JPPI Vol 10 No 1 (2020) 15 - 26

Jurnal Penelitian Pos dan Informatika

32a/E/KPT/2017

e-ISSN 2476-9266
p-ISSN: 2088-9402

Doi:10.17933/jppi.2020.100102

Information Security Governance and Management Capability Assessment: A Lesson Learned from Directorate General of Taxes

Penilaian Tata Kelola dan Kemampuan Manajemen Keamanan Informasi: Pembelajaran dari Direktorat Jenderal Pajak

Bandi Ashari

Faculty of Computer Science, University of Indonesia, Jl. Margonda Raya, Depok, 16424, Indonesia

Bandhi.ashari@ui.ac.id

Received: 9 January 2020 ; Received in revised from: 25 June 2020; Accepted: 20 August 2020

Abstract

Information has a pivotal role in improving business operation and serving decision-making process. The emergence of e-commerce and e-government require more frequent data exchanges, including sensitive data. This study will focus on the Directorate General of Tax's (DGT) effort in planning and building the ability to enforce IT governance, especially those related to information security. In addition, this research can be used as a basis for their continuous improvement. We used the ISGM capability model to combine COBIT 5 and ISO 27001 as an approach to measure the capability of organizations in governing and manage their information security. We found that the overall DGT's information security governance and management capability is at a level of well-defined. Almost all of ISGM building blocks have been established properly into their tailor-made policies and standards. As a consequence, DGT's ISGM could contribute to the business as shown in several DGT's programs. However, in order to acquire an optimum value from ISGM implementation, DGT needs to improve its capability level, particularly in relation to some organizational aspects such as alignment with business strategies and resource management.

Keywords: information, security, maturity, capability, ISM, ISGM

.

INTRODUCTION

Information is a valuable asset of an organization [1]. It has an important role in improving business operation and serving decision-making process [2]. Private and public organizations have recognized the importance of information. Today, the emergence of e-commerce and e-government requires more frequent data exchanges included sensitive data. The government becomes more and more concerned about information security because of the implementation of e-government which practices data sharing among public agencies and partners [3].

The Directorate General of Taxes (DGT) as our case study, has introduced many electronic channels to provide services to taxpayers, such as e-registration, e-filing, e-billing, and e-tax invoice as a means to increase taxpayers' compliance and provide better services for its stakeholders. In addition, DGT also has the authority to collect data and information related to taxation from various channels. This new role was added in Government Regulation Number 31 of 2012, every government agencies, institutions, and business associations are obliged to share data and information related to taxation upon request of the DGT.

As a consequence, DGT has a responsibility to protect the confidentiality of data and information submitted by taking into account information security governance and management practices. They are needed by the DGT to ensure that information security policy is already in place and aligned with business objectives.

Trust from taxpayers and other parties is critical for the DGT in transforming into a digital organization. This trust will also affect the taxpayers to use tax electronic services in fulfilling tax obligations and exercising their rights. When exchanging financial data and information, all parties involved must trust each other. Trust could be built by governing information security management. The DGT also needs to build capabilities that enable governance enforcement.

This study will focus on looking at the Directorate General of Tax's (DGT) endeavours in planning and building the ability to enforce IT governance, especially those relating to information security. Moreover, this research may also be used as a basis for continuous improvement. Hence, our research questions are:

Can the DGT's information security management contribute to its business?

How can information security management be aligned with its business?

A. Theory

Information Security Management (ISM) is the process of applying security practices and controls to safeguard the organization's information assets [4]. ISM is relevant to all types of organizations including private and public organizations. Most of them have an interest in addressing information security risks related to their employees, contractors, consultants, and external suppliers of information services. However, specific information risk and control requirements may differ in detail among organizations.

There are several definitions of Information Security Governance (ISG). Veiga and Eloff explained that ISG can be described as the overall manner in which information security is deployed to mitigate risks [5]. In another article, Johnston and

Hale described that ISG is an essential element of enterprise governance and consists of leadership, organizational structures, and processes involved in the protection of informational assets; ISG can more effectively and efficiently address the issues of information security leading to improve outcomes, including strategic alignment, risk management, business process assurance, value delivery, resource management, and performance measurement[6].

Information Security Management Maturity Model (ISM3) is a tool created to measure the level of ISM implementation in an organization. ISM3 was created to ensure that the information security process in an organization is implemented at a consistent level and following the organization's business needs [7].

B. Previous Work

There are several case studies about the assessment of maturity level in information security management or governance. They used a combination of information security standards and frameworks such as COBIT 5, ITIL, ISO/IEC 27001, and other ISO/IEC that related to process assessment.

Kusumah, Sutikno, and Rohmansyah [8] conducted some case studies at an IT-related organization, the problem was that the applied information security solution was partially implemented and not aligned with the enterprise business goal. They proposed a combination of COBIT 5 and ITIL as an approach to measure the capability level of information security management and governance. They found that a combination of COBIT 5 and ITIL is better at measuring the capability level of organization in governing information security while delivering Information Technology (IT) services.

Rimawati and Sutikno [9] conduction case study at the statistic agency. Census-related activities which involve outsourcing and use of mobile technology could increase the security risk during data collection and information processing. To overcome those problems, the organization needs to implement an information security management. Due to a long period of implementation processes, the organization must assess its current capability level in information security management to define the target capability level. They proposed an approach based on ISO/IEC 27001:2013 to evaluate the capability maturity level of information security management.

Yulianto, Lim, and Soewito [10] highlighted the importance of information security standards in the payment card industry. Compliance to the security standard in the payment card industry is mandatory for every participating organizations in the industries. Complying with the standard is not simple; many organizations had failed to satisfy the minimum-security requirements while managing the sensitive information of cardholders. Hence, the researchers proposed some information security capability models that could be used to measure the capability level of an organization for satisfying minimum requirements of the information security standard in the payment card industry. The proposed model is constructed based on ISO/IEC 27001 and Security Engineering Capability Maturity Model (SE-CMM).

Muthukrisnan and Palaniappan [11] had disscussed their concern with regard to metrics in the information security maturity model. Recognize that the decision to invest in information security must be supported by some indicators or metrics that could be comprehended by the stakeholders and

in-the-process, convince them that the investment will reduce the risk from information security issues.

There are many information security management and governance frameworks that could be used by the organization. However, they often to be a generic and less suitable for practitioners [12]. Hence, Carcary et al. depeloved an Information Security Governance and Management capability maturity framework that is more practitioner oriented. This framework is developed under The Innovation Value Institute (IVI) program and becomes an integral part of the IT Capability Maturity Framework (IT-CMF).

The proposed ISGM framework groups information security management and governance-related activities into six categories. Each category has several capability building blocks [12]. The categories are: 1) governance, which consists of activities related to the information security strategy, policies, and control, 2) technical security, which consists of activities related to the information security architecture and components, 3) security resources management, which consists of activities related to the information security resources management such as budgeting, 4) security control risk, which consists of activities related to the information security risk management, 5) security data administration, which consists of activities related to the data life cycle management, and 6) business continuity, which consists of activities related to the business continuity and incident management.

Based on the previous works, there are several ISM frameworks and standards that could be used for measuring the capability level of an organization in governing and managing information security. It is found out that the practicality of ISGM Capability Model covers both governance and management aspects of information security. On the other hand, COBIT 5 has more advantages in IT Governance and ISO 27001 has more strong points in information security management system.

In this study, the ISGM capability model is used to combine COBIT 5 and ISO 27001 as an approach to measure the capability of organizations in governing and managing their information security. The capability measurement in this study refers to ISO 21287 which provides standard for security engineering capability maturity model. The theoretical framework for this study is shown in Figure 1.

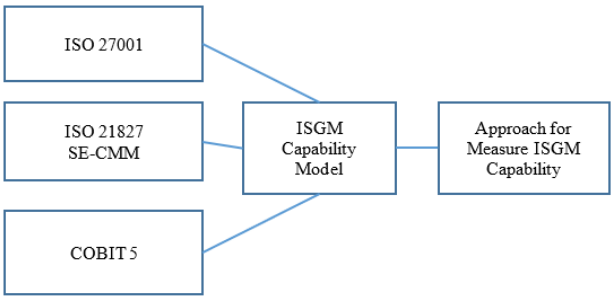

Figure 1 Theoretical Framework

METHODOLOGY

This section describes the data and methods used in this study.

A. Method

This research is a mixed-method with a case study. Data were elicited through interviews, observation, and document study. Interview and document study is conducted to understand the organization profile, its strategy to become a digital organization, an information security policy that has been in place, and capability that has been built to govern and manage security information.

Evaluation to assess the adequacy of the information security management and its capability refers to best practices such as COBIT and ISO 27001. Recommendations will be offered on some actions based on the evaluation result. Additionally, results of several studies will be provided as grounds for the recommendation proposal for the DGT.

B. Research Instrument

This study uses an instrument to assess the level of information security governance and management capability. Essentially, the instrument was adopted from the information security capability building blocks that were introduced at the ISGM framework by Carcary et al. [12] and COBIT 5 and ISO/IEC 27001. Questions which are derived from the instrument above have been designed for each building block to assess its capability level. The question list is shown in Table I.

Table I Question List

Question	Reference	
	ISO/IEC 27001 (Annex A)	**COBIT PAM**
A. Governance		
Have the information security objectives been defined and communicated to all relevant stakeholders?		APO01.04
is there an alignment between information security strategy and business strategy in place? For example, information security threat is considered in SWOT analysis		APO02-01
Has DGT establish formal information security policies?	A.5.1.1	APO13-BP1
Are the information security policies reviewed regularly?	A.5.1.2	APO13-BP3
Is roles and responsibilities in information security management clearly assigned?	A.6.1.1	APO01-WP08
Is there a training program regarding information security policy for employee, taxpayers or other parties?	A.5.1.1, A.7.2.2	APO13-BP3
Has the analysis of information security performance been implemented?	A.18.2.2	APO13-BP3
Does DGT establish an agreement regarding third party access and require it?	A.15.1, A.15.2	
B. Technical security		
Is the information security aspect included in information system requirement gathering?	A.14.1.1	
Does DGT implement security protection for information that transmitted through public network?	A.14.1.2	
Does DGT implement security protection on devices to reduce the risk of unauthorized access?	A.11.2.1	DSS05-BP3
Are critical devices protected from power outages?	A.11.2.2	DSS05-BP3
Are devices maintained to ensure their availability and integrity?	A.11.2.4	DSS05-BP3
Has control over usage of IT devices outside organization area been established?	A.11.2.6	DSS05-BP3
Are safe areas for protecting information and its processing facilities defined?	A.11.1.1	DSS05-BP5
Are safe areas protected by access control?	A.11.1.2	DSS05-BP5
Are security protection for physical facilities been designed and implemented?	A.11.1.3	DSS05-BP5
Have the protection to disaster, attack and accident been designed and implemented?	A.11.1.4	DSS05-BP5
Is there a procedure for working in a safe area?	A.11.1.5	DSS05-BP5
C. Security resource management		
Has priority-based budgeting been implemented to support strategic goal? For example, through program portfolio		APO06-BP3
Have the planning which consist of requirement analysis, detail design, architecture principle and standard, and contract procedure been implemented in information security solution acquisition?		BAI03-BP4
Is there a procedure to guide the installation of new information security component?		BAI03-BP5
Is the IT investment portfolio related to information security management evaluated regularly to measure it realized value at some acceptable cost?		EDM02-BP1
D. Security risk control		
Does DGT performsinformation security risk assessment process?		DSS05-WP2
Does DGT evaluate threat and vulnerability as part of information security management?		DSS05-WP2

Question	Reference	
	ISO/IEC 27001 (Annex A)	COBIT PAM
Have the information security risks been classified and prioritized?		APO12-BP2
Has the portfolio of risk management action been defined?		APO12-BP5
has the monitoring of security incident on infrastructures been performed?		DSS05-BP7
E. Security data administration		
Is there an information asset classification based on legal requirement, value, criticality, and sensitivity in place?	A.8.2.1	
Is there a sufficient procedure for information labeling?	A.8.2.2	
Have the information asset handling procedures based on classification scheme developed and implemented?	A.8.2.3	
Are there formal procedures for user registration and deletion implemented to grant information and services access privilege?	A.9.2.1	
Are there any procedures for providing or revoking access rights to information and services?	A.9.2.2	
Are there any restriction and control over access privilege allocated to users?	A.9.2.3	
Have the privileged access rights been reviewed regularly?	A.9.2.5	
Are there any policies on data management that ensuring compliance to regulation related to both physical and electronic documents?	A.18.1.1	
F. Business continuity		
Have requirements about information security and continuity of its management been defined?	A.17.1.1	
Are there documents, procedures, and controls to ensure continuity of information security management system in crisis?	A.17.1.2	
Does DGT serve additional resources as redundancy for information processing facilities?	A.17.2.1	
Have management responsibilities and procedures been established to ensure quick, effective and orderly response to information security incidents?	A.16.1.1	
Are there communication channels for reporting information security incidents to the management?	A.16.1.2	
Are there policies and procedures that required all employee and business partners using information system to note and report any suspected information security weaknesses?	A.16.1.3	
Has DGT implemented procedures for assessing information security events and for deciding whether it is classified as an information security incident?	A.16.1.4	
Does information incident response according to formal and documented procedures?	A.16.1.5	
Is there any knowledge management regarding information security incident implemented to reduce the probability and impact of future security incidents?	A.16.1.6	
Have procedures to identify, collect, and store evidence been defined and applied in DGT?	A.16.1.7	

The list of questions are used to interview the respondents to measure the capability of their organization in governing and managing information security. It is necessary that the respondents' answers are measured with a standard measurement to allow the scores of the governance and management condition to be reflected in a consistent manner.

The scoring method was influenced by the ISO/EIC 21827:2008 System Security Engineering Capability Maturity Model (SSE-CMM)[13]. It is an interval which has a range score from 0 to 5. The capability score description is shown in Table II.

Table II Scoring And Capability Level[13]

Score	Level	Definition
0	Not Performed	There is no security process or plans in place. The controls are nonexistent.
1	Performed Informally	Base practices of the process area are generally performed on an ad hoc basis. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort
2	Planned and Tracked	Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified
3	Well Defined	Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes
4	Quantitatively Controlled	Detailed measures of performance are collected and analyzed. This

Score	Level	Definition
		leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known
5	Continuously Improving	Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies

The instrument is divided into six sets of questions. Each question set represents an ISGM category. It appears that no respondents are equipped with thorough comprehension on information security governance and management in DGT. Therefore, each subset of the instrument are delivered to appropriate respondents based on the relevant category.

C. Respondent

The information security management maturity assessment employed a survey for data collection. Purposive sampling is used in respondent selection. Criteria that represent the competencies needed in each ISGM category is defined for those selections. The selected respondents consist of several DGT officers who have the capacity and experience in each ISGM activity category. The respondent criteria for each ISGM activity category is shown in Table III.

Table III Respondent

Category	Respondent Criteria	Number of Respondent
Governance	Involved in IT governance and policy development experienced in IT for more than 10 years	3 persons
Technical Security	Involved in software engineering, or network administration experienced in IT for more than 3 years	3 persons
Security Resource Management	Involved in budget preparation experienced as procurement/ commitment officers for more than 3 years	1 person
Security Control Risk	Involved in risk management experienced in information security management	3 persons
Security Data Administration	Involved in IT governance and policy development experienced in IT for more than 10 years	1 person
Business Continuity	Involved in preparation of Business Continuity Plan experienced in IT for more than 10 years	1 person

RESULTS AND DISCUSSION

Data is collected through an online questionnaire. The target respondents are 3 appropriate individuals for each category. The request of information is sent to the targeted respondents via emails and text messages. All respondents for categories of governance, security control risk, and technical security have given their responses. However, for other categories, only one respondent for each category had responded to the request.

The data from respondents are tabulated, and then used for calculating the capability score for each building block. The score summarization from response data in this assessment follows calculation in the ISGM capability maturity framework. It uses an average score as a base to define the capability level for each capability building block. The calculation score result is shown in Table IV.

Table IV ISGM Assessment Result

Capability Building Blocks		Score
A-Governance		3.2
	A1-Information security strategy	2.2
	A2-Security policies and control	4.0
	A3-Security roles, responsibilities, and accountabilities	4.0
	A4-Communication and training	2.7
	A5-Security performance reporting	3.3
	A6-Supplier security	3.3

Capability Building Blocks	Score
B-Technical security	2.8
B1-Security architecture	2.0
B2-IT component security	2.9
B3-Physical infrastructure security	3.1
C-Security resource management	1.3
C1-Budget for security	1.0
C2-Tools and resources	2.0
C3-Resource effectiveness	0.0
D-Security risk control	2.9
D1-Security threat profiling	2.8
D2-Security risk assessment	3.3
D3-Security risk prioritization	2.8
D4-Security risk handling	3.0
D5-Security risk monitoring	2.8
E-Security data administration	4.3
E1-Data identification and classification	4.3
E2-Access right management	4.5
E3-Data life-cycle management	3.0
F-Business continuity	3.4
F1-Business continuity planning	4.7
F2-Incident management	2.9

ISGM building blocks under the governance category has an average score of 3.2. These scores indicated that the capability of governance building blocks has reached a well-managed level. It means almost all of the process related to the information security governance are performed according to the standard that has been modified to match the organization's needs.

The building blocks which have a higher score than others in the governance category are security policies and control and security roles, responsibilities and accountabilities. Both categories stand at the 4.0 interval; meaning that the DGT has enough capability in defining information security policies, control, and also in defining roles and responsibilities, as well as accountabilities.

The DGT's capability in defining policies, control, roles and responsibilities related to the information security is reflected by the availability of security policy and procedures which adopt the ISO 27001 Information Security Management System, ISO 27002 Code of Practice for Information Management, and ISO 27005 Risk Management System, which are composed in a tailor-made specific to their needs. The information security policy was officially established based on Regulation of Director-General of Taxes number PER-41 / PJ / 2010 on DGT's information security management policy. DGT also has several formal procedures in place for guiding the implementation of the information security management policy.

The building block which has the lowest score under the governance category is information security strategy, with score 2.2. The score resulted from one out of the three respondents who provided a response stating that there is no alignment between information security strategy with business strategy. In this regard, a study on the DGT's strategic plan 2015-2019 and the DGT's IT Blueprint 2015 – 2019 documents was conducted as a follow up.

The DGT's strategic plan is formalized with Regulation of Director-General of Taxes number KEP-95/PJ/2015. However, there are no specific threats or challenges related to information security stated on those documents. Furthermore, the DGT IT-Blueprint stated some concerns about information security management, especially related to maintaining business continuity during a disaster. Based on the presented facts above, it appears that the DGT's IT Blueprint could act as a bridge for the business strategy and the IT strategy including information security management.

The technical security category has an average score of 2.8. Thus, indicating that the capability of building blocks under that category is between planned and well defined. According to the Information and Communication Technology (ICT) development guidance, which is part of DGT's ICT Development policy, a nonfunctional requirement related to the information security can be accommodated in Software Requirement

Specification (SRS) documents.

The infrastructure for network security support is well managed. Mainly because the DGT has implemented enterprise solutions related to network management. It provides several capabilities related to network security, a respondent claims "that capabilities are application firewall, web application firewall which are effective in handling attack which exploits a vulnerability in the web application announced in OWASP, application security manager which provide single sign-on service and Virtual Private Network (VPN) connection, and load balance which distributed traffic/connection with configurable manner".

Security resource management category has a low score of 1.3. Since only a part of information security need is identified in IT Blueprint, it can be concluded that the budgeting for information security management is still performed informally, not based on a well-defined IT investment portfolio. Other contributing factors to this low score was lack of information security portfolio investment management, and no evaluation procedure in place to measure the effectiveness of the information security investment portfolio.

Security risk control category has a score of 2.9. Meaning that the capability level is between planned and well defined. Support form sophisticated enterprise network solution as described in the previous paragraph about technical security, enable the risk management team to identify potential security threats, prioritizing the risks, and define the action portfolio action based on the risk priority.

Security data administration category has a higher score than other categories. Its capability score is 4.3. That means this category has the capability at quantitatively controlled. The DGT has defined the classification of information. Information receive different treatments along in its life cycle based on this classification. Access to information is restricted and controlled. Only authorized personnel could access information. Role-based access control is established. For example, access to the DGT integrated data warehouse through its channels is controlled by role-based access so that the information access is granted based on employee's profile. This profile is connected to an identity source that is synchronized with staff, finance, and asset information system.

The business continuity category has a score of 3.4. This reflects that DGT has a good capability in business continuity planning. A business continuity plan has been developed, for instance, a team responsible to execute a disaster recovery operation during and after the disaster occurred has been established. A respondent also claims that "Disaster Recovery Center (DRC) is in place, scenario to switch from Data Center (DC) to DRC has been tested and simulated. The incident management is performed based on the formal procedure and roles and responsibilities in incident management have been defined". However, knowledge management capability which needs to be improved particularly in an area about information security incident.

Figure 2 shows DGT's maturity in ISGM according to capability building blocks categories. There are 22 building blocks from 6 categories. The chart shows that DGT's capabilities are skew. Building block category which needs more attention is security resource management.

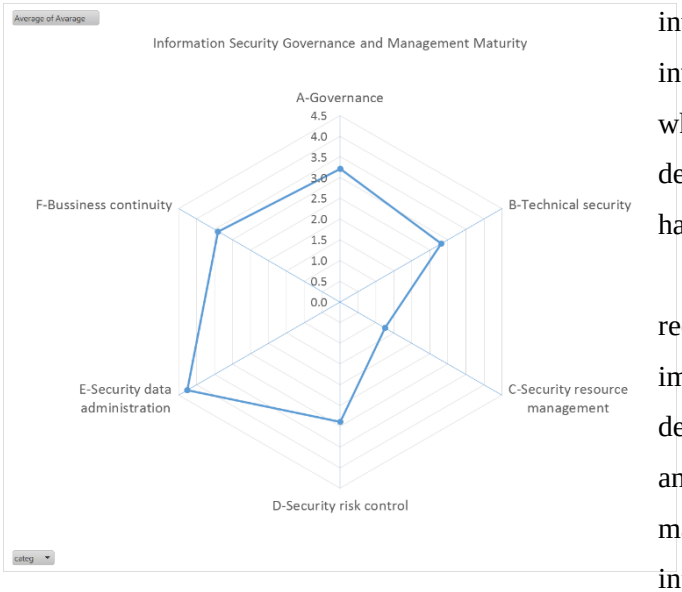

Figure 2 ISGM Maturity

The document study indicates that the information security governance and management in DGT has been implemented based on tailor-made policy and standard. It is adapted from a well-known information security framework and standard that has been adopted by many organizations. DGT's information security policy and procedures are quite detailed and adopted most of the best practices required by ISO/EIC 27001, 27002, and 27005.

According to the policy and procedures, it is required to build many technical capabilities by implementing appropriate technology solutions. It is necessary to communicate the required technical capabilities with top-level management and include these into the project portfolio in order to allow the accommodation of the fund allocation in the budget plan.

DGT has established information security management policy and its related procedures in 2011. Guidance for encryption and key management is also part of the procedures. Although it was formalized in 2011 through regulation number SE-56/PJ/2011, according to the interview with the key person in electronic tax invoice system development at DGT, until 2013 when DGT initiated the electronic tax invoice development project, the public key infrastructure has not been established yet.

Due to the electronic tax invoice system requirements for a delicate digital certificate implementation, public key infrastructure was developed to manage taxpayers' digital certificate and associated key, therefore the top-level management are aware that the public key infrastructure is important and needs to be established. The related solution needs to be acquired and implemented to support this business initiative. Finally, DGT made a development collaboration with the National Cryptographic Agency to design and build a dedicated public key infrastructure for the DGT. This project was successfully built and the business initiative to digitalize the taxpayer interaction through electronic tax invoice system was implemented gradually in 2014 and was well accepted by taxpayers.

The illustration above shows us that the information security initiative will receive high attention from the top management if it is linked to the business strategy. Based on the assessment result, the alignment between information security strategy and business strategy is still low. According to our document study on DGT's strategic plan and IT Blueprint, it is found that information security is not yet considered as a factor in Strength, Weakness, Opportunities, and Threat (SWOT) analysis. The IT Blueprint only gives little attention to the information security.

CONCLUSION

This study found that DGT's information security governance and management capability at overall stands at the level of well defined. Almost all of the ISGM building blocks has been established according to tailor-made policies and standards. The building block category which has the lowest score is security resources management. Therefore, the study suggests that the DGT is required to implement its IT investment portfolio and carry out regular evaluation of the effectiveness of investment.

With this capability level, the DGT's ISGM could contribute more to the business. As briefly mentioned in the discussion section, the DGT's key management has a contribution to the success of business strategy execution which digitalize the interaction between taxpayer and DGT through the electronic tax invoice system. The implementation of role-based access control in DGT's integrated data warehouse enables secure data services that support taxpayer compliance supervision. The contribution of ISGM will be higher if its building block capability is increased.

The study also suggests that DGT needs to determine the ability of ISGM building blocks to obtain an optimal value that can support DGT's digital transformation strategy. ISGM must be aligned with the business strategy. It is necessary to raise the potential advantages of ISGM and the information security challenges to be faced by the organization while executing business strategy in a discussion with the top-level management to increase their awareness and include the ISGM in considering their decisions thus making the ISGM aligned with their business strategy.

ACKNOWLEDGEMENT

REFERENCES

[1] DAMA, *DAMA-DMBOK2 Framework*, V.2. DAMA International, 2017.

[2] T. C. Zhiling, "Strategic value alignment for information security management: a critical success factor analysis," *Inf. Comput. Secur.*, vol. 26, no. 2, pp. 150–170, Jan. 2018.

[3] F. Piedrabuena, L. González, and R. Ruggia, "Enforcing data protection regulations within e-Government Master Data Management Systems," in *17th International Conference on Enterprise Information Systems, ICEIS 2015*, 2015, vol. 3, pp. 316–321.

[4] T. Ioanna, "From theory to practice: guidelines for enhancing information security management," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 326–342, Jan. 2019.

[5] A. Da Veiga and J. H. P. Eloff, "An information security governance framework," *Inf. Syst. Manag.*, vol. 24, no. 4, pp. 361–372, 2007.

[6] A. C. Johnston and R. Hale, "Improved Security Through Information Security Governance," *Commun. ACM*, vol. 52, no. 1, pp. 126–129, Jan. 2009.

[7] I. C. Vicente Aceituno, *Information Security Management Maturity Model Handbook*, v02 ed. Madrid, Spain: ISM3 Consortium, 2007.

[8] P. Kusumah, S. Sutikno, and Y. Rosmansyah, "Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC)," in *2014 International Conference on ICT For Smart Society (ICISS)*, 2014, pp. 1–6.

[9] Y. Rimawati and S. Sutikno, "The assessment of information security management process capability using ISO/IEC 33072:2016 (Case study in Statistics Indonesia)," in *2016 International*

Conference on Information Technology Systems and Innovation (ICITSI), 2016, pp. 1–6.

[10] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to PCI DSS compliance," in *2016 IEEE Region 10 Symposium (TENSYMP)*, 2016, pp. 65–70.

[11] S. M. Muthukrishnan and S. Palaniappan, "Security metrics maturity model for operational security," in *2016 IEEE Symposium on Computer Applications Industrial Electronics (ISCAIE)*, 2016, pp. 101–106.

[12] M. Carcary, K. Renaud, S. McLaughlin, and C. O'Brien, "A Framework for Information Security Governance and Management," *IT Prof.*, vol. 18, no. 2, pp. 22–30, Mar. 2016.

[13] ISO, "Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model," Geneva, CH, Oct. 2008.