinsip dasar *Business Requirement*, *IT Resources*, dan *IT Process*. Penelitian lain juga menggunakan COBIT (Budiono, 2010; Purwanto, 2010; Yulianti & Patria, 2011) sebagai acuan dalam audit kinerja sistem informasi.

Di dalam Undang-Undang Republik Indonesia Nomor 15 Tahun 2004 Tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara, dikatakan bahwa pemeriksaan adalah proses identifikasi masalah, analisis, dan evaluasi yang dilakukan

secara independen, objektif, dan profesional berdasarkan standar pemeriksaan, untuk menilai kebenaran, kecermatan, kredibilitas, dan keandalan informasi mengenai pengelolaan dan tanggung jawab keuangan negara.

Peraturan Menteri Negara Pendayagunaan Aparatur Negara Nomor: Per/05/M.PAN/03/2008 tentang Standar Audit Aparat Pengawasan Intern Pemerintah mendefinisikan, Audit adalah proses identifikasi masalah, analisis, dan evaluasi bukti yang dilakukan secara independen, objektif dan profesional berdasarkan standar audit, untuk menilai kebenaran, kecermatan, kredibilitas, efektifitas, efisiensi, dan keandalan informasi pelaksanaan tugas dan fungsi instansi pemerintah. Dijelaskan bahwa Aparat Pengawasan Intern Pemerintah (APIP) adalah instansi pemerintah yang mempunyai tugas pokok dan fungsi untuk melakukan pengawasan. Instansi tersebut meliputi: Badan Pengawasan Keuangan dan Pembangunan (BPKP), inspektorat jenderal/inspektorat utama/ inspektorat kementerian/lembaga, inspektorat pemerintah provinsi, serta inspektorat pemerintah kabupaten/kota. Selanjutnya didefinisikan, Auditor adalah pegawai negeri sipil (PNS) yang mempunyai jabatan fungsional auditor dan/atau pihak lain yang diberi tugas, wewenang, tanggung jawab dan hak secara penuh oleh pejabat yang berwenang melaksanakan pengawasan pada instansi pemerintah untuk dan atas nama APIP. Sehingga pengertian auditor dalam hal ini bisa merujuk pada individu yang melakukan audit, maupun institusi yang memerintahkan individu tersebut melakukan audit. Menurut pihak yang melakukannya, jenis audit terdiri dari Audit Intern dan Audit Ekstern, sementara jenis audit menurut tujuan pelaksanaan audit terdiri dari Audit Keuangan, Audit Kinerja/ Operasional dan Audit dengan Tujuan Tertentu.

Dalam struktur pemerintahan di Indonesia, institusi tersebut meliputi Badan Pemeriksa Keuangan (BPK), Badan Pengawasan Keuangan dan Pembangunan (BPKP), Inspektorat Jenderal Departemen, Unit

Pengawasan pada Lembaga Pemerintah Non Departemen (LPND) dan Lembaga Negara, Badan Pengawasan Daerah (Bawasda) atau Inspektorat Provinsi dan Kabupaten/Kota.

Dari berbagai pemahaman atas tinjauan pustaka mengenai *IT Governance* dan audit, dapat disimpulkan bahwa Audit *IT Governance* adalah suatu bagian dari tata kelola organisasi (atau instansi pemerintah) yang berfokus pada manajemen kinerja dan risiko dalam sistem Teknologi Informasi (TI). Sedangkan berdasar tujuannya, audit tata kelola TI belum diatur secara khusus di instansi pemerintah Indonesia.

## **METODE**

Penelitian ini memiliki tujuan untuk mengusulkan metodologi audit tata kelola TI di instansi pemerintah Indonesia. Metodologi yang diusulkan ini berdasarkan kerangka teori dari kajian literatur, perundang-undangan, *IS Auditing Standard IT Governance*; Document S10, *IS Auditing Guideline IT Governance*; Document G18, dan ISACA *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*.

Berbeda dengan audit keuangan, audit kinerja dan audit dengan tujuan tertentu, lingkup audit tata kelola TI tidak dapat dilakukan secara parsial, namun harus dilakukan secara utuh dengan melibatkan semua bagian instansi yang menggunakan sumber daya TI. Setiap langkah audit *IT Governance* yang diusulkan berpedoman pada ruang lingkup *best practices* bidang *IT Governance*.

Selanjutnya, auditor yang melakukan audit tata kelola TI dituliskan sebagai Auditor TI. Kerangka kerja dan langkah-langkah proses audit TI yang diusulkan, meliputi:

### **Praaudit**

Auditor TI harus memastikan dengan jelas lingkup dan tanggung jawab pekerjaan, termasuk definisi yang jelas tentang bidang fungsional dan isu-isu yang akan dibahas, serta kemudahan akses data dan informasi yang dibutuhkan.

### **Perencanaan**

Auditor TI harus memiliki informasi tentang struktur dan tanggung jawab masing-masing bagian tata kelola TI, mengidentifikasi dan memiliki pemahaman umum atas proses tata kelola TI yang berjalan dan informasi rencana strategi sistem informasi.

Tujuan audit Tata Kelola TI harus difokuskan pada penilaian tingkat keselarasan dan integrasi strategi TI dengan strategi bisnis, penilaian terhadap *output* komponen TI dan nilai tambah yang disediakan organisasi.

Ruang lingkup audit harus mencakup proses-proses audit yang relevan untuk perencanaan, pengorganisasian dan proses pemantauan aktivitas TI. Tim Auditor TI harus memiliki keahlian dan kompetensi yang memadai.

### **Pelaksanaan**

Untuk mengumpulkan bukti yang paling relevan dan spesifik, auditor TI menganalisis dan menilai area kritis yang diidentifikasi dalam langkah perencanaan, berupa: Proses Perencanaan Strategis Bisnis; Proses Perencanaan Strategis TI; Manajemen Layanan TI; Manajemen Investasi TI; Manajemen Proyek TI; Manajemen Risiko TI; Proses Pengukuran Kinerja TI, sesuai dengan standar dan aturan perundang-undangan yang berlaku.

### **Pelaporan**

Panduan audit tata kelola TI merekomendasikan bahwa laporan audit harus mencakup a). deskripsi prosedur kunci manajemen tingkat atas dan dokumen pendukung terkait telah dibentuk untuk menyediakan sistem pengelolaan TI yang efektif, b). informasi utama tentang risiko yang tidak terkontrol, c). informasi pada setiap struktur kontrol yang tidak efektif dan tidak efisien, d). informasi tentang ketidakpatuhan apapun sesuai kebijakan organisasi atau aturan perundang-undangan, e). kesimpulan Auditor secara menyeluruh tentang tata kelola TI sebagaimana didefinisikan dalam referensi.

### Tindak Lanjut

Auditor TI harus memastikan rekomendasi yang dibuat dalam laporan audit telah diterapkan.

### HASIL DAN PEMBAHASAN

Berdasarkan kerangka kerja yang diusulkan, maka langkah-langkah tim Audit TI dalam implementasinya adalah sebagai berikut:

#### Praaudit

Secara umum teknik audit *IT Governance* di sektor publik dan sektor privat memiliki kesamaan, hanya saja audit *IT Governance* di sektor publik memerlukan perhatian khusus, karena karakteristik manajemen sektor publik berkaitan erat dengan kebijakan dan pertimbangan politik serta ketentuan perundang-undangan.

Berdasar Permen PAN No.: 05/PER/M.PAN/03/2008, pelaksana audit dapat menggunakan auditor dari Aparat Pengawasan Intern Pemerintah (APIP), dengan persyaratan tambahan memiliki pengetahuan dan keterampilan dalam pemahaman konsep *IT Governance*.

Tugas dan tanggung jawab organisasi dalam audit *IT Governance* disesuaikan dengan struktur tata kelola TI di instansi pemerintah sesuai Permen Kominfo No.: 41/PER/MEN.KOMINFO/11/2007.

Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik Tahun 2008, memberikan dasar kemudahan untuk mendapatkan data dan informasi yang dibutuhkan.

#### Perencanaan

Fokus Audit Tata kelola TI (*IT Governance Audit*) bukan hanya pada program dan kegiatan, juga bukan hanya pada sistem akuntansi dan manajemen, tetapi memastikan pemanfaatan dan pengelolaan seluruh sumber daya TI dapat memberikan nilai tambah sesuai tujuan organisasi.

Perencanaan audit mencakup perencanaan yang dilakukan oleh lembaga audit dalam memberikan layanan dan penugasan audit, dibutuhkan persiapan dalam perencanaan audit yang menyangkut penugasan, waktu, metode dan perhitungan biaya audit yang dibutuhkan.

Jika metode dalam Audit Keuangan memiliki standarisasi dalam bidang Akuntansi, begitupun Audit Tata kelola TI memiliki standarisasi berdasarkan *best practice* bidang *IT Governance*. Namun standar tersebut tidak berbeda antara satu proyek dan proyek lainnya seperti halnya audit Kinerja.

Tujuan umum dari Audit Tata Kelola TI terdiri dari penilaian struktur dan tingkat keselarasan antara strategi TI dan strategi bisnis. Entitas-entitas struktur tata kelola TIK di instansi pemerintah adalah:

- Eksekutif Institusi Pemerintahan, yaitu pimpinan institusi pemerintahan (Kabupaten/Kota, Provinsi, Departemen, LPND)
- Satuan Kerja Pengelola TIK, yaitu satuan kerja yang bertugas dalam pengelolaan TIK institusi pemerintahan. Posisi struktural satuan kerja pengelola TIK ini saat ini mempunyai level struktural yang berbeda-beda di institusi-institusi pemerintahan.
- Satuan Pemilik Proses Bisnis, yaitu satuan kerja di luar satuan kerja pengelola TIK sebagai pemilik proses bisnis (*Business Process Owner*).

Setelah tujuan umum ditetapkan, harus dirumuskan juga tujuan khusus yang menetapkan kriteria dan persyaratan audit. Diusulkan tujuan spesifik dan materi risiko audit terkait dengan Tata kelola TI. Kriteria yang relevan dalam proses audit didasarkan pada:

- Strategi TI selaras dengan strategi bisnis organisasi.
- Struktur Tata kelola TI, dengan kompetensi dan tanggung jawab terkait dengan setiap bagian.

- Mengidentifikasi biaya dan keputusan alokasi sumber daya TI untuk investasi, pengembangan proyek TI, dan pengendalian yang diterapkan untuk mengurangi risiko TI.
- Pemantauan dan penilaian kinerja TI.

Auditor TI harus melakukan beberapa prosedur khusus (untuk melakukan prosedur ini metode yang digunakan dengan mengumpulkan dokumentasi dan catatan resmi), seperti:

- Mengkaji struktur tata kelola TI. Auditor harus menganalisis struktur organisasi sesuai kompetensi dan tanggung jawab masing-masing.
- Mempelajari struktur organisasi dan manajemen staf TI. Auditor harus menganalisis ketidaksesuaian pemisahan fungsi kebijakan manajemen staf TI,
- Mengkaji strategi tata kelola organisasi (rencana strategis organisasi)
- Mempelajari strategi organisasi tata kelola TI (perencanaan TI, rencana taktis subordinasi sesuai terhadap rencana strategis, dan anggaran TI).
- Menganalisis dan menilai keselarasan dan integrasi antara: strategi TI, tujuan dan strategi organisasi.
- Menilai kinerja struktur tata kelola TI.
- Mengkaji infrastruktur TI.
- Mengkaji rencana investasi TI, proyek pengembangan TI, kebijakan *outsourcing*.
- Mengkaji ketersediaan layanan TI.
- Mengkaji metodologi penilaian risiko TI, pemantauan risiko dan implementasi kontrol penurunan risiko
- Mengkaji kebijakan keamanan untuk menjaga aset organisasi, rencana bisnis selanjutnya, dan pemulihan setelah bencana.
- Mengkaji indeks kinerja TI dihitung berdasarkan entitas.
- Menilai risiko yang terkait tata kelola TI untuk mengidentifikasi area kritis.

Untuk mendapatkan pemahaman umum

tentang struktur tata kelola TI, auditor TI harus menganalisis entitas dokumen-dokumen yang relevan (ISACA, *CISA Review Manual*, 2008):

- Strategi, rencana dan anggaran TI. Sebagai bukti perencanaan dan kontrol manajemen untuk keselarasan strategi bisnis.
- Dokumentasi kebijakan keamanan
- Struktur Organisasi. Menggambarkan pembagian tugas dan tanggung jawab dalam organisasi.
- Deskripsi Pekerjaan.
- Menentukan fungsi dan tanggung jawab di seluruh bagian organisasi. Berdasar deskripsi pekerjaan memberikan indikasi dari tingkat pemisahan tugas dalam organisasi dan dapat membantu mengidentifikasi tugas yang mungkin bertentangan.
- Laporan Komite Pengarah. Laporan-laporan ini memberikan informasi mengenai dokumentasi sistem proyek.
- Prosedur Operasional. Prosedur ini menggambarkan tanggung jawab staf operasional.
- Pengembangan dan prosedur perubahan sistem.

Setelah menganalisis dokumen-dokumen, aktivitas Auditor TI harus melakukan wawancara kepada pimpinan institusi, staf dan pengguna TI yang dipilih. Dapat digunakan kuesioner untuk melakukan penilaian tata kelola TI. Auditor harus melakukan analisis dan peringkat risiko spesifik tata kelola TI berdasarkan data yang dikumpulkan. Prosedur ini mendukung identifikasi wilayah kritis audit sistem yang akan diverifikasi dan diuji.

### **Pelaksanaan**

Audit *IT Governance* dilakukan menyeluruh di seluruh bagian instansi, dan tidak dilakukan hanya spesifik berdasarkan objek dan subjek lingkup tertentu saja.

Atas dasar proses audit yang dilakukan sebelumnya, kemudian dilanjutkan dengan pengujian kepatutan atas kebijakan, praktek

manajemen dengan standar dan aturan yang relevan di beberapa area materi penilaian efisiensi struktur tata kelola TI. Proses pengujian ini tidak harus lengkap tetapi tetap berfokus pada identifikasi area kritis dalam langkah perencanaan.

Tindakan khusus yang harus dilakukan Auditor TI untuk setiap domain Audit Tata kelola TI.

- Untuk penilaian proses perencanaan strategis TI, auditor TI harus mempertimbangkan apakah:
  - terdapat definisi yang jelas tentang visi dan misi TI,
  - terdapat informasi strategis metodologi perencanaan teknologi,
  - metodologi berkorelasi antara tujuan bisnis dan tujuan bisnis TI, proses perencanaan diperbarui secara periodik (minimal sekali per tahun),
  - rencana tersebut mengidentifikasi kegiatan utama TI dan sumber daya yang dibutuhkan
- Untuk penilaian manajemen organisasi TI, auditor harus:
  - memverifikasi struktur organisasi TI untuk menjamin rantai perintah dan tanggung jawab operasional organisasi TI dan untuk menjamin pemisahan kompetensi yang tidak kompatibel.
  - memverifikasi jika pemberhentian pekerja sesuai dengan prosedur yang dipahami dan jelas.
  - memverifikasi kebijakan pelatihan staf TI.
- Untuk proses penilaian *delivery* TI dan proses perencanaan investasi TI, auditor harus:
  - memverifikasi dan menilai manajemen layanan yang diberikan pihak ketiga.
  - menilai manajemen *Service Level Agreement* (SLA), dan memeriksa seberapa baik pengetahuan fungsi *help desk* yang dikelola.
    - memeriksa dan meninjau semua laporan SLA, dan memeriksa

kontrak untuk memastikan aspek lain dari manajemen layanan TI.

- menilai proses prioritas dan persetujuan investasi TI.
- menilai realisasi manfaat bisnis dari investasi TI.
- Untuk penilaian manajemen proyek, auditor harus mempertimbangkan:
  - metodologi manajemen proyek yang digunakan.
  - kontrol manajemen proyek yang diterapkan.
  - metodologi pengembangan aplikasi.
  - pengelolaan infrastruktur TI dan manajemen perubahan.
  - kegiatan TI termasuk pengembangan aplikasi dan pemeliharaan prasarana dukungan yang telah dikerjakan oleh pihak luar.
- Untuk penilaian manajemen risiko TI, auditor harus memverifikasi:
  - proses penilaian kelemahan dan ancaman TI.
  - metode penilaian risiko TI.
  - prosedur pelaporan insiden keamanan.
  - perencanaan bisnis berkelanjutan (diuji dan diperbaharui tepat waktu)
- Untuk penilaian proses kinerja TI, auditor harus memverifikasi:
  - indeks kinerja TI yang memadai.
  - indeks manajemen kinerja TI.
  - proses pemantauan kinerja TI.

### **Pelaporan**

Auditor TI harus memberikan laporan audit sesuai bentuk yang diinginkan pengguna jasa dengan mempertimbangkan dan mendiskusikan laporan tersebut sebelum diinformasikan secara terbuka.

Dalam pembuatan laporan, Audit Tata kelola TI menghasilkan bentuk laporan yang standar (seperti laporan Audit Keuangan), dan laporan yang struktur dan isi laporan bervariasi (seperti laporan Audit Kinerja).

Laporan yang disepakati harus dalam bentuk prosedur dan temuan. Laporan tersebut harus mengandung unsur-unsur sebagai berikut :

- Independen.
- Identifikasi pihak yang ditetapkan.
- Identifikasi pokok permasalahan dan jenis keterlibatan.
- Identifikasi pihak yang bertanggung jawab.
- Pernyataan bahwa materi pelajaran merupakan tanggung jawab dari pihak yang bertanggung jawab.
- Pernyataan bahwa prosedur yang dilakukan disepakati oleh para pihak tertentu yang diidentifikasi dalam laporan.
- Sebuah pernyataan bahwa daftar prosedur yang dilakukan (atau referensi tambahan) dan temuan terkait kelengkapan prosedur dan sanggahan adalah tanggung jawab pihak tertentu atas kecukupan prosedur tersebut.

Instansi pemerintah sebagai lembaga publik, sudah selayaknya mempublikasikan laporan audit yang dihasilkan kepada masyarakat, sebagai sarana mengoptimalkan pengawasan publik terhadap penyelenggaraan negara dan segala sesuatu yang berakibat pada kepentingan publik.

### Tindak Lanjut

Sebuah proses tindak lanjut membantu memberikan keyakinan bahwa setiap *review* yang telah dilakukan oleh auditor TI memberikan manfaat yang optimal bagi organisasi.

Faktor-faktor yang harus dipertimbangkan dalam menentukan prosedur yang tepat adalah:

- Setiap perubahan dalam lingkungan SI dapat berdampak signifikan terhadap pengamatan yang dilaporkan.
- Signifikansi dari temuan yang dilaporkan atau direkomendasikan.

- Dampak yang seharusnya dapat mengakibatkan kegagalan tindakan perbaikan.
- Tingkat usaha dan biaya yang diperlukan untuk memperbaiki masalah yang dilaporkan.
- Kompleksitas dari tindakan perbaikan.
- Jangka waktu yang dibutuhkan.

### PENUTUP

Pertama, penerapan metodologi audit Tata Kelola TI yang diusulkan dapat digunakan sebagai bagian dari Audit Kinerja sesuai UU No. 15 tahun 2004.

Kedua, metode yang akan digunakan auditor dalam audit tata kelola TI dapat dikembangkan sesuai kebutuhan, berdasar pada *best practices* pada bidang ini 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.

Ketiga, tidak dapat dipungkiri bahwa Teknologi Informasi merupakan bagian dari keberhasilan pengelolaan instansi pemerintah, karenanya penilaian atas ketercapaian efektivitas dan efisiensi tata kelola TI yang ada harus dilakukan, pemerintah disarankan untuk mengeluarkan pedoman audit resmi yang memiliki tujuan khusus dalam tata kelola TI.

### DAFTAR PUSTAKA

- Amancei, Cristian, and Traian Surcel. "Increasing the Efficiency of IT Audit Methodology by Using the Organizations Tolerance to IT Systems Availability." *Informatica Economică* 14, no. 1 (2010).
- Budiono, Gatut. "Audit Kinerja Sistem Informatika Manajemen Pemeliharaan Unit Pembangkit Listrik Berbasis CobIT Domain." *EECCIS IV*, no. 1 (2010).
- Cilli, Claudio. "IT Governance: Why a Guideline?" *Information Systems Control Journal* 3 (2003).

- Committee of Sponsoring Organizations of the Treadway Commission. *"Enterprise Risk Management — Integrated Framework"* September (2004).
- Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta, 2011.
- Haes, Steven De, and Wim Van Grembergen. *"IT Governance and Its Mechanisms."* *Information Systems Control Journal* 1 (2004).
- Hardy, Gary. *"The Role of the IT Auditor in IT Governance."* *ISACA Jurnal* 1 (2009).
- Iliescu, Mihai. *"Auditing IT Governance."* *Informatica Economică* 14, no. 1 (2010).
- Kutsikos, Konstadinos. *"IT Governance Auditing in Virtual Organizations"* 1, no. 1 (2007).
- Lusiani, Cecilia. *"Audit IT Governance Kabupaten Sleman."* *Informatika Mulawarman* 4, no. 2 (2009).
- Menteri Komunikasi Dan Informatika. *Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional*. Jakarta, 2007.
- Menteri Negara Pendayagunaan Aparatur Negara. *Peraturan Menteri Negara Pendayagunaan Aparatur Negara Nomor: Per/05/M.PAN/03/2008 Tentang Standar Audit Aparat Pengawasan Intern Pemerintah*, 2008.
- OECD. *OECD Principles of Corporate Governance*. Paris: OECD Publishing, May 3, 2004.
- Presiden Republik Indonesia. *Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik*. Jakarta, 2008.
- . *Undang-Undang Republik Indonesia Nomor 15 Tahun 2004 Tentang Pemeriksaan Pengelolaan Dan Tanggung Jawab Keuangan Negara*, 2004.
- Purwanto, Yudha. *"Audit Teknologi Informasi Dengan Cobit 4.1 Dan IS Risk Assessment (Studi Kasus Bagian Pusat Pengolahan Data PTS XYZ)." Bali*, 2010.
- Pusat Pendidikan Dan Pelatihan Pengawasan Badan Pengawasan Keuangan Dan Pembangunan. *Dasar-Dasar Auditing*. 6th ed. BPKP, 2009.
- Radovanovic, Dalibor, Tijana Radojevic, Dubravka Lucic, and Marko Sarac. *"Analysis of Methodology for IT Governance and Information Systems Audit."* In *The 6th International Scientific Conference "Business and Management 2010"*. Vilnius, Lithuania: Vilnius Gediminas Technical University Publishing House Technika, 2010.
- Yulianti, Diana Trivena, and Michel Canggih Patria. *"Jurnal Sistem Informasi Jurnal Sistem Informasi."* *Sistem Informasi* 6, no. 1 (2011)

#### Sumber Internet:

- COSO. *Internal Control – Integrated Framework*. 2nd ed. Jersey City: American Institute of Certified Public Accountants, 1994. Diakses 21 Februari 2013. <http://www.snai.edu/cn/service/library/book/0-framework-final.pdf>.
- Institute de la Gouvernance des Systems d'Information. *The Place of IT Governance in the Enterprise Governance*. Paris, 2005. Diakses 11 Januari 2013., [http://cigref.typepad.fr/itgifrance/files/place\\_IT\\_governance\\_in\\_enterprise\\_governance.pdf](http://cigref.typepad.fr/itgifrance/files/place_IT_governance_in_enterprise_governance.pdf).
- ISACA. *CISA Review Manual*. Illinois, 2008. [www.isaca.org](http://www.isaca.org).
- . *COBIT 5-A Business Framework for the Governance and Management of Enterprise IT*. Illinois, 2012. [www.isaca.org](http://www.isaca.org).
- . *IS Auditing Guideline IT Governance*. Illinois, 2002. [www.isaca.org](http://www.isaca.org).
- . *IS Auditing Standard IT Governance*. Illinois, 2005. [www.isaca.org](http://www.isaca.org).
- . *IT Standards , Guidelines , and Tools and Techniques for Audit and Assurance and Control Professionals*. Illinois, 2010. [www.isaca.org](http://www.isaca.org).
- ISO/IEC. *International Standard ISO/IEC 27002*. Switzerland, 2005. <http://www.iso.org>.
- . *International Standard ISO/IEC 38500*. Switzerland, 2007. <http://www.iso.org>.

Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia  
(Herri Setiawan dan Khabib Mustofa)

IT Governance Institute. *Board Briefing on IT Governance*. 2nd ed. IT Governance Institute, 2003. [www.itgi.org](http://www.itgi.org).

———. *ISO/IEC 38500-2008 Adoption*. Illinois, 2008. [www.itgi.org](http://www.itgi.org).

ITIL. *An Introductory Overview of ITIL*® V3. Edited by Alison Cartlidge and Mark Lillycrop. 1st ed. Wokingham, UK: itSMF Ltd, 2007.

OXLEY. *Sarbanes-Oxley Act Of 2002*. Washington, 2002. <http://www.sec.gov>.