JOURNAL OF MULTIDISCIPLINARY ISSUES
Journal Website: www.jmis.site
J. Multi. Discp. Issues 1(2) 62-74 (2021)

INFLUENCE OF INFORMATION SECURITY CULTURE ON THE INFORMATION SECURITY GOVERNANCE CAPABILITIES (CASE STUDY: PT XYZ)

Kevin Suwandi[a], **Johan Setiawan**[b]
[a, b] Universitas Multimedia Nusantara, Jakarta, Indonesia

ABSTRACT

Objective – To analyze the relationship between a company's information security approach/culture with its information security governance capabilities based on COBIT 5 framework and provide recommendations that can be used to improve the company's information security capabilities per COBIT 5 standard.
Methodology – The research uses qualitative and quantitative methods by conducting interviews and distributing questionnaires to 3 members of the IT Department at PT XYZ.
Findings – The research found that the measured COBIT 5 processes (APO13 and DSS05) failed to reach the expected target (level 4), with each DSS05 and APO13 can only reach level 1 and 2 respectively. In addition, several flaws were also found in the company's information security culture that may have contributed directly or indirectly to the current state of the company's information security capabilities.
Novelty – In this study, the researchers combine and expand the previous studies on information security culture conducted in 2010 and 2019 by performing a security audit on a company's IT department to analyze the connection between corporate culture, especially information security culture and the capability level of information security governance. The company thus can make improvements or corrections to its information security approach/culture based on the recommendations provided with COBIT 5 framework.
Keywords: *Capability Level; COBIT; Governance; Information Security Culture.*

JEL Classification: C83, L83, M14
Article Info: Received July 2021; Revised August 2021; Accepted August 2021
Article Correspondence: johan@umn,ac,id
Recommended Citation: Suwandi and Setiawan (2021). Influence of Information Security Culture on The Information Security Governance Capabilities (Case Study: PT. XYZ**. *Journal of Multidisciplinary Issues*, 1 (2), 62-74.**

I. INTRODUCTION

Compared to many years ago, the information security environment has become even more dynamic and complex in recent days. Simply implementing state-of-the-art security controls and technologies may no longer be adequate to protect enterprises from increasingly sophisticated threats. The threats facing today's organizations are far more advanced than in the past, so are the information security technology and frameworks that are constantly being developed to deal with emerging threats. However, despite all the recent advancements in information security technology and frameworks, high-profile security incidents are still a frequent occurrence to this day, sometimes even involving multinational companies that already have supposedly state-of-the-art information security systems. Several factors may contribute to this phenomenon, including but not limited to the ineffective implementation of information security governance which is partly or wholly caused by the executives who are still sticking to the ineffective old approach to the information security framework (Tan et al., 2010).

For the information security governance framework to run effectively, it must be supported by a corporate security culture and a decision-making system that is dynamic and adaptive to the company's information security needs. Many companies are currently still applying the security governance doctrine that is often based on a centralized decision-making model and a risk management approach to information security commonly used in the 20th century. This old-fashioned centralized approach is relatively simple to manage as it hardly needs any security governance below the top level of the enterprise where the majority of the decision-making process is conducted and still provides roles for additional governance practices, regulations, and new methods to overcome the weakness of the organizational security governance.

However, the relevancy of this type of approach has been increasingly questioned in an increasingly complex and dynamic information security environment which puts more emphasis on flexibility and adaptability. When observed from its implementation in various companies, this old-fashioned approach tends to place more emphasis on compliance and control than on the information security itself. This type of approach resulted in the IT division, especially those responsible for maintaining the organization's information security to put more emphasis on meeting organizational standards and policies than improving the quality of the system's security, thus reducing the flexibility and adaptability of the company's information security posture. As a result, this can make it difficult for the organization to respond quickly and promptly to rapid or sudden changes in its information security environment (Tan et al., 2010).

The consequences of failure to adapt to this rapidly changing information security environment can be very serious for both the enterprise and customers who use their services. The company can be caught unprepared in the face of ever-developing information security threats. One of the most common examples is data breach incidents that are happening at an increasingly alarming rate even as we already entered the third decade of the 21st century where information security technologies are supposed to be advanced and developed enough to deal with emerging threats. In 2018, a popular Q&A website Quora suffered a data leak that compromised about 100 million of its user accounts data, including names, email addresses, and encrypted passwords. More recently Tokopedia, an Indonesian e-commerce company also experienced a data breach in March 2020 with about 91 million user accounts and 7 million merchant accounts allegedly stolen and sold on the dark web for tens of millions of rupiah.

Several studies have already been conducted on the relationship between the company's information security approach/culture and the implementation of its security governance. One of them is the research conducted by Terrence C.C. Tan, Anthoine B. Ruighaver, and Atif Ahmad (2010) with the title "Information Security Governance: When Compliance Becomes More Important Than Security." Qualitatively, this journal is useful in providing a comprehensive explanation of the security decision-making approach and its impact on IT staff and the implementation of corporate information security governance. However, it has not yet conducted a quantitative audit or survey on corporate information security capabilities to strengthen the results obtained from the interview process.

A more recent related study on this problem was conducted in 2019 by Ashleigh Wiley, Agata McCormac, and Dragana Calic of the University of Adelaide. This study aims to examine the relationship between organizational culture and information security awareness. Unlike the previous 2010 study, the data collection in this research was administered through an online survey to hundreds of respondents divided across age groups. The result of this study shows that there is a positive linear relationship between organizational culture, security culture, and information security awareness. Essentially, individuals from companies with stronger information security cultures were more likely to have better information security awareness (Wiley et al., 2020).

Based on the previous studies of the relationship between information security culture and IT security governance capabilities, this study aims to combine and expand the researches that have been conducted on this issue using both qualitative and quantitative methods with COBIT 5 framework as guidelines. The results are then analyzed and compared with each other in order to produce necessary recommendations for the enterprise.

The research object in this study is a hotel franchise company in Indonesia named PT XYZ. Currently, PT XYZ's IT services are managed by the IT division, with most of them are still limited to internal uses. Hence, the customers are still unable to order via the company's website. However, the hotel's website already has a chat service that allows potential customers to contact the company's customer services to make a booking. In recent years, the IT division has conducted regular audits on the enterprise's IT governance, including the information security aspect, but still not using an internationally recognized IT Governance framework in the process. Based on the preliminary observations and discussions with the company IT manager, it was discovered that there were several problems in the company's information security governance, as listed in Table 1.

Table 1 Preliminary Findings of Information Security Issues at PT XYZ

No	Preliminary Findings	Possible Impact
1	Two-way authentication has not been implemented on some devices	Devices are vulnerable to unauthorized access if password confidentiality is compromised
2	Lack of physical protection on server room	Server room is vulnerable to access from unauthorized parties
3	There is a communication gap between the IT division and company management	Inputs from the IT team are often not taken into account in the decision-making process of information security policies

From the description of the initial findings, it could be concluded that in-depth measurement of corporate information security governance capabilities using standards or frameworks that can function as references are necessary to obtain valid results. In this study, the research only focuses on the company's IT department to measure its information security capability level using the COBIT 5 framework and its relationship with its information security approach or culture. This framework was chosen because the processes related to information security in COBIT 5 have been integrated into a broader IT Governance framework and have directly or indirectly influenced other COBIT processes unrelated to information security. As a result, it can facilitate further research that intends to find relationships between the level of IT governance capability in the processes measured in this research with the capabilities of other related COBIT processes.

Based on the result of this research, the company's IT division is expected to be able to understand the results of the evaluation of the level of its information security capability and its relationship with the company's information security approach, as well as trying to make improvements in the company's information security management approach in order to achieve the expected level of capability using the recommendation provided.

II. LITERATURE REVIEW

COBIT 5

Control Objective for Information and Related Technologies (COBIT) is an IT Governance framework created by ISACA in order to define a set of generic processes for information technology management (Dahlberg et al., 2016). The advantage of COBIT as a framework for information security governance is that its functions are not confined to information security alone but encompassing IT governance as a whole so that the measurement result can be integrated into a broader IT Governance framework (Von Solms, 2005). COBIT divides Information Technology governance into 37 processes and provides a high-level Control Objective (CO) for each process. Each CO is subdivided into a series of Direct Control Objectives (DCOs) that specify how the CO should be run. In total, there are 316 DCO for 37 COBIT processes (ISACA, 2012). The downside of using COBIT as an Information Security Governance framework is that it does not provide more detailed instructions on "how" to do certain things. Each DCO is more directed to "what" to do, whereas in most cases, more detailed guidance is needed on "how" things should be done (Von Solms, 2005).

Process Assessment Model (PAM)

Process Assessment Model (PAM) is the basis or guide for evaluating a company's IT processes based on the COBIT 5 framework (ISACA, 2012). In the COBIT 5 framework, this model is also called the Process Capability Model. Assessment of process capability in COBIT 5 is carried out based on the ISO/IEC 15504 standard. This assessment aims to find the level or degree of maturity/capability of an organization's IT governance (Pasquini & Galiè, 2013). COBIT 5 PAM consists of a set of performance indicators and process capabilities that can be used as a guide to collect information and objective evidence to support the evaluation process (ISACA, 2012).

In COBIT 5 Process Assessment Model, there are six levels of capability that a process can achieve, ranging from level 0 (process not completed) to level 5 (optimized process) (ISACA, 2012).

- 0 (Incomplete process) – The process is not implemented or fails to achieve its process purpose.
- 1 (Performed process) – The implemented process achieves its purpose.
- 2 (Managed process) – The process is implemented in a managed fashion and its work products are appropriately established, controlled, and maintained.
- 3 (Established process) – The previous process is implemented using a defined process that is capable of achieving its process outcomes.
- 4 (Predictable process) – The process has operated within defined limits to achieve its process outcomes.
- 5 (Optimizing process) – The process has been able to improve continuously in order to meet current relevant and projected business goals.

Information Security

Information security is generally defined as the protection of information and the systems and hardware that use, store, and transmit that information from risks or unauthorized modifications through the application of policies, education, and technology, as well as ensuring the availability of information when needed (Arnason & Willett, 2007; Whitman & Mattord, 2011). Information security has three core components that make up a security model called the CIA Triangle, namely Confidentiality, Integrity, and Availability (CIA).

- Confidentiality – The information access is limited to only those with the rights and privileges to do so.
- Integrity – Information must always be whole, complete, and uncorrupted.
- Availability – Enables authorized users to access information without obstruction or interference.

Information Security Culture

Every organization or company must have a set of beliefs and ethical codes that serve as guidance in their daily operations called corporate culture. Corporate culture is the values or beliefs shared by people in the company and serves to direct all activities within the company (Van Niekerk & Von Solms, 2006). Information Security Culture is a part of the corporate culture that directs activities related to implementing corporate information security governance.

PT XYZ

PT XYZ is an Indonesian 3-star hotel franchise based in Makassar, South Sulawesi, which was founded in 2004 and until 2020 has expanded by establishing hotel sites in Mataram, Malang, Kendari, Blora, and Bulukumba. PT XYZ carries the slogan "Where Luxury is Affordable," which means providing luxury services at affordable costs. The company's first hotel was established in 2004 under the name Banua Hotel Makassar. In 2014, the company began to expand out of Makassar by trying to take advantage of the momentum of the government's program to boost Indonesian tourism. PT XYZ currently has an IT division that is responsible for the company's information security aspects, including defining and managing the company's Information Security Management System (ISMS), planning for countermeasures or treatment for information security risks, and keeping information security risks at an acceptable level based on the security policies established by the organization. The IT division has already performed a monthly audit on the enterprise's IT system, although it has yet to use internationally recognized frameworks in its implementation.

III. METHODOLOGY

The research conducted in this study can be classified as both qualitative and quantitative. It was carried out by distributing questionnaires (quantitative) and conducting interviews (qualitative) to the company’s IT department leaderships to determine the relationship between the level of information security capability at PT XYZ. The research was carried out following the stages depicted in Figure 1.

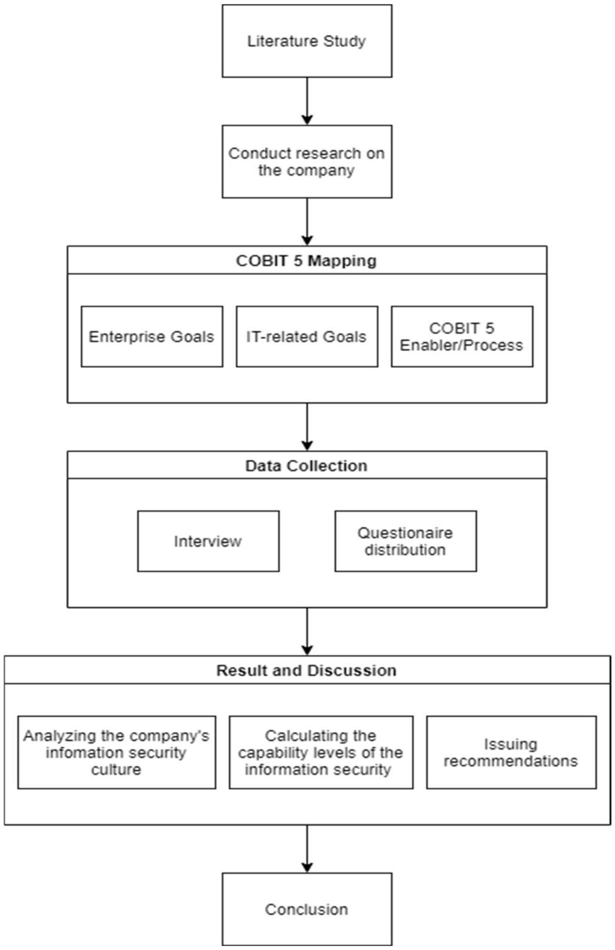
Literature Study
Conduct research on the company
COBIT 5 Mapping
Enterprise Goals
IT-related Goals
COBIT 5 Enabler/Process
Data Collection
Interview
Questionaire distribution
Result and Discussion
Analyzing the company's infomation security culture
Calculating the capability levels of the information security
Issuing recommendations
Conclusion

Figure 1 Research Flow Diagram

Based on the flowchart shown in Figure 1, the first step of this research is conducting a literature study. The literature study aims to find the information that can be used as references from various sources. The literature study was then followed by looking for more detailed information about the company through the internet and discussions with the IT manager. After all the necessary data and information is collected, the research can then enter the planning stage by mapping the enterprise goals or company goals, IT-related goals, and relevant COBIT processes, namely APO13 and DSS05.

After the planning stage was carried out, the next process is data collection which was carried out by interviewing the company's IT manager Mr. Joko Sartono and distributing questionnaires based on the COBIT 5 references to three selected respondents from IT department (IT manager, IT administrator, and head of engineering division). From the interview and questionnaires' answers, it is possible to analyze and compare the relationship between the information security approach applied and the degree of capability of the company's information security system to produce recommendations that can be used as references by the company.

IV. RESULTS AND DISCUSSION

COBIT 5 Mapping

At this stage, preliminary observations are carried out on the company to find the COBIT 5 domain that will be evaluated to measure the company's information security capabilities. The first step in the mapping process is to identify the Enterprise Goals of the corporate's information security governance adjusted to the Enterprise Goals in the COBIT 5 framework. The determination of enterprise goals is carried out by conducting a discussion with the company's IT manager. In the discussion process, IT managers were asked to choose the 3 Enterprise Goals that are regarded as the most important to the organization's information security governance culture and management, as seen in Table 2:

Table 2 Enterprise Goals Determined By Company's IT Department

Dimension	No	Enterprise Goals
Financial	3	Managed business risk (safeguarding of assets)
Customer	7	Business service continuity and availability
Internal	15	Compliance with internal policies

After the Enterprise Goals are determined, the next step is to map the Enterprise Goals into IT-related goals in order to find IT-related goals that can support the determined enterprise goals.

Table 3 Mapping of Enterprise Goals to IT-related Goals

Enterprise Goals			**IT-related Goals**	
Dimension	**No**	**Enterprise Goals**	**No**	**IT-related Goals**
Financial	3	Managed business risk (safeguarding of assets)	4	Managed IT-related business risk
			10	Security of information, processing infrastructure and applications
			16	Competent and motivated business and IT personnel
Customer	7	Business service continuity and availability	4	Managed IT-related business risk
			10	Security of information, processing infrastructure and applications
			14	Availability of reliable and useful information for decision making
Internal	15	Compliance with internal policies	2	IT compliance and support for business compliance with external laws and regulations
			10	Security of information, processing infrastructure and applications
			15	IT compliance with internal policies

Using the mapping result as references, the IT department decided to choose two IT-related goals that are considered most supportive to the previously selected enterprise goals, namely number 4 (Managed IT-related business risk) and 10 (Security of information, processing infrastructure and applications).

The last stage of the mapping process is to map the IT-related goals into COBIT 5 Enabler Goals or processes. The process or domain obtained is shown in Table 4 below.

Table 4 Mapping of IT-related Goals to COBIT 5 Enabler

IT-related Goals	COBIT 5 Process
Managed IT-related business risk	EDM03
	APO10
	APO12
	APO13
	BAI01
	BAI06
	DSS01
	DSS02
	DSS03
	DSS04
	DSS05
	DSS06
	MEA01
	MEA02
	MEA03
Security of information, processing infrastructure, and applications	EDM03
	APO12
	APO13
	BAI06
	DSS05

From the results shown in Table 4, the IT department settled for two domains to become the research focus, namely APO13 (Manage Security) and DSS05 (Manage Security Services).

1. Manage Security (APO13) – Keeping the impact and frequency of information security incidents at an acceptable level for the company.
2. Manage Security Services (DSS05) – Minimize the business impact of operational information security vulnerabilities and incidents.

Data Collection

Data collection is one of the most important processes of information systems audit activities because this will greatly affect the validity of all activities carried out. In this study, data collection was conducted by interviewing the IT manager and distributing questionnaires to 3 IT staff representatives.

The data collection process began by conducting interviews virtually with the IT manager via the Zoom application on April 30, 2021. The purpose of this interview is to find an overview of the company's information security culture to analyze its relationship with the company's information security capability levels.

The interview was then followed up with the distribution of questionnaires to 3 representatives of PT XYZ's IT staff consisting of the IT Manager, IT Administrator, and Head of Engineering. The questionnaires have been compiled based on the APO13 and DSS05 domains of the COBIT 5 framework. The questionnaire is answered with a percentage scale of 0% – 100%, which is divided into four categories, Not Achieved (0% – 15%), Partially Achieved (15 % – 50%), Largely Achieved (50% – 85%), and Fully Achieved (85% – 100%). From the obtained results of the questionnaire and recapitulation of answers from respondents, it was discovered that the value of the capability level in the APO13 process was at level 2 (Managed Process), while the DSS05 process was at level 1 (Performed Process). The results of the recapitulation can be seen in Table 5:

Table 5 Recapitulation of Questionnaire Results

Process	Sub-process	Average value given by respondents (%)	Average score (%)
Level 1			
APO13	APO13.01	88.10	87.21
	APO13.02	86.86	
	APO13.03	86.67	
DSS05	DSS05.01	85.44	85.03
	DSS05.02	90	
	DSS05.03	87.22	
	DSS05.04	85.5	
	DSS05.05	83.57	
	DSS05.06	76.33	
	DSS05.07	87.13	
Level 2			
APO13	APO13 PA2.1	86.78	85.56
	APO13 PA2.2	84.33	
DSS05	DSS05 PA2.1	77.72	79.28
	DSS05 PA2.2	80.83	
Level 3			
APO13	APO13 PA3.1	77.33	76.86
	APO13 PA3.2	76.39	

Analysis and Discussion

The capability model is a measurement tool to determine the condition of information security governance at PT XYZ. This activity will result in an evaluation of the current state of the company's information security from processes that have been adapted to organizational goals, including Manage Security (APO13) and Manage Security Services (DSS05) (Wella & Tampi, 2017).

In measuring the company's information security capability level, data were collected through questionnaire distribution and interviews. Three respondents were involved in filling out the questionnaires, consisting of the IT Manager, Head IT Administrator, and the head of the engineering department. The achievements of system capabilities in each process obtained from the results of the questionnaire measurements can be seen in Table 6.

Table 6 Capability Achievement of APO13 and DSS05

Process	Level 1	Level 2	Level 3	Level 4	Level 5
APO13	F	F	L	N	N
DSS05	F	L	N	N	N

Notes: F=Fully Achieved, L=Largely Achieved, P=Partially Achieved, N=Not Achieved

After the achievement status of each process's level is known, the next step is to construct a gap analysis. The company's IT department expected the information security capabilities to be at level 4 or predictable. Table 7 shows the gap analysis in the APO13 and DSS05 processes.

Table 7 Gap Analysis of APO13 and DSS05

COBIT 5 Process	Current Level	Expected Level	Gap
APO13 (Manage Security)	2	4	2
DSS05 (Manage Security Services)	1	4	3

Based on the gap analysis shown in Table 7, a chart could be made to compare the capability level of each domain at the time of measurement with the desired capability level.

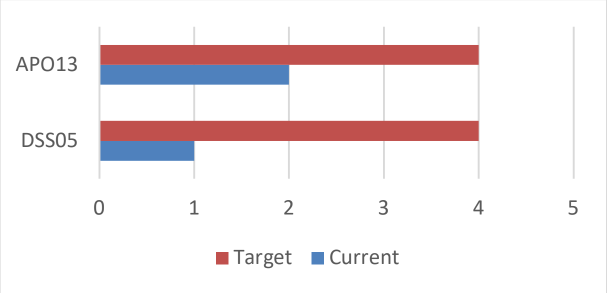

Figure 2 Comparison of Each Process Current Capabilities with Expected Targets

The evaluation result of the measurement of information security capabilities with COBIT 5 framework in APO13 and DSS05 shows that both process capabilities are still at level 1 and 2 respectively or have not reached the desired target of the company's IT department (Level 4).

The probable cause is that there are still some shortcomings that have not been addressed or activities that have not been implemented in each process that became the focus of the research. However, even though both processes failed to reach the expected target level, the average value of every sub-process at each measured level never falls below 75% as seen in Table 5, so it can be concluded that majority of activities in both processes have been performed, although not at the level expected by the company. Following is a description of each measured COBIT 5 process and the interview result with the IT Manager.

1. The APO13 (Manage Security) process discusses the definition, operation, and supervision of an ISMS (Information Security Management System). Measurement of APO13 capability in the IT department of PT XYZ is at level 2 with rating scores at levels 1, 2, and 3 respectively are 87.21% (fully achieved), 85.56% (fully achieved), and 76.86% (largely achieved). In this process, several shortcomings were found which could prevent the process from moving to the next level, some of them including many security personnel did not have adequate competence, infrastructure and work environment had not been identified as part of the standard, standard processes as well as interaction flow of security management processes and other processes are not clearly defined, and not to mention that the company's information security training programs are still limited to basic things.

2. The DSS05 (Manage Security Services) process discusses the protection of company information to keep the information security risks at an acceptable level based on company policy. Capability measurement in this process only reached level 1 with level 1 and 2 scores of 85.03% (fully achieved) and 79.28% (largely achieved). In this process, it was discovered that there is no procedure for the disposal of unused output devices, lack of awareness training in regards to the physical security of devices, inadequate quality of physical perimeter boundaries on servers, no device locking mechanism, no clear definition of information security service's management authority, and the unavailability of resources and information for the management of security services. These are shortcomings that still need to be addressed before this process can go to the next level.

3. From the results of interviews with company IT managers, several findings were obtained; namely, there is no acceptable risk level threshold set by the company, there is no special division that manages information security, there is no mission statement related to information security, information security approach which still relies on the old paradigm that prioritizes absolute compliance, and members of the IT team who feel there is no need to develop information security standards and guidelines.

The information obtained during the interview and filling out the questionnaires shows connections between several aspects of the company's information security approach or culture with some of the findings of the questionnaire results. Among them is the absence of a company mission statement related to information security. This absence could result in information security management's direction becoming unclear as one of the mission statement functions is to provide direction to achieve organizational goals. One example can be seen from the company's information security training program, which is less developed in both APO13 and DSS05 domains.

In addition, the company's general approach to information security that prioritizes compliance above other aspects on one hand is quite successful in ensuring that standards and guidelines are always followed in managing information security. However, on the other hand it also causes little room to be given to explore other methods that might be better than the current method.

At the level 1 capability, the drawbacks of this approach have no significant impact on the ratings of the two domains. It was only on testing at a higher maturity level that this weakness could be seen in the rating. One example is one of the findings in the APO13 domain where infrastructure and work environment have not been incorporated into process standards by the IT department. It is possible that the IT department has already realized the need to incorporate these two aspects into the standard process but failed to do so because there is a possibility that they will be penalized by the company for making changes to information security standards and guidelines. The same thing may also happen in the DSS5 process in the level 2 activities of identifying resources and information to manage security services, resulting in a lack of supporting data to perform the activities.

Recommendation

From the findings of the audit and interviews conducted, several recommendations can be given to the IT department of PT XYZ as a solution to increase the level of information security capability to the desired level (level 4).

Table 8 Suggested Recommendations to Increase Capability Levels

APO13 Level 3	
1	Define process standards with guidelines that have been determined in information security management planning
2	Determine the sequence and interactions between security management processes
3	Identify the role of enterprise information systems in security management
4	Identify the infrastructure and work environment for security s management
5	Determine appropriate methods to monitor the effectiveness of enterprise information systems in security management planning

6	Determine the security services management process in accordance with the standards and needs
7	Determine and communicate the roles and responsibilities required in the management of information security
8	Determine competent individuals in carrying out the process based on appropriate education, experience, and training.
9	Resources and information necessary for performing the security services management must be made available, allocated and used.
10	The infrastructure and work environment used to carry out the information security management process must be well managed.
11	Appropriate data are collected and analysed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the security management, and to evaluate where continuous improvement of the security management can be made.
APO13 Level 4	
12	Determine relevant information needs to support the company's business objectives in IT security management
13	Determine the objectives of the measurement process based on the information needs of the IT security management process
14	Setting relevant quantitative objectives to support business objectives
15	Measures and frequency of measurement must be identified and defined in line with process measurement objectives and quantitative objectives for security management performance.
16	Monitor the extent of which IT security management process performance objectives are being met
17	Use measurement results to characterize the performance of IT security management processes
18	Determine the analysis and control techniques applied in the IT security management process
19	Define controls for process performance
20	Analyze measurement data to analyze special causes of variation
21	Take corrective action to address the special causes of variation
22	Determine the control according to the corrective action to be taken
DSS05 Level 2	
23	Identify the performance objectives of the IT framework management process
24	Planning and monitoring the performance of the IT framework management process
25	Adjust process performance to meet IT framework management plan
26	Define and communicate IT framework management responsibilities and authorities
27	Identify, provide, allocate and use resources and information in IT framework management planning
28	Conducting meetings with related parties to maintain good communication in IT framework management planning
29	Defining the work product requirements of the IT framework management process
30	Define the requirements for process documentation and control of the security services product
31	Identify, document and control IT security services products appropriately
32	Reviewing the security services product in accordance with planned arrangements and adjusted as necessary to meet requirements.
DSS05 Level 3	
33	Define process standards with guidelines that have been determined in information security services management planning
34	Determine the sequence and interactions between security services management processes
35	Identify the role of enterprise information systems in security services management
36	Identify the infrastructure and work environment of the security services management

37	Determine appropriate methods to monitor the effectiveness of enterprise information systems in security services management planning
38	Determine the security services management process in accordance with the standards and needs
39	Determine and communicate the roles and responsibilities required in the management of information security services
40	Determine and select competent individuals in carrying out the process based on appropriate education, experience, and training.
41	Resources and information necessary for performing the security services management must be made available, allocated and used.
42	The infrastructure and work environment used to carry out the information security services management process must be well managed.
43	Relevant data must be collected and analyzed to understand the behavior of security services, demonstrate the suitability and effectiveness of the security services management, and evaluate where continuous improvement of the security services processes can be made.
DSS05 Level 4	
44	Determine relevant information needs to support the company's business objectives in IT security services management
45	Determine the objectives of the measurement process based on the information needs of the IT security services management process
46	Setting relevant quantitative objectives to support business objectives
47	Measures and frequency of measurement must be identified and defined in line with process measurement objectives and quantitative objectives for security services management performance.
48	Monitor the extent to which IT security services management process performance objectives are being met
49	Use measurement results to characterize the performance of IT security services management processes
50	Determine the analysis and control techniques applied in the IT security services management processes
51	Define controls for process performance of IT security services
52	Analyze measurement data to analyze special causes of variation
53	Take corrective action to address the special causes of variation.

All recommendations issued are accepted by the company's IT department. The company set a deadline for implementing the recommendations from July 2021 to January 2022 in order to increase the capability level of information security to level 4.

V. CONCLUSION

Based on the research conducted at the IT department of PT XYZ with the COBIT 5 framework, the following conclusions can be drawn.

1. Neither of the two processes that became the focus of this study reached the level of capability expected by the IT department, with APO13 reaching level 2 while DSS05 only reached level 1. As majority of the sub-process activities in the selected processes have already been performed by the company, recommendations for increasing the capability level of both processes can be issued.

2. There are few relationships between some aspects of the company's information security approach or culture with some of the questionnaires results in both domains that are the focus of research, especially on APO13.02 (Information security risk management plan) and DSS05.05 (Physical access management) to IT assets). This effect can be seen from the lack of

development of the training programs on the company's information security aspects and the lack of attention paid to the infrastructure and work environment factors, as well as the process of identifying resources and information in the management of security services which are either directly or indirectly influenced by the company's information security culture that stifles innovation.

3. The recommendations submitted to the IT department of PT XYZ are issued based on the COBIT 5 processes evaluated in this study, namely APO13 and DSS05. The purpose of these recommendations is to be used as references or guides for the IT department in making improvements to the company's information security governance to achieve the desired level of information security capability in the upcoming audit.

REFERENCES

Arnason, S. T., & Willett, K. D. (2007). How to achieve 27001 certification: An example of applied compliance management. In *How to Achieve 27001 Certification: An Example of Applied Compliance Management*.

Dahlberg, T., Kivijärvi, H., & Saarinen, T. (2016). IT investment consistency and other factors influencing the success of IT performance. In *Strategic IT Governance and Alignment in Business Settings*. https://doi.org/10.4018/978-1-5225-0861-8.ch007

ISACA. (2012). COBIT5 Framework. In *Trust And Partnership*.

Pasquini, A., & Galiè, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. *Fikusz 13*, 67–76. http://kgk.uni-obuda.hu/fikusz

Tan, T. C. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *IFIP Advances in Information and Communication Technology*, *330*, 55–67. https://doi.org/10.1007/978-3-642-15257-3_6

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. *Proceedings of ISSA 2006*.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers and Security*, *24*(2), 99–104. https://doi.org/10.1016/j.cose.2005.02.002

Wella, W., & Tampi, A. (2017). Tingkat Kapabilitas Tata Kelola TI Pusat Teknologi Informasi dan Komunikasi Universitas Sam Ratulangi. *Jurnal ULTIMA InfoSys*, *8*(1), 9–14. https://doi.org/10.31937/si.v8i1.550

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security*, *88*. https://doi.org/10.1016/j.cose.2019.101640