The Implementation of COBIT 4.1 and COBIT 5-Based IT Governance Audits in the Ministry of Finance of Indonesia

NUR IMROATUN SHOLIHAT*

Inspectorate General of Ministry of Finance

Abstract: *Lately, organizations including the governmental ones started to realize the crucial role of IT for their organizations. For example, in the last 3 years, The Ministry of Finance (MoF) has spent Rp1.244 billion (USD 93,57 million) for IT investment itself. Weill (2004) stated that the benefit received from the IT investment is influenced by its governance. To ensure that IT is well-governed, IT governance audit is performed. In Indonesia, Inspectorate General of MoF is the first and only internal audit organization to carry out IT governance audit to date. IT governance audit in the Ministry of Finance has also implemented the globally accepted framework, COBIT. For those reasons, IT governance audit practice in the MoF could be the acceptable benchmark for another public sector organization about the aforesaid area of audit. This research aims to get the understanding about the implementation of IT governance audits in the Ministry of Finance (MoF) and compare them with Assessor Guide: Using COBIT 5. This study is important because meanwhile IT governance audit is important, to the best of author's knowledge, research about IT governance audit practice in Indonesia's public sector is very limited. To achieve the research's purpose, this research will be served as a qualitative descriptive research. The result showed that MoF's IT governance audit practice implemented Assessor Guide: Using COBIT 5 with some adjustments were done. Despite being in the early stage, the IT governance audit which combined COBIT 4.1 and COBIT 5 assessment approaches is fair performed.*

Keywords: COBIT 4.1, COBIT 5, IT Governance Audit, Ministry of Finance

Intisari: *Dewasa ini, organisasi termasuk organisasi pemerintah mulai menyadari peran penting TI untuk organisasi mereka. Misalnya, dalam 3 tahun terakhir, Kementerian Keuangan (Kemenkeu) telah menghabiskan Rp1.244 miliar (USD 93,57 juta) untuk investasi TI. Weill (2004) menyatakan bahwa manfaat yang diterima dari investasi TI dipengaruhi oleh tata kelolanya. Untuk memastikan bahwa TI dikelola dengan baik, audit tata kelola TI dilakukan. Di Indonesia, Inspektorat Jenderal Kemenkeu adalah organisasi audit internal pertama dan satu-satunya yang melakukan audit tata kelola TI hingga saat ini. Audit tata kelola TI di Kemenkeu juga telah menerapkan framework yang diterima secara global, COBIT. Untuk alasan tersebut, praktik audit tata kelola TI di Kemenkeu dapat menjadi tolok ukur bagi organisasi sektor publik lainnya tentang bidang audit tersebut.. Penelitian ini*

* Corresponding author: nurimroatun90@gmail.com

bertujuan untuk mendapatkan pemahaman tentang pelaksanaan audit tata kelola TI di Kemenkeu dan membandingkannya dengan Assessor Guide: Using COBIT 5. Studi ini penting sebab meskipun audit tata kelola TI penting, sepanjang pengetahuan penulis, penelitian tentang praktik audit tata kelola TI di sektor publik Indonesia sangat terbatas. Untuk mencapai tujuan penelitian, penelitian ini akan disajikan sebagai penelitian kualitatif deskriptif. Hasil penelitian menunjukkan bahwa praktik audit tata kelola TI Kemenkeu telah menerapkan Assessor Guide: Using COBIT 5 dengan beberapa penyesuaian. Meskipun berada di tahap awal, audit tata kelola TI yang menggabungkan pendekatan assessment COBIT 4.1 dan COBIT 5 telah dilakukan secara cukup baik.

Kata kunci: COBIT 4.1, COBIT 5, Audit Tata Kelola TI, Kementerian Keuangan

1. Introduction

These days, no longer can we imagine organization runs without information technology (IT). The utilization of IT is not a choice anymore but an obligation to make the business process functioned more efficiently and effectively. No wonder, many organizations make huge investments in IT to secure or maintain competitive advantages (Applegate et al., 2003). IT is not just critical to the private sector but has also become integral to the public sector in delivering efficient and cost-effective services to the public (Omari et al., 2013). Government organizations themselves have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information.

The evidence of this phenomenon is the utilization of IT by the government to give the information and public services to the people, that widely known as e-government. To promote the wide-scale utilization of IT, Indonesia's government established the regulations required and the newly "Palapa Ring" mega-project. Palapa Ring, which involves a huge undersea fiber-optic cable network that will offer faster broadband to the entire archipelago, signifies the government's commitment for ease and adequacy of IT access around the country.

The positive impacts of IT come as one package with the negative ones. Information systems encounter serious security threats that may arise from the weakness of the internal controls and/or the nature of the competitive environment as the need and dependency on information increases (Al-Hayale and Khadra, 2006).

Indonesia news site Tempo reported that network attack in Indonesia by the hacker counted until August 2015, had costed the country reached Rp33,29 billion. For that reason, organizations include the government ones started to pay attention to IT governance. For example, this year Indonesia State Owned Enterprise (BUMN) has to achieve maturity level 3 (defined) out of 5 which means IT governance processes are documented and communicated (PER-02/MBU/2013).

Furthermore, nowadays organizations spend a huge fund on IT investment. In Van Grembergen, De Haes and Guldentops (2004) terminology, proper IT governance is needed to ensure that the investments in IT will generate the required business value and that risks associated with IT are mitigated. To assess the IT governance level of an organization, IT assurance and/or audit process is being performed. Many companies around the world are aware of the benefits of IT auditing, including IT governance audit, which results in efficiency and profitability (Nkwe, 2011).

Ministry of Finance (MoF) uses IT to perform its duty better. The applications developed and used within MoF proved IT helps MoF's for the daily business process. This significant dependency on IT makes the relevance of IT audit growing bigger in the MoF. Moreover, the amount of IT investment fund in the MoF is also tremendous. In the last 3 years, MoF has spent Rp1.244 billion (USD 93,57 million) for IT investment itself (table 1). Inevitably, IT governance and IT audit practice need to be applied.

Table 1

IT investment fund in The Ministry of Finance (in thousand rupiah)

Year	2015	2016	2017
The planned fund	971.817.504	208.691.113	64.090.047
Total IT investment fund	1.244.598.664		

Calculated based on the data taken from rkakldipa.anggaran.depkeu.go.id Inspectorate General of Ministry of Finance becomes one of Government Internal Supervisory Apparatus (APIP) that achieves level 3, securing the first rank, based on Internal Audit Capability Model (IACM) assessment by Finance and Development Supervisory

Agency (BPKP) (kemenkeu.go.id). Besides, Inspectorate General of MoF is the first and the only government's internal audit institution to carry out the IT Audit Unit to date. With the importance of IT that is only growing greater and the IT investment fund which is getting bigger over time, every organization needs IT audit function, specifically IT governance audit, runs within it. For those aforementioned reasons, Inspectorate General of the MoF could serve as the role model of IT governance audit implementation.

Moreover, IT audit unit in the Inspectorate General of the Ministry of Finance has adopted the combination of COBIT 4.1 and COBIT 5 frameworks. COBIT is widely accepted by the profession and allows management to benchmark the governance and control practices of the IT environment. As to date, it is regarded as the best practice of IT governance practice. Study about IT audit unit in the Inspectorate General of MoF becomes important for it could serve as the benchmark for another internal audit institutions, or even larger, to build IT audit unit within them. Lastly, to the best of author's knowledge, the research about IT governance audit practice in Indonesia's public sector is very limited. Hence, the author senses the urgency to conduct this research.

This research seeks to understand the implementation of IT governance audit in the MoF compared to Assessor Guide: Using COBIT 5. This research is motivated by the question "How is the implementation of IT governance audit in the Ministry of Finance compared to Assessor Guide: Using COBIT 5?" This research attempts to address the question; that is to say, this research aims to describe the implementation of IT governance audit in the MoF and also address the gap that exists between the guide with the implementation of IT governance audits in the Ministry of Finance.

2. Theoretical Framework

2.1. IT Governance

In the today's complex business environment, Weill and Ross (2004) identified six key assets namely, human, financial, physical, intellectual property, IT as well as and relationships that must be governed to create value. Hence, while IT is one such

key resource that needs to be governed for organizational value creation as shown in figure 1.

Figure 1
The Assets firms govern to create value

Source: Weill and Ross (2004)

Information Technology Governance Institute (ITGI) (2007) defined IT governance as “the responsibility of the board of directors and executive management”. Weill and Ross (2004) defined IT governance as specifying the decision rights and accountability framework to encourage desirable behavior in using IT. Information System Audit and Control Association (ISACA) (2009) stated that IT Governance is basically concerned with the way IT delivers value and it’s the management of the risks associated with it which can be brought about through the strategic alignment of business and IT, resource management and performance management. Moreover, IT governance was acknowledged as significant, as evidenced by the statement, “An effective IT governance structure is the single most important predictor of getting value from IT.” (isaca.org). Guldentops (2003) mentioned that IT governance is important to the enterprise because of these issues (figure 2):

Figure 2
IT governance drivers

Source: Guldentops, 2003

1. Trust—With investors willing to pay significantly more for shares of well-governed enterprises
2. Value—When considering the majority of enterprise market value is in intangible assets
3. Survival—When trust can vanish overnight when based on intangibles and governance practices
4. Assurance—With its increasing requirements for risk transparency and increasing focus on internal controls

IT governance is directly related to IT investment. In the linkage between the two, Sethibe, et al. (2007) stated that IT governance is the structure of relationships, processes, and mechanisms used to develop, direct as well as control IT strategy and resources as the best achieve the goals and objectives of an enterprise. As Weill (2004) stated, IT governance matters because it influences the benefits received from IT investments. Weill (2004) further claimed that through a combination of practices (such as redesigned business processes and well-designed governance mechanisms)

and appropriately matched IT investments, top performing enterprises generate superior returns on their IT investments (up to 40% greater return than their competitors for the same investment). This statement is supported by Crawford (2006) that stated: "IT governance is needed to ensure that the investments in IT will generate the required business value and risks associated with IT are mitigated".

Amali, et al. (2015) reported that the use of IT in public organization has evolved into every aspect as part of their efforts in improving their services. According to Juiz, et al. (2014), a good governance principle as a public asset should be included and implemented on IT governance practices. It is agreed by Bermejo, et al. (2014) who claimed that IT governance is a major resource to the aggregate value of the public service offered to the community.

2.2. COBIT 4.1 and COBIT 5 Frameworks

ISACA (www.isaca.org) and ITGI (www.itgi.org) defines COBIT (Control Objectives for Information and related Technology) as a comprehensive set of resources that contains all the information organizations need to adopt IT governance and control framework. Spremic, et al. (2012) argued that COBIT is the widely accepted IT governance and IS auditing framework and represents an 'umbrella' framework for implementing IT governance policies and procedures and for conducting IT auditing. It is a broad and comprehensive de-facto standard which comprises all activities, processes, and services which can help companies manage the level of operational (IS/IT related) risks.

COBIT is a widely accepted IT governance framework organized by key IT control objectives, which are broken into detailed IT controls (Spremic, et al., 2012). COBIT 4.1 framework stated that version 4.1 of COBIT divides IT into four domains which are broken into 34 key IT processes, and then further divided into more than 300 detailed IT control objectives. Gheorghe (2010) proposed that by considering the 34 key IT processes, the owner can ensure that an appropriate control system is achieved in the IT environment. Meanwhile, COBIT 5 which is claimed as the expanded version of its predecessor, COBIT 4.1, is the only business framework for

the governance and management of enterprise IT (isaca.org). The COBIT 5 framework defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5 framework defines seven categories of enablers: Principles, Policies and Frameworks; Processes; Organizational Structures; Culture, Ethics, and Behaviour; Information; Services, Infrastructure, and Applications; and People, Skills, and Competencies.

2.3. Assessor Guide: Using COBIT 5

Africa (2009) stated that auditing IT governance deals with the audit approach and procedures in reviewing IT governance processes within a business firm. It aims to show the critical areas of IT governance as well as their effects on the quality of IT service delivery to satisfy business objectives. To assure that COBIT 5-based IT governance is well-implemented, COBIT provides Assessor Guide: Using COBIT 5 (ISACA, 2013) as the step by step guide for IT auditors. The audit steps based on the guide is shown in figure 3.

Figure 3
Assessment Project Step

Source: Assessor Guide: Using COBIT 5

3. Research Method

This study shall serve as an exploratory study as research in this area is in early stages and there has been little research material developed in Indonesia. The study is conducted by exploring the implementation of IT governance audits in the Ministry of Finance of Indonesia. In an attempt to obtain a thorough description of the matter, this research is conducted with the qualitative method. This research incorporates the result of an interview with 9 members of IT Audit Unit and 3 members of IT Department of the Inspectorate General of MoF. To get the better overall understanding of the subject, the related documents are also being studied. The interview process is held on January 8, 2018 until January 12, 2018 at Inspectorate General of MoF. Document analysis is held shortly after that, on January 13, 2018 until January 17, 2018.

This research will attempt to translate interview transcripts into a qualitative description of the organization's implementation of IT governance audit. The analysis is concluded in the five stages of IT governance audit processes: initiation, planning, briefing, data collection, data validation, process attribute rating, and reporting. The result of the interview and documents analysis will then be addressed in this writing in order to provide the understanding of the topic. To ensure the credibility of the data collected, respondents validated the interview transcripts by signing them.

4. Results

4.1. *IT Audit Unit of Inspectorate General of MoF*

To understand IT governance audit practice in the MoF could be begun by understanding the unit which performs the task, IT Audit Unit. IT Audit Unit of the Ministry of Finance is established by Regulation of Minister of Finance No.234/PMK.01/2015 about Organization and Job Structure in the Ministry of Finance. The Regulation describes that IT Audit Unit itself has the duty to "carry out the research and development, formulate the supervisory policy, and carry out the supervisory action towards IT management in Ministry of Finance and as internal audit unit and develop the audit report.". The unit's vision is "To be the best IT Audit

Unit which is professional and having the integrity to support the accomplishment of public trust of finance management by the Ministry of Finance”. (IT Audit General Strategy, 2013: 2). The unit is led by Head of IT Audit Unit. The operating model chosen for IT Audit Unit is the centralized operating model (IT audit function run as an independent function instead of being integrated to the other kind of audit functions).

Even though the centralized operating model was chosen for the IT audit unit, there are 2 kinds of IT audit strategy used. The first one is integrated IT audit where the risk emerges from a certain business process and IT control is believed to be able to mitigate the risk. The other IT audit strategy is thematic IT audit. This strategy is used when the needed audit is all about IT and is separable from the operational aspect. Thematic IT audit is held based on specific IT risk, policymakers’ expectation, current issue, and mandated regulation.

Currently IT Audit Unit consists of 1 *auditor madya* (middle-level auditor) as the group coordinator, 3 entry-level auditors, and 8 junior auditors. The middle-level auditor takes the role as the technical supervisor (*pengendali teknis*) and the audit quality is supervised by quality supervisor (*pengendali mutu*). In Inspectorate General, each unit does not have their own designated quality supervisor. Usually, in an inspectorate, there is 1 or 2 quality supervisor(s) for all the audit groups or units under the inspectorate. After getting approved by the technical supervisor, the quality supervisor gives the final authorization. Afterward, all those procedures completed, the audit report is issued. Every auditor level is obtained through certification training and examination by The Education and Training Centre, Finance and Development Supervisory Agency. The auditor leveling is explained below:

1. Middle-level auditor from structure perspective usually holds audit group coordinator title and from the function perspective could be placed as the technical supervisor or quality supervisor.
2. Entry-level auditor is the one who passed the team leader exam and acts as the team leader for audit engagement.

3. Junior auditor is the one with skilled or expert auditor certification. Junior auditor plays the role of audit team member.

To perform IT governance audit efficiently and effectively, IT Audit Unit is supported by these regulations:

1. Regulation of Inspectorate General No. PER-9/IJ/2014 about IT Governance Audit with Control Objective Approach Guidelines
2. Regulation of Inspectorate General No. PER-10/IJ/2014 about Computer Assisted Audit Techniques (CAATs).
3. IT Audit General Strategy (2013)
4. IT Audit Standard (2013)
5. IT Audit Annual Planning and Reporting Guidelines (2013)
6. IT Governance Audit Practice Guidelines (2013)
7. IT Governance Audit Implementation Guidelines (2013) (Using COBIT 4.1)
8. IT Governance Audit Implementation Guidelines (2018) (Using COBIT 4.1 and COBIT 5)

Based on the interview with the head of IT Audit Unit, Mr. JB. Widodo Lestarianto, the unit is established because of the massive utilization of IT to help MoF finishes the duty. The impact of IT governance audit has not been measured yet since it has not been 5 years since IT governance audit is officially performed in MoF. However, IT auditors are invited to the board meeting of *Komite Pengarah Teknologi Informasi dan Komunikasi (KPTIK)* (MoF's Steering Committee of Information and Communication Technology) and are asked about the improvement suggestion about IT management in the MoF. Even though it has not been measured, the most visible impact of IT governance audit was the increasing awareness of the auditees (in this case, every institution in the MoF) about IT governance in managing their IT unit/division.

Human resources played important role in the unit establishment. In the first stage of the IT Audit Unit, 10 personnel who are interested to be IT auditors, without

considering their IT skill and knowledge, are recruited. It happened due to the lack of human resources who were capable to be IT auditor in the early stage of IT Audit Unit establishment.

“If they want to be IT auditor, it easy to make them capable by giving them training.” (Head of IT Audit Unit)

Currently, there is 16 personnel of IT Audit Unit, consists of 12 IT auditors and 4 IT auditor interns. They are given the training to enhance their skill and competency to achieve the collective competencies needed by the unit. There are 5 of them held COBIT5F (COBIT 5 Foundation) certification. By this certification, the holder is considered fully understand about the framework. Beside COBIT5F, currently IT auditors collectively are the holders of certifications namely CIA, CISA, CISM, CEH, COBIT 5 Foundation, CRISC, CEH, CGEIT, CCNA, CCNP, etc.

Meanwhile, for the infrastructure, IT Audit Unit is equipped with adequate required supporting infrastructures. The current time, the software managed by IT audit unit are vulnerability assessment/penetration test software, virtualization software, and database management interface software. The newest audit supporting infrastructure added to the list is audit laboratory. This laboratory provides experience to the auditors before performing the real audit. To manage their audit working papers and audit report, Inspectorate General is helped by Teammate application.

4.2. The Implementation of COBIT 4.1 and COBIT 5 Assessment Approaches for IT Governance Audits

This year, Inspectorate General performs IT governance audit engagement to MoF's four biggest institutions since their IT governance level at average became one of the Minister's key performance indexes. The reason behind this circumstance is the MoF needs to make sure that the huge IT investment fund providing them the proportional benefits.

“IT governance audit provides a holistic overview of the policymakers' expectation to find out how well MoF's IT management is accountable for the state's investment for IT.” (Tri Achmadi, Technical Supervisor)

To perform their audit engagement, IT governance audit team implements the combination of COBIT 4.1 and COBIT 5 for the assessment approaches. COBIT is chosen because it is the only all-in framework of IT governance audit. Around the time IT Audit Unit is established (2014), although COBIT 5 had been introduced by ISACA, there was no organization implemented it already. For that reason, MoF picked the latest one before COBIT 5 published, COBIT 4.1, as their framework. However, to keep up the pace with IT improvement time by time, IT Audit Unit tries to implement COBIT 5 with 2 assessment approaches: COBIT 4.1 and COBIT 5 started from this year.

“COBIT 5 is implemented this year as a part of our commitment to improving the quality of our IT governance audit. We have prepared that as 5 of our auditors are COBIT5F certification holders. We plan to have more COBIT5F certification holders this year.” (Head of IT Audit Unit)

“IT governance audits that have been done already refer to the best practice which is used worldwide i.e. COBIT 4.1 and COBIT 5 so that the results are comparable within MoF or with other organizations in Indonesia and abroad.” (Technical Supervisor)

As the expanded version of COBIT 4.1, COBIT 5 provides a holistic approach to support governance and management system of enterprise IT. In performing IT governance audit engagement, 7 enablers of COBIT 5 are assessed with 2 approaches: maturity assessment approach of COBIT 4.1 and capability assessment approach of COBIT 5. One enabler i.e. processes is assessed by Process Assessment Model (PAM): Using COBIT 5 as the assessment tool. By the said model, the organization is able to know the capability of IT processes. The other six enablers

(Principles, Policies, and Frameworks; Organizational Structures; Culture, Ethics, and Behaviour; Information; Services, Infrastructure, and Applications, People, Skills, and Competencies) are assessed with maturity assessment approach of COBIT 4.1 because COBIT 5 has not released assessment model for those enablers. This approach is chosen because the urgency to know IT governance state from the perspective of all enablers.

“We believe that 7 enablers are all important but COBIT 5 has not provided the assessment tool except for processes. It is better to assess the six enablers (7 enablers minus processes) with our own approach (maturity assessment approach used in COBIT 4.1) rather than not doing it at all” (Riza Faiz Ahmad, Team Member)

Based on the found knowledge, this kind of combination is never been performed by any IT governance audit team. Asked about the reason behind this unusual combination, the team leader said:

“If I am not mistaken, this combination is the first one existed. But we thought that we need to do this unusual thing to achieve our purpose: not just telling the management about the weakness of (their IT) processes but also giving the right suggestion about corrective actions needed. Imagine telling the management ‘you have this weakness’ but cannot provide the clear suggestion and corrective action needed. Then what do we achieve as auditor when we cannot add a value to the auditee? We assess the capability of (IT) processes using COBIT 5 and maturity of the other enablers using COBIT 4.1. The other six enablers’ maturity can be analogized as lifestyle and (processes) capability as the health condition. We need to know our health state and our lifestyle such as our dietary habit, exercise routine, etc behind that. By that auditors can tell the management about how well the processes performed include their gap from the best practice. But to know why that gap happened, we need to know the maturity of (the other six) enablers. That is why we undertake six enablers assessment with maturity assessment approach introduced by COBIT 4.1 and process

capability assessment using COBIT 5 as described in PAM (Process Assessment Model: Using COBIT)."

Combining COBIT 4.1 and COBIT 5 offers an advantage for both auditor and auditee. The auditor can provide the accurate corrective action suggestion so that auditee can improve their processes. As for the auditees, they could easily identify which area to be improved and how the improvement should be done.

4.2.1. Process Capability Assessment

Process capability is a characterization of the ability of a process to meet current or projected business goals. Based on COBIT 5 Framework, there are 37 IT processes in 5 domains (Evaluate, Direct, Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate and Assess (MEA)) to be assessed. Each process is assessed to define in which level the IT capability is using an assessment tool provided in Process Assessment Model (PAM): Using COBIT 5. IT Auditors in the MoF used COBIT Enabling Processes to get an in-depth understanding of IT processes assessed. There are six levels of capability that a process can achieve starts from 0 (incomplete process) until 5 (optimizing process) as described by PAM: Using COBIT 5.

4.2.2. Enablers Maturity Assessment

Even though one enabler i.e. processes is considered as the heart of enablers, the other six are just as important as the aforementioned enabler to achieve good IT governance. These six enablers: Principles, Policies and Frameworks; Organizational Structures; Culture, Ethics and Behavior; Information; Services, Infrastructure and Applications, People, Skills and Competencies, are assessed to define the maturity level. General explanation of maturity leveling is explained below:

Table 2
Enabler maturity leveling

Maturity Level	Description
Level 0 (non-existing)	The IT enabler's indicators are not existed/performed. There is no management awareness that the existence/performance of the indicators is needed to support business goals.
Level 1 (Ad-Hoc)	The need for enabler's indicators is known by IT management. Indicators are performed on an as-needed basis in response to a specific business requirement. Indicators performed by ad-hoc (personal initiative), without binding standards
Level 2 (repeatable but intuitive)	IT enabler's indicators have performed consistently with the absence of formal procedure or standard or in contrary the formal procedure/standard existed, however, the indicators are performed inconsistently.
Level 3 (defined)	IT enabler's indicators are performed consistently as defined by the formal procedure/standard and adequately documented.
Level 4 (managed)	There are mechanisms for monitoring and measuring the consistency of IT enabler's indicators in supporting the business processes and achieving business goals. The indicators monitoring has been conducted periodically to add a value to the organization.
Level 5 (optimized)	The IT enabler's indicators have been implemented in accordance with the principles of good practices and continuous improvement of the indicators have been running systematically and continuously. The indicators clearly provide benefits in achieving business goals effectively and are recognized by every element of the organization.

Source: IT Governance Audit Implementation Guidelines (2018)

4.3. Comparison Between IT Governance Audit Practice in the MoF with Assessor Guide: Using COBIT 5

To undertake an IT governance audit, IT auditors apply Assessor Guide: Using COBIT 5 as the guidance. The Guide provides a methodology to perform an IT governance audit engagement. Asrulsani Muhamad, the leader of IT governance audit team said that:

“Because we decided to use COBIT 5 with two assessment approaches (COBIT 4.1 and COBIT 5), we apply the Assessor Guide: Using COBIT 5. Conformance to The Guide is something we strived to be achieved to assure the quality of audit engagement.”

The implementation of the Assessor Guide: Using COBIT 5 in IT governance audits in the MoF is described below:

1. Initiation

The first phase of an IT governance audit is audit initiation. IT governance audit is initiated annually through annual audit program mentioning the engagement plan includes the budget and resources allocated and key performance index (KPI) of the IT auditors. The annual audit program is defined by the IT Audit Unit through an annual audit planning meeting.

“Audit plan has to be developed or renewed at least once every year... The plan has to be approved by the Inspector General” (IT Audit Standard, 2013)

Audit universe is already defined as it is stated in Peraturan Menteri Keuangan Nomor 234/2015 (Regulation of Minister of Finance No. 234/2015) that Inspectorate General including IT Audit Unit has to oversee all the institution in the MoF. There are 11 institutions under MoF which become IT audit universe of IT governance audit. The head of IT Audit Unit established assessment team and their roles. Team leader (referred to the lead assessor in COBIT terminology) is chosen based on the proficiency about IT governance audit and the capability to manage a team. Audit team possesses the competencies to undertake IT governance audit with the members collectively held CIA, CISA, COBIT 5 Foundation, CRISC, CGEIT, CCNA, and CCNP certifications. Assessment purpose and framework used to perform the engagement are stated in IT Governance Audit Implementation Guidelines (2018). There is no scoping step due to the need to assess all areas of IT governance. It is consistent with the Head of IT Audit Unit’s argument that in its early stage, the main purpose of the IT governance audit is to know the overall state and score of IT governance.

All of the steps are conform with Assessor Guide except the scoping step. Audit scoping will be performed on their next IT governance audit (approximately 2 years from the previous IT governance audit). Vini Estrawan, a team member, stated that:

“The auditee will be audited again after 2-3 years.”

Head of IT Audit Unit confirmed Vini's statement by saying:

“Ideally, IT governance audit will be performed again after 3 years or if there is a fundamental change in the organization. In less than 3 years usually, public service organization does not significantly change.”

Their statement is in line with International Standards for the Professional Practice of Internal Auditing (The Institute of Internal Auditors, 2012) that IT governance audit could be performed on an annual basis or up to two or three years apart.

2. Planning

After the initiation, the audit team meets to discuss the audit planning. They decided on the activities to gather the evidence e.g. interview and document analysis. They also determine the necessary resources, schedule, and tenure based on the difficulty of each engagement. In the meeting, they discussed the assessment tool, the planned output, and verify the conformance to the Assessor Guide. Overall, the planning step is in accordance with the Assessor Guide.

3. Briefing

A briefing is held by the team leader to ensure that the assessment team understands the assessment input, process, and output and auditee understands how the assessment will be performed. Team leader gathers the audit team to discuss the assessment tool including the input (documents, interviewees, etc), process (how to analyze the input) and output (what they want to achieve in the audit process). The audit team will hold a socialization to the auditees about the audit process. The audit team will also provide a self-assessment tool for auditees so they can assess themselves first before the auditors do. Briefing step performed by IT governance audit team conforms with the Assessor Guide.

4. Data Collection

In obtaining objective evidence to support the assessment, audit team decided the data collection strategy and perform it. In the entry meeting, they asked the auditee to provide the documents needed (in COBIT terminology is called as 'work product'). Audit team conducted an interview with the personnel related to processes to assess management practices required in Process Assessment Model (PAM): Using COBIT 5

and also the enablers' indicators. If there is something the auditors need to know more, they can confirm it with the related parties. Some management practices demand the auditor to do observation. From 37 processes, some of them are not audited for example cost charging process due to MoF attribute as the public service organization. This process is irrelevant because MoF serves the people without considering profit-taking. The data collection step conforms with the Assessor Guide.

5. Data Validation

In the data validation step, the auditors confirming that the evidence collected is objective and sufficient. Audit team gathers to discuss whether the evidence of each process is objective and sufficient. If not, the audit team will look for another evidence needed. This step is performed in accordance with the Assessor Guide.

6. Process Attribute Rating

The auditors give each process and enabler indicator a rating based on the objective evidence collected before. The auditor presents the rating for each process and each enabler indicator he assessed and seeks approval from the team leader. After getting approved, the processes rating is recorded in the audit working paper. Audit team calculates the capability level rating based on each process rating and also the maturity level of each enabler. This step is in accordance with the Assessor Guide.

7. Assessment Reporting

Each audit team member writes the audit result that will be compiled as an audit report. IT auditors will release audit result minutes to get the auditee's approval. After being discussed with the auditee, the audit team will finalize the report. This report is supervised with tiered supervision from audit team leader, technical supervisor, and quality supervisor. The audit team will distribute the report to the relevant parties. The audit team will also get feedback from auditee about the audit performed. This step conforms with the Assessor Guide.

The follow-up process is monitored with Team Central feature of Teammate application. In the application, the auditor will write down the recommendation(s) and the needed follow-up action(s) that must be followed up within the specified time. The auditee will report the result of the follow-up recommendation(s) accompanied with

supporting evidence through this application. If the auditor accepted the report as the right follow-up action(s) then the follow-up process is considered successful.

Figure 4
Audit report authorization flow

Source: Inspectorate General of MoF

Quality assurance is performed for IT governance audit through peer review by another team annually and external auditor every 5 years. Asked about the problem and obstacles faced by the organization to perform IT governance audit practice, the auditors expressed some opinions:

1. Lack of concern about IT governance.

Not every institution engaged to IT governance. While a lot of organization put their concern on their IT governance, some argued that it is less urgent.

“For some people, (IT) governance is just an administrative burden which provides minor impact to the organization, that is why there is a resistance to the (IT governance) audit process.” (Riza Faiz Ahmad, Audit Team Member).

2. The Difficulty to map the practices performed by the auditee to the COBIT Terminologies

In the real IT governance audit engagement, the documents and management practices performed by the auditee are sometimes different with COBIT terminologies. The auditor needs to do some complex judgments and further analysis to assess the IT enablers of the auditees.

“.....to overcome this problem, the audit team holds a regular meeting to discuss some matters regarding what we find during the engagement.”
(Yohanes Beato Dionisius, Audit Team Member)

3. Lack of audit tenure

IT governance audit is usually given strained tenure approximately a month. Based on the interview result with the auditors, this tenure is too short to get the deep understanding about IT governance condition of an institution. It also happened because there is a great number of documents that need to be collected and the difficulty to arrange the interview schedule with the related personnel of the IT unit of the auditee.

5. Conclusion, Implication and Limitation

5.1 Conclusion

MoF's IT governance audit practice has implemented COBIT 5 framework with two approaches: maturity assessment approach of COBIT 4.1 and capability assessment approach of COBIT 5 to assess IT governance and Assessor Guide: Using COBIT 5 to perform the audit engagement. Despite being on its early stage, IT governance audit is fair performed. Almost all the audit steps conform with the Guide. The decision to put aside audit scoping, according to the Head of IT Audit Unit, went through careful consideration. The IT auditors also expressed that they commit to performing the said unperformed step in the future.

5.2 Implication of Research

To date, the research about IT governance audit revolves around the private sector, and furthermore, in the developed countries. Research into IT governance in developing countries such as Indonesia is limited. So this writing will enrich the discourse in IT governance audit, especially for public sector organizations. The information provided by this study about the implementation of IT governance audit can also help the public sector organizations as the benchmark of the aforementioned area of audit.

5.3 Limitation of Research

Although the research has reached the aims, there were some limitations. First, due to time limitation, this research could not capture the deeper understanding about IT governance audits in the MoF. Due to the absence of other public sector's internal audit unit which has performed IT governance audit, this research could not present comparison—something that will make the research better.

References

- Africa, D. 2009. Auditing IT Governance Seminar. ISACA Manila Professional Development Center. Manila: ISACA Manila Chapter.
- Al-Hayale, T., & Abu Khadra, H. 2006. Evaluation of The Effectiveness of Control Systems in The Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector. *Journal of Accounting, Business, and Management* 13: 39-68.
- Bermejo, P.H.S., Tonelli, A.O. Zambalde, and A.L. 2014. Developing IT Governance in Brazilian Public Organizations. *Int. Bus. Res* 7(3): 101-114.
- Crawford, Adam. 2006. Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing And Security. *Theoretical Criminology* 10(4): 449-479.
- DiCicco, Barbara, and Crabtree, Benjamin F. 2006. "The Qualitative Research Interview". *Medical Education* 40: 314-321.
- Gheorghe, M. 2010. Audit Methodology for IT Governance. *Informatica Economica* 1: 32-42.
- Grembergen, De Haes, and Guldentops. 2004. *Structures, Processes and Relational Mechanisms for IT Governance*. London: Idea Group Inc.
- Guldentops, E. 2003. *Governing Information Technology Through COBIT*. In W. Van Grembergen (Ed.), *Strategies For Information Technology Governance*. Hershey, PA: Idea Group Publishing.
- ITGI. 2003. "IT Governance Institute, *Board Briefing on IT governance. 2nd Edition*". <http://www.itgi.org>
- ITGI. 2007. "COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Value". <http://www.itgi.org>
- ITGI. 2007. "IT Assurance Guide: Using COBIT". <http://www.itgi.org>
- ISACA (Information System Audit and Control Association). 2009. *Implementing and Continually Improving IT Governance*. Rolling Meadows, IL: Information Systems Audit and Control Association.
- ISACA. <https://cobitonline.isaca.org/about>

Juiz, C., C. Guerrero, and I Lera. 2014. Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks. *Open Journal of Accounting* 3: 9-27.

Kemenkeu. rkakldipa.depkeu.go.id

Kemenkeu. 2015. "BPKP: MoF's Government Internal Supervisory Apparatus Could Be Role Model". <http://www.kemenkeu.go.id/en/Berita/bpkp-mof%E2%80%99s-government-internal-supervisory-apparatus-could-be-role-model>

LM, Applegate., Austin RD, and McFarlan FW. 2003. *Corporate Information Strategy and Management: Text and Cases*. 6th Ed. New York: McGraw-Hill.

Nkwe, Nugi. 2011. State of Information Technology Auditing in Botswana. *Asian Journal of Finance & Accounting* 3: 125-136.

Omari, Loai Al: Paul Barnes: and Grant Pitman. 2013. Delphy Study into the Audit Challenges of IT Governance in the Australian Public Sector. *Electronic Journal of Computer Science and Information Technology* 4(1): 5.

Sethibe, T., J. Campbell, and C. McDonald. 2007. "IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions". *18th Australian Conference on Information Systems*: 833-843.

Spremic, Mario., Marijana Ivanov. and Bozidar Jakovic. 2012. IT Governance and Information System Auditing Practice in Credit Institutions in The Republic of Croatia. *International Journal of Applied Mathematics and Informatics* 6: 101-108.

Tempo. 2015. "Cyber Crime, Lebih dari Rp 33 M Melayang Gara-gara Hacker". <http://m.tempo.co/read/news/2015/08/26/172695105/cyber-crime-lebih-dari-rp-33-m-melayang-gara-gara-hacker>

Van Grembergen, W. and S. DeHaes. 2008. *Enterprise Governance of IT*. Belgium: Idea Group Publishing Antwerp University.

Weill, P and J.W. Ross. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Performance*. USA: Harvard Business School Press.

Weill, P. 2004. Don't Just Lead, Govern: How Top Performing Firms Govern IT, MIT Sloan School of Management, Center for Information Systems Research, Working Paper No. 34.

intentionally blank