ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 3, pp. 127-145
DOI:10.33168/JSMS.2024.0308

Assessing Information Security Using COBIT 2019 And ISO 27001:2013

Elok Aflakhah, Benfano Soewito

Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia

elok.aflakhah@binus.ac.id, bsoewito@binus.edu

Abstract. One of the vulnerabilities organizations face against cyberattacks arises from the absence of standardized governance for information system security. This encompasses insufficient security policies and a lack of consistent security updates and monitoring. This study aims to evaluate and gauge the information system security governance of the Directorate General of Human Settlements. COBIT 2019 and ISO 27001:2013 frameworks are employed to bolster the administration and safeguarding of information assets, while also establishing more robust and secure IT governance. The research methodology encompasses gathering data through interviews, observations, and analysis of pertinent security policy documents and information management practices. From this study, 12 specific information security domains are identified: EDM03, APO11, APO12, APO13, BAI06, BAI10, DSS02, DSS03, DSS04, DSS05, DSS06, and MEA03. Evaluating the present analysis, it is evident that the Directorate General of Human Settlements has not yet attained the targeted maturity level, set at level 5. This underscores the existing gaps in the organization's information system security governance. Based on the research findings, recommendations and a roadmap are proposed to rectify these deficiencies in information system security governance. This initiative aims to elevate information security measures and curtail risks arising from various threats like cyberattacks, data breaches, and unauthorized access. Additionally, the organization's overall average maturity level achieved, calculated at 3.07, further emphasizes the need for comprehensive enhancements in its information system security governance practices.

Keywords: COBIT 2019, Design Factor, IT Governance, Maturity Level, Gap

1. Introduction

Information systems are crucial to government duties in the current digital era. In managing information systems, the government is responsible for ensuring that the information stored and processed by the government is safe from various security threats, such as cyber-attacks, data theft, and unauthorized access. Government information security governance is critical in ensuring and minimizing security risks. Information system governance aims to align stakeholder needs, company goals, and company performance in business activities supported by technology and information (ISACA, 2018). The benefits of implementing IT governance are realizing benefits, optimizing risks, and optimizing resources (Aditya et al., 2019).

In implementing information technology governance, frameworks such as the Information Technology Infrastructure Library (ITIL), The Open Group Architecture Forum (TOGAF), Project Management Body of Knowledge (PMBOK), PRojects IN Controlled Environments 2 (PRINCE2), Committee of Sponsoring

Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards ISO/IEC 38500, ISO/IEC 31000, ISO/IEC 27000, ISO/IEC 20000 and COBIT (Control Objective for Information and related Technology) 2019 can be used (ISACA I. , 2012). Each framework focuses on its objectives, and the implementation of frameworks depends on the organization's characteristics. The ITIL framework focuses on improving the quality of IT services (Axelos, 2019), and COSO focuses on integrated risk management with all aspects of business (Wiley, 2011). ISO 38500 focuses on managing IT investment and services (Commission), 2008), COBIT (Control Objective for Information Technology) 2019 is a standard and guideline for IT governance and management published by ISACA (Information Systems Audit and Control Association). This framework is an improved version of COBIT 5 which provides more in-depth guidance on enterprise IT governance according to each company's needs containing 40 core governance and management objectives. This guide also references other frameworks and standards (ISACA, 2018)

In previous studies conducted by (Bayastura et al., 2021), (Utomo et al., 2022), (Ishlahuddin et al., 2020), (Safitri et al., 2021), they have discussed the implementation of one of the above frameworks, namely COBIT. They concluded that every company needs IT governance so that the company's business goals are aligned with the use of information technology and the business goals of a company can be achieved effectively and efficiently with the help of information technology (Yasin et al., 2021) The COBIT 2019 Framework was chosen in this study as it defines the capabilities of information systems that offer universally recognized principles, tools, practices, and models that can help increase trust levels. COBIT 2019 also provides recommendations to companies in managing IT governance and provides business flexibility to create practical governances (Utomo et al., 2022) solutions tailored to their organization's purposes and objectives (ISACA, 2018).

The Directorate General of Human Settlements has the task of formulating and implementing policies in the field of water supply system management, domestic wastewater management, environmental drainage management, waste management, building and construction arrangement, urban area development, and strategic infrastructure development in accordance with the provisions of the laws and regulations. Ensuring the security of their technological information systems is also imperative, as it safeguards sensitive data related to building plans, water supply network, process of building construction applications. citizen records, employee information and other critical information, allowing them to fulfill their responsibilities efficiently and protect against potential risks. The Directorate General of Human Settlements has experienced four instances of cyberattacks, underscoring the susceptibility of their information systems. These incidents emphasize the immediate requirement for strong security measures to protect valuable information, mitigate unauthorized entry, and uphold the credibility of their digital services. COBIT is an IT management framework focusing on excellent and effective IT governance. However, since COBIT does not have a comprehensive guide in the field of information security, integration with ISO 27001:2013 as a guide for information security management can help organizations improve the management and protection of their information assets. By integrating COBIT 2019 and ISO 27001:2013, organizations can create better and more secure IT governance, reducing risks and improving overall performance. Research on ISO 27001:2013 has been conducted by (Nawir et al., 2022), (Prapenan & Pamuji, 2020), (Putra et al., 2020).

The Directorate General of Human Settlements has 7360 employees spread across 34 provinces throughout Indonesia and has 28 applications that support its business processes. Information security governance must be implemented at the Directorate General of Human Settlements to protect data and assets from threats that may harm business processes so that application users can transact and conduct other information-related activities without fear. This study's required governance is related to management and focuses on Security. Hence, the approach combines the ISO/IEC 27001 and COBIT 2019 standards and frameworks.

Several studies have focused more on governance related to Security by COBIT 2019 or ISO 27001:2013. At the of Human Settlements directorate, the focus will be on all information system assets, including hardware and software. A study discusses the combination of COBIT 2019 and ISO 27001:2013 (Yasin et al., 2021), but it was conducted in a different business process, namely criminal investigation. This study shows that the number of domains selected in IT governance in each organization is influenced by various design factors. Hence, organizations that plan and build public infrastructure have different domain selection and design factor results than organizations in criminal investigations. In this case, the various design factors between the two organizations can affect the selection of appropriate domains for building effective IT governance that aligns with the organization's needs. In a previous study (Yasin, 2021), the set benchmark for Polda XYZ was 3, as per their observations. The focus of their research was on cybercrime. In this study, the goal was set at 5, aiming for a higher level of effectiveness. The testing, however, was only done within the regional police department, which makes it less adaptable when compared to other agencies. On the other hand, when it comes to human settlements, it involves many different organizations like regional development agencies, water utility companies, health departments, environmental agencies, and more. This complexity needs to be considered when trying to apply the results more broadly.

This research aims to design an information security governance based on the integration of COBIT 2019 and ISO 27001:2013, with the expectation of providing recommendations for developing information security governance for the government and ensuring the Security and confidentiality of the information stored and processed by government information systems. Additionally, this research is beneficial for the following purposes:

a. To determine the current state of information system management that can be measured at a certain level.
b. To identify and mitigate potential threats and attacks that may occur.
c. To develop a reference for future implementation by the goals of the Directorate General of Human Settlements.
d. To monitor information system management according to the reference.

These efforts will help increase public trust and ensure the government can provide high-quality public services.

2. Related Works

In previous studies, several methods for creating information system security governance have been conducted, with commonly used methods including the COBIT 2019 and ISO 27001:2013 frameworks

2.1. Governance Using Cobit 2019

In general, the chosen method to be used should follow the organization's needs. Among the existing techniques, COBIT 2019 is a well-known method of governance framework. There are several versions of COBIT 2019, including COBIT 4, COBIT 5, and COBIT 2019. The latest product in the COBIT series is COBIT 2019.

COBIT 2019 is a framework used to evaluate the governance and management of IT. COBIT 2019 plays a role in controlling and maximizing the value of information and technology to help organizations achieve risk optimization, realize benefits, and achieve resource optimization. One of the main drivers for the formation of COBIT 2019 is the demand for faster, more agile, and innovation-supporting IT management in organizations (ISACA, 2018). COBIT 2019 has six governance principles, namely (ISACA, 2018):

a. Provide Stakeholder Value
b. Holistic Approach
c. Dynamic Governance System
d. Governance Distinct From Management
e. Tailored to Enterprise Needs
f. End-to-End Governance System

Several new aspects in COBIT 2019 compared to 2015 include design factors that can drive the design of enterprise governance systems (such as corporate strategy, risk profile, IT role, IT implementation method, and threat landscape), (Steuperaert, 2019). Here is a list of the domains and processes in COBIT 2019 (ISACA, 2018):

- Evaluate, Direct, and Monitor (EDM) - aims to group corporate governance objectives.
- Align, Plan, and Organize (APO) - discusses the organization, strategies, and activities supporting enterprise technology and information.
- Build, Acquire, and Implement (BAI) - discusses IT solutions' design, acquisition, and implementation, including business process integration.
- Deliver, Service, and Support (DSS) - This domain discusses operational and T&I service support.
- Monitoring, Evaluate, and Assess (MEA) - discusses monitoring T&I performance and compliance with performance targets and internal and external control objectives.

Then, from these processes, maturity assessment is carried out in COBIT 2019, which is divided into six levels (ISACA, 2018):

- Level 0 (Incomplete)
- Level 1 (Initial)
- Level 2 (Managed)
- Level 3 (Defined)
- Level 4 (Quantitative)
- Level 5 (Optimizing)

In determining the sources for interviews and questionnaires, the RACI (Responsible, Accountable, Consulted, and Informed) chart is used as a matrix of all decision-support activities or authorizations that must be taken in an organization by being linked to all parties or positions involved (Aditya et al., 2019).

2.2. Security Governance using ISO 27001:2013

Generally, the cybersecurity standards framework should be appropriate to the type of business organization. ISO/IEC 27001:2013 is an international standard that provides best practices in information security management that can be universally used. This standard uses a process-based approach to establish, implement, operate, monitor, evaluate, maintain, and improve information security. ISO/IEC 27001 contains 114 control objectives grouped into 14 domain groups from Annex 5 to Annex 18, while Annex 1 to Annex 4 is introductions and definitions (Razikin & Soewito, 2022). Implementing ISO 27001:2013 allows organizations to determine and evaluate information security risks and implement procedures and mechanisms that maintain the integrity, confidentiality, and availability of information (Carvalho & Marques, 2019).

IT governance analysis and design in the Directorate General of Human Settlements have not been conducted before. However, several studies can be used as references for this research, such as the "Analysis and Design of Information Technology Governance Using the Cobit 2019 At PT. XYZ". This study is research on a food and beverage company that uses information technology to support the company's business goals, namely daily transaction bookkeeping. The company is categorized as large as it has 2800 employees and uses 11 design factors that result in 5 selected domains, namely DSS02 (managed service request and incidents), DSS03 (managed problems), DSS05 (managed security service), BAI09 (managed assets), and MEA03 (managed compliance with external requirements).

Another study, "Leveraging COBIT 2019 to Implement IT Governance in SME Context: a case study of higher education in Campus A". This study was conducted at campus A, which has around 224 employees and is categorized as a medium-sized organization. This organization does not have an internal IT person. It relies on the performance of external vendors for applications and infrastructure, so IT governance is needed to manage the organization's risks. The company's analyst uses COBIT 2019 using 11 design factors resulting in 12 domains, namely APO07, BAI02, BAI03, BAI07, BAI11, DSS01, DSS02, DSS04, DSS05, MEA01, MEA02, and MEA03, and determining the RACI Chart.

A study titled "Identifying the Level of SIPERUMKIM Governance based on COBIT 2019 in the Department of Housing and Settlements of Salatiga City". The information system used by the department is called SIPERUMKIM, a digitalization process of public service recommendations for housing licensing. The department wants to obtain a bit of advice through Capability Level and a gap in DPKP Salatiga so that the application can be more optimal for improving good IT governance and as an evaluation material for enhancing the company's performance and providing good services to the community, especially in Salatiga City. Determination of the domains is carried out using 11 design factors. Four of the 40 domains are valued at more than 80, namely APO12, DSS02, and DSS03.

The research titled Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013 was conducted on XYZ Company, which has produced various fabrics for 20 years. The research aimed to determine the level of information system security in the company to enhance it and minimize potential threats, as well as to plan for obtaining the ISO about information security management. The auditor mapped the company's vision and mission based on the COBIT 5 Enterprise objectives for the SMKI scope, using the PAM COBIT 5 to produce domains APO12, DSS05, MEA02, and EDM03.

Another research, Designing Recommendations and Road Map of Governance for Quality Management System of Online SKCK Based on Information Security Using ISO 9001:2015 and ISO 27001:2013 (Case Study: Ditintelkam Polda ABC) focused on the Online SKCK (Police Record Certificate) and compared the clauses of ISO 9001:2015 and ISO 27001:2013. The selected clauses were evaluated using ISO 21827:2008 and rated from zero to five (0-5) based on the ISO 27001:2013. The evaluation results were analyzed to determine the recommendations and roadmap of activities that Ditintelkam Polda ABC should undertake to address the identified gaps.

The study investigated the implementation of ISO 27001 and COBIT COBIT 2019 frameworks in securing the information of an intelligent tourism application developed by PT. YoY Manajemen Internasional. The smart tourism app provides recommendations for tourist attractions and amenities based on location through a location-based service, as well as the personal preferences of the tourists. Information damage in the intelligent tourism application can affect the company and its business. Therefore, PT. YoY Manajemen Internasional should protect customer data and assets from attacks or threats that may harm the innovative tourism business process. The organizational objectives were mapped, and domain APO13 was selected and adapted to PT. YoY conditions and preferences. From the selected domain, the ISO 27001 controls/policies became recommendations for PT. YoY was identified.

In these research studies, the authors determined the domains based on design factors, such as (Bayastura et al., 2021), (Utomo et al., 2022), (Safitri et al., 2021), and selected the appropriate domains for the organizational needs. COBIT 2019, which is more up-to-date than COBIT 2015 (Steuperaert,

2019) was the focus of the research, and it was integrated with ISO 27001:2013. The domains of COBIT 2019 were mapped with the ISO 27001:2013 clauses, and the questionnaire was distributed according to the RACI (responsible, accountable, consulted, and informed) chart to determine the respondents, as described in (Utomo et al., 2022). The results were used to make recommendations that must be fulfilled and implemented to achieve an ideal information security governance, as described in (Putra et al., 2020). The research aimed to provide recommendations based on the evaluation of each COBIT 2019 domain.

In this case study, the COBIT 2019 and ISO/IEC 27001 frameworks for information security management are employed as best practices to design governance recommendations and an information security roadmap. Because the COBIT 2019 framework shares similarities with COBIT 5, which generally encompasses aspects of procedures and activities from various standardized models and frameworks accepted by the IT community, it is recognized as dynamic and flexible. For instance, the EDM domain represents ISO/IEC 38500 and ISO/IEC 31000, while the APO, BAI, DSS, and MEA domains encompass Project in Controlled Environment (PRINCE2)/Project Management Body of Knowledge (PMBOK), TOGAF, ISO/IEC 31000, Capability Maturity Model Integration (CMMI), ITIL V3, ISO/IEC 20000, and ISO/IEC 27000, as depicted in Fig. 1 : COBIT 5 coverage of other standards and frameworks (Information Systems Audit and Control Association., 2012).

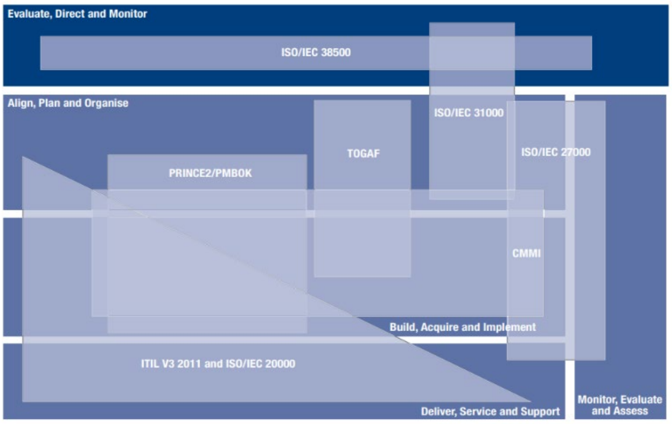
Evaluate, Direct and Monitor
ISO/IEC 38500
Align, Plan and Organise
TOGAF
ISO/IEC 31000
ISO/IEC 27000
PRINCE2/PMBOK
CMMI
Build, Acquire and Implement
ITIL V3 2011 and ISO/IEC 20000
Deliver, Service and Support
Monitor, Evaluate and Assess

Fig. 1: COBIT 5 coverage of other standards and frameworks (ISACA, 2012)

To delve deeper into security aspects of governance, ISO 27001:2013 is employed. This aligns with the Regulation of the Minister of Communication and Informatics of the Republic Indonesia No. 4 of 2016 regarding Information Security Management Systems, which mandates that Providers of Strategic Electronic Systems and Providers of High Electronic Systems must adhere to the SNI ISO/IEC 27001 standard (Chapter III, Article 7, Paragraph 1 and Paragraph 2). Additionally, in accordance with Ministry of Public Works and Public Housing of the Republic Indonesia Regulation No. 27 of 2020, Information Security Management in the Ministry follows the SNI ISO/IEC 27001:2013 Information Security Management System. Furthermore, according to Sama et al. (2021), the ISO 27001 standard is highly suitable for implementing information security management within an organization/company, as it provides certification indicating effective information security implementation

3. Research Metodology

This research used the Design Science Research Methodology (DSRM), which focuses on developing innovative technology-based solutions to support organizational needs and improve information system performance (K. Peffers, 2018) The DSRM process consists of six steps: problem identification and motivation, objective solution definition, design and development, demonstration, evaluation, and communication. (Peffers et al., 2007) Figure 1 illustrates the stages conducted in this research.

The DSRM process is particularly well-suited for implementation within the Directorate General of Human Settlements due to its comprehensive and structured approach, consisting of six well-defined steps: problem identification and motivation, objective solution definition, design and development, demonstration, evaluation, and communication. Given the diverse nature of the Directorate's responsibilities, which include managing water supply systems, building approvals, and urban development, the DSRM process provides a clear framework to systematically identify and address security challenges across these different domains. By systematically identifying and defining objectives, designing tailored solutions, and demonstrating their effectiveness, the Directorate General of Human Settlements can enhance its capacity to effectively manage risks, protect critical data, and ensure the security of its operations. Furthermore, the evaluation and communication stages of the DSRM process enable ongoing improvement and the dissemination of best practices, fostering a culture of continuous enhancement in the Directorate's cybersecurity efforts.

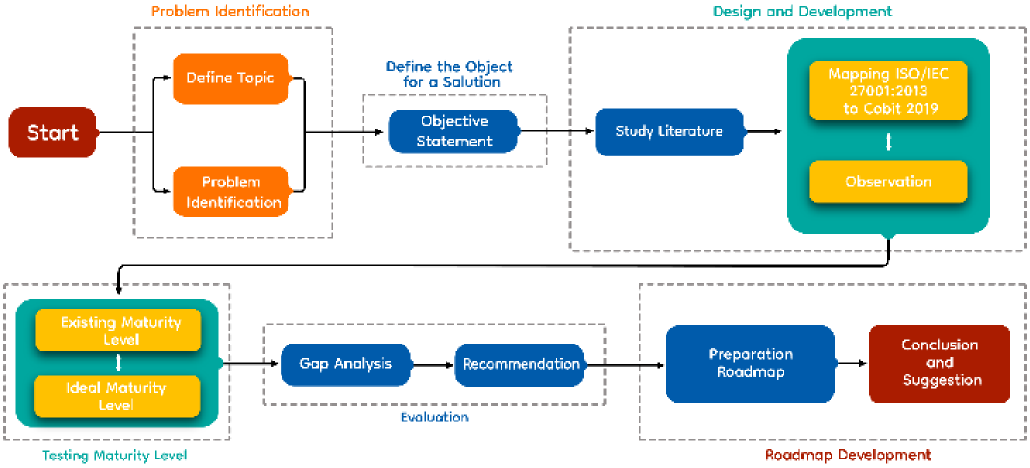

Fig. 2: Research Stage

3.1. Problem identification.

In this stage, the research topic is determined, the research problem is formulated/defined, and solutions are sought for the problem related to the chosen topic, information security in the The Directorate General of Human Settlements information system.

3.2. Define the object for the solution.

Define the objective of the problem formulation related to information security governance. The goal is expected to be better than the current condition, which can support the resolution of information security problems. This stage aims to assist the organization The Directorate General of Human Settlements in achieving a higher capability maturity level for an adapted IT governance system.

3.3. Design and development.

The design and development stage describes the process of creating artifacts, which is the design of the information system security governance of The Directorate General of Human Settlements based on ISO 27001: 2013 on the Information Security Management System and COBIT 2019. The first step is data collection and observation, then analysis of each factor of the COBIT 2019 design. Next, determine the selected domain in the COBIT 2019 framework according to the scope of needs. This stage is the most essential stage of the entire COBIT 2019 process. ISO 27001:2013 and COBIT 2019 clauses are mapped from the selected domain. Then we will see which clauses are the same and which can be integrated to become a new clause on security-based governance. This goal is expected to be better than the current condition or can become a new artifact supporting the resolution of information security problems. In designing and developing the governance, it is aligned with the COBIT 2019 governance framework.

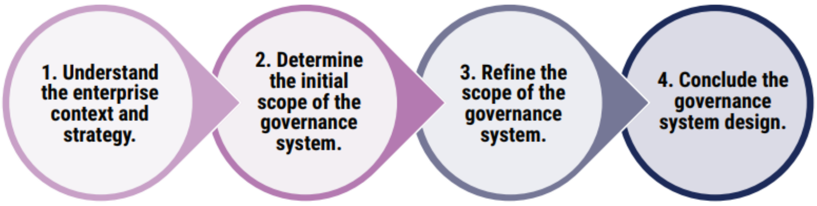
1. Understand the enterprise context and strategy.
2. Determine the initial scope of the governance system.
3. Refine the scope of the governance system.
4. Conclude the governance system design.

Fig. 3: Governance Design Workflow

In this phase, the first step is to understand the organization's needs and context, including a deep understanding of the organization's profile and objectives. The second step involves defining the initial scope of governance, based on the insights gained from the organization's needs and planned context. The third step involves refining and expanding the scope of the existing governance system by identifying threats to the organization, compliance requirements, IT roles in the form of a source model, and more. The fourth step encompasses the results from all ten design factors. Design factors are elements that can influence the design of the organizational governance system and position it for success in using information and technology. During the selection of design factors, interviews will be conducted with the Head of Data and Information System Development Subdivision and the team. The Directorate General's vision, mission, and strategic objectives are incorporated into the eleven design factors within COBIT 2019, as depicted in Figure 4

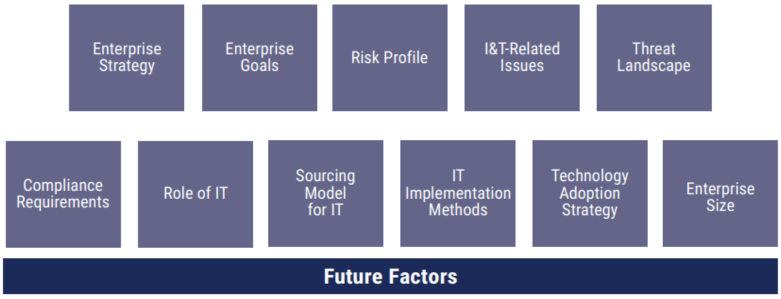

Fig. 4: Governance Design Workflow

The mapping of design factors utilizes the COBIT 2019 toolkit provided by the Information Systems Audit and Control Association (ISACA) website, employing the degree of influence for each design factor on the 40 models to determine the scope or core model selected. The assessment is conducted by creating a questionnaire that aligns with the activities of the selected domains. These activities will form the questions in the distributed questionnaire. The activities from the chosen domains are derived from the COBIT 2019 framework (Maulana Fikri et al., 2020).

The selection of respondents for the questionnaire is determined using a RACI Diagram, which is employed to identify stakeholders within the business process or company stakeholders. This approach helps in selecting suitable participants for this research (Information Systems Audit and Control Association, n.d.). The chosen respondents within the Environment of the Directorate General of Spatial Planning, among others, are:

1. Head of the Subdivision for Data and Information System Development in Human Settlements
2. Program Coordinator for Evaluation and Management
3. Head of the Subdivision for Administrative Affairs, Directorate of Housing and Settlement Development
4. Head of the Sub-coordinator for Information System Development
5. Network Specialist and Information System Specialist in the Subdivision for Data and Information System Development in Human Settlements

6. Information and Communication Technology (ICT) Responsibility Holder within the Directorate General of Spatial Planning

The assessment of maturity levels is carried out through a questionnaire that aligns with COBIT 2019 governance and management objectives and ISO 27001:2013. The results of the assessment on the selected core domains of COBIT 2019 are subsequently aligned with ISO 27001:2013. To measure maturity values, the response range is divided into a 5-point scale: Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree. Each weight of the fulfillment value indicates the level of agreement with a statement, as presented in Table 1 below:

Table 1. Value for Agreement with Statements

Scale	Response to Question	Fulfillment Value
1	Strongly Disagree	1
2	Disagree	2
3	Neutral	3
4	Agree	4
5	Strongly Agree	5

3.4. Measuring maturity level value

In this stage, the current maturity level of The Directorate General of Human Settlements is measured, as well as the expected maturity level and the ideal maturity level of the selected COBIT domain. Assessment is done using COBIT 2019 with six ratings ranging from zero to five (0-5). The evaluation is done by creating a questionnaire based on the activities of the selected domain. These activities will be the questions in the questionnaire that will be distributed. The actions of the chosen domain are taken from the activities in the COBIT 2019 framework (Fikri AM, 2020). For the respondents in the questionnaire, the RACI Diagram is used to determine the stakeholders in the business process or the company so that they can be used as respondents in this research (ISACA, 2018).

Maturity level measurement is conducted to determine the process of implementing the information system in the The Directorate General of Human Settlements. In measuring the maturity level, a questionnaire is distributed to employees responsible for the application system used in the The Directorate General of Human Settlements using the calculation formulas (1), (2), and (3) according to Table 1.

$$Attribute\ Maturity\ Index\ = \frac{number\ of\ answers\ x\ weight\ bobot}{number\ of\ questions} \quad (1)$$

The attribute maturity index is obtained by weighing the questionnaire responses and dividing them by the total number of questions. The weight used is the weight of each response option, which indicates each option's value or importance level in the context of the questionnaire question. The questionnaire consists of five response options with weights as follows: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), and Strongly Disagree (1).

$$Maturity\ Index\ = \frac{Attribute\ Maturity\ Index}{number\ respondents} \quad (2)$$

The maturity index is obtained by dividing the attribute maturity index result by the number of respondents available.

$$Maturity\ Level = \frac{Maturity\ Index}{number\ of\ subdomains} \quad (3)$$

The level of maturity or maturity assessment is obtained by calculating the maturity index and then dividing it by the activities or subdomains that have been selected.

The data is accurate as it aligns with the provided instructions, which specify the required positions for survey respondents. Those who are filling out the questionnaire must hold the mentioned positions. This ensures that the collected information is relevant and reliable for the intended analysis.

Table 2. RACI Chart Identification Results

No	Raci Chart in COBIT 2019	Position at Directorate General of Human Settlement	Domain
1.	*Chief Information Officer*	Head of Subdirectorate for Data and Information System Development	APO11,APO12,APO13, BAI06, BAI10, DSS03, DSS04, DSS05, DSS06, EDM03 dan MEA03
2.	*Head Human Resources*	Head of Administration for Technical Development	DSS05
3.	*Head IT Operation*	Information Systems sub coordinator	APO11,APO12, APO13, BAI06, BAI10, DSS02, DSS03, DSS04, DSS05, MEA03
4.	*Program Manager*	Program Planning and Evaluation Coordinator	APO11
5.	*Business Process Owner*	Application owner in each Directorate (7 people)	APO11,APO12, APO13, DSS02, DSS04, DSS05, DSS06 dan MEA03
6.	*Information Security Manager*	Network Experts (1 people) and Information System Experts (1 people)	APO11,APO12, APO13, BAI06, BAI10, DSS02, DSS03, DSS04, DSS05, DSS06, MEA03
7.	*Privacy Officer*	Members of the Risk Management Working Group related to Data and Information Systems	APO12, APO13, BAI06, MEA03

3.5. Evaluation

At this stage, evaluation and analysis of the maturity assessment are conducted to generate gaps between the current level of maturity and the ideal level of maturity referring to the maturity results. The evaluation and analysis results become the basis for determining recommendations for activities The Directorate General of Human Settlements must undertake to fill these gaps. After evaluating an organization's IT governance maturity level, the next step is to identify the gaps between the current and desired level of maturity. This gap is the difference or discrepancy between recent performance and expected performance. Recognizing this gap will help organizations determine which areas need to be optimized or improved to achieve the desired level of IT governance maturity.

3.6. Development of Roadmap

The evaluation results will be communicated to the leaders and information system implementers in the The Directorate General of Human Settlements to determine the direction of leadership policies from 2024 to 2028, which will be embodied in a roadmap. Then, conclusions and suggestions are made for the next steps. The roadmap development is one of the essential steps in the solution development process. Still, for this paper, the roadmap development is not included in the scope of the research. This study focuses on the initial action stages to evaluate the applied solutions.

4. Result and Discussion

The results of Directorate General of Human Settlements mains consist of 5 stages. These stages include problem identification, defining the solutions object, design and development, measuring maturity level, and evaluation.

4.1.Problem identification.

This research is conducted because the Directorate General of Human Settlements has 28 applications spread across eight directorates, as shown in Figure 5. However, the Directorate General of Human Settlements has faced several difficulties in running its applications and network, such as experiencing seven power outages and six disruptions from the service provider in the last two years. In addition, the Directorate General of Human Settlements has also experienced four hacker attacks and lost data due to a crash in the data center's storage. Therefore, this research is conducted to identify the causes and find solutions to overcome these obstacles so that the information system at the Directorate General of Human Settlements can run smoothly and securely.

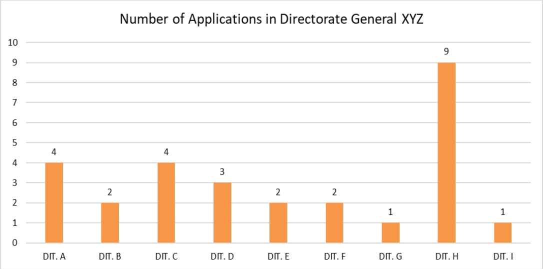

Fig. 5: Number of Applications in Directorate General Human Settlements

4.2.Define the object for the solution.

The solution to the problem identified above relates to information security governance, which involves measuring the maturity of the information system in Directorate General Human Settlements using the combined framework of COBIT 2019 and ISO 27001:2013 and providing recommendations as needed by Directorate General Human Settlements to help the organization achieve a better level of capability maturity.

4.3. Design and development.

The first step is data collection and observation, followed by selecting the relevant domain in the COBIT 2019 framework through design factors according to the scope of the requirements. Next, mapping the clauses in ISO 27001:2013 and COBIT 2019. Based on the observation results, there are potential threats to information system assets, as shown in Table 3.

Table 3. Potential Threats to Information System Assets in Directorate General of Human Settlements

No	Name	Potential Threats	Causes
1	Software	Malware Attacks: Virus, Worm, Trojan, spyware Hacker Attacks Integration Issues Security Coding Weaknesses	Lack of software, firewall, and antivirus updates Downloading untrusted software Phishing and fake emails Design flaws, software compatibility, non-standard coding, untested coding, undocumented coding

2	Data and Information	Server Failures Data Theft Illegal Data Alterations	Overload, cyber attacks, power outages, hardware damage Weak passwords or outdated security systems, cyber-attacks, and information leakage by staff who can facilitate data theft
3	Hardware	Component failures such as hard drive, RAM, or CPU failures, printers Physical damage, such as cable damage Loss/theft	device age, overheating, electromagnetic interference, component damage, overload Theft
4	Network and Communication/ Telecommunication	DDoS Attacks, Hacking, and Network Configuration Weaknesses Overload	Weak network protocol settings such as default settings, incorrect configurations, insufficient technical ability, outdated network devices
5	Human Resources	Communication Failures Motivation Issues Ethical Issues (data forging/theft) Lack of Competence Stress	Misinterpretation, lack of information, cultural differences -Poor management, lack of rewards, uncomfortable work environment (pollution and noise) -Lack of supervision, organizational culture, lack of ethics education -Lack of education and training, lack of experience, lack of support, organizational culture -Excessive workload

The information assets are needed to select the appropriate design factors for the needs of the Directorate General of Human Settlements. From these assets, the COBIT 2019 domain is chosen using the design factors carried out using the toolkit provided by the COBIT 2019 design guide in the form of a spreadsheet. The toolkit uses 10 out of 11 design factors in the COBIT 2019 design guide. One of the design factors that is not used is enterprise size because, according to ISACA 2019, an organization is considered significant if it has more than 250 employees, while the Directorate General of Human Settlements has 7360 employees. The selected design factors are by the conditions of the case study object. Each design factor selection has a weight value in each domain. In this stage, the priority and non-priority domains will be determined based on weighting results. Stakeholder interviews are conducted to acquire data on the values of design factors 1 through 10 To collect information about the design factors. The design factors are as follows:

1. Enterprise Strategy
2. Enterprise Objectives
3. IT Risk Profile
4. IT-related Issues
5. IT Landscape/Threat Potential
6. Compliance Requirements
7. IT Role
8. IT Source Model
9. IT Implementation Method
10. Technology Adoption Strategy

The output generated at this stage is a summary of values in each process on a scale of -100 to 100. In COBIT 2019, all processes are evaluated, but not all are important. The processes the author will evaluate are essential for the Directorate General of Cipta Karya, with a value of 50 or higher. By following these steps, the organization will achieve a governance system tailored to the needs of the

Directorate General of Cipta Karya. After analyzing the objective in determining Design Factors (DF1-DF11), the process objectives to be further evaluated are concluded, as shown in Figure 6.

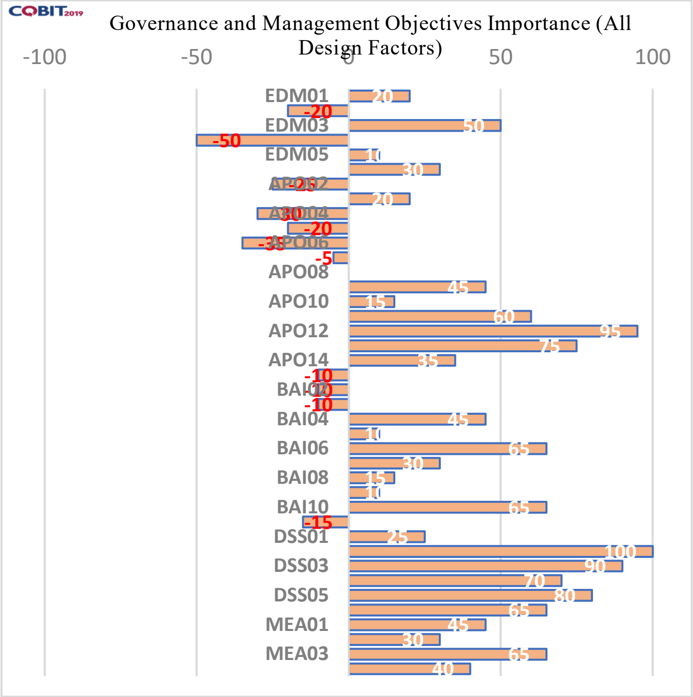

Fig 6. Results of All Design Factors

Based on the figure, the process objectives that have a value of ≥50 are:

Table 4. Priority Design Factor Results

No	Reference	Governance/Management Objective	Priority
1.	EDM03	Ensured Risk Optimization	50
2.	APO11	Managed Quality	60
3.	APO12	Managed Risk	95
4.	APO13	Manage Security	75
5.	BAI06	Managed IT Change	65
6.	BAI10	Managed Configuration	65
7.	DSS02	Managed Service Requests and Incidents	100
8.	DSS03	Managed Problems	90
9.	DSS04	Manage Continuity	70
10.	DSS05	Manage Security Service	80
11.	DSS06	Managed Business Process Controls	65
12	MEA03	Manage compliance with an external requirement	65

After obtaining the 12 critical domains from COBIT 2019 design factors, the next step is to combine the selected domains with clauses from ISO 27001:2013 to obtain the following table.

Table 5. Combination of COBIT 2019 Domains and ISO 27001:2013 Clauses.

COBIT 2019 Domain Name		ISO 27001:2013 Clause Name	
APO13	Managed Security	A.18.2	Information Security Reviews
		A.14.1	Information system security requirements
DSS04	Managed Continuity	A.17.1	Information security continuity
		A.17.2	Redundancies

DSS05	Manage Security Service	A.9 A.9.1 A.9.2 A.9.3 A.9.4 A.10.1 A.11 A.11.1 A.11.2	Access control Business requirements for access control User access management User Responsibilities System and application Access control Cryptography controls Physical and environmental security Secure areas Equipment
DSS05	Manage Security Service	A.12 A.12.2 A.12.4 A.12.5 A.12.6 A.13 A.13.1 A.13.2 A.16.1	Operations security Malware protection Logging and monitoring Operational software controls Technical vulnerability management Communication security Network security management Information transfer Information security incident management and improvement
MEA03	Managed Compliance With External Requirements	A.18.1	Compliance with legal and contractual requirements

Then a questionnaire was created based on the detailed guidance book in COBIT 2019 Governance and Management Objective and the ISO 27001:2013 domain based on the selected clauses in the KAMI (Information Security) Index 4.2 by the State Cyber and Code Agency (BSSN). An example of mapping the KAMI 4.2 index into COBIT domain statements is shown in Table 6 below

Table 6. Mapping of KAMI Index and ISO 27001:2013 Clauses

No	Information Governance	ISO 27001:2013 Clause	COBIT 2019
Information Security Risk Assessment			
3.1	Is there a documented and officially utilized security risk management program within the organization?	A.16.1.1 A.16.1.4	DSS05 DSS05
3.2	Has the organization designated a risk management responsible person and established escalation for reporting the status of information security risk management up to the management level?	A.16.1.3 A.16.1.6	DSS05 DSS05
3.3	Is there a documented and officially utilized security risk management framework within the organization?	A.16.1.6	DSS05

After identifying the questions from the KAMI 4.2 index, they were combined with the statements in the detailed guidance of COBIT 2019 Governance and Management Objective. From the questionnaire results, respondents were selected to fill out the questionnaire in each domain. Fourteen respondents were obtained from the Human Settlements Agency, as shown in Table 2. After obtaining respondents for each domain, the next step is for respondents to give a weighted score ranging from 0 to 5 by giving the value of Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), and Strongly Disagree (1).

4.4.Measurement of maturity level

At the measured maturity level, based on the questionnaire results, the maturity level of each domain in the information system of Directorate General Human Settlements was obtained with an average of 3.07. Directorate General Human Settlements has managed the information system using established standards (defined) and implemented processes consistently in line with business objectives. Directorate General Human Settlements also aims to improve the security maturity level of the information system to reach the highest level (level 5). To achieve this goal, Directorate General Human Settlements needs to continue to evaluate, improve, and consider using the latest technology and innovation.

After the maturity level is obtained, information technology governance gaps are analyzed to facilitate improvements in information technology governance. This analysis is obtained by comparing the current and expected maturity levels. Thus, which process objectives have gaps and require improvement will be known. Comparing the maturity levels will determine which process objectives do not meet the desired maturity level. If there are gaps, recommendations based on findings and the gap between desire and expectation will be given to achieve the desired maturity level by Directorate General Human Settlements. The maturity level and gap analysis results can be seen in Table 7 and Figure 7 below.

Table 7. Maturity Level and Gap Results

No	Domain	Meaning	Expected Level Maturity	Level Maturity	Gap
1.	EDM03	Ensured Risk Optimization	5	3,39	1,61
2.	APO11	Managed Quality	5	3,28	1,72
3.	APO12	Managed Risk	5	3,36	1,64
4.	APO13	Manage Security	5	3,09	1,91
5.	BAI06	Managed IT Change	5	2,91	2,09
6.	BAI10	Managed Configuration	5	1,50	3,50
7.	DSS02	Managed Service Requests and Incidents	5	3,68	1,32
8.	DSS03	Managed Problems	5	3,30	1,70
9.	DSS04	Manage Continuity	5	2,32	2,68
10.	DSS05	Manage Security Service	5	3,24	1,76
11.	DSS06	Managed Business Process Controls	5	3,44	1,56
12.	MEA03	Manage compliance with an external requirement	5	3,43	1,57
		Average		3,07	1,93

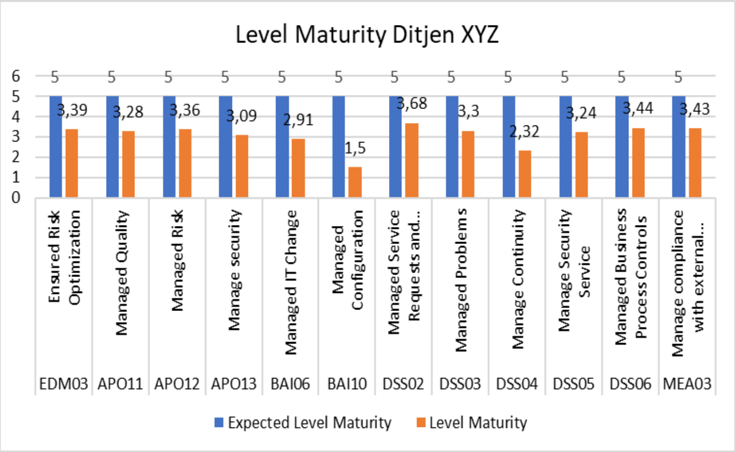

Fig 7. Level Maturity Directorate General Human Settlements

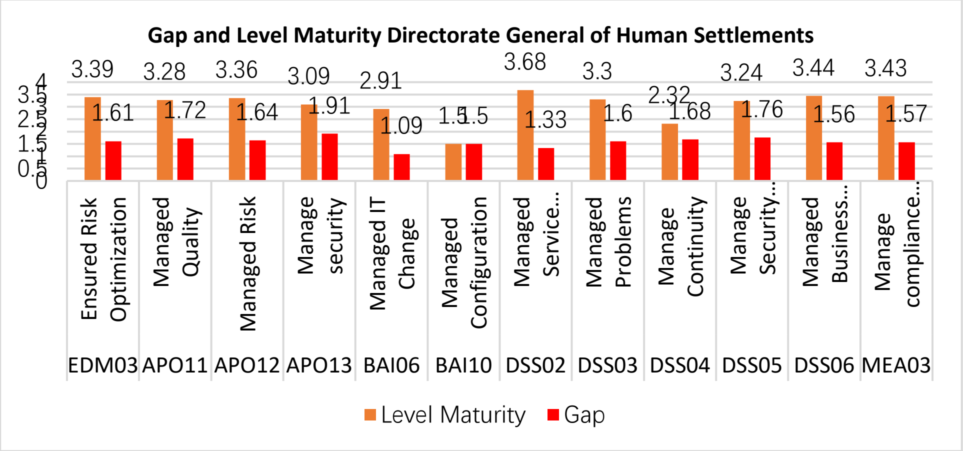

Fig 8. maturity levels vs gaps for each domain

4.5.Evaluation

The recommendations for improvement in the previous study (yasin,2020) consisted of a 5-year policy roadmap, encompassing areas such as I&T governance, policy alignment, planning and organization, establishment and implementation, service delivery and support, as well as monitoring, evaluation, and assessment of I&T policies.

In contrast, the current study places heightened emphasis on refining and recommending specific enhancements within the selected domains, as delineated in COBIT 2019. This tailored approach delves into the intricacies of each domain, leveraging the framework to provide nuanced solutions that align with the organization's needs and challenges. The current study systematically examines distinct areas, such as strategic alignment, risk management, quality assurance, security protocols, change management, configuration control, incident handling, problem resolution, business continuity, and compliance. Each domain's improvement recommendations are tailored to maximize efficiency, minimize risks, and ensure compliance with industry standards. This targeted approach is designed to yield practical and actionable insights, facilitating the organization's precise evolution and advancement within the specific I&T management dimensions delineated by COBIT 2019.

This assessment shows that the information security governance at Directorate General of Human Settlement has not yet achieved the target maturity level of 5. Level 5 can be achieved by continuously improving and enhancing information system management and optimizing information technology resources to support organizational goals. Recommendations for the 12 Information System Processes are necessary to improve and increase the maturity level in the subsequent measurement. The recommendations for each information system process that has a value of less than 5 are as follows:

a. Evaluate the effectiveness of implemented risk controls and mitigation actions according to the subdomain EDM03 (Ensured Risk Optimization).
b. The quality of information system services should be documented (customer satisfaction survey) by measuring and monitoring performance regularly to determine the effectiveness of established quality management processes so that improvements and preventive actions can be taken more effectively and timely according to the subdomain APO11 (Managed Quality).
c. Using an integrated risk management information system with digital and analytical technologies (Risk and Compliance Information System) is recommended to support identifying, evaluating, managing, and reporting risks automatically and in real time. Data analysis and risk prediction can also be made using big data analytics and machine learning technologies to identify risks more quickly, accurately, and measurably and estimate the potential impact and likelihood according to the subdomain APO12 (Managed Risk).

d. Implement integrated procedures and policies to manage information security, conduct regular internal audits, and increase knowledge/training of information security among all staff to ensure safe technology management and business processes aligned with company management according to the subdomain APO13 (Manage Security).
e. Manage and record the emergency change status, which records the initial status of the change and the final status according to the subdomain BAI06 (Managed IT Change).
f. Evaluate and improve configuration management, create and manage configuration repositories, and control configuration baselines according to the subdomain BAI10 (Managed Configuration).
g. Automate the service request and incident management process to improve efficiency and consistency in handling them according to the subdomain DSS02 (Managed Service Requests and Incidents).
h. Expected to create a system for monitoring the IT service desk. It is necessary to create incident tickets, record incidents, and monitor incident developments so that they know the extent of the problem according to the subdomain DSS03 (Managed Problems).
i. Create a business continuity plan (BCP) to identify risks and overcome their impact on business continuity. It includes a disaster recovery plan to ensure the business can operate again quickly after a significant disruption or disaster according to the subdomain DSS04 (Manage Continuity).
j. Conduct routine evaluations, at least once a month, of information systems that may pose new potential threats, measure the quality of security systems and access rights given, and evaluate or monitor access rights given to guard against potential threats according to the subdomain DSS05 (Manage Security Service).
k. Create procedures to correct errors in entering information. These procedures can take the form of anticipation and regular data backups according to the subdomain DSS06 (Managed Business Process Controls).
l. Conduct regular internal audits to ensure compliance with external requirements, take necessary corrective actions to address non-compliance and provide regular training and development for employees to improve their understanding and awareness of external requirements to ensure appropriate compliance according to the subdomain MEA03 (Manage Compliance with External Requirements).

5. Conclusion

Based on the evaluation of information security governance conducted at Directorate General of Human Settlement, the following conclusions can be drawn:

a. Based on the research that has been conducted, it can be concluded that the identification of maturity levels in governance can be made through a step-by-step process starting from the planning stage of the research, which is identifying the problem, conducting data collection through the creation of questionnaires to document review, and finally the data analysis stage, which is done through maturity level calculation to provide recommendations.

b. The result of identifying the level of information system management at Directorate General of Human Settlement shows that the maturity level calculation of all domains averages above three except for BAI06 Managed IT Change, BAI10 Managed Configuration, and DSS04 Manage Continuity, which are at level 2, indicating that they are not standardized and not widely adopted throughout the organization. A gap emerges in each domain from identifying the expected level of information system management and the achieved level. The gaps in the BAI06, BAI10, and DSS04 domains are 2.09, 3.50, and 2.68, respectively. The average maturity level attained by the Directorate General of Human Settlements is 3.07.

c. In improving the quality of service management, it is recommended to implement the recommendations on the evaluation results (subbab 4.5) to reach the expected level of ability, namely level 5. These recommendations include 12 Information System processes for improvement and refinement in order to increase the maturity level score in the system next measurement.

d. In this study, the governance of information system security produced will be highly beneficial for the Directorate General of Cipta Karya by implementing the stages of information system security governance based on the recommended Roadmap. Furthermore, this study has not specifically addressed risk management as outlined in ISO 31000, ISO/IEC 27005:2018 on Information Security Risk Management, COSO Enterprise Risk Management 2017, CRISC (certified in Risk and Information System Control) and other risk management frameworks. Hence, this presents a potential area for further research that can complement the recommended roadmap.

Reference

Aditya, M. A., Mulyana, R. D., & Mulyawan, A. (2019). Perbandingan COBIT 2019 dan ITIL V4 Sebagai Panduan Tata Kelola dan Manajemen TI. Jurnal Computech & Bisnis, 100-105.

Axelos. (2019). ITIL Foundation. Norwich: TSO (The Stationery Office).

Bayastura, S., Krisdina, S., & Widodo, A. (2021). Analisis dan Perancangan Tata Kelola Teknologi Teknologi Informasi Menggunakan Framework COBIT 2019 Pada PT. XYZ. Jurnal Informatika dan Komputer (JIKO), 68-75.

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. Conference on Information Systems and Technologies (CISTI) . Coimbra, Portugal: Institute of Electrical and Electronics Engineers.

Commission), I. (. (2008). Corporate governance of information technology. Jenewa.

Fikri AM, P. H. (2020). Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 (Studi Kasus PT.XYZ). Information Management for Educators and Professionals. 5 (1), 1-14.

ISACA. (2018). Cobit 2019 Framework-Introduction-and-Methodology.

ISACA, I. (2012). COBIT 5 : a business framework for the governance and management of enterprise IT. USA: Information Systems Audit and Control Association.

ISACA, I. S. (2018). COBIT 2019 Framework Governance and Management Objectives. USA.

Ishlahuddin, A., Handayani, P. W., Hammi, K., & Azzahro, F. (2020). Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu). 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020, (pp. 236-241). Jakarta.

K. Peffers, T. T. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research. European Journal of Information Systems, vol. 27, no. 2, 129-139.

Ken, P., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems.

Maulana Fikri, A., Shofia Priastika, H., Octaraisya, N., Happy Trinawati, L., Kalimantan, T., Soekarno-Hatta Km, J., Joang, K., & Timur, K. (2020). Information Management For Educators And Professionals Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: PT XYZ). 5(1), 1–14.

Nawir, M., AP, I., & Wajidi, F. (2022). Integration Of Framework ISO 27001 and COBIT 2019 In Smart Tourism Information Security PT. YoY International Management. Jurnal Komputer dan Informatika, 122-128.

Prapenan, G. G., & Pamuji, G. C. (2020). Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013. IOP Conference Series: Materials Science and Engineering. Jakarta: IOP.

Putra, P. P., Arman, A. A., Edward, I. M., & Shalannanda, W. (2020). Designing Recommendations and Road Map of Governance for Quality Management System of Online SKCK Based on Information Security Using ISO 9001: 2015 and ISO 27001: 2013 (Case Study: Ditintelkam Polda ABC). IEEE.

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing informationtechnology security system based on risk analysis and cybersecurityframework. Egyptian Informatics Journal, 383-404.

Safitri, A., Syafii, I., & Adi, K. (2021). Identifikasi Level Pengelolaan Tata Kelola SIPERUMKIM Kota Salatiga berdasarkan COBIT 2019. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 429-438.

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). STUDI KOMPARASI FRAMEWORK NIST DAN ISO 27001 SEBAGAI STANDAR AUDIT DENGAN METODE DESKRIPTIF STUDI PUSTAKA. Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab, 6(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Steuperaert, D. (2019). COBIT 2019: A Significant Update. The EDP Audit, Control, and Security (EDPACS) VOL. 59, NO. 01, 14-18.

Utomo, D., Wijaya, M., Suzzana, Efendi, & Maretta, S. T. (2022). Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A. CommIT Journal, 129-141.

Wiley, J. (2011). COSO Enterprise Risk Management_ Establishing Effective Governance, Risk, and Compliance Processes. New Jersey: John Wiley & Sons, Inc.

Yasin, M., Arman, A. A., Edward, I. J., & Shalannanda , W. (2021). Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). IEEE.