

## IT PROCESS DARI COBIT 5 UNTUK AUDIT SISTEM INFORMASI KEUANGAN DALAM AUDIT LAPORAN KEUANGAN

Aris Irwanto<sup>1\*</sup>, Lukito Edi Nugroho<sup>2</sup>, Eko Nugroho<sup>3</sup>

<sup>\*123</sup> Jurusan Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada,  
Yogyakarta, Jl. Grafika No.2, 55281  
<sup>\*</sup>Email: aris.irwanto@mail.ugm.ac.id

### ABSTRAK

Sistem informasi keuangan negara merupakan sistem yang digunakan pemerintah dalam melaksanakan pengelolaan keuangan negara. Sistem informasi keuangan diharapkan dapat menghasilkan laporan keuangan yang handal, akurat, tepat waktu dan akuntabel. Untuk dapat meyakini kehandalan laporan keuangan yang dihasilkan dari sistem informasi, Badan Pemeriksa Keuangan (BPK) perlu melakukan audit sistem informasi dalam audit laporan keuangan. Penelitian ini akan meneliti melalui survey yang dilakukan kepada auditor BPK untuk menentukan *IT process* terpenting dari 37 *IT process* yang ada dalam kerangka kerja COBIT 5 yang dapat dijadikan acuan dalam melakukan audit sistem informasi dalam audit laporan keuangan. Hasil yang didapatkan terdapat 8 (delapan) *IT process* terpenting dari 5 domain yang terdapat dalam kerangka kerja COBIT 5. *IT process* terpenting tersebut dinilai penting oleh auditor untuk dapat diterapkan oleh auditor BPK dalam melaksanakan audit sistem informasi dalam audit laporan keuangan.

**Kata Kunci:** audit sistem informasi, COBIT 5, *IT Process*, audit laporan keuangan

### ABSTRACT

*Government financial information system is a system that used by the government in implementing financial management. Financial information system is expected to produce financial statements are reliable, accurate, timely, and accountable. To ensure reliability of financial statements, that generated from information system, Badan Pemeriksa Keuangan (BPK) need to do information system audit during financial audit. This research will examine by survey to BPK auditor to determine the important of IT process from COBIT 5 which can be used as a guidance to do information system audit during financial audit. The result there are 8 (eight) IT process from 5 domain in the COBIT 5. The important of IT process that choosen by auditor can be implemented by BPK auditor to do information system audit during financial audit.*

**Keywords:** information system audit, COBIT 5, *IT Process*, financial audit

### PENDAHULUAN

Undang-undang keuangan negara membawa dampak pada perlunya sebuah sistem pengelolaan keuangan negara yang transparan dan akuntabel. Pengelolaan keuangan negara yang transparan dan akuntabel dapat dicapai jika pemerintah pusat/daerah menyelenggarakan pengendalian atas pengelolaan keuangan negara. Penyelenggaraan kegiatan dan pengelolaan keuangan negara mulai dari perencanaan, pelaksanaan, pengawasan sampai pertanggungjawaban diselenggarakan secara tertib, terkendali, efektif dan efisien.

Menurut undang-undang no.60 tahun 2008 sistem pengendalian internal merupakan sebuah proses yang integral pada aktivitas yang dilakukan secara berkelanjutan oleh pimpinan organisasi dan seluruh bawahannya untuk dapat memeberikan keyakinan akan tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien, keandalan dalam pelaporan keuangan, pengamanan asset negara, dan kepatuhan terhadap peraturan perundang-undangan (Indonesia 2008).

Pemanfaatan teknologi informasi dalam pengendalian internal dapat dilakukan melalui penambahan prosedur pengendalian baru yang dilakukan oleh komputer dan bisa juga melalui

penggantian pengendalian yang biasa dilakukan secara manual yang rentan akan kesalahan dengan pengendalian berbasis teknologi.

Salah satu bentuk pertanggungjawaban pemerintah dalam pengelolaan keuangan negara adalah laporan keuangan pemerintah. Seiring dengan semakin pesatnya perkembangan teknologi informasi, membuat organisasi pemerintah mengandalkan teknologi informasi ke dalam aktivitasnya. Teknologi informasi berperan dalam menyediakan informasi yang bermanfaat bagi para pengambil keputusan dalam organisasi termasuk dalam hal pelaporan sehingga mendukung proses pengambilan keputusan dengan lebih efektif (Nugroho 2001).

Dalam hubungannya dengan pengelolaan keuangan negara, teknologi informasi membawa perubahan pada proses pencatatan, pengolahan dan pelaporan keuangan dari sistem yang manual menjadi terkomputerisasi. Salah satunya dengan memanfaatkan sistem informasi dalam pengelolaan keuangan pemerintah. Sistem informasi keuangan negara merupakan sistem informasi yang digunakan pemerintah dalam melaksanakan pengelolaan keuangan negara. Pemanfaatan sistem informasi keuangan tersebut diharapkan dapat menghasilkan laporan keuangan yang handal, akurat, tepat waktu dan akuntabel.

Pengendalian internal merupakan media utama auditor untuk meyakini bahwa laporan keuangan bebas dari kemungkinan kesalahan saji dan kecurangan. Pengendalian internal yang baik akan menjamin ketelitian data yang dihasilkan sehingga data dan informasi yang dihasilkan dapat diyakini kebenarannya (Syafriana 2014).

Sesuai dengan amanat Undang-undang No.15 tahun 2006, Badan Pemeriksa Keuangan (BPK) bertugas memeriksa pengelolaan dan tanggung jawab keuangan negara yang dilakukan yang dilakukan oleh pemerintah pusat, pemerintah daerah, badan dan lembaga yang mengelola keuangan negara (Republik Indonesia 2006). Pemeriksaan keuangan dilakukan BPK dalam rangka memberikan pernyataan opini tentang tingkat kewajaran informasi yang disajikan dalam laporan keuangan pemerintah (Republik Indonesia 2004). Menurut SA 335 dan SA 314 dalam Standar Profesional Akuntan Publik (SPAP),

mengharuskan pemeriksa melakukan audit TI apabila pemeriksa melakukan pemeriksaan di lingkungan TI (Ikatan Akuntan Indonesia n.d.). Lingkungan TI tersebut adalah lingkungan dimana pengelolaan keuangan negara dilakukan dengan memanfaatkan teknologi informasi dalam sebuah sistem informasi.

Ron Webber (1999) menyatakan audit sistem informasi sebagai sebuah proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah sistem informasi terkomputerisasi telah menetapkan dan menerapkan sistem pengendalian internal yang memadai, semua aktiva organisasi dilindungi dengan baik/ tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer.

Audit sistem informasi tersebut dilakukan untuk dapat menilai (a) apakah sistem informasi terkomputerisasi suatu organisasi dapat mendukung pengamanan aset organisasi, (b) apakah sistem informasi terkomputerisasi dapat mendukung pencapaian tujuan organisasi, (c) apakah sistem informasi terkomputerisasi tersebut efektif, efisien, dan dapat menjamin integritas data.

Audit sistem informasi dapat digolongkan ke dalam jenis: (1) Audit laporan keuangan, audit ini dilakukan untuk mengetahui tingkat kewajaran laporan keuangan yang disajikan oleh organisasi ( apakah sudah sesuai dengan standar akuntansi yang ada dan tidak menyalahi uji materialitas. Apabila organisasi menerapkan sistem informasi dalam pengelolaan keuangan maka perlu dilakukan audit terhadap sistem informasi akuntansi apakah proses dan program telah sesuai, apakah pengendalian umum dan pengendalian aplikasi telah memadai. (2) Audit operasional, dalam audit ini dibedakan menjadi tiga jenis antara lain: (a) *Post implementation audit*, audit yang dilakukan terhadap sistem-sistem yang telah diimplementasikan pada suatu organisasi apakah telah sesuai dengan kebutuhan (efektif) dan apakah telah dijalankan secara efisien. Pada audit ini akan dievaluasi apakah sistem informasi yang telah diimplementasikan perlu adanya modifikasi, atau perbaikan atau penghentian apabila sudah tidak sesuai dengan organisasi. (b) *Concurrent Audit*, dimana auditor menjadi bagian dari tim pengembangan sistem informasi, guna membantu

meningkatkan kualitas sistem yang sedang dibangun dan akan diimplementasikan. (c) *General audit*, dimana untuk mengevaluasi kinerja unit fungsional/ pengelola sistem informasi untuk menilai apakah sistem informasi telah dikelola dengan baik, apakah kontrol dalam pengembangan sistem informasi sudah baik, apakah sistem informasi dikelola dan dioperasikan dengan baik.

Audit sistem pengendalian dalam sebuah sistem informasi komputerisasi sangat penting untuk dilaksanakan, menurut Ron Weber (1999, p11) hal tersebut dikarenakan: (1) Besarnya biaya dan kerugian apabila data yang ada dalam sebuah sistem informasi komputer hilang. (2) Biaya yang harus dibayarkan apabila salah dalam proses pengambilan keputusan bagi organisasi, hal ini dikarenakan informasi yang disajikan dari sebuah sistem informasi tidak valid. (3) Potensi kerugian yang harus diterima organisasi jika terjadi kesalahan penyalahgunaan sistem informasi komputer (*fraud*). (4) Pentingnya pengamanan aset organisasi karena perangkat *hardware*, *software* dan *brainware* bernilai tinggi. (5) Dapat mendeteksi risiko *error* komputer. (6) Menjaga kerahasiaan data dari pihak yang tidak berkepentingan. (7) Meningkatkan pengendalian evolusi penggunaan komputer (Ciptaningrum 2015).

Penelitian yang dilakukan Achyar 2015 tentang analisis audit sistem informasi berbasis COBIT 5 pada PT.Telkom, memilih domain *Deliver*, *Support*, dan *Service* (DSS) dan berfokus pada penilaian pengiriman dan layanan teknologi informasi dan dukungan terhadap proses bisnis organisasi. Hasil yang didapat dapat menilai *Capability Level* dan *Optimizing Process*, namun masih perlu untuk melakukan dan menilai inovasi yang dilakukan dengan menggunakan domain *Align*, *Plan* dan *Organize* (APO) (Al-rasyid 2015).

Menurut Ciptaningrum (2015) dalam penelitiannya untuk melakukan audit Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta dengan menggunakan COBIT5. Penelitian dilakukan dengan memetakan 17 tujuan TI organisasi dan selanjutnya dipetakan lagi terhadap 37 proses yang terdapat dalam kerangka kerja COBIT 5. Dari hasil pemetaan terhadap tujuan TI organisasi yaitu “Keamanan Informasi, Infrastruktur Pengolahan dan Aplikasi” dengan 37 proses COBIT 5. Hasil yang didapatkan 5

proses primer yang terkait untuk kewanaman informasi adalah EDM03-Memastikan Optimasi Risiko, APO12 - Mengelola Risiko, APO13 - Mengelola Keamanan, BAI06 - Mengelola Perubahan dan DSS05 - Mengelola Perubahan. Selanjutnya ke lima proses tersebut digunakan untuk melakukan penilaian/audit kapabilitas keamanan SI (Ciptaningrum 2015).

Zulkarnaen meneliti dengan menggunakan framework COBIT 4.1 untuk mengevaluasi Sistem Informasi Manajemen Kepegawaian (SIMPEG) pada Kementerian Agama Kantor Kota Pekanbaru. Domain yang digunakan untuk mengevaluasi sistem informasi tersebut adalah domain DS1-*Define and Manage Service*. Metode yang digunakan adalah dengan melakukan survey untuk menilai *management awareness* dari organisasi terhadap pengelolaan SIMPEG. Selain itu juga dengan melakukan analisa terhadap tingkat kematangan pada domain *Deliver and Support DS-1*. Untuk melihat kondisi sistem organisasi dan manajemen organisasi tidak cukup dengan melihat pada domain DS-1 *Define and Manage Service* tetapi bisa dengan melihat seluruh *control objective* yang ada pada domain *Deliver and Support* (Zulkarnaen 2016).

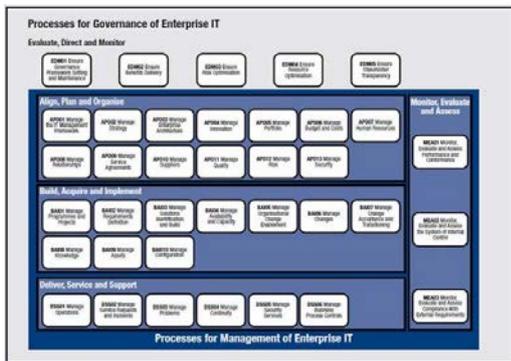
Penelitian ini akan menentukan *IT process* dari 37 proses dalam kerangka kerja COBIT 5, yang terpenting menurut auditor BPK dalam pengelolaan teknologi informasi khususnya sistem informasi pengelolaan keuangan negara. Hasil dari *IT process* terpenting tersebut akan digunakan oleh auditor BPK untuk dijadikan pedoman dalam melakukan audit sistem informasi dalam audit laporan keuangan.

*Control Objectives for Information and Related Technology* (COBIT) dapat dijelaskan sebagai alat pengendalian untuk informasi dan teknologi terkait dan merupakan standar untuk pengendalian terhadap teknologi informasi yang dikembangkan oleh *Information System Audit and Control Association* (ISACA). COBIT mendefinisikan pengendalian internal sebagai sebuah kebijakan, prosedur, dan praktik dan struktur organisasi yang dirancang untuk memberikan keyakinan yang wajar bahwa tujuan organisasi dapat dicapai dan hal-hal yang tidak diinginkan dapat dicegah atau dideteksi dan diperbaiki. Sedangkan tujuan pengendalian menurut COBIT adalah suatu pernyataan atas hasil yang diinginkan atau tujuan yang ingin dicapai dengan

mengimplementasikan prosedur pengendalian dalam aktivitas TI tertentu (ISACA 2012).

Kerangka kerja COBIT menjelaskan beberapa pengendalian TI dan proses keamanan yang bisa digunakan organisasi untuk meningkatkan tujuan bisnis organisasi dan meningkatkan pengendalian internal. [Kerr, Murt]. COBIT memiliki fokus pengendalian yang kuat, sejak itulah banyak auditor baik internal atau eksternal menerapkannya pada audit laporan keuangan, selain digunakan pada audit operasional dan kinerja (Tuttle & Vandervelde 2007).

Fokus kerangka pengendalian COBIT adalah pada pengelolaan dan pengendalian TI. Dalam kerangka kerja COBIT 5 menyebutkan ada 5 tujuan pengendalian tingkat tinggi yang terbagi dalam 5 domain, 1 domain berada di area “governance” (*Evaluate, Direct, Monitor*) EDM dan 4 domain di area “management” yaitu: (*Align, Plan, Organize*) APO, (*Build, Acquire, Implement*) BAI, (*Deliver, Service, Support*) DSS, (*Monitor, Evaluate, Assess*) MEA. Dalam setiap domain terdapat proses spesifik yang yang harus dijalankan organisasi untuk mencapai tujuan pengendalian TI secara detail dan spesifik.



Gambar 1. Proses TI dalam COBIT 5

Dari 5 domain tersebut terbagi menjadi 37 proses antara lain: **Domain EDM** (*Evaluate, Direct, and Monitor*). Proses pada domain ini berurusan dengan para pemangku kepentingan dalam melakukan penilaian, optimasi risiko, dan sumber daya. Tujuan domain ini adalah untuk mengevaluasi rencana strategis TI, memberikan arahan kepada TI, dan pemantauan hasilnya.

Tabel 1. Proses TI domain EDM

EDM 01	Pengaturan Kerangka Tata Kelola dan Pemeliharaan
--------	--

EDM 02	Memastikan Adanya Nilai Tambah
EDM 03	Memastikan Identifikasi Risiko
EDM 04	Memastikan Sumber Daya Yang Dipilih Tepat
EDM 05	Memastikan Keterbukaan Antar Stakeholder

**Domain APO** (*Align, Plan, Organize*).

Proses pada domain ini mencakup strategi dan taktik, dan mengidentifikasi cara terbaik TI agar dapat berkontribusi pada pencapaian tujuan bisnis organisasi.

Tabel 2. Proses TI domain APO

APO 01	Mengelola Kerangka Kerja Manajemen
APO 02	Mengelola Strategi
APO 03	Mengelola Arsitektur Sistem
APO 04	Mengelola Inovasi
APO 05	Mengelola Pemetaan Strategi
APO 06	Mengelola Pembiayaan
APO 07	Mengelola Sumber Daya Manusia
APO 08	Mengelola Hubungan
APO 09	Mengelola Perjanjian Kesepakatan Layanan
APO 010	Mengelola Penyedia Layanan TI
APO 011	Mengelola Kualitas
APO 012	Mengelola Risiko
APO 013	Mengelola Keamanan

**Domain BAI** (*Build, Acquire, and Implement*).

Proses pada domain ini mengidentifikasi solusi TI, dikembangkan dan diimplementasikan untuk mewujudkan strategi TI yang sesuai dengan tujuan organisasi.

Tabel 3. Proses TI domain BAI

BAI 01	Menyiapkan Program dan Kegiatan
BAI 02	Mengidentifikasi Kebutuhan
BAI 03	Mengidentifikasi Solusi dan Pengembangan
BAI 04	Mengelola Ketersediaan dan Kemampuan
BAI 05	Mengelola Pemberdayaan Perubahan Organisasi
BAI 06	Mengelola Perubahan
BAI 07	Mengelola Penerimaan Perubahan dan Masa Transisi Perubahan
BAI 08	Mengelola Pengetahuan
BAI 09	Mengelola Aset
BAI 010	Mengelola Konfigurasi

**Domain DSS** (*Deliver, Support, and Service*).

Proses pada domain ini mencakup penyampaian hasil actual dari layanan yang

yang diminta termasuk pengelolaan kelancaran dan keamanan, dukungan layanan terhadap pengguna serta pengelolaan data dan operasional.

Tabel 4. Proses TI domain DSS

DSS 01	Mengelola Operasional
DSS 02	Mengelola Permintaan User dan Perbaikan
DSS 03	Mengelola Permasalahan
DSS 04	Mengelola Keberlanjutan
DSS 05	Mengelola Layanan Keamanan
DSS 06	Mengelola Pengawasan Proses Bisnis

**Domain MEA (Monitor, Evaluate, and Assess).** Proses pada domain ini terkait dengan kinerja manajemen, kontrol internal, pemenuhan terhadap aturan serta menyediakan tata kelola. Fungsi domain ini sendiri adalah untuk memastikan seluruh proses TI dapat dikontrol secara periodik yang bermaksud untuk menjaga kualitas dan pemenuhan kebutuhan organisasi.

Tabel 5. Proses TI domain MEA

MEA 01	Mengawasi, Mengevaluasi, dan Menilai Kinerja dan Kesesuaian
MEA 02	Mengawasi, Mengevaluasi, dan Menilai Internal Kontrol
MEA 03	Mengawasi, Mengevaluasi, dan Menilai Kepatuhan Terhadap Peraturan Eksternal

Menurut Whitten (2004), sistem informasi merupakan susunan dari orang-orang, kegiatan, data, jaringan dan teknologi yang diintegrasikan sedemikian rupa dengan tujuan untuk mendukung dan memperbaiki operasi sehari-hari organisasi serta memenuhi kebutuhan informasi baik untuk pengambilan keputusan maupun pemecahan masalah.

Untuk dapat memenuhi tujuan organisasi, informasi harus memenuhi kriteria tertentu, 7 kriteria informasi yang menjadi fokus kerangka COBIT antara lain: (1) Efektivitas, menitik beratkan pada sejauh mana efektifitas informasi dikelola dari data-data yang diproses oleh sistem informasi yang dibangun (2) Efisiensi, menitik beratkan pada sejauh mana efisiensi investasi terhadap informasi yang diproses oleh sistem (3) Kerhasiaan, menitikberatkan pada pengelolaan

kerahasiaan informasi secara hierarkis (4) Integritas, menitikberatkan pada integritas data/informasi dalam sistem (5) Ketersediaan, menitikberatkan pada ketersediaan data yang dihasilkan dari sistem (6) Kepatuhan, menitikberatkan pada kesesuaian data/informasi dalam sistem informasi dan (7) Keandalan, menitikberatkan pada kemampuan/ketangguhan sistem informasi dalam pengelolaan data/informasi.

Sistem informasi tersusun atas tiga komponen utama, yaitu *building block*, komputer, dan organisasi (Hernyka 2014). Dalam *building block*, sistem informasi terdiri atas: (1) Blok masukan (input) yang mewakili sejumlah data yang masuk ke dalam sistem informasi. (2) Blok model yang terdiri dari kombinasi prosedur, logika, dan model matematika yang akan memanipulasi data input dan data yang tersimpan di database dengan cara tertentu untuk menghasilkan output yang diinginkan. (3) Blok keluaran (output), produk dari sistem informasi adalah keluaran yang merupakan informasi dan dokumentasi yang dapat digunakan oleh semua pemakai sistem informasi. (4) Blok teknologi, merupakan tool dalam sistem informasi yang digunakan untuk menerima masukan, menjalankan model, menyimpan dan mengakses data menghasilkan dan mengirimkan keluaran dan membantu pengendalian sistem. (5) Blok basis data, merupakan kumpulan dari data yang saling berhubungan satu sama lain, tersimpan pada perangkat keras komputer dan menggunakan perangkat lunak untuk mengolahnya. (6) Blok kendali (control), bagian ini dirancang dan diterapkan untuk memelihara sistem dari hal-hal yang dapat merusaknya, seperti factor alami, virus, sabotase. Di sisi komputer, tersusun atas: (1) *Hardware* (perangkat keras) yang terdiri dari perangkat input, output dan perangkat jaringan telekomunikasi. (2) *Software* (perangkat lunak), merupakan sejumlah instruksi untuk mengendalikan operasi dari sistem pemrosesan dan digunakan untuk mengelola sumber daya komputer. (3) *Brainware* (operator) adalah manusia yang terlibat secara langsung dalam pengelolaan sistem informasi. (4) Prosedur, merupakan serangkaian peraturan-peraturan atau langkah yang menentukan operasi sistem informasi, atau bisa juga berisi kebijakan-kebijakan organisasi dalam menentukan arah sistem

informasi. (5) Basis data, berisi data yang saling berhubungan dan terorganisir, terpadu dan teratur disimpan menurut aturan tertentu yang memudahkan untuk mengakses kembali. Pada sisi organisasi komponen yang mendukung sebuah sistem informasi antara lain: (1) Tempat kerja, tempat dimana SDM bekerja menjalankan sistem informasi. (2) Sumber daya manusia operasional, merupakan SDM yang berhubungan langsung dengan aktivitas organisasi di luar SDM sistem informasi. (3) Budaya organisasi, merupakan cara-cara yang dilakukan oleh para anggota dalam organisasi dalam mengelola sistem informasi. (4) Aset, yaitu aset yang dimiliki organisasi seperti hak cipta, peralatan, paten. (5) Pengaruh, merupakan pengaruh lingkungan terhadap organisasi dalam penerapan sistem informasi.

**METODE**

Penelitian ini akan menggunakan metode kualitatif yang dilakukan dalam 3 (tahap). Tahap pertama adalah dengan melakukan kajian pustaka dan studi literatur, tahap kedua dengan melakukan survey yang ditujukan kepada auditor Badan Pemeriksa Keuangan (BPK) baik yang berada di kantor pusat BPK maupun yang ada di unit kerja kantor perwakilan BPK yang tersebar di seluruh Indonesia. Instrument pertama yang digali dari partisipan adalah jenis kelamin, usia, masa kerja di BPK, unit kerja saat ini, jabatan dalam sebuah tim audit, dan pernah atau belum dalam mengikuti pelatihan audit TI.

Partisipan akan diberi pertanyaan untuk menilai dalam skala likert dengan skala 1 sampai 6, dimana skala N = tidak mungkin diterapkan, 1 = sangat tidak penting, 2 = tidak penting, 3 = cukup penting, 4 = penting, 5 = sangat penting. Partisipan diminta untuk menilai pentingnya 37 proses TI dari COBIT 5 dalam hal pengelolaan sistem informasi keuangan untuk menghasilkan informasi yang akurat dan handal dalam penyusunan laporan keuangan. Karakteristik partisipan tersaji dalam tabel 6.

Tabel 6. Karakteristik partisipan

	Frekuensi	Prosentase
<b>Jenis Kelamin</b>		
Laki-laki	23	63,89
Perempuan	13	36,11

<b>Usia</b>		
25-30	11	30,56
31-35	13	36,11
36-40	4	11,11
41-45	5	13,89
46-50	2	5,56
51-55	1	2,78
<b>Masa Kerja</b>		
<4 tahun	2	5,56
4-6 tahun	6	16,67
7-9 tahun	15	41,67
10-12 tahun	4	11,11
> 12 tahun	9	25,00
<b>Jabatan dalam Tim audit</b>		
Anggota Tim	29	80,56
Ketua Tim	7	19,44
<b>Pelatihan audit TI</b>		
Pernah	19	52,78
Belum	17	47,22

Rata-rata usia partisipan berada di usia 30-35 tahun, 64% berjenis kelamin laki-laki, 42% telah bekerja di BPK 7-9 tahun, 64% merupakan auditor yang unit kerjanya di kantor perwakilan, 82% memegang peranan sebagai anggota tim dalam sebuah tim audit, dan 53% sudah pernah mengikuti pelatihan terkait audit TI/ sistem informasi.

Survey dilakukan untuk mendapatkan masukan terkait *IT process* terpenting dari 37 *IT process* yang terdapat dalam kerangka kerja COBIT 5, yang dapat dijadikan pedoman atau acuan dalam melaksanakan audit sistem informasi dalam audit laporan keuangan. Tahap ketiga adalah dengan melakukan perhitungan untuk mendapatkan 10 besar proses COBIT yang paling penting melakukan analisa terhadap *IT process* yang paling penting.

**HASIL DAN PEMBAHASAN**

Dari hasil survey yang didapatkan dari 36 orang partisipan, selanjutnya dilakukan perhitungan jumlah dan nilai rata-rata dari tiap proses TI yang terdapat dalam 5 (lima) domain COBIT. Dari hasil perhitungan jumlah dan rata-rata selanjutnya 37 proses TI tersebut diurutkan berdasarkan nilai rata-rata tertinggi sampai rata-rata terendah. Hasil perhitungan jumlah dan rata-rata serta peringkat tersaji dalam tabel 7.

**Tabel 7.** Hasil perhitungan dan rata-rata

No	Proses TI domain COBIT 5	Jumlah	Rata-rata
1	APO07 - Mengelola Sumber Daya Manusia	162	4,5
2	APO013 - Mengelola Keamanan	159	4,42
3	DSS02 - Mengelola Permintaan User dan Perbaikan	154	4,28
4	APO03 - Mengelola Arsitektur Sistem	153	4,25
5	DSS05 - Mengelola Layanan Keamanan	153	4,25
6	DSS03 - Mengelola Permasalahan	152	4,22
7	MEA02 - Mengawasi, Mengevaluasi, dan Menilai Internal Kontrol MEA03 - Mengawasi, Mengevaluasi, dan Menilai Kepatuhan Terhadap	152	4,22
8	Peraturan Eksternal	152	4,22
9	EDM02 - Memastikan Adanya Nilai Tambah	151	4,19
10	EDM04 - Memastikan Sumber Daya Yang Dipilih Tepat	151	4,19
11	APO06 - Mengelola Pembiayaan	151	4,19
12	BAI03 - Mengidentifikasi Solusi dan Pengembangan	151	4,19
13	DSS04 - Mengelola Keberlanjutan MEA01 - Mengawasi, Mengevaluasi, dan Menilai Kinerja dan	151	4,19
14	Kesesuaian	151	4,19
15	APO011 - Mengelola Kualitas	150	4,17
16	BAI01 - Menyiapkan Program dan Kegiatan	150	4,17
17	BAI09 - Mengelola Aset	150	4,17
18	EDM01 - Pengaturan Kerangka Tata Kelola dan Pemeliharaan	149	4,14
19	EDM05 - Memastikan Keterbukaan Antar Stakeholder	149	4,14
20	APO02 - Mengelola Strategi	149	4,14
21	APO08 - Mengelola Hubungan	149	4,14
22	BAI04 - Mengelola Ketersediaan dan Kemampuan	149	4,14
23	DSS06 - Mengelola Pengawasan Proses Bisnis	149	4,14
24	APO04 - Mengelola Inovasi	148	4,11
25	APO05 - Mengelola Pemetaan Strategi	148	4,11
26	APO09 - Mengelola Perjanjian Kesepakatan Layanan	148	4,11
27	APO010 - Mengelola Penyedia Layanan TI	148	4,11
28	APO012 - Mengelola Risiko	148	4,11
29	BAI06 - Mengelola Perubahan	147	4,08
30	BAI07 - Mengelola Penerimaan Perubahan dan Masa Transisi Perubahan	147	4,08
31	DSS01 - Mengelola Operasional	147	4,08
32	BAI02 - Mengidentifikasi Kebutuhan	146	4,06
33	EDM03 - Memastikan Identifikasi Risiko	145	4,03
34	BAI08 - Mengelola Pengetahuan	145	4,03
35	BAI05 - Mengelola Pemberdayaan Perubahan Organisasi	144	4,00
36	BAI010 - Mengelola Konfigurasi	144	4,00
37	APO01 - Mengelola Kerangka Kerja Manajemen	142	3,94

Dari hasil perhitungan rata-rata dan peringkat dapat diperoleh proses TI dari domain di COBIT 5 yang terpenting untuk dapat dijadikan panduan dalam melaksanakan audit sistem informasi keuangan dalam audit laporan keuangan. Dari peringkat proses TI dengan rata-rata tertinggi sampai rata-rata

terendah dapat ditentukan lagi peringkat 5 (lima) besar proses TI yang menjadi prioritas untuk dijadikan acuan dalam audit sistem informasi dalam audit laporan keuangan berdasarkan nilai rata-ratanya.

Tabel 8. Proses TI yang menjadi prioritas.

No	Domain	Jumlah	Rata-rata
1	APO07 - Mengelola Sumber Daya Manusia	162	4,5
2	APO013 - Mengelola Keamanan	159	4,42
3	DSS02 - Mengelola Permintaan User dan Perbaikan	154	4,28
4	APO03 - Mengelola Arsitektur Sistem	153	4,25
5	DSS05 - Mengelola Layanan Keamanan	153	4,25
6	DSS03 - Mengelola Permasalahan	152	4,22
7	MEA02 - Mengawasi, Mengevaluasi, dan Menilai Internal Kontrol MEA03 - Mengawasi, Mengevaluasi, dan Menilai Kepatuhan Terhadap	152	4,22
8	Peraturan Eksternal	152	4,22

Berdasarkan tabel 8, terdapat 8 (delapan) proses TI dalam COBIT 5 yang dapat dijadikan pedoman dalam melakukan audit sistem informasi keuangan dalam audit laporan keuangan. Proses TI tersebut adalah APO07 (mengelola sumber daya manusia) proses TI ini digunakan untuk memastikan struktur sumber daya manusia dalam organisasi, penempatan sumber daya manusia apakah telah sesuai dengan tugas pokok dan fungsinya serta kompetensinya dalam organisasi, peningkatan pengetahuan dan ketrampilan yang optimal apakah telah dilakukan untuk menunjang kinerja sumber daya manusia, dan memastikan apakah personil dalam organisasi termotivasi untuk mengoptimalkan kinerjanya dalam organisasi untuk memenuhi tujuan organisasi. APO13 (mengelola keamanan), proses ini digunakan untuk memastikan apakah sistem keamanan informasi dalam organisasi telah didefinisikan dan ditetapkan dengan sebuah peraturan, dijalankan dan dimonitor. DSS02 (mengelola permintaan user dan permintaan perbaikan), proses ini digunakan untuk memastikan apakah permintaan user dan *incident* telah diklasifikasi, diinvestigasi, diprioritasi, dan mendapat persetujuan dari atasan dan dilaporkan secara berkala. APO03 (mengelola arsitektur sistem), digunakan untuk memastikan apakah sebuah arsitektur sistem yang terdiri dari proses bisnis, informasi, data, aplikasi, dan arsitektur teknologi informasi telah dikembangkan dan dikelola sesuai dengan kebutuhan organisasi. Pada DSS05 (mengelola layanan keamanan) digunakan untuk memastikan data dan informasi yang dimiliki organisasi terjaga keamanannya dari akses

yang illegal serta memastikan pengelolaan keamanan pada sisi jaringan dan infrastruktur. DSS03 (mengelola permasalahan) proses TI ini digunakan untuk memastikan apakah permasalahan terkait sistem informasi telah diidentifikasi, diklasifikasikan, dicari akar permasalahannya, dicarikan solusi dan pencegahan untuk terjadinya permasalahan yang sama dalam sebuah organisasi.

Pada domain MEA (*monitor, evaluate, dan asses*) terdapat dua proses terpenting yakni: MEA02 (mengawasi, mengevaluasi, dan menilai internal kontrol), proses ini digunakan untuk menilai apakah organisasi telah mengawasi, mengevaluasi serta menilai pengendalian internalnya secara independen, dan menilai apakah organisasi telah mengidentifikasi kelemahan atas internal kontrolnya, dan merancang untuk perbaikan pengendalian internal dalam organisasi. MEA03 (mengawasi, mengevaluasi, dan menilai kepatuhan terhadap peraturan eksternal), proses ini digunakan untuk menilai apakah organisasi telah menilai secara internal proses TI dan proses bisnis TI organisasinya telah sesuai dengan peraturan hukum perundangan yang berlaku.

Dari hasil wawancara dengan beberapa auditor, memastikan pengelolaan sumber daya manusia dalam audit sistem informasi dinilai penting karena dari hasil pengalaman audit di lapangan banyak dijumpai lemahnya pengelolaan sumber daya manusia sebagai pengguna sistem informasi keuangan, seperti penempatan personil yang tidak sesuai dengan background pendidikannya, tidak dapat mengelola personil-personil unggulan dalam

organisasi, kurangnya pelatihan dan pengembangan ketrampilan personil, tidak adanya evaluasi terhadap kinerja sumber daya manusia yang dimiliki. Selanjutnya yang menjadi prioritas dalam melakukan audit sistem informasi keuangan adalah menilai keamanan sebuah sistem informasi dan pengelolaan layanan keamanan informasi yang dimiliki organisasi. Keamanan sistem informasi dan layanan keamanan sistem merupakan hal yang penting dalam organisasi, namun perhatian dari pemilik dan pengelola sistem informasi keuangan masih sangat relatif kurang. Perlindungan terhadap data dan informasi yang dimiliki organisasi merupakan hal yang mutlak harus dilakukan secara total oleh pimpinan dan pengguna sistem informasi yang bersangkutan. Termasuk di dalamnya terkait kebijakan, prosedur, proses dan aktivitas untuk melindungi data dan informasi dari ancaman dan penyalahgunaan guna menjaga kerahasiaan, integritas, dan ketersediaan informasi (Indrajit n.d.).

Yang perlu mendapat perhatian berikutnya adalah terkait permintaan user pengguna, pengelolaan arsitektur, dan pengelolaan permasalahan atas sistem informasi keuangan. Dari hasil pengamatan auditor di lapangan pengembangan sebuah sistem informasi keuangan oleh organisasi tidak direncanakan dan dikaji secara sistematis terkait pengembangan dan arsitektur sistem informasi yang akan digunakan. Pengelolaan permasalahan dan permintaan user pengguna sistem informasi keuangan perlu mendapat sorotan karena banyaknya permasalahan-permasalahan yang timbul dari pengembangan dan penggunaan sistem informasi yang tidak dikelola secara memadai dan permintaan user terkait perubahan sistem informasi keuangan tidak adanya otorisasi dari pihak yang berwenang terkait permintaan perubahan sistem.

Mengawasi, mengevaluasi dan menilai pengendalian internal organisasi dan kepatuhan terhadap peraturan eksternal oleh organisasi juga perlu mendapat perhatian auditor. Hal ini dikarenakan masih banyak ditemukan dalam audit laporan keuangan terkait lemahnya pengendalian internal organisasi dalam pengelolaan keuangan negara. Menilai dan mengevaluasi kepatuhan terhadap peraturan eksternal dinilai penting karena disamping kepatuhan terhadap

peraturan perundangan yang ada dalam organisasi guna menjaga kehandalan dan integritas sistem informasi keuangan yang digunakan.

## SIMPULAN

Dari hasil pembahasan, didapatkan hal-hal yang perlu mendapat perhatian auditor pertama kali dalam melakukan audit TI dalam audit laporan keuangan, antara lain: menilai pengelolaan sumber daya manusia pengguna sistem informasi, pengelolaan keamanan sistem informasi dan layanan keamanan, pengelolaan arsitektur sistem, permintaan user pengguna sistem dan pengelolaan permasalahan yang timbul selama pengembangan dan penggunaan sistem informasi. Penilaian terhadap evaluasi dan pengawasan yang dilakukan pengawas internal organisasi terkait pengendalian internal dan kepatuhan terhadap peraturan eksternal juga perlu mendapat perhatian untuk pertama kalinya.

## DAFTAR PUSTAKA

- Al-rasyid, A., 2015. Analisis Audit Sistem Informasi Berbasis COBIT 5 Pada Domain Deliver , Service , and Support ( DSS ) ( Studi Kasus : SIM-BL di Unit CDC PT Telkom Pusat . Tbk ) . , 2(2), pp.6110–6123.
- Ciptaningrum, D., 2015. Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5. *Sentika*, 2015(Sentika), p.6.
- Hernyka, Di.S., 2014. Audit Sistem Informasi Akademik Perguruan Tinggi PT XYZ menggunakan CObit. 4.1.
- Ikatan Akuntan Indonesia, Standar Profesional Akuntan Publik, SA315, SA314.
- Indonesia, 2008. Peraturan Pemerintah No.60 Tahun 2008 Tentang Sistem Pengendalian Intern Pemerintah.
- Indrajit, R.E., Kerangka Standar Keamanan Informasi.
- ISACA, 2012. COBIT 5, Business Framework for the Governance and Management of Enterprise IT.
- Nugroho, W., 2001. Sistem Informasi Akuntansi. Erlangga: Jakarta.
- Republik Indonesia, 2004. Undang-Undang Republik Indonesia No.15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan

- Tanggung Jawab Keuangan Negara. , pp.1–25.
- Republik Indonesia, 2006. Undang-Undang Republik Indonesia No.15 Tahun 2006 tentang Badan Pemeriksa Keuangan. , pp.1–25.
- Syafriana, F., 2014. Peranan pengendalian internal dalam mengantisipasi kecenderungan kecurangan akuntansi (Studi kasus PT.Taspen, Tanjungpinang).
- Tuttle, B. & Vandervelde, S.D., 2007. An empirical examination of CobiT as an internal control framework for information technology. , 8(2), pp.240–263.
- Zulkarnaen, A., 2016. EVALUASI SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN ( SIMPEG ) MENGGUNAKAN FRAMEWORK COBIT 4 . 1 ( Studi Kasus : Kementerian Agama Kantor Kota Pekanbaru ). , 2(2), pp.1–5.