COBIT 5 SEBAGAI METODE ALTERNATIF BAGI AUDIT KEAMANAN SISTEM INFORMASI
(Sebuah Usulan Untuk Diterapkan di Pemerintah Kota Yogyakarta)

Dewi Ciptaningrum[1)], Eko Nugroho[2)], Dani Adhipta[3)]

[1), 2), 3)] Teknik Elektro dan Teknik Informatika Uviversitas Gadjah Mada Yogyakarta
Jl Grafika, Condongcatur, Sleman, Yogyakarta 55281
Email : dewi.cio13@mail.ugm.ac.id[1)], nugroho@ugm.ac.id[2)], dani@ugm.ac.id[3)]

Abstrak

Kerentanan dalam Information Exchange Environment (IEE) telah meningkat menjadi ancaman yang lebih luas dan rumit, sehingga keamanan informasi kini menjadi masalah yang mendasar untuk bisnis, organisasi, dan pemerintahan. Audit keamanan informasi menjadi suatu kebutuhan bagi organisasi pemerintahan. Paper ini dimaksudkan untuk menunjukkan kelebihan COBIT 5 sebagai sebuah metode yang paling cocok (fit) untuk digunakan dalam rencana audit keamanan sistem informasi di lingkungan Pemerintah Kota Yogyakarta.

Kata kunci: *Keamanan, sistem informasi, COBIT 5.*

1. Pendahuluan

Keamanan informasi pada era Teknologi Informasi dan Komunikasi (TIK) ini sangat penting. Kerentanan *Information Exchange Environment* (IEE) telah meningkat menjadi ancaman yang lebih luas dan rumit, sehingga keamanan informasi kini menjadi masalah yang mendasar untuk bisnis, organisasi, dan pemerintahan [1]. Laporan Ancaman Keamanan Internet (*Internet Security Threat Report*) yang disajikan oleh Symantec menunjukkan bahwa administrasi publik atau pemerintahan menjadi target utama dalam pelanggaran data (*data breach*) pada Tahun 2013 dalam kategori *Spear-Phishing* [2]. Tentunya hal ini meresahkan karena sektor administrasi publik atau pemerintahan merupakan lembaga yang seharusnya kredibel dan akuntabel dalam melayani, melindungi dan menjamin kepentingan rakyat.

Keamanan informasi umumnya berfokus pada melindungi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi. Sementara kesadaran keamanan informasi berhubungan dengan penggunaan program kesadaran keamanan untuk menciptakan dan menjaga keamanan perilaku positif sebagai elemen penting dalam sebuah lingkungan keamanan informasi yang efektif [3].

Secara tradisional, audit keamanan dilakukan saat insiden telah terjadi (audit reaktif) yaitu ketika aset telah diganggu, untuk menentukan bagaimana peristiwa itu terjadi. Tapi audit keamanan sistem informasi bukan hanya tentang menyelidiki pembobolan keamanan, tetapi lebih untuk memastikan bahwa [4]:

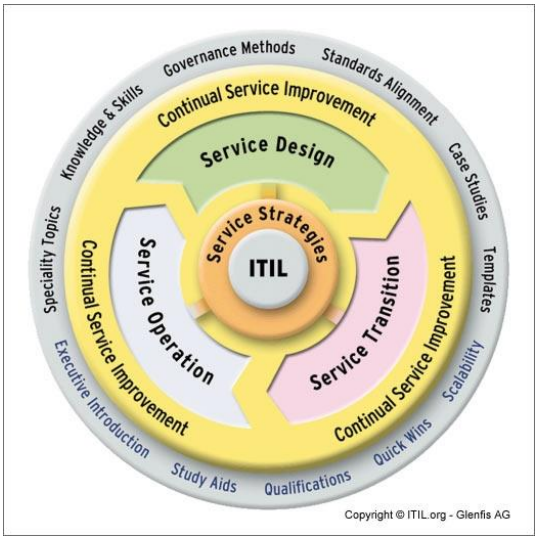
1. kepatuhan terhadap peraturan dan keamanan dipenuhi dan dipelihara;
2. aset berharga atau penting dilindungi, dan bahwa mekanisme perlindungan yang ditawarkan kepada aset tersebut memadai dan berfungsi seperti yang direncanakan;
3. proses berada pada jalurnya dan terus ditingkatkan;
4. pengendalian ditegakkan.

Sejak 15 Desember 2007, Pemerintah Kota Yogyakarta telah memiliki Dokumen Perencanaan Pembangunan *e-government* yang mengacu pada *Master Plan* (Rencana Induk) *e-government* [5]. Rencana Induk *e-government* tesebut memuat pernyataan visi dan misi, strategi pengembangan, cetak biru pengembangan, tahapan pengelolaan dan implementasi sebagaimana tertuang dalam Peraturan Walikota tentang Standar Operasional dan Prosedur Manajemen Pengamanan Sistem Informasi dan Komunikasi pada Pemerintah Kota Yogyakarta, namun sejak saat itu sampai sekarang Pemerintah Kota Yogyakarta belum pernah melaksanakan audit terhadap keamanan sistem informasi (SI).

Dewasa ini terdapat beberapa metode dan standar yang bisa digunakan untuk mendukung proses audit secara efektif, efisien dan tepat sasaran. Paper ini dimaksudkan untuk menunjukkan kelebihan COBIT 5 sebagai sebuah metode yang paling sesuai digunakan dalam rencana audit keamanan sistem informasi di lingkungan Pemerintah Kota Yogyakarta.

2. Pembahasan

Salah satu standar audit yang sudah banyak dipakai adalah ITIL (*Information Technology Infrastructure Library*). ITIL menyediakan satu set kohesif praktik terbaik, yang diambil dari sektor publik dan swasta internasional [6]. ITIL adalah sebuah kerangka kerja yang bagus untuk manajemen layanan dan penyampaian TI. Sayangnya ITIL mempunyai keterbatasan fokus pada domain keamanan yang menjadikannya tidak cocok untuk manajemen keamanan informasi [7]. ITIL cenderung bersangkutan pada proses TI, mendefinisikan strategi, rencana dan proses [8] [9]. Pada ITIL, keamanan menyangkut aspek *reliability*, *maintainability*, *serviceability* dan *resilience* [9].



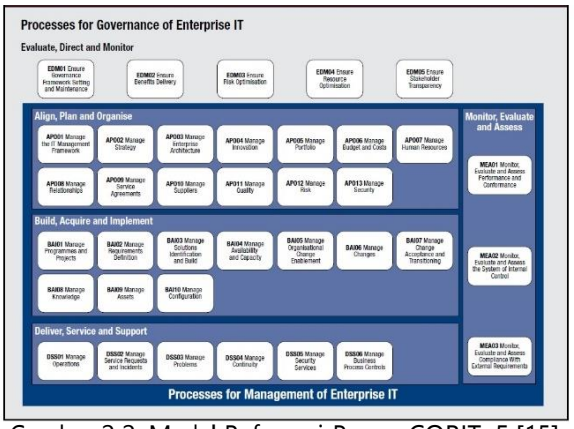
Gambar 2.1. Siklus Hidup ITIL (ITIL *Lifecycle*) [10]

Selain itu, ISO/IEC 27001 standar diterbitkan pada bulan Oktober 2005, pada dasarnya menggantikan standar BS7799-2. Isi ISO/IEC 27001 ini adalah spesifikasi untuk ISMS (*Information Security Management System*) atau Sistem Manajemen Keamanan Informasi. Tujuan dari standar ini adalah untuk memberikan persyaratan untuk penetapan, penerapan, memelihara dan terus meningkatkan sebuah Sistem Manajemen Keamanan Informasi (SMKI) [11] [12].

ISO/IEC 27002 standar pada awalnya diterbitkan sebagai ganti dari ISO 17799, kode praktik untuk keamanan informasi. Pada dasarnya menguraikan ratusan kendali potensial dan mekanisme kendali, yang dapat diimplementasikan, dalam teori, tunduk/patuh pada panduan yang diberikan dalam ISO 27001. Standar ini berisi tentang pedoman yang ditetapkan dan prinsip- prinsip umum untuk memulai, melaksanakan, memelihara, dan meningkatkan manajemen keamanan informasi dalam sebuah organisasi. Kendali yang sebenarnya tercantum dalam standar dimaksudkan untuk mengatasi kebutuhan spesifik diidentifikasi melalui penilaian risiko formal. Standar ini juga dimaksudkan untuk memberikan panduan untuk pengembangan standar keamanan organisasi dan praktik manajemen keamanan yang efektif dan membantu membangun kepercayaan dalam kegiatan antarorganisasi [11] [13].

Sementara COBIT adalah singkatan dari *Control Objectives for Information and Related Technology* merupakan seperangkat kerangka kerja (*framework*) terbaik untuk tata kelola dan manajemen teknologi informasi yang diciptakan oleh *Information Systems Audit and Control Association* (ISACA), dan *Information Technology Governance Institute* (ITGI) pada tahun 1996 [9] [14]. Telah banyak penelitian terdahulu yang menggunakan COBIT dalam penelitiannya. Ada yang melakukan audit, evaluasi maupun membuat rancangan (perancangan) tata kelola TI menggunakan kerangka kerja COBIT.

Model referensi proses COBIT 5 adalah penerus dari model proses COBIT 4.1, dengan Risk IT dan Val IT model proses yang terintegrasi juga. Gambar 2.5. menunjukkan set lengkap dari tiga puluh tujuh (37) tata kelola dan manajemen proses dalam COBIT 5 [15]. Proses Tata Kelola diwakili oleh domain *Evaluate, Direct and Monitor* (EDM) atau Mengevaluasi, Mengarahkan dan Memantau. Sedangkan proses Manajemen diterjemahkan dalam domain *Plan, Build, Run and Monitor* (PBRM) yang terdiri dari domain *Align, Plan and Organise* (APO), *Build, Acquire and Implement* (BAI), *Deliver, Service and Support* (DSS) dan yang terakhir adalah *Monitor, Evaluate and Assess* (MEA).



Gambar 2.2. Model Referensi Proses COBIT 5 [15]

COBIT, ISO/IEC 27001 & 27002, dan ITIL masing-masing memiliki kelebihan dan kekurangan. Berikut gambaran kelebihan yang dimiliki masing-masing standar.

Tabel 2.1. Perbandingan antara COBIT, ISO/IEC 27001 & 27002, dan ITIL [9] [16]

ITIL	COBIT	ISO/IEC 27001 dan 27002
Konsep/proses	*Critical Success Factors*	Keamanan Informasi
Aktivitas	Metrik (*Critical Success Factors and Key Performance Indicator*)	
Biaya/ keuntungan	*Benchmarking* (CMM)	
Merencanakan untuk penerapan	Kendali	
	Audit	

Dari tabel 1.1. dapat diketahui bahwa kelebihan ITIL adalah untuk mendefinisikan strategi, rencana dan proses. Kelebihan COBIT untuk metrik, tolok ukur dan audit, sedangkan kelebihan ISO/IEC 27001 dan 27002 untuk mengatasi masalah keamanan untuk mengurangi risiko [9] [16]. Meski disebutkan bahwa kelebihan ISO/IEC 27001 dan 27002 adalah keamanan informasi, tetapi kelebihan dalam keamanan informasi tersebut

hanya bersifat teknis saja [17]. Pada praktiknya, keamanan SI tidak hanya menyangkut aspek teknis saja melainkan juga menyangkut aspek nonteknis. Kelebihan COBIT untuk metrik, tolok ukur dan melaksanakan audit [9] [16], serta menyediakan tata kelola dan manajemen menyeluruh yang mampu mencakup aspek teknis dan aspek nonteknis yang melandasi pemilihan COBIT 5 untuk audit keamanan SI. Kelebihan-kelebihan COBIT 5 inilah yang melandasi penulis untuk memilih COBIT 5 sebagai metode audit, terutama dikaitkan dengan rencana objek penelitian yaitu Pemerintah Kota Yogyakarta yang sudah memiliki Rencana Induk Pengembangan *e-government* dan Standar Operasional dan Prosedur Manajemen Pengamanan Sistem Informasi dan Komunikasi.

Sebagai gambaran lanjutan, COBIT 5 memiliki tujuan kaskade yang memungkinkan modifikasi metode sesuai kebutuhan, terutama disesuaikan dengan kondisi objek yang akan diaudit. Tujuan kaskade COBIT 5 adalah mekanisme untuk menerjemahkan kebutuhan para pemangku kepentingan menjadi tujuan perusahaan yang spesifik, bisa dilaksanakan dan disesuaikan, tujuan terkait TI dan tujuan *enabler*. Memperkenankan penetapan tujuan yang spesifik pada setiap tingkatan dan di setiap wilayah dari perusahaan dalam mendukung tujuan keseluruhan dan kebutuhan para pemangku kepentingan [18].

Gambar 2.3. Tujuan Kaskade COBIT 5 [18]

COBIT 5 terdiri dari lima (5) domain yang menaungi tiga puluh tujuh (37) proses, dan hal ini sesuai dengan struktur organisasi Pemerintah Kota Yogyakarta.
Domain-domain itu adalah:

1. Mengevaluasi, Mengarahkan dan Memantau (*Evaluate, Direct and Monitor*/EDM)

   Proses tata kelola ini menangani tujuan pemangku kepentingan pengiriman (penyampaian nilai, optimasi risiko dan optimasi sumber daya) dan termasuk praktik dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan memantau hasilnya.

   Tabel 2.2. Domain Mengevaluasi, Mengarahkan dan Memantau

Proses		**Praktik**
Domain Mengevaluasi, Mengarahkan dan Memantau		
EDM01	Memastikan Penetapan Kerangka Kerja Tata Kelola dan Pemeliharaan	3
EDM02	Memastikan Penyampaian Keuntungan	3
EDM03	Memastikan Optimasi Risiko	3
EDM04	Memastikan Optimasi Sumber Daya	3
EDM05	Memastikan Transparansi Pemangku Kepentingan	3

2. Menyelaraskan, Rencana dan Mengorganisir (*Align, Plan and Organise*/APO)

   Menyediakan arah untuk solusi penyampain membangun, memperoleh dan melaksanakan (BAI) dan penyediaan layanan dan dukungan (DSS). Domain ini mencakup strategi, taktik, dan kekhawatiran mengidentifikasi cara terbaik TI dapat berkontribusi pada pencapaian tujuan bisnis. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda. Sebuah organisasi yang tepat, serta infrastruktur teknologi, harus diletakkan pada tempat yang tepat.

   Tabel 2.3. Domain Menyelaraskan, Rencana dan Mengorganisir

Proses		**Praktik**
Domain Menyelaraskan, Rencana dan Mengorganisir		
APO01	Mengelola Kerangka Kerja Manajemen TI	8
APO02	Mengelola Strategi	6
APO03	Mengelola Arsitektur Perusahaan	5
APO04	Mengelola Inovasi	6
APO05	Mengelola Portofolio	6
APO06	Mengelola Anggaran dan Biaya	5
APO07	Mengelola Sumber Daya Manusia	6
APO08	Mengelola Hubungan	5
APO09	Mengelola Perjanjian Layanan	5
APO10	Mengelola Penyedia	5
APO11	Mengelola Kualitas	6
APO12	Mengelola Risiko	6
APO13	Mengelola Keamanan	3

3. Membangun, Memperoleh dan Menerapkan (*Build, Acquire and Implement*/BAI)

   Menyediakan solusi dan menyampaikan solusi tersebut untuk berubah menjadi layanan. Untuk mewujudkan strategi TI, solusi perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan terintegrasi ke dalam proses bisnis. Perubahan dan pemeliharaan sistem yang ada juga dijamin dengan domain ini, untuk memastikan bahwa solusi terus memenuhi tujuan bisnis.

Tabel 2.4. Domain Membangun, Memperoleh dan Melaksanakan

Proses		**Praktik**
Domain Membangun, Memperoleh dan Menerapkan		
BAI01	Mengelola Program dan Proyek	14
BAI02	Mengelola Penetapan Persyaratan	4
BAI03	Mengelola Identifikasi Solusi dan Membangun	11
BAI04	Mengelola Ketersediaan dan Kapasitas	5
BAI05	Mengelola Pemberdayaan Perubahan Organisasi	7
BAI06	Mengelola Perubahan	4
BAI07	Mengelola Penerimaan terhadap Perubahan dan Masa Transisi	8
BAI08	Mengelola Pengetahuan	5
BAI09	Mengelola Aset	5
BAI10	Mengelola Konfigurasi	5

4. Penyampaian, Layanan dan Dukungan (*Deliver, Service and Support*/DSS)

   Menerima solusi dan membuat solusi tersebut dapat digunakan bagi pengguna akhir. Domain ini berkaitan dengan penyampaian aktual dan dukungan dari layanan yang dibutuhkan, yang meliputi penyampaian pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data dan fasilitas operasional.

Tabel 2.5. Domain Penyampaian, Layanan dan Dukungan

Proses		**Praktik**
Domain Penyampaian, Layanan dan Dukungan		
DSS01	Mengelola Operasi	5
DSS02	Mengelola Permintaan Layanan dan Insiden	7
DSS03	Mengelola Masalah	5
DSS04	Mengelola Kelangsungan	8
DSS05	Mengelola Layanan Keamanan	7
DSS06	Mengelola Kendali Proses Bisnis	6

5. Memantau, Mengevaluasi dan Menilai (*Monitor, Evaluate and Assess*/MEA)

   Memantau semua proses untuk memastikan bahwa arah yang disediakan diikuti. Semua proses-proses TI perlu dipantau secara berkala dari waktu ke waktu untuk kualitas dan kepatuhan mereka dengan persyaratan kendali. Domain ini membahas manajemen kinerja, memantau pengendalian internal, kepatuhan terhadap peraturan dan tata kelola.

Tabel 2.6. Domain Memantau, Melakukan Evaluasi dan Menilai

Proses		**Praktik**
Domain Memantau, Melakukan Evaluasi dan Menilai		
MEA01	Memantau, Melakukan Evaluasi dan Menilai Kinerja dan Kesesuaian	5
MEA02	Memantau, Melakukan Evaluasi dan Menilai Sistem dari Kendali Internal	8
MEA03	Memantau, Melakukan Evaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal	4

Untuk tolok ukur penilaian digunakan Tingkatan Kapabilitas dan Atribut Proses, seperti ditunjukkan pada Tabel 2.12. Tingkat kemampuan proses ditentukan berdasarkan pencapaian proses tertentu atribut sesuai dengan ISO / IEC 15504-2: 2003. COBIT 5 sengaja mengadopsi ISO/IEC 15504-2:2003 untuk Model Penilaian Proses (*Process Assessment Model*). Seperangkat persyaratan minimum yang ditetapkan dalam ISO/IEC 15504-2:2003 memastikan bahwa hasil penilaian adalah objektif, berimbang, konsisten, berulang dan merupakan representatif dari proses yang dinilai [19].

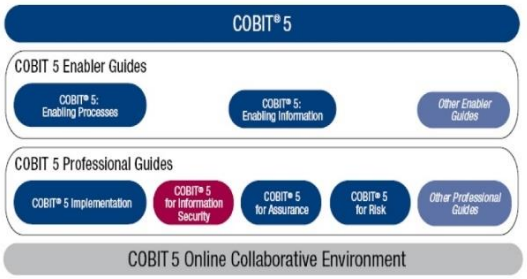
Tabel 2.7. Tingkatan Kapabilitas dan Atribut Proses [20]

Atribut Proses	**Tingkat Kemampuan dan Atribut Proses**
	Level 0 : Proses tidak lengkap
	Level 1: Proses dilaksanakan
PA 1.1	Kinerja Proses
	Level 2: Proses dikelola
PA 2.1	Manajemen Kinerja
PA 2.2	Manajemen Produk Kerja
	Level 3: Proses didirikan
PA 3.1	Penetapan proses
PA 3.2	Penyebaran proses
	Level 4: Proses diprediksi
PA 4.1	Pengukuran proses
PA 4.2	Pengendalian proses
	Level 5: Proses mengoptimalkan
PA 5.1	Inovasi proses
PA 5.2	Optimasi proses

Atribut Proses	Tingkat Kemampuan dan Atribut Proses
Sumber: Angka ini diadaptasi dari ISO / IEC 15504-2: 2003, dengan izin dari ISO / IEC di www.iso.org. Hak cipta tetap milik ISO / IEC.	

Indikator kinerja proses (dasar praktik dan produk kerja) spesifik untuk setiap proses dan digunakan untuk menentukan apakah suatu proses berada pada kemampuan tingkat 1. Indikator kinerja ini terdiri dari praktik dasar dan produk kerja dan eksklusif untuk tingkat 1. Praktik-praktik dasar dan produk kerja untuk setiap COBIT 5 proses ditunjukkan didasarkan pada konten COBIT 5. Indikator kemampuan proses atribut generik untuk setiap atribut proses untuk tingkat kemampuan 1 sampai 5. Level 1 hanya memiliki indikator praktik generik tunggal untuk kemampuan yang sejalan langsung ke pencapaian indikator kinerja tertentu yang digariskan dalam model referensi proses.

COBIT 5 *for Information Security* (untuk Keamanan Informasi) adalah salah satu produk dari COBIT 5. Dalam COBIT 5 untuk Keamanan Informasi ini mengandung rekomendasi bagi praktisi keamanan informasi tentang bagaimana menerapkan keamanan informasi dalam cakupan COBIT 5.



Gambar 2.4. Rumpun Produk dari COBIT 5 [21] COBIT

5 untuk Keamanan Informasi memberikan panduan spesifik yang berhubungan dengan semua enabler, yaitu pada prinsip dan kerangka kerja; proses; struktur organisasi; budaya, etika dan perilaku; informasi; kemampuan layanan; dan manusia, keahlian dan kompetisi [21]:

1. Kebijakan prinsip, dan kerangka kerja keamanan informasi
   Prinsip, kebijakan dan kerangka kerja mengacu pada mekanisme komunikasi dimasukkan ke dalam tempat untuk menyampaikan arah dan instruksi dari badan tata kelola dan manajemen. Prinsip, kebijakan dan model kerangka kerja; Prinsip keamanan informasi; Kebijakan keamanan informasi; Menyesuaikan kebijakan untuk lingkungan perusahaan; Siklus hidup kebijakan.
2. Proses, termasuk rincian spesifik dan kegiatan keamanan informasi
   COBIT 5 untuk Keamanan Informasi memeriksa setiap proses (ada 37 proses dalam COBIT 5) dari perspektif keamanan informasi.
3. Struktur organisasi khusus keamanan informasi
   COBIT 5 untuk Keamanan Informasi meneliti model struktur organisasi dari perspektif keamanan informasi. Ini mendefinisikan peran dan struktur keamanan informasi, meneliti pertanggungjawaban atas keamanan informasi. Memberikan contoh peran dan struktur tertentu serta apa tugas mereka, dan melihat pada jalur potensial untuk pelaporan keamanan informasi dan kelebihan dan kekurangan yang berbeda dari masing-masing kemungkinan.
4. Budaya, etika dan perilaku merupakan faktor penentu keberhasilan tata kelola dan manajemen keamanan informasi
   Memeriksa budaya, etika dan perilaku model dari perspektif keamanan informasi memberikan contoh-contoh spesifik keamanan, misalnya perilaku membagikan kata sandi pada rekan kerja, kebutuhan akan kepemimpinan yang bagus untuk memberikan teladan dan mempengaruhi rekan-rekan kerja, dan budaya-budaya kerja lainnya yang akan memberikan pengaruh positif terhadap keamanan informasi perusahaan.
5. Jenis informasi khusus keamanan informasi
   Informasi tidak hanya subjek utama keamanan informasi tetapi juga merupakan *enabler* kunci.
6. Kemampuan layanan diperlukan untuk menyediakan fungsi keamanan informasi untuk suatu perusahaan
   Layanan, infrastruktur dan aplikasi model yang mengidentifikasi kemampuan layanan yang dibutuhkan untuk menyediakan keamanan informasi dan fungsi yang berhubungan dengan suatu perusahaan.
7. Manusia, keterampilan dan kompetensi khusus untuk keamanan informasi
   Untuk secara efektif mengoperasikan fungsi keamanan informasi dalam suatu perusahaan, individu dengan pengetahuan dan pengalaman yang sesuai harus menerapkan fungsi tersebut. Beberapa keterampilan yang berhubungan dengan keamanan dan kompetensi yang tercantum adalah: Tata kelola keamanan informasi, Manajemen risiko informasi dan Operasi keamanan informasi

3. Kesimpulan

COBIT adalah sebuah kerangka kerja yang sangat ideal untuk melakukan audit terhadap keamanan sistem informasi terhadap suatu organisasi [17] [22] [23]. COBIT berisi tentang tata kelola TI dan mengacu pada masalah teknis dan non teknis, termasuk di antaranya memiliki komponen substansial yang terkait dengan Keamanan Informasi [24] [25]. Apabila seluruh proses dalam COBIT dikelola dengan baik, maka akan menghasilkan tata kelola TI yang tepat [24]. Salah satu dari Tujuan Terkait TI pada COBIT 5 yaitu keamanan informasi, infrastruktur pengolahan dan aplikasi dan salah satu produk keluaran COBIT 5 yaitu COBIT 5 untuk Keamanan Informasi (*for Information Security*) [18] [21]. Dalam lingkungan suatu organisasi pemerintahan seperti Pemerintah Kota Yogyakarta, COBIT 5 layak dijadikan sebagai metode yang paling cocok untuk audit keamanan sistem informasi.

Daftar Pustaka:

[1] M. Hassanzadeh, N. Jahangiri, and B. Brewster, "A Conceptual Framework for Information Security Awareness, Assessment, and Training," in *Emerging Trends in ICT Security*, 1st ed., B. Akhgar and H. R. Arabnia, Eds. 2014, pp. 99 – 109.
[2] Symantec, "INTERNET SECURITY THREAT REPORT," vol. 19, no. April, p. 98, 2014.
[3] H. a. Kruger and W. D. Kearney, "A Prototype for Assessing Information Security Awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, Jun. 2006.
[4] C. Onwubiko, "A Security Audit Framework for Security Management in the Enterprise," in *Global Security, Safety, and Sustainability SE - 2*, H. Jahankhani, A. Hessami, and F. Hsu, Eds. Springer Berlin Heidelberg, 2009, pp. 9–17.
[5] P. K. Yogyakarta, *Peraturan Walikota Yogyakarta*. 2007, p. 36.
[6] "ITIL® Home | ITIL®." [Online]. Available: http://www.itil-officialsite.com/. [Accessed: 13-Apr-2014].
[7] A. N. Shivashankarappa and L. Smalov, "Implementing it Governance Using Cobit: A Case Study Focusing on Critical Success Factors," *World Congr. Internet Secur.*, pp. 144–149, 2012.
[8] Z. Huang, P. Zavarsky, and R. Ruhl, "An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002," *2009 Int. Conf. Comput. Sci. Eng.*, vol. 198, pp. 386–391, 2009.
[9] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," *2008 Second Asia Int. Conf. Model. Simul.*, pp. 749–753, May 2008.
[10] "ITIL.org - ITIL." [Online]. Available: http://itil.org/en/vomkennen/itil/index.php. [Accessed: 13-Nov-2014].
[11] "Introduction to ISO 27002 / ISO27002." [Online]. Available: http://www.27000.org/iso-27002.htm. [Accessed: 12-Nov-2014].
[12] D. Brewer, "Moving from ISO / IEC 27001: 2005 to ISO / IEC 27001 : 2013," 2013.
[13] "BS ISO/IEC 27002:2005 - BS 7799-1:2005 Information technology -- Security techniques -- Code of practice for information security management," 2007. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612. [Accessed: 13-Apr-2014].
[14] D. Greefhorst, "TOGAF & Major IT Frameworks, Architecting the Family," 2013.
[15] ISACA, *COBIT 5 Enabling Processes*. ISACA, 2012, p. 230.
[16] J. Wallhoff, "Combining ITIL with COBIT and 17799," 2000.
[17] M. Spremić, "Governing Information System Security: Review of Approaches to Information System Security Assurance and Auditing," *Latest Trends Appl. Informatics Comput.*, pp. 42–48, 2011.
[18] ISACA, "COBIT 5 A Business Framework for the Governance and Management of Enterprise IT," 2012. [Online]. Available: http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR. [Accessed: 13-Apr-2014].
[19] A. Piamonte, "VALIT2.0 – COBIT 5 Unlocking the Value of Technology Investments," 2012, pp. 1–41.
[20] ISACA, *Process Assessment Model (PAM): Using COBIT ® 5*. ISACA.
[21] ISACA, *COBIT 5 for Information Security*. ISACA, 2012, p. 220.
[22] M. Spremic, "Standards and Frameworks for Information System Security Auditing and Assurance," *World Congr. Eng.*, vol. I, p. 6, 2011.
[23] M. Spremić, D. Ph, M. Ivanov, and P. D. Full, "Using CobiT Methodology in Information System Auditing: Evidences from measuring the level of Operational Risks in Credit Institutions 2 . Managing Risks in Credit Institutions System Auditing and Assessing The," *Recent Adv. Bus. Adm.*, pp. 45–50, 2010.
[24] B. von Solms, "Information Security governance: COBIT or ISO 17799 or both?," *Comput. Secur.*, vol. 24, no. 2, pp. 99–104, Mar. 2005.
[25] B. von S. R. von Solms, *Information Security Governance*. 2009, p. 141.

Biodata Penulis

Dewi Ciptaningrum, memperoleh gelar Sarjana Sosial (S.Sos), Jurusan Ilmu Komunikasi Massa Universitas Negeri Sebelas Maret Surakarta, lulus Tahun 2005. Saat ini menjadi PNS di Pemerintah Kota Yogyakarta.

Dr. Ir. Eko Nugroho, M.Si., memperoleh gelar Insinyur (Ir.), Jurusan Teknik Elektro Universitas Gadjah Mada Yogyakarta, lulus Tahun 1978. Memperoleh gelar Magister Sains (M.Si.) Jurusan Akuntasi Manajemen Universitas Gajah Mada Yogyakarta, lulus Tahun 1992. Memperoleh gelar Doktor (Dr.) Jurusan *Cognitive Psychology* Universitas Gajah Mada Yogyakarta, lulus Tahun 2004. Saat ini menjadi Dosen di Universitas Gadjah Mada Yogyakarta.

Dani Adhipta, S.Si., M.T., memperoleh gelar Sarjana Sains (S.Si.), Jurusan Fisika Universitas Gadjah Mada Yogyakarta pada Tahun 1994. Memperoleh gelar Magister Teknik (M.T.) dari Jurusan Teknik Elektro Universitas Gadjah Mada Yogyakarta pada Tahun 1998. Saat ini menjadi Dosen di Universitas Gadjah Mada Yogyakarta.