INFORMATION SYSTEM SECURITY EVALUATION USING COBIT 5 FRAMEWORK

Lilis Griffith Toyner [1)], **Sfenrianto** [2)]
[1,2)] *Master of Information Systems Management Bina Nusantara University*
email : lilis.toyner@binus.ac.id[1)], sfenrianto@binus.ac.id[2)]

Abstraksi

Sebagian besar perusahaan menggunakan teknologi informasi untuk mengembangkan bisnisnya. Namun ada hal yang perlu diperhatikan, beberapa ancaman bisa saja terjadi dan menimbulkan kerugian. Peristiwa yang tidak diinginkan menghambat pencapaian tujuan dan strategi perusahaan. PT XYZ percaya bahwa keamanan informasi penting dalam semua aktivitas bisnis. Ancaman yang dapat membahayakan keamanan informasi. Informasi merupakan aset penting bagi PT XYZ. Oleh karena itu, perlu dilakukan evaluasi atau pengukuran terhadap pengendalian dan aktivitas yang telah dilaksanakan untuk melindungi data/informasi perusahaan. Evaluasi dalam makalah ini menggunakan Framework COBIT 5 yang berfokus pada Manage Security Services (DSS05).

Kata Kunci:
Evaluasi, COBIT 5, Kelola Layanan Keamanan, Tingkat Kapabilitas.

Abstract

Most companies use information technology to develop their business. But there are things to note, some threats can occur and cause losses. Undesirable events hinder the achievement of company goals and strategies. PT XYZ believes that information security is important in all business activities. Threats that can compromise information security. Information is an important asset for PT XYZ. Therefore, it is necessary to evaluate or measure the controls and activities that have been implemented to protect company data/information. Evaluation in this paper uses the COBIT 5 Framework which focuses on Manage Security Services (DSS05).

Keywords:
Evaluation, COBIT 5, Manage Security Services, Capability Level

Introduction

Information technology is a combination of hardware and software used by a company to achieve the company's business goals [1]. The implementation of the applied information system must be aligned with the company's business strategy. Thus, the need for good and structured information system security governance starts from the process of planning, developing, implementing, and evaluating the health industry [2]. PT XYZ was founded in 1973 in Solo, has more than 250 branches located in major cities. PT XYZ is a clinic that has implemented a fairly sophisticated information and technology system, ranging from service support systems to the company's operational support systems. To add value to the effectiveness and efficiency of the company must be able to manage a good information system [4]. Efficient information system governance that is in line with business needs and supported by strong business partnerships is very important to achieve company goals [5]. PT XYZ maintains its mission by providing the best inspection results and wholehearted service that is carried out optimally by PT XYZ. The transformation of the digitalization system is carried out by PT XYZ to produce product innovations and be able to develop business [6].

Today there are many system security incidents that plague several companies and businesses. Information systems are important assets companies must be able to protect these assets from various threats [7]. Integrated information systems with good information system arrangements can affect the company's overall performance [8]. Factors that can affect the high trust of customers in companies with a good reputation or image [9].

In Q3 2022, there were 4 cases of data leakage in Indonesia. 17 million PLN customer data leaks including customer ID, consumer name, consumer address, electricity consumption, and type of energy on August 19, 2022. On August 21, 2022, Indihome experienced 26 data leaks. Displays domain information, platform, URL, browser, Google keywords, IP, screen resolution, user location, email, gender, name, and NIK of Indihome customers. The leakage of 1.3 billion cellular user card numbers in Indonesia along with the Population Identification Number (NIK) and using cell phone numbers occurred on September 1, 2022. Furthermore, there was a leak of 105 million Indonesian population data from Permanent Voters Registered in the General Election of September 6, 2022. The data contains information on full name, identification number (NIK), family card number (KK No.), complete address, place, date of birth, age, and gender for information on disability. Leaked data is traded on the Infringed Forum. Is a web page that provides discussion services with online forums with certain

Marketplace topics such as Leaks Market carried out by hackers [11].

Data leakage incidents can harm the organization or company [12]. The government issued regulations on the protection of personal data. Regulates how to protect someone's data from the government's information system/technology side, and legal arrangements if there is a violation committed related to personal data. Implementation of a good security system to protect customer data as data owners and data processors [13].

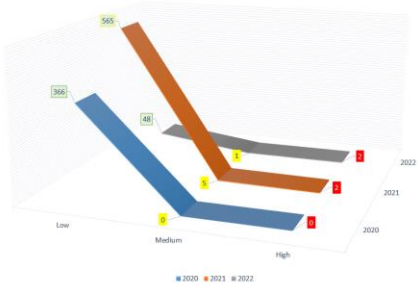

Figure 1. The threat of Jan 2020 - Juni 2022
(Sumber: Company data).

The occurrence of data leakage incidents experienced by several agencies that have been mentioned above and the inauguration of the regulation on the protection of personal virgins. PT XYZ is more proactive in protecting the company's information system and customer data. Currently, the company has implemented several information security tools with monitoring carried out by the 7x24 SOC team. Looking at the monitoring results, starting from the beginning of 2020 to June 2022. There are so many attacks that try to get into the company's information system. The number of attacks that attacked PT XYZ's information system, namely 366 attacks that occurred in 2020, 572 attacks in 2021, and 51 attacks that occurred from January to June 2022. From the list of attacks, none of them resulted in an attack on the security of PT XYZ's information system.

To protect company information assets from cyber-attacks and protect stakeholders' privacy, especially customers. Related to the consumer perspective that will affect the company's reputation [14]. This paper evaluates the DSS05 focus domain of the COBIT 5 framework.

Literature Review

The researcher conducted a case study of one of the journals that had the same background, as follows:

Table 1. Other Research.

Title	Application of the Cobit 5 Framework for Auditing Information Security Governance at the Regional Office of the Ministry of Religion in Lampung Province
Author	Dedi Darwis, Nur Yulianti Solehah, and Dartono
Year of made	2021
Overview	Have not been able to implement information security governance properly and optimally. Checked with domains EDM03 (Ensuring Risk Optimization), APO01(Managing IT Management Framework), APO07 (Managing Human Resources), APO12 (Managing Risk), BAI06 (Managing Change), DSS01 (Managing Operations), DSS02 (Managing Requests Services and Incidents), DSS03 (Managing Problems), DSS05 (Managing Security Services), MEA01 (Monitor, Evaluate and Assess Performance and Compliance), and MEA02 (Monitor, Evaluate and Assess Systems from Internal Control).
Result	Assessment with a Maturity level scale which is divided into 6 levels. The research phase begins with audit planning, documentation, field observation, problem finding, and validation which is carried out by direct observation based on the results of interviews and developing solutions from the results of risk identification with recommendations, the results of the research are compiled and made in the form of reports, and a process needs to be carried out monitoring of problems to be able to ensure that the results of the problems found can be resolved properly by the results of the recommendations. From the results of the assessment carried out by distributing questionnaires, it received a value of 3.3 which is at the Manage and Measurable maturity level, which means that the Ministry of Religion of Lampung Province has carried out the standard and formal data and information security processes but has not yet reached the optimized point in improving information security governance.

Evaluation

Evaluation is a systematic and continuous process to provide an assessment of the quality of something, based on certain criteria a reference to obtain and determine the best decision [15]. This stage is often called the assessment stage or audit stage, assessing current and future conditions to obtain quality information, based on certain criteria on a reference that can obtain and determine the best decisions on information security systems [16].

IT Governance

IT Governance has 5 main IT-related focuses; Information technology accountability, compliance, IT regulatory requirements, the aim of providing stakeholder satisfaction, risk management, and assessment of operational processes that have been carried out for business operations. That IT Governance is a specific reference for decision-making and accountability to support companies in using information technology in assisting their operational business processes [17].

The purpose of implementing information technology must be planned and have good governance so that it can provide maximum impact and results. With good IT governance, it can also provide convenience for business organizations or companies in conducting supervision and assessment of the implementation of existing technology [18]. Managed systematically controlled, effective, efficient, and required commitment from various parties including stakeholders and system users [19]. Information technology governance as internal control carried out by companies by utilizing IS/IT can help companies achieve organizational goals and can increase long-term value for stakeholders [20].

Information system security

Information system security is a process or method used to protect information and important elements/assets [21]. Information security is very important to protect the system from threats and detect fraud [22].

The application of information security has 3 important elements, namely the CIA Triad which consists of confidentiality, integrity, and availability.

COBIT 5.0

COBIT (Control Objectives for Information & Related Technology) is a governance guide issued by ISACA (Information System Audit Control Association), an international organization founded in the United States in 1967 which is an expert in information technology governance as a corporate reference that reflects the broad the scope of governance to manage information technology in the company. COBIT is also an internal control designed in the form of policies, procedures, and practices in the organizational structure that is formed to provide organizational achievements, things that are prevented or detected to be improved, and things that are not desirable [23]. Guidance balancing benefits with risks with the use of information technology resources to achieve organizational goals and optimize IT investment [23].

The following is an explanation of the domain in COBIT 5.0:

1. EDM (Evaluate, Direct, and Monitor)

A domain that describes activities or processes carried out to obtain value, and optimize risk and resources by determining what practices will be carried out for information technology management, including evaluation, direction, and monitoring processes.

2. APO (Align, Plan, and Organize)

A domain that provides strategic direction and tactics that can provide IT risk identification. The implementation of the strategic vision must be planned, communicated, and managed to maximize the achievement of the organization or company. From those generated in this domain process will be solutions or results for the BAI domain and support the DSS domain.

3. BAI (Build, Acquire and Implement)

To realize the IT solutions and strategies that have been identified, developed, and obtained by building, procuring, and implementing. In this domain, the process of system change and maintenance must be able to help ensure that solutions and strategic plans can continue to meet the needs of the organization or company.

4. DSS (Deliver, Service, and Support)

The domain consists of the process of sending, serving, and providing support to be able to support the goals of the organization or company.

5. MEA (Monitor, Evaluate, and Assess)

The domain deals with the actual delivery of processes and support services required for the process of monitoring, evaluating, and assessing a defined strategy or tactic.

Domain Focus - DSS05 (Manage Security Services)

The process of protecting company information or data to ensure and guarantee the security of information systems also ensures that information system risks can be accepted by applicable security policies and is responsible for regulating user access rights in the company so that the use of user access rights is by the rules and authorities that have been established in the company. The process part of Manage Security Services [23]:

a) DSS05.01 Protect against malware.

Software to detect and protect the system from viruses/Malware. The following is also how to block software that is not allowed by the IT Team and is contained in the regulations/guidelines applied by the company.

b) DSS05.02 Manage network and connectivity security

Settings for user access and penetration test activities must be carried out periodically to ensure system security.

c) DSS05.03 Manage endpoint security

Endpoint security, to ensure that the computer will be locked automatically within a certain time, when not in use. And the setting is not allowed to use removable for data transfer.

d) DSS05.04 Manage user identity and logical access

Manage user access rights on the operating system related to privileges and review the access. To re-assure the ownership of the relevant user.

e) DSS05.05 Manage physical access to IT assets

Managing physical access, users who have the right to access server rooms and data centers, where the Infrastructure Team has full privileges. There is an access log, to print anyone who has entered the server room and server data. Logs must be stored in the database. The Infrastructure Team also has privileges over these logs. Logs cannot be updated and edited. To get accurate and real data.

f) DSS05.06 Manage sensitive documents and output devices.

Organize important documents in hardcopy or softcopy on how to collect and store these documents as a work reference used by the IT Team.

g) DSS05.07 Monitor the infrastructure for security-related events.

Manage the grouping of information security event characteristics and how to respond to system security events and procedures that have been defined and must be well documented.

RACI Chart

The matrix provided by COBIT 5.0 of all activities or authority in decision-making carried out in an organization or company against all people or roles for each process in understanding the rules and being responsible for the process is the key to the effectiveness of control [25].

The description of the RACI Chart is as follows:

1. Responsible, who has a role and is responsible for carrying out tasks and ensuring operational activities or processes can run well and are achieved.
2. Accountable, who is responsible for the success of the tasks and processes that have been carried out and has the authority to decide a case.
3. Consulted, people or departments needed to provide feedback, opinions, and input and contribute to an activity or process.
4. Informed, the person or department who needs to receive information related to the achievement of the process and results of action from a decision.

Assessment Process

Results of the questionnaire to obtain the percentage and Capability by using a Likert Scale calculation after recapitulating the questionnaire. The calculation that will be used to get the percentage is the total number of answers from the questionnaire on each question divided by the number of respondents who have filled out the questionnaire and then multiplied by 100 to get the percent result.

The achievement scale used for assessment according to the ISO/IEC 15504 standard, is as follows [23]:

a. N (Not achieved / not achieved)
   There is no or little evidence of the achievement of these process attributes (0-15%).
b. P (Partially achieved / partially achieved)
   There is some evidence of the approach and some of the achievement attributes of the process (15-50%).
c. L (Largely achieved / broadly achieved)
   There is evidence of a systematic approach, and significant achievement of the process, although there may still be insignificant weaknesses (50-85%).
d. F (Fully achieved)
   There is evidence of a systematic and comprehensive approach and full achievement of the attributes of the process. There are no weaknesses related to the attributes of the process (85-100%).

Methodology

This research is qualitative, calculating the maturity of the DSS05 subdomain (Manage Security Services). The following are the steps taken by the author to conduct an information system security assessment at PT XYZ.

The picture below is the stages of information system security evaluation activities at PT XYZ. Provide recommendations for the process needed. As a reference, the security system management process can be optimized.

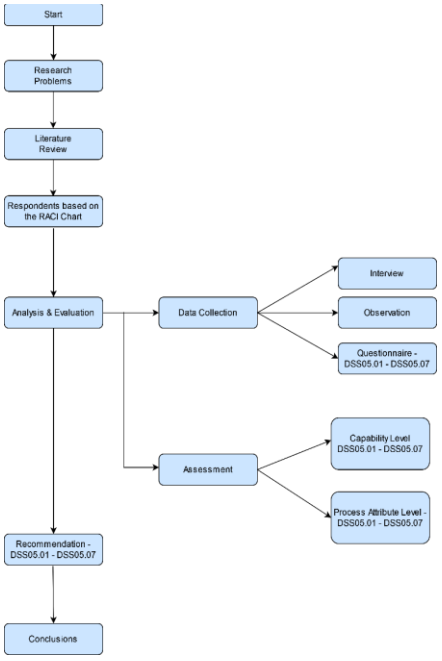

Figure 2. Research Methodology.

It starts with determining the respondents first. Respondents will fill out a questionnaire related to the Manage Security Services (DSS05) process. Obtaining respondents by mapping the roles and responsibilities of the organizational structure at PT XYZ with the 4 roles on the RACI Chart.

Data Collection

The author interviews, observations, and questionnaires. Interviews or questions and answers were conducted with the Manager of IT Enterprise Security & Assistant Vice President of IT Solutions. The interview process was conducted to obtain information that will be used as evaluation material in this study related to the Manage Security Service (DSS05) process at PT XYZ.

Capability Level

The researcher makes an assessment of the results of the questionnaire calculations and the achievement of the capability level, on the current and expected conditions. Using a Likert Scale for the calculation of quantitative data obtained from filling in the respondents. With the following provisions:

Table 2. Likert Scale Score.

Options	Score	Description
a	1	The process is not implemented or can not achieve the goal.
b	2	The process has been implemented but has not been able to achieve the goal.
c	3	The process has been implemented but is still in planning, monitoring, and assessment/evaluation.
d	4	The process has been implemented and is expected to be able to achieve the objectives
e	5	The process has been operated with limitations and can achieve the goal.
f	6	Processes are continuously improved to meet the organization's business objectives.

From results of the questionnaires conducted by the respondents, the calculation of the achievement of the level of capability, the current conditions, and the expected conditions is carried out. Using the maturity level used as a measure of the maturity

level of IT governance. By using the following calculation formula:

$$X = \frac{\sum Xi}{n} \times 100\%$$

X = Average of the answer to the type of answer choice
∑ Xi = Accumulated answer to the type of answer choice
n = The value should be following the number of respondents

Then the value of the company's capability to manage information system security can be obtained. Then the level of capability obtained for current conditions and compared with future conditions, it is possible to find out the existing process gaps at PT XYZ. Which is obtained from the expected value minus the value of the current ability.

The following describes the level of Process Capability [23]:

a. Incomplete Process: The process is not implemented or fails to achieve its process goals. At this level, there is little or no evidence of any achievement of the process goals.
b. Performed Process: The process is implemented to achieve its business goals.
c. Managed Process: Implemented processes are managed (planned, monitored, and adjusted) and their results are defined and controlled
d. Established Process: Process is documented and communicated (for organizational efficiency)
e. Predictable Process: The process is monitored, measured, and predicted to achieve results.
f. Optimizing Process: Processes are predicted and then improved to meet relevant business objectives and future goals.

Process Attribute Level

Recapitulation of the totality of processes contained in the specified domain. Check Generic Work Product (GWP) sequentially in each domain. Checking whether the existing documents are by the standards that must be met at each level in a percentage count. The summary of the template is as follows;

Table 3. Capability Level Achievement Template.

Domain	Penilaian	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
			PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
DSS05	Capability Level										
	Rating dalam %										

Perform validation at the previous stage and ensure that the process has met the documentation requirements that must be met by each level. The results of the assessment with the status of F (Fully achieved), can continue to the next level. Fulfillment the template with the ISO/IEC 15504 standard.

Results and Discussion

The results of interviews in this study with the resource person IT Enterprise Security Manager, as the person in charge of the Manage Security Service process at PT XYZ, can run well. The following is the information on the company's implementation based on the subdomains in the DSS05 domain:

a. DSS05.01 Protect against malware
   Enterprise to protect IT assets from malware has implemented antivirus software for clients and servers. As well as a security system that functions as a filter system for a network or server which is commonly referred to as a firewall. The company also has Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) software which functions to detect suspicious activity.
   PT XYZ also has standardized software that can be installed on the client's PC. And only certain accounts can carry out the software installation process. The company sets a limit on sending emails per day and submission. The company also regularly provides awareness regarding Malicious Software.
b. DSS05.02 Manage network and connectivity security
   PT XYZ implements the company's internal network access authentication. The company imposes restrictions on internal network access. Only computers that have joined the domain can access the internal network. Implement company-owned laptop encryption. Implement configuration on security protocols that access the internal network to regulate the entry and exit of data from the system.
   The company also routinely performs penetration testing on core and critical applications as well as samples for several types of network architectures. The results of these tests carried out corrective actions.
c. DSS05.03 Manage endpoint security
   The company applies encryption to the core database. Use of VPNs for remote access and certain VPNs for third parties. There are CCTV, fire detectors, and generators for the server room. The existence of a Mobile Device Management policy to control company devices that contain company data remotely. There is a filtering of network protocols from external to internal connections, and vice versa.
d. DSS05.04 Manage user identity and logical access
   PT XYZ has implemented special access management following its roles and functions, and regularly reviews the suitability of access for core applications, VPN access, and domain accounts that exist in PT XYZ's information system. There is an approval process for new access requests, changes, and disabled access (if not reused). The account naming for application access is unique. PT XYZ has an audit trail that is only limited to ERP applications.
e. DSS05.05 Manage physical access to IT assets
   The company already has arrangements for physical assets, door access with fingerprint

access to enter sensitive spaces. Taking care of guests by exchanging the Resident Identity Card owned by the guest with PT XYZ's Guest ID. The Human Capital section routinely conducts socialization for the use of ID Cards. Currently, PT XYZ has CCTV only in sensitive parts, namely the server room and door access with fingerprints.

f. DSS05.06 Manage sensitive documents and output devices
PT XYZ has regulations regarding the acceptance, use, and destruction of forms and output devices. Already have rules related to physical document classification and very good implementation, but not yet been implemented for documents in the form of softcopy. PT XYZ performs routine backups to several storages, to prevent unwanted things from happening.

g. DSS05.07 Monitor the infrastructure for security-related events
PT XYZ implements an Event Management Information System, monitored 7x24, and regularly reviewed events that occur. The monitoring team always follows up on events that are harmful to the information system. Perform risk identification according to the level of risk. PT XYZ already has rules or policies for the management of information security incidents along with their handling and mitigation.

RACI Chart

Adjustment of job titles with RACI diagrams in determining respondents who explain roles in the process of measuring capability scale. DSS05 (Manage Service Security) domain to obtain data or information, as follows:

Table 4. RACI of DSS05 (Manage Security Services).

No.	Component	Functional Structures - COBIT 5	Functional Structure of PT XYZ
1.	Informed	Business Process Owners	IT Security Engineering & Asset Security Supervisor
2.	Consulted	Head Development	IT Development Manager
3.	Responsible	Head IT Operations	IT Infrastructure Assistant Manager
4.	Responsible	Information Security Manager	IT Enterprise Security Manager

Based on the table above, there are 2 components to the role of someone in charge. First, the Information Security Manager in the organizational structure position at PT XYZ with the position of IT Enterprise Security Manager. In PT XYZ's organizational structure, the IT Enterprise Security Manager has the same responsibilities as the Information Security Manager, which is responsible for managing, designing, monitoring, and/or assessing the security of the organization's information systems. Second, the Head of IT Operations in the organizational structure position at PT XYZ with the position of IT Infrastructure Assistant Manager. Because the IT Infrastructure Assistant Manager has the same responsibilities as the Head of IT Operations. Responsible for PT XYZ's IT operational infrastructure.

Head of Development because they have the same responsibility for components and roles in the RACI Chart, namely as a party that has authority over IT processes and solution development processes and is responsible for information security. The IT Security Engineering & Asset Security Supervisor as an Informed party has the same role as the Business Process Owner in the RACI Chart, namely the person responsible for realizing its goals, encouraging process improvements, and approving process changes**.**

Capability Level

The questionnaire from the 4 respondents above has been adjusted to activities in the Manage Security Service process subdomain. The percentage of answers from each domain (as is):

Table 5. Current capability level of DSS05 (Manage Security Services).

No	Management Practice	Capability Score	Capability Status
1	DSS05.01 (Protect against malware)	3,53	Predictable Process
2	DSS05.02 (Manage network and connectivity security)	3,58	Predictable Process
3	DSS05.03 (Manage endpoint security)	3,85	Predictable Process
4	DSS05.04 (Manage user identity and logical access)	3,60	Predictable Process
5	DSS05.05 (Manage physical access to IT assets)	3,60	Predictable Process
6	DSS05.06 (Manage sensitive documents and output devices)	3,63	Predictable Process
7	DSS05.07 (Monitor the infrastructure for security-related events)	3,93	Predictable Process

All subdomains of the Manage Service Security (DSS05) domain have a Predictable Process state for the current state capability level. This means that all subdomains have been implemented, monitored, measured and predictive analysis for the future. The results of the fulfillment of the questionnaire also assessed the value of the gap. Gap Analysis is obtained from the expected ability level minus the current ability level. The following are the results of each subdomain process:

Table 6. Result Capability of DSS05 (Manage Security Services).

No	Aktivitas	Nilai Kapabilitas		Tingkat Kapabilitas		Gap
		As is	To be	As is	To be	
1	DSS05.01	52,78	61,11	3,53	4,56	1,03
2	DSS05.02	40,00	77,50	3,58	4,78	1,2
3	DSS05.03	47,50	80,00	3,85	4,80	0,95
4	DSS05.04	54,17	75,00	3,60	4,75	1,15
5	DSS05.05	35,42	83,33	3,60	4,83	1,23
6	DSS05.06	50,00	75,00	3,63	4,75	1,12
7	DSS05.07	57,14	75,00	3,93	4,75	0,82
Rata - rata		48,14	75,28	3,67	4,74	1,07

The average value obtained from the calculation on the DSS05 process, the current capability level with a value of 3.67 is included in

the maturity level measurement scale at level 4 (Predictable Process). This means that the control over the protection of information system security has been implemented, and is monitored and measured properly. In the DSS05 process, there is a gap of 1.07 from the comparison of current conditions to achieve Management expectations with a value of 4.74 at level 5 (Optimizing Process). Where the Management expects the Manage Security Service process to be predictable and then improved to meet the relevant business objectives and future goals.

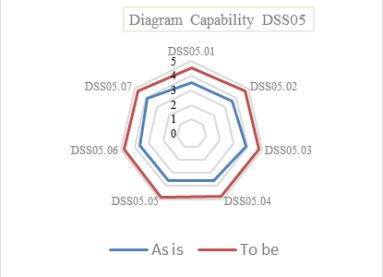

Figure 3. Gap Chart of Each Process Subdomain.

There are different gap conditions from Protecting against malware, managing network and connectivity security, managing endpoint security, managing user identity and logical access processes, managing physical access to IT assets, managing sensitive documents and output devices, and Monitoring infrastructure for security-related events.

Process Attribute Level

After obtaining the capability value, analyze each process attribute (PA) by giving an assessment rating. In the DSS05 process, there are seven Base Practices (BP) with Generic Work Product (GWP) documents. Then score sequentially from level PA 1.1, PA 2.1, and so on. If the assessment at the first level gets a score of 85% and above. You can take the assessment to the next level. The following is an assessment of the PA capability level 1.1.;

Table 7. Process Attribute 1.1 Process Performance - DSS05.

Base Practise	Output (Work Products)	Yes / No	Evidence
DSS05.01 (Protect against malware)	Malicious software prevention policy	Y	Information Security Management System Policy, Malware Protection Guidelines
	Evaluations of potential threats	Y	Threat Monitoring Report, Monthly report IT Enterprise Security.
DSS05.02 (Manage network and connectivity security)	Connectivity security policy	Y	Information Security Management System Policy
	Results of penetration tests	Y	Report Pentest
DSS05.03 (Manage endpoint security)	Security policies for endpoint devices	Y	Information Security Management System Policy
DSS05.04 (Manage user identity and logical access)	Approved user access rights	Y	Information Security Management System Policy, Core Application Access Rights Guidelines
	Results of reviews of user accounts and privileges	Y	User Access Review Report
DSS05.05 (Manage physical access to IT assets)	Approved access requests	Y	Information Security Management System Policy, Guidelines for Determining & Controlling Access to Computers/Information Systems
	Access logs	Y	Information Security Management System Policy, Logging & Monitoring Guidelines
DSS05.06 (Manage sensitive documents and output devices)	Inventory of sensitive documents and devices	Y	Information Security Management System Policy, Information Security Level Classification Guidelines
	Access privileges	Y	Information Security Management System Policy
DSS05.07 (Monitor the infrastructure for security-related events)	Security event logs	Y	Information Security Incident Management Guidelines
	Security incident characteristics	N	-
	Security incident tickets	Y	Information Security Incident Management Guidelines

Table 7 describes the base practices of the DSS05 (Manage Security Service) process and the supporting documents. Based on the mapping results with the output document produced by the DSS05 (Manage Security Service) process at PA level 1.1. (Performed Process). The results of interviews and observations, along with the results of the mapping;

a. DSS05.01 - Already has Malicious software prevention policy, Information Security Management System Policy document, and Malware Protection Guidelines. Explain the steps and actions taken by the company to prevent Malware and monitor the results of the prevention. Work Procuk evaluation of threats that have the potential for incidents, the company always evaluates the results of monitoring regularly. The result of the evaluation is a summary of incident monitoring reports managed by the Security Operations Center Team.
b. DSS05.02 - The company already has a connectivity security policy and an Information Security Management System Policy document that regulates company network security. Starting from maintaining internal devices that can connect to the internal network and verifying internal accounts with AD accounts to connect to the internal network. The company also conducts penetration tests for the head office network.

c. DSS05.03 - Currently, the company has implemented security management of mobile devices, company-owned devices, and employees' devices. Settings to secure data and information contained on the device remotely. By implementing the Data Leak Protection function, which can wipe data remotely when the device is lost. It is contained in the Information Security Management System Policy and details it is regulated in the Guidelines for the Management and Use of Personal Devices for employee-owned devices.
d. DSS05.04 - The process of managing accounts and logical access, the company already has a user matrix for access that has been approved in the form of a fixed reference. As well as conducting a review process for core application access users. Documents produced by the company against this process, Information Security Management System Policy documents, Core Application Access Rights Guidelines, and User Access Review Reports.
e. DSS05.05 - The company has implemented an approval process flow for access requests. The company makes account submissions for all applications through the Helpdesk system. Approval and follow-up of account requests can also be seen from the Helpdesk ticket. Enterprise has access logging for enterprise core applications. Both processes are contained in the Information Security Management System Policy document, Guidelines for Determining & Controlling Access to Computers/Information Systems, and Logging & Monitoring Guidelines.
f. DSS05.06 - The company already has policies in place to manage sensitive documents and output devices. It is regulated in the Information Security Management System Policy and Information Security Level Classification Guidelines. The company has regulated special/privileged access, as stated in the Information Security Management System Policy.
g. DSS05.07 - The company has logs of threats trying to enter PT XYZ's information system. Implement a ticketing process for security incidents, through the Helpdesk application to track problems and monitor the follow-up of these security incidents. However, the company does not have the characteristics of a security incident.

Based on the results of the mapping with the output document produced by the DSS05 (Manage Security Service) subdomain process at PA level 1.1. (Performed Process). PT XYZ's assessment has reached Fully Achieved status. By the criteria, mapping to the next level is carried out. As follows:

Table 8. Process Attribute 2.1 Performance Management - DSS05.

Generic Practices	Generic Work Product	Y / N	Evidence
Identify the objectives	Identification of information system security management objectives.	Y	IT Blueprint
Plan and monitor the performance	Planning and monitoring information system security performance.	Y	IT Blueprint
Adjust the performance	Adjustment of the information system security performance	Y	Information Security Incident Management Guidelines
Define responsibilities and authorities	Identify roles and responsibilities for managing information system security	Y	Information Security Incident Management Guidelines
Identify and make available	Resource identification	Y	Information Security Management System Policy
Manage the interface	Management of interface in business processes	N	-

The company already has documents or provisions to identify information system security management objectives, plan and monitor information system security performance in the form of an IT Blueprint. Adjustment of information system security performance, identification of roles and responsibilities, and identification of information security resources are in the Information Security Management System Policy and Information Security Incident Management Guidelines. However, the company does not yet have provisions for the management of the information system security interface in general.

Based on the results of the mapping with the output document produced by the DSS05 (Manage Security Service) process at the PA 2.1 level. (Performance Management). PT XYZ's assessment reached Largely Achieved status. Then the mapping is done again at PA 2.2 (Work Product Management) level. As follows:

Table 9. Process Attribute 2.2 Work Product Management-DSS05

Generic Practise	Generic Work Product	Y / N	Evidence
Define the requirements for the work products	Job requirements	Y	IT Blueprint
Define the requirements for documentation and control	IT-related services security documentation	Y	IT Enterprise Security Monthly Report
Identify, document and control	Management of work results related to information system security	Y	IT Blueprint
Review and adjust work products	Evaluation of the work related to information system security	Y	-

Based on the mapping results with the output document produced by the DSS05 (Manage Security Service) process at PA level 2.2. (Work Product Management). The company already has an IT Blueprint document, to define information system security requirements and manage the work results. The company has implemented the process of determining the needs and monitoring the security of the company's information systems in the form of the IT Enterprise Security Monthly Report. However, PT XYZ does not yet have a document related to the evaluation of work results related to information system security. Assessments at this level achieve Largely Achieved status. Attribute mapping is sufficient at this level.

Table 10. Result Capability Level Attribute of DSS05 (Manage Security Services).

DSS05	Level 1	Level 2		Level 3		Level 4		Level 5	
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.2	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria	F 92.68%	L 83,33%	L 75%						
Capability Level Achieved	1	2	2						

The results from the table above, at level 1 previously the achievement of level 2 was 92.68% with Fully Achieved status. Then it can continue the analysis to level 2, getting results of 83.3% on PA 2.1 Performance Management and 75% on PA 2.2 Work Product Management with Largely Achieved status. This means that an analysis is needed to improve the fulfillment of the criteria in the attribute process.

Discussions

Here, the researcher will describe based on the results of the distribution of questionnaires, interviews, and observations that result in the calculation of Capability Level and Gap Analysis. Recommendations to improve the quality of the Manage Security Service subdomain process at PT XYZ:

a) Subdomain DSS05.01 (Protect against malware).

The company has carried out the process of evaluating potential threats from the results of threat monitoring. However, there is no documentation of a mitigation plan to prevent the occurrence of threats that may potentially interfere with the security of PT XYZ's information system. This can help the company and the IT Enterprise Security team in the event of such a threat and can do so in a structured manner.

b) Subdomain DSS05.02 (Manage network and connectivity security).

The company routinely performs penetration testing with attempted attacks to find loopholes in applications, systems, and networks [26]. Meanwhile, the company's findings show that information security testing is only carried out on certain applications and not all network topologies that exist at PT XYZ. There may be still gaps in PT XYZ's information system. Because no attack testing experiments were carried out. And there is no reference to the duration of the completion of the penetration test and vulnerability assessment results. So the possibility of delays in handling in the event of an attack. The benefit to the company is that it can spot vulnerabilities immediately and can make fixes as quickly as possible.

In the Information Security System Policy, there is no detailed statement of what configuration should exist on the system. This can provide a standard reference for companies to configure connectivity settings for information systems when the responsible PIC is no longer working at PT XYZ.

c) Subdomain DSS05.03 (Manage endpoint security).

Endpoint security management, is currently still being carried out by their respective branches. While the management officers are in the regional office and head office. This causes gaps in the follow-up process, resulting in the possibility of information security incidents occurring. Companies must configure endpoint security so that they can be managed from the regional office or head office.

d) Sub domain DSS05.04 (Manage user identity and logical access).

The company does not yet have a reference and review of the access privileges used to access production servers. This is necessary to prevent unauthorized access. Ensure the activities are carried out by officers who already have the competence.

e) Subdomain DSS05.05 (Manage physical access to IT assets).

The company must have a record system for critical and customer-oriented applications. As well as logging for privileged access user activity logs. To be able to conduct searches that are information security incidents. There is no management of information security in the IT workspace, such as CCTV monitoring in sensitive areas. To be able to monitor visitors in and out of the IT workspace.

f) Subdomain DSS05.06 (Manage sensitive documents and output devices).

Currently managing server room access does have fingerprint access. However, recording server

room visitors are still done manually. It is recommended to implement system logging. To avoid unrecorded visitors entering and leaving the server room.

g) Subdomain DSS05.07 (Monitor the infrastructure for security-related events).

Based on the document mapping process. The company does not have a reference to the characteristics of a security incident, this is to make it easier to map the impact of a security incident on the business and determine the follow-up to the incident. In addition, the characteristics of information security risks are carried out to record the risks that may occur in the IT infrastructure in detail. Can define risks that may occur from internal sources such as network failure, hardware or software damage, data loss, viruses, or external risks such as natural disasters [26].

Conclusions

From the results of the assessment and analysis conducted in the research above. PT XYZ's information system security in the DSS05 (Manage Security Service) domain. Based on filling out the questionnaire, it can be concluded that the current value of PT XYZ's information system security process capability is 48.14. This means that the DSS05 (Manage Security Service) domain is at capability level 4. "Predictable process" which means the whole process has been implemented, monitored, and measured properly to produce predictive analysis. Meanwhile, the expected capability value is 75.28, which is at capability level 5. "Optimizing process" hopes that PT XYZ Process Manage Security Service can be more optimal and can predict to help achieve relevant business goals in the future. The gap owned by PT XYZ between the current capability value and the expected capability value is 1.07. PT XYZ must meet the requirements of the process capability attribute at Level 1.1 reaching the Fully Achieved criteria and at the PA level 2.1 and PA 2.2 levels each achieving the Largely Achieved criteria, which means some attributes have not been met. Such as document characteristics of security incidents and information system security interface management activities.

For further research, it is recommended to use the Align, Plan, and Organise (APO) or Evaluate, Direct, Monitor (EDM) domain owned by the COBIT 5 framework to carry out the evaluation and analysis process of overall information technology governance at PT XYZ. Or use additional reference frameworks such as ITIL, COSO, and others. So that it can provide various evaluation results and recommendations according to the added domain or framework.

References:

[1] Laudon, K., & Laudon, J. Management Information Systems Managing the Digital Firm: Thirteenth Edition. Edinburgh: Pearson Education: 2014.

[2] Setiyowati and Sri Siswanti. Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1. SATIN - Sains dan Teknologi Informasi, 2021.

[3] Resmiaty, Tetty. Aplikasi Sistem Informasi Dan Manajemen Laboratorium. Edisi ke-1. Jakarta. Indo.Kemkes.BPPSDM ; 2013.

[4] Hutari Maulida Kurnia1, Rahmi Nur Shofa2, Rianto3, "Jurnal Sistem Informasi Dan Tenologi". 2018. Sitech Vol 1, No: 1–6.

[5] Selig J., "Implementing Effective IT Governance and IT Management," Amersfoort: Van Haren Publishing, 2015.

[6] Susilo Y, Wijayanti E, Santoso S. PENERAPAN TEKNOLOGI DIGITAL PADA EKONOMI KREATIF PADA BISNIS MINUMAN BOBA. JEMSI [Internet]. 2021Mar.11 [cited 2022Oct.25];2(4):457-68. Available from:https://dinastirev.org/JEMSI/article/view/383

[7] Meilita Karenda Putri, Hakim AR. Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005:2018 dan NIST SP 800-30 Revisi 1. IK [Internet]. 2021 Nov. 17 [cited 2022 Oct. 25];15(3):134-41. Available from:https://infokripto.poltekssn.ac.id/index.php/infokripto/article/view/34

[8] Yi Wang, Si Shi, Saggi Nevo, Shaorui Li, and Yang Chen," The interaction effect of IT assets and IT management on firmperformance: A systems perspective," International Journal of Information Management, pp. 580-593, 2015.

[9] Magdalena G. International Conference on Entrepreneurship (IConEnt-2016). How Innovation could Improve the Performance and Productivity in Entrepreneurship?". Tanggerang: Business School Universitas Pelita Harapan; 2016.

[10] https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all.

[11] https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia?page=all

[12] Ichwani, A. dan Farida. A.D. "Pengukuran Tingkat Kapabilitas Manajemen Risiko Sistem Informasi Koperasi Syariah Menggunakan Framework Cobit 5." Jurnal Komputasi 8 (1): 1–14. 2020.https://doi.org/10.23960/komputasi.v8i1.2528.

[13] https://www.kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-pribadi/0/sorotan_media

[14] Kaplan, R.S. and David P. Norton, "The Balanced Scorecard: Measures that Drive Performance", Harvard Business Review, Massachusetts, 1992.
[15] Kim, S and Park, H. 2013. "Effects of various characteristics of social commerce (s-commerce) on consumers trust and trust performance". International Journal of Information Management. Vol. 33, pp.318–332
[16] DHS, "Cyber resilience review," Department Homeland University, Carnegie Mellon University, 2011.
[17] NCC, I. , Governance-Developing a successful governance strategy: A Best Practice Guide for decision makers in IT, John Wiley & Sons, Incorporated, 2005.
[18] Jurnal, H., Ali, R. M., & Agushinta, D, Jurnal Manajemen Informatika Evaluasi Tata Kelola Teknologi Informasi Pada Sistem Informasi Akademik Fakultas Teknik Universitas Khairun Ternate Menggunakan Framework COBIT 5, JUTEKINVol, 6(2), 2019.
[19] Swastika, I. P. A., Kom, M., & Putra, I. G. L. A. R, Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus, Penerbit Andi, (2016).
[20] Kusuma, Ricky Perdana, "Audit Teknologi Informasi Menggunakan Framework Cobit 5 Pada Domain Dss (Deliver,Service, and Support) (Studi Kasus : Konsultan Manajemen Pusat)," Jurnal Digit 9 (1): 97, https://doi.org/10.51920/jd.v9i1.137, 2020.
[21] Whitman, M.E., & Mattord, H.J, "Management of Information Security", Third Edition, Boston: Course Technology, 2010.
[22] Rosmiati, Riadi, I., Prayudi, Y., 2016. "A Maturity level framework for the measurement of information security performance", International Journal of Computer Applications, 141(8), 975–8887., 2016.
[23] ISACA, "COBIT 5.0: A Business Framework for the Governance and Management of Enterprise IT", USA: ISACA,2012
[24] ISACA. Self-assessment Guide: Using COBIT 5. Rolling Meadows: ISACA. 2013a.
[25] Stoneburner, G., Goguen, A. & Feringa, A., Risk Management Guide for Information Technology Systems. Gaithersburg: NIST Special Publication 800-30. 2002.