https://doi.org/10.1051/matecconf/202237204015

How to Design the Best Audit Instrument for Evaluate E-Government Security?

Eristya Maya Safitri [1] [*], *Arrandi* Muhamad Riesta[1,] *Abdul Reza Efrat* Najaf[1], *Anita* Wulansari[1], *Dhian Satria Yudha* Kartika[1] and *Anindo Saka* Fitri[1]

[1]Information System Department, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya Indonesia

Abstract. The United Nation e-government survey reports that the implementation of e-government in Indonesia will increase in 2021. This proves that the Indonesian government is trying to transform all its business processes by digitalization. System digitization is expected to increase the efficiency of government performance. Information security is one of the important aspects to ensure that this digitization process really provides efficiency for government performance. A good information security management approach is management that adheres to the deeming cycle of quality. The management process includes plan, development, act and check. The audit enters the check cycle which functions as a control whether the process implemented in securing information is correct or not. A good audit process will encourage to produce good findings and recommendations as well. So, we need the right information security audit instrument so that the audit instrument is appropriate in the auditing process. A comprehensive information security audit instrument is an instrument that explains the COBIT 5 goals cascade, RACI chart mapping, briefing preparation and interview design protocol as well as key work-products.

Keywords. E-government, security services, instrument audit

1 Introduction

E-government is the implementation of electronic-based government business processes. Utilization of information technology is used to optimize the arrangement of management systems and work processes in the government environment. In addition, the increasing trend of people in the use of information technology encourages the government to transform from manual business processes to automated business processes. The implementation of e-government is expected to increase the effectiveness and efficiency of activities that are G2C, G2B and G2G. These three types of activities are the main services provided by the government. G2C is an activity related to government services to citizens directly [1]. G2B are activities related to government services to business stakeholders. G2G is an intergovernmental business process activity in Indonesia. The progress of e-government implementation in Indonesia at the end of 2021 is shown in the United Nation e-government Survey data which places Indonesia in 18th place. This ranking has increased from where Indonesia was previously ranked 19th in e-government implementation. It can be concluded that the implementation of e-government in Indonesia has begun to increase by more than 50 percent.

With the increasing use of e-government, the use of own-cloud is also increasing as an electronic-based data storage technique [2]. Various important data and information are in an unlimited range. This raises new problems which previously did not occur in manual business processes. Own-cloud-based data storage is often a security threat in e-government. Data on e-government that is not managed properly will be an attack on the government itself. Misuse of data by unauthorized persons will increase and benefit their own side. As in several cases of large companies that suffered losses due to the vulnerability of company data security, namely Bhinneka.com, the 2014 Elections case and others. Bhinneka.com suffered a loss due to an individual who sold 1.2 million Bhinneka.com users with a tag of 1,200 dollars in May 2020. In the 2014 election, it was suspected that population data belonging to Indonesian citizens was leaked as a result of hacker fraud. Therefore, the security of this data is an aspect that needs to be considered and accounted for.

In implementing e-government, the government must have made various programs related to data security [3]. Various e-government security programs can be referred to as information technology governance [4]. E-government governance is decisions related to e-government implementation that have an impact on creating value for government [5]. Governance related to data security can be demonstrated in every effort

[*] Corresponding author: maya.si@upnjatim.ac.id

made by the government to improve e-government security services [6]. Deming cycle of quality is one of the cycles that need to be implemented in improving e-government security services every period of time [7]. Deming cycle of quality includes plan, develop, check and act. This cycle explains that in every IT governance, development is needed, which is based on the evaluation results [8]. The form of evaluation is obtained from the results of previous IT governance process audits. Therefore, the audit process is an important component that needs to be prepared. The success of the audit process is influenced by the concept of the audit instrument used. Appropriate and efficient audit instruments will help achieve the effectiveness of the auditing process [9].

The importance of developing the right audit instrument in e-government security governance is the background of this research to design the best audit instrument that can help improve the effectiveness of the audit process [8]. The audit instrument developed in this study uses the COBIT 5 approach. The results of this study are an audit instrument for auditing e-government security at the Department of Communication and Information of East Java Province. The audit instrument that has been developed is expected to provide recommendations and be implemented in the e-government security audit process at the Department of Communication and Information Technology of East Java.

2 Research Methodology

2.1 Research Location

This research was developed using the COBIT 5 approach. Fig 1. The methodology below shows step-by-step research work from start to finish. There are 5 stages in the research method, namely COBIT Goals Cascade Analysis, RACI Chart Mapping is Organization, Briefing Preparation, protocol interview design and key work-product and documentation.

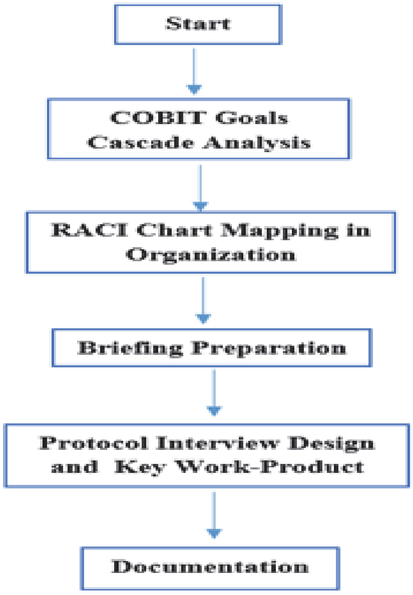
Start
COBIT Goals Cascade Analysis
RACI Chart Mapping in Organization
Briefing Preparation
Protocol Interview Design and Key Work-Product
Documentation

Fig. 1. A Methodology Flow

The COBIT Goals Cascade Analysis stage is the process of identifying prioritized scopes for auditing [10]. The priority of the audit scope is adjusted to the needs of the organization in improving e-government governance [11]. This is initiated by analyzing stakeholder drivers, stakeholder needs, enterprise goals, IT-related goals and enabler goals. The output of this stage is the process of prioritized e-government governance for audit [12].

The RACI stage Chart mapping in organization is the mapping of interviewees according to the type and importance of the data to be taken [13]. This mapping process is adjusted to the organizational structure of the government with the RACI chart which means Responsible, Accountable, Consulted and Informed [14]. The output of this stage is the interviewee who became the key-informant has been mapped according to the RACI Chart [15].

The briefing preparation stage is to analyze the method used for retrieval of each type of data or information [16]. At this stage, it is identified what activities are needed during the data collection process [17]. Methods and details of activities related to the fulfillment of data collection are also identified when conducting audit activities. The output of this stage is the identification table of data collection activities.

The protocol interview design and key work product stage is the stage of designing questions that will be given to informants. In addition, it also analyzes the types of documents that support or prove that the process has been carried out. The two points were analyzed according to the COBIT 5 approach. The output of this stage is the question design and supporting work-products.

The documentation stage is documenting the design of the audit instrument in accordance with the needs of the e-government security audit. The output of this activity is that the e-government security audit instrument at the East Java Province Communications and Information Office has been compiled and documented

3 Results and Discussion

In analyzing the Goals Cascade based on COBIT, it is necessary to analyze the alignment between business goals and IT goals that have been implemented. The goals cascade analysis aims to find out aspects of IT governance that need attention to be improvised in the coming period. There are three main aspects that become the focus of stakeholder needs, namely benefit realization, risk optimization and resource optimization. The results of an interview with the Head of the Division of Governance and ICT Empowerment of the Communication and Information Technology Office, East Java, stated that the priority aspect to be followed up was information security, especially information on e-government managed by the Communication and Information Office, East Java. Information security in the stakeholder needs map based on COBIT is represented by the question “Is the Information I am processing well secured?”

To achieve the company's goals, it is necessary to align the achievement of performance between the company's goals and IT processes. From a number of IT processes, it is necessary to prioritize IT processes that provide an important role in achieving organizational goals. With the organizational goal of “compliance with internal”, it is necessary to prioritize IT processes using a “p” and “s” scale. The "p" scale can be interpreted as a primary process. Primary process means that IT processes are the main processes that should not be abandoned in achieving organizational goals. While the "s" scale can be interpreted as a secondary process. Secondary process means IT processes that are not the main process in achieving organizational goals. In the organizational goal of "compliance with internal policies" which is included in the "internal" dimension, there are two primary processes. Between the two primary processes, priority selection is carried out according to the needs of the organization in improving IT governance in the scope of e-government. The results of more detailed interviews about the IT processes that have been implemented, the IT processes that support the achievement of organizational goals are "security of information, processing infrastructure and applications".

Enablers are factors that can drive the success of governance. Enablers include processes, organizational structures and information. Each enabler represents a specific set of goals that are relevant to supporting IT-related Goals. COBIT 5 defines 37 processes grouped in five domains selected based on the primary scale. In accordance with the results of the mapping of IT-related goals, there are five processes that have process priorities on a primary scale. Of the five processes that are in accordance with the information security needed by the company, management is in the "manage security" process. So the research on the design of audit instruments is focused on processes related to managing security. Manage Security in COBIT 5 is a process in the APO 13 domain. APO stands for align, plan and organize

3.1 RACI Chart Mapping in Organization

This study aims to analyze how IT can be used to achieve operational agility which focuses on the interdependence of operational processes in the organization with reference to IT and company capabilities [18]. This research is motivated by the hope that companies that have invested heavily in IT can have a positive impact on their supply chain operations. However, success is not only limited to IT adoption but also must be able to compete with information asymmetry and interdependence between resources simultaneously. Peter Drucker's statement as a famous management professor in highlighting information asymmetry is "Management by objective work - If you know the objectives, ninety percent of the time you don't. Most of what we call management consist of making it difficult for people to get their work done”.

Previous research stated that to form information asymmetry, it is necessary to facilitate workflow coordination to overcome problems in decision making and conflicts between departments. The complexity of IT management systems will lead to a cultural shift that unifies and coordinates the core entities of the organization. This potential will support the organization to innovate and create agility within the organization. With varying degrees of uncertainty about IT capabilities, current researchers are expected to seek developments beyond issues of structure, processes and people interacting with IT. Therefore, this study focuses on organizational operational agility by looking at the interdependence of IT capabilities and organizational capabilities in every organizational operational process. The result of the research is to develop an interdependence model between IT and organizational capabilities with the type of resource dependence required at each operational stage

Table 1. Informant mapping.

No	COBIT 5 Functional Structure	DISKOMINFO JATIM Functional Structure
	APO 13.01 Establish and maintain an ISMS	
1	Chief information officer	Head of informatics application
	APO 13.02 Define and manage an information security risk treatment plan	
2	Chief Information Officer	Head of informatics application
	APO 13.03 Monitor and review the ISMS	
3	Business Process Owners	Head of ICT governance and empowerment section

3.2 Briefing Preparation

In the auditing process, several stages of activities are carried out. The following is a table of activities carried out in the information system security audit process managed by the East Java Communication and Information Office:

Table 2. Briefing preparation

No	Activity	Actor	Method
1	Explain the research objectives, scope, stages and schedule of assessment	Audi tee & auditor	Discussion
2	Assessment process (data collection and validation)	Audi tee & auditor	Interview and Review Document
3	Recapitulation of assessment results	Auditor	Discussion
4	Assessment result reporting	Auditor	Discussion

3.3 Protocol Interview Design and Key-Work

The main audit instrument is a question that will be given to informants to measure whether the information security process has been implemented and documented properly. It is said that the information system security process matures if HR implements the right process. The following are question instruments and also work-products.

Table 3. Protocol Interview Audit

No.1	**Process**	**APO 13.01. Build and maintain information system security management system**
	Description	The process that establishes and maintains an ISMS with a standard, formal and sustainable approach to information security management. In addition, it also ensures that the technology security management applied is in line with the business process needs that require the company's information security.
	Work-product	ISMS Policy, ISMS Scope statement
	Protocol Interview	1. How does the East Java Diskominfo build and maintain an ISMS? Are there standards that have been referenced and is maintenance carried out on an ongoing basis? 2. Have the scope and boundaries of the ISMS been defined? 3. Is the established ISMS in accordance with company policies and objectives? 4. Is the implementation of ISMS in line with the implementation of overall security management? 5. Who has the authority to implement, operate and modify this ISMS? 6. Is there a division of roles and responsibilities in information security management? 7. Is the ISMS approach well communicated?
No.2	**Process**	APO 13.02 Determine and manage information security risk management plans.
	Description	The process that maintains the information security plan. The plan describes how information security risks are managed and aligned with the company's strategy and architecture. In addition, provide recommendations for implementing security enhancements based on approved business cases and implemented as an integral part of the development of services and solutions, then operated as an integral part of business operations.
	Work-product	Information security risk treatment plan, information security business cases
	Protocol Interview	1. How is the information security plan maintained? Is there a plan for handling information security risks, starting from identifying appropriate and optimal management practices and security solutions with resources, responsibilities and priorities including in terms of funding and sharing of responsibilities? 2. How are information security risks managed to align with the company's strategy and architecture? 3. How to measure the effectiveness of information security management practices that have been carried out so far? 4. Are there training programs related to information security awareness? 5. Is there any documentation regarding possible incidents? 6. Has there been an integration between planning, design, implementation and monitoring of security procedures with other controls that allow for prevention, detection of security events, and rapid incident response?
No.3	**Process**	APO 13.03 Monitor and review ISMS
	Description	The process that maintains communicates the need for and benefits of continuous improvement of information security on a regular basis. It also collects and analyzes data about ISMS and improves the effectiveness of ISMS. Then correct non-conformances to prevent the risk from reoccurring and promote a culture of continuous security improvement.
	Work-product	ISMS Audit report, recommendations for improving ISMS
	Protocol Interview	1. How is the ISMS monitoring and review process at the East Java Diskominfo? 2. Has the maintenance and improvement of information security been communicated regularly and periodically? 3. Have internal audits related to ISMS been carried out regularly and periodically? 4. Has management conducted regular reviews of the ISMS? 5. Has an information security plan been maintained that takes into account the findings during monitoring and review? 6. Has documentation been carried out regarding events that could impact the effectiveness of ISMS performance?

4 Conclusions

There are two conclusions that can be drawn from this research. The first conclusion is that the design of the audit instrument was initiated with the COBIT 5 goals cascade analysis. The results of the analysis of the alignment between stakeholder drivers, stakeholder needs, enterprise goals, IT-related goals and enabler goals show that the IT governance process that needs to be considered in government is the IT security process. The second conclusion is the completeness of the audit instrument consisting of key-informant mapping according to the RACI Chart, identification of the required information and the efficient method chosen for data collection, interviewee protocol and work-product of each process.

For further research, it is possible to develop research by conducting the audit process directly using audit instruments that have been developed in this study. In addition, further researchers can also develop e-government security audit instruments by combining the COBIT 5 approach and other frameworks related to e-government security. Continuing research on topics related to this research will support the results of developing a more comprehensive audit instrument

References

[1]. K. M, "Information Technology and The Networked Economy," Information Technology, vol. **3**, pp. 305-330, (2018).

[2]. O. C.Williams, "A Technological Approach Towards the Measurement of Enterprise Agility," Iberian Conference on Information Systems and Technologies , vol. **15**, pp. 30-45, (2020).

[3]. H. T. H. Hemantha, "Post-audits for managing cyber security investments: Bayesian post-audit using Markov Chain Monte Carlo (MCMC) sIMULATION," Journal of Accounting and Public Policy, vol. **37**, no. 6, pp. 545-563, (2018).

[4]. L. K. S. D. B. L. B. Julian Thome, "Security slicing for auditing common injection vulnerabilities," Journal of Systems and Software, vol. **137**, no. 5, pp. 766-783, (2018).

[5]. T. C. H. Hemantha S.B. Herath, "IT security auditing: A performance evaluation decision model," Decision Support Systems, vol. **57**, no. 7, pp. 54-63, (2014).

[6]. "Comments on a Lightwight cloud auditing scheme: Security analysis and improvement," Journal of Network and Computer Applications, vol. **139**, no. 67, pp. 49-56, (2019).

[7]. J.-H. L. T. W. C. H. Ju-Chen Yen, "The impact of audir firms characteristics on audit fees following information security breaches," Journal of Accounting and Public Policy, vol. **37**, no. 6, pp. 489-507, (2018).

[8]. R. L. R. G. G. W. N. Paul John Steinbart, "The Relationship Between Internal Audit and Information Security: An Exploratory Investigation," International Journal of Accounting Information System, vol. **13**, no. 3, pp. 228-241, (2012).

[9]. D. F. e. all, "Security Audits in Mixed Environments," Network Security, vol. **2009**, no. 3, pp. 17-19, 2009.

[10]. B. S. H. H. S. Khaerul Manaf, "Digital Report Application Audit Using the COBIT 5 Framework," in INSPEC ACCESS, Bali, Indonesia, (2022).

[11]. E. F. M. I. Dina Fitria Murad, "Implementation of COBIT 5 Framework for Academic Information System Audit Perspective: Evaluate, Direct, and Monitor," in INSPEC Access, Padang, Indonesia, (2018).

[12]. A. T. L. George Morris Willian Tangka, "Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University," in INSPEC Access, Manado, Indonesia, (2021).

[13]. P.-E. Pablo Alejandro Quezada-Sarmiento, "Development of an Information System Audit in a Data Center: Implementation of Web Application to the Management of Audited Elements," in INSPEC Access, Lisbon, Portugal, (2017).

[14]. P. A. L. Ilya I. Livshitz, "The Effect of Cyber-security Risks on Added Value of Consulting Services for IT-Security Management Systems in Holding Companies," in International Conference Quality Management, Transport and Information Security, Information Technologies, Yaroslavl, Russia, (2021).