

MEASURE THE LEVEL CAPABILITY IT GOVERNANCE IN EFFECTIVENESS INTERNAL CONTROL FOR CYBERSECURITY USING THE COBIT 2019 IN ORGANIZATION: BANKING COMPANY

FRANCISKUS XAVERIUS ADRIAN¹, GUNAWAN WANG²

^{1,2}Information System Management Department, Binus Graduate Program – Master of Information system Management, Bina Nusantara University, Jakarta, Indonesia 11480.

Email: ¹franciskus.adrian@binus.ac.id, ²gwang@binus.edu

ABSTRACT

Nowadays, Companies must be able to use information technology effectively and efficiently in order to support company goals in the face of rapid technological advancements. Banking is one of the industries that must use IT to compete with banks and other financial technology firms. This research conducted to assess the level of capability IT Governance which is the method that the Author used for this research is COBIT 2019 Framework and NIST Cybersecurity for point of view about cybersecurity. The purpose of this research is to make readers know about Domain COBIT 2019 and Cybersecurity that can be used to optimize IT process and cyber security. In this study, qualitative data was gathered through interviews and observations, while quantitative data was gathered through questionnaires based on COBIT 2019 Framework controls. Furthermore, an analysis of the current and expected IT capability levels was performed, and recommendations were made to help the company achieve the expected capability level. Furthermore, the NIST cybersecurity framework is being used as an additional recommendation for companies in terms of cybersecurity and preventing cybersecurity attacks. The Selected COBIT Process in This Research are APO07 (Managed Human Resources), BAI07 (Managed IT Change Acceptance and Transitioning), BAI09 (Managed Assets), DSS01 (Managed Operations), DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), DSS05 (Managed Security Services.). The result of the capability levels of IT governance processes at company are at level 2 and level 3 and Based on the calculations that the Author had done, the score of capability rate in this IT function is 2.28 and the company has a target for future is to reach max level 5, that about having a Gap Score 2.72. As a result, a recommendation is made to improve these processes by referring to the best practices suggested by COBIT and in accordance with company needs. There are also some recommendations from the NIST Cybersecurity framework so the company is aware of data protection in an era where all systems are interconnected and integrated with one another. Making applications that provide LMS and Incident/IT Service Recording, as well as analysing trends that occur in the company for incidents/services, monitoring and reporting on a regular basis, and creating a policy, procedure, and team that handles cybersecurity within the company, are the main recommendations.

Keywords: *COBIT, Framework, Internal Control, Banking, Cybersecurity*

1. INTRODUCTION

Nowadays, technological developments are increasing rapidly, which is make information technology (IT) an inseparable part of every aspect of daily life as well as in an organization. The first time IT was widely used for the automation of the manual activity process. As time goes by, the complexity of IT processes makes it widely used in

applications. The functions of IT extend not only to use at the operational level but in strategic level, for analysing and forecasting data & trend data, so it can be used for decision making by leaders [1].

Due to a number of factors, including the requirement to successfully deploy IT resources, align IT strategy with business strategy, establish suitable internal controls, and avoid problems caused by software faults, industry needs a

comprehensive framework that covers all elements of IT administration. Frameworks offer best practices that businesses can use to implement different processes and procedures. [1]. The issues that exist are caused by information technology, which occasionally does not align with the organization's objectives and has little impact on improving company performance. Knowledge of the relative importance of various IT control and security processes is critical for company management responsible for IT governance and maintenance. As a result, for the best results, information technology in the workplace must be properly planned and managed, with good IT governance in place.

IT governance assists organizations /companies in monitoring and evaluating the use of information technology in order to improve business performance. The final reason for IT governance is the gap between expectations and reality. The manager always expects management to provide high-quality, on-time, and efficient IT solutions. Increased IT utilization provides business value returns and increases IT utilization to improve efficiency and productivity when risk management [2]. Aside from IT governance, cybersecurity governance is becoming increasingly important as technology becomes more interconnected and integrated with other systems or devices.

To ensure that companies are operating efficiently and profitably, they must first understand the term and scope of a cyber security system, which provides a higher level of security for both users and workers. One of the most important aspects of increasing employees' knowledge about day-to-day enhancement is training. On the other hand, IT governance is a must if a company wants to achieve a higher level of security, which can definitely help members of the board of directors and employees make the right decisions and align with the company's objectives.

A bank is a type of financial institution that lends and borrows money. Banks accept customer deposits in exchange for an annual interest payment. The majority of these deposits are then used by the bank to lend to other customers for a variety of loans. The authors conduct this research in a private banking company based on Sharia principles, with headquarters in Jakarta. The IT Division is in charge of managing the entire IT infrastructure within the organization, including IT assets, IT operations, IT system development, IT problem resolution, IT services for all stakeholders, and company security. In this case, the IT division plays an important role in the long-term viability of the organization's

business processes. This study's author restricts himself to seven domains in order to assess the maturity level of IT governance within a company. Because of the complexity of the business area, the seven domains were chosen because it required conformity between control models business process to process model.

Based on information that Author got from Director and head of IT Division the problem occur such as:

Table 1: Problem Scope

Problem Scope	Description
Operation	The process of overseeing IT operations has not yet undertaken because IT service supervision/monitoring has not been performed in accordance with procedures.
Asset	The accountability process for recording assets used for hardware/software is still insufficient and imprecise, the asset management process has not been carried out optimally.
IT Changes	The company's change process has not been carried out optimally because there are still unresolved application developments aimed at accelerating the company's core business processes.
Security	Inadequate hardening/monitoring of security processes results in a lack of security processes for data, devices, or networks.
Incident	Monitoring process that runs on complaints / IT incidents that occur is not currently optimal.
Human Resource	The majority of IT staff members have approached retirement age, and there is a knowledge transfer gap with new employees.

About research questions, the problem formulation of this research are:

1. What is the current level of IT governance capability in internal control at IT Division and what is the expected level of capability?
2. How to create IT governance recommendations based on current conditions in order to achieve the desired results at IT Division for internal control effectiveness.

The purpose and benefits of this research are

1. Analyse the current level of implementation of information technology capability and the expected level of information technology process capability.
2. Create an information technology governance plan that includes recommendations that must be implemented in order for the company to

achieve the expected level of information technology process capability.

3. The outcomes of an evaluation of the company's capability level for information technology governance are expected to help in the achievement of IT governance.
4. Provide guidelines and references for IT Division information technology governance process.

The author provides limits on the scope of this study:

1. This study was carried out at IT Division work unit.
2. The design recommendations are based on the level of capability gap between the current information technology process and the level of capability expected by IT Division.
3. An information systems governance design that refers to the 2019 COBIT standard and the NIST Framework for cybersecurity is used to assess the level of capability.

2. LITERATURE REVIEW

IT Governance is defined as a structure, process, and related mechanism for making IT-related decisions that organizations want to ensure that their investment in information technology facilitates strategic and tactical objectives [3]. IT governance is a component of overall organizational governance that involves stakeholders to ensure the sustainability of IT in institutions that can support the organization's goals and strategies. [4].

IT Governance should have concept 1) How IT can provide a value for the business 2) IT risk should be controlled and mitigated. IT Governance consist [5]:

- a) Business/IT Strategic Alignment
- b) Performance measurement in IT
- c) IT Value creation and delivery
- d) IT Risk Management and/or value preservation
- e) IT Resource Management

In other words, IT Governance is a process that ensure the effective and efficient use of IT in enabling an organization to achieve the goals. There are many IT Governance Framework that can be used for company with a variety of framework objectives [6], here are the example:

Table 2 the Comparison of It Governance Framework

Frame Work	Goals	Targeted Audiences
CMII	Provides guidance for process development	System application development leader
COSO	Improve organizational supervision by establishing integrated systems.	Leaders, management , users, and internal auditors
ISO	A set of processes for managing effective services.	Management level
TOGAF	Build enterprise architecture to provide strategies for achieving goals.	Division/person that are responsible for EA management
COBIT	Provides IT governance guidelines for business, IT risk, information security, and quality assurance are provided.	Internal organizations, practitioners, and consultants
NIST	Helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data	Internal Organization

The choice of IT governance is an important role because a suitable framework lead to a better result and help making a better decision system to the company needs

2.1 Cybersecurity

Cybersecurity is the practice of guarding against digital attacks on systems, networks, and programs. These cyberattacks are typically intended to gain access to, change, or destroy sensitive information; extort money from users via ransomware; or disrupt normal business processes. The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. An approach or series of steps taken to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and, if necessary, restoration of electronic information and communications systems and the information contained within them, in order to strengthen the confidentiality, integrity, and availability of these systems. Some examples include phishing, denial of service, zero-day

exploits, ransomware, and unauthorized access to information systems. Each of these types of breaches has the potential to have economic and reputational consequences for the affected company. Variety type of breach, economic costs might include those for detection, regulatory notification, customer redressal and compensation, litigation, loss of market value or investments, regulatory fines, extortion payments, and cost of lost business. There are six interdependent components can be used to assess the design and operating effectiveness of management's cybersecurity controls and governance. It can be seen in figure below.



Figure 1 Cybersecurity Component

- a) Cybersecurity Governance depends on:
 - A well-defined strategic goal with accountable stakeholders and roles and responsibilities
 - Line of reporting to ensure appropriate authority and objectivity
 - Knowledge of how to deploy security tools and enforce policy
 - Element of practices
 - Communication, metrics, reporting, and action tracking are all ongoing.
 - Incident management
 - Planning for business continuity in the event of a cyberattack
 - Visibility and participation of senior management and the board of directors
- b) Inventory of Information Assets depends on:
 - Inventory information
 - Device inventory, both authorized and unauthorized
 - Software inventory, both authorized and unauthorized
- c) Standard Security Configurations depends on:

- Endpoint device (mobile device, laptop, workstation) and server hardware and software security configuration
 - Secure network device configurations such as firewalls, routers, and switches
- d) Information Access Management depends consist of:
 - Restricted use of administrative powers
 - Account monitoring and management
 - Restriction on remote access control
 - Access is restricted based on the need to know.
 - e) Prompt Response and Remediation consist of:
 - Malware protection
 - Network port, protocol, and service limitations and controls
 - Application software protection
 - Wireless access management
 - Boundary defence
 - Pen testing, phishing, and red team exercises
 - Change event maintenance, monitoring, and analysis
 - Data security/prevention of data loss.
 - f) Ongoing Monitoring consist of:
 - Continuous implementation of the cybersecurity program based on raisin recommendations and timely completion
 - Analyse threat intelligence, identify gaps, and assess vulnerabilities
 - Performance should be measured and compared to industry benchmarks and peer organizations.
 - Determine the specific knowledge, skills, and abilities required to support the program.

2.2 COBIT Framework

A method to managing IT risk are prescribed in the "Control objective for information and related technology" (COBIT) framework which the policies, procedures, practices and organization structures designed to provide reasonable assurance that business objective can be achieved and undesired events will be prevented or detected and corrected. COBIT is a well-known industry IT governance framework to implement a set of best practices for management, control, and assurance of IT. COBIT was originally designed as a framework for conducting IT audit assignments, but it has since evolved into one of the major de facto frameworks for implementing and assessing the maturity of IT governance practices in organizations. [7].

COBIT Framework is divided by several IT control and security with purpose to achieve business goals and make an effective internal control. COBIT Framework use for guideline for managing IT organization which has a maturity model that can be used to asses to development of management process in organization, any others advantage can be used to understand and manage all significant risk of IT types.

COBIT was created in 1996 by the Information Systems Audit and Control Association (ISACA) to assist businesses in developing, organizing, and implementing information management and governance strategies. ISACA released its second version of COBIT in 1998, expanding the framework's application beyond the audit community. COBIT4 was released in 2005, and COBIT4.1 was released in 2007. These versions included more information on IT governance. ISACA released COBIT5 in 2012, and in 2013 it added new functions to COBIT5 that included more information for businesses about risk management and information management. COBIT 2019 has been designed to keep up with the most frequent updates, contribute to the development of more flexible and collaborative governance strategies, and adapt to new and changing technology, where COBIT 2019 updates organizations' frameworks by taking into account new security trends, technologies, and needs. [8].

2.3 NIST Cybersecurity

The National Institute of Standards and Technology Framework (NIST) framework was created to help organizations manage and reduce cybersecurity risk to critical infrastructure and industrial control systems. NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. The NIST Cybersecurity Framework can be seen in figure below

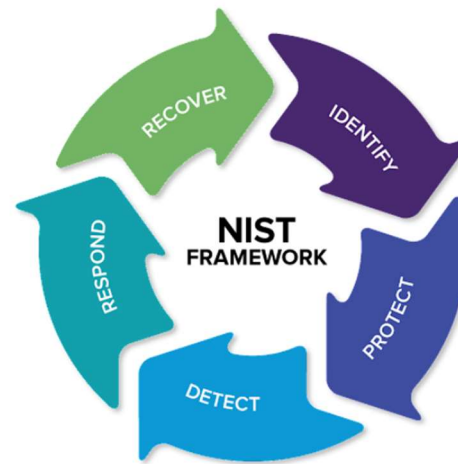


Figure 2 Key Attribute NIST Framework

Every Attribute have Category which determine support for each attribute. The support activity can be seen below

NIST CYBER SECURITY FRAMEWORK				
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training		Communications	
Governance	Data Security	Security Continuous Monitoring	Analysis	Improvements
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance	Detection Processes	Improvements	Communications
	Protective Technology			

Figure 3 NIST Cybersecurity Framework

- Identifying** is the process of developing an organizational understanding of cybersecurity risk to systems, assets, data, and capabilities.
- Protect** is defined as activities that develop and implement appropriate safeguards to ensure service delivery.
- Detection** is the process of determining the occurrence of a cybersecurity event.
- Responding** is the action taken in response to a detected cybersecurity event.
- Recover** activities include maintaining resilience plans and restoring capabilities or services that have been compromised as a result of a cybersecurity event.

3. RESEARCH METHOD

This research flow process as shown in figure below.

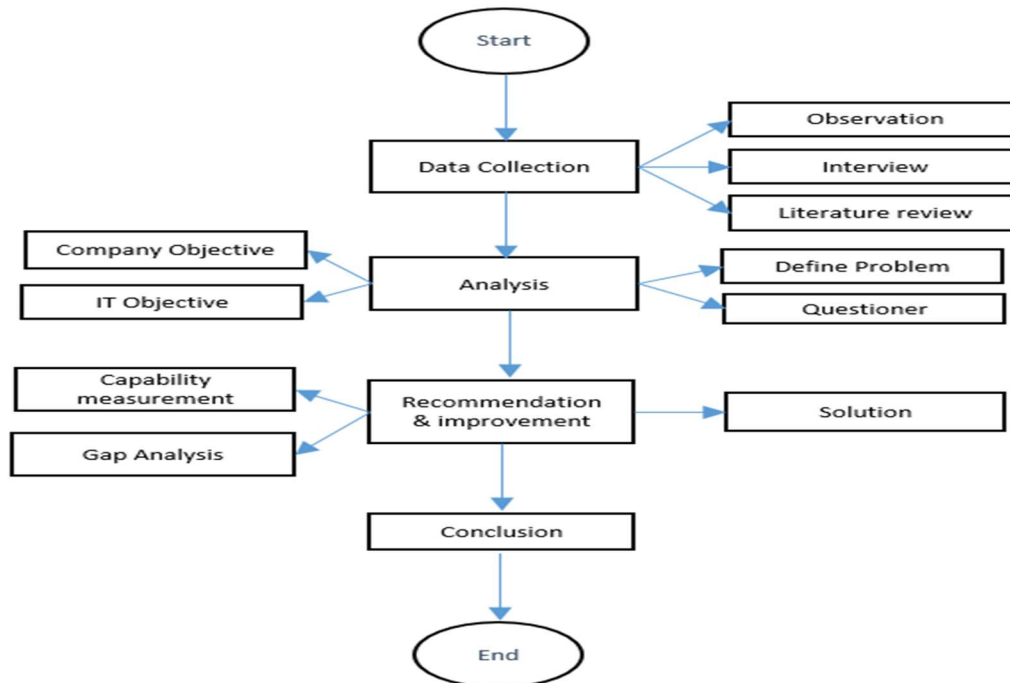


Figure 4 Flow Process

Data Collection are obtained by quantitative and qualitative. Quantitative method were carried out through interview with the Chief Information System and Head IT Division, document review such as internal control review report, and observation the current condition in IT division. Data collection phase is to knowing the initial behaviour of the IT Division to know what the problem can be solved by COBIT. Analysis phase is to mapping the company objective with COBIT framework and the result will be mapping to the IT objective within COBIT framework to define problem. The last part of analysis phases is questioner that adopt from COBIT framework which done by IT staff within company. From the result of questioner it can be define the current capability level which using ISO/IEC 33004 as follows [9]:

- Fully (F)—The capability level is achieved for more than 85 percent
- Largely (L)—The capability level is achieved between 50 percent and 85 percent
- Partially (P)—The capability level is achieved between 15 percent and 50 percent
- Not (N)—The capability level is achieved less than 15 percent

The next part is analysis the gap from the current level capability to expected reach capability. Furthermore, make the recommendation and

solution for the company to reach the expected capability level. This Research collect information from 5 department in IT Division that is:

- IT Operation Department
- IT Development Department
- IT Policy and Procedure Department
- IT Logistic Department
- Security Administrator

The total respondent for this research are 31 respondents which is full team in IT Division. Also the recommendation and the solution the company is both by COBIT and NIST framework which IT governance from the COBIT and NIST from cybersecurity perspective.

4. RESULT & DISCUSION

4.1 Mapping Company Objective to Enterprises Goals

To get understanding what focus should the research take and measure, first it's necessary to find relation company objective with the enterprise goals. The Author studies about the vision & mission within company and conduct an interview with the chief of information technology to get the strategic plan ahead. The information are mapped into the enterprise goals from cubit 2019 guideline.

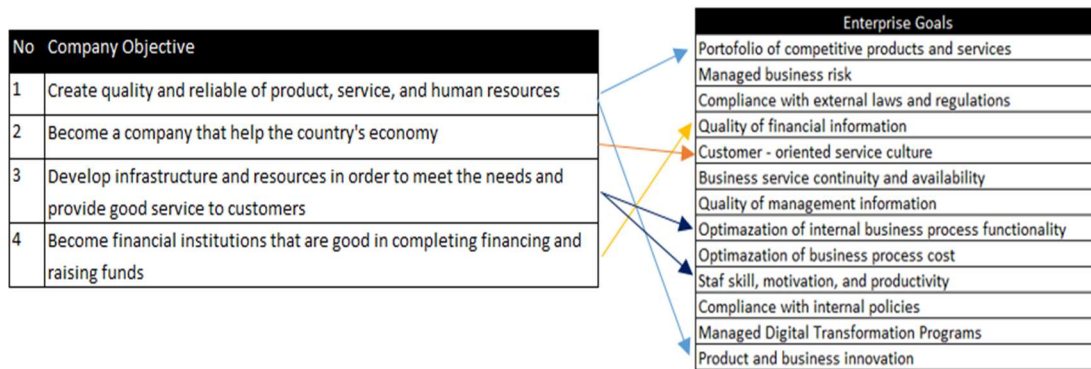


Figure 5 Mapping Organizational Goals to Enterprise Goal

4.2 Mapping Of Enterprise Related Goals To Alignment Goals

There are four enterprise goals that were mapped into alignment goals of COBIT 2019, the alignment goals base on interview and observation that related to IT management in company. The alignment goal chosen because they have primary scale. Overall the result get seven alignment goals that are the focus of company.

Table 3 Mapping Results From Enterprise Related Goals

Perspective	Code	Alignment Goals
Financial	AG02	Managed I&T-related risk
Financial	AG03	Realized benefits from IT enabled investments and services portfolio
Financial	AG04	Quality of technology related financial information
Customer	AG05	Delivery of I&T services in line with business requirements
Internal	AG06	Agility to turn business requirements into operational solutions
Internal	AG07	Security of information, processing infrastructure and applications, and privacy
Internal	AG08	Enabling and supporting business processes by integrating applications and technology
Learning and Growth	AG12	Competent and motivated staff with mutual understanding of technology and business
Learning and Growth	AG13	Knowledge, expertise and initiatives for business innovation

Based on COBIT 2019 these are criteria of each capability level in COBIT 2019. Here are the list capability in COBIT 2019 [10].

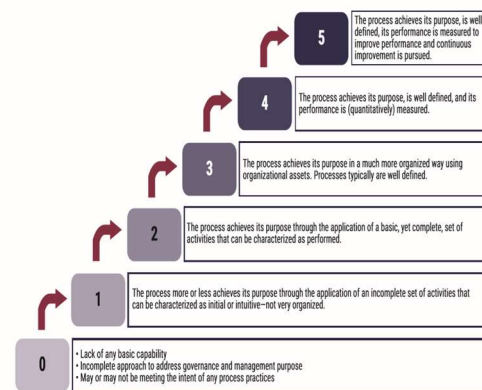


Figure 6 COBIT 2019 Capability Level

4.3 Mapping Alignment Goals To C 2019 Process

There are seven alignment goals that are mapped into the IT governance process base on COBIT 2019 guidelines. From the IT governance process are the related processes that will be evaluated for capabilities.

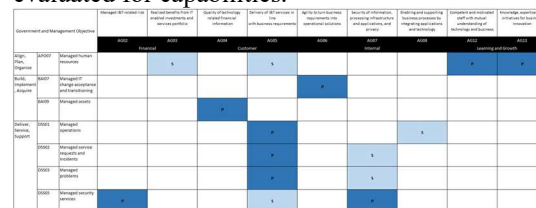


Figure 7 Mapping Results from Alignment Goals to COBIT Process

4.4 Define COBIT Process

According to the information obtained from interviews and document reviews, there are a number of issues within the IT Division for IT Governance at the company. These issues concern human resources (HR), IT assets, incidents and problems, and IT operation infrastructure. This issue was incorporated into the COBIT 2019

process. Seven selected processes were obtained as a result of the mapping, namely APO07 - Managed human resources, BAI07 - Managed IT change acceptance and transitioning Ensured Resource Optimization, BAI09 - Managed assets, DSS01-Managed operations, DSS02 - Managed service requests and Incidents, DSS03 - Managed problems, and DSS05 - Managed security services.

4.5 Current Capability

After obtaining the 2019 COBIT processes that were prioritized in the improvement process, an assessment of the capability level for each process is performed using COBIT 2019 standards. The percentage fulfilment level is determined for each process.

APO07 - Managed Human Resources						
Purpose	Optimize human resources capabilities to meet enterprise objectives					
Description	Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation and development of human resources					
Align, Plan, and Organize	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	100%	59.90			
Color Rating	F	F	L			

Figure 8 APO07 Capability Current Level

Based on APO07 evaluation, there are still weaknesses in the IT change process, which are as follows:

- There is a lack of knowledge sharing in the company, which makes it difficult for employees to read old applications/application programs.
- Employees believe that the skills or competencies required by the company have not improved.
- Due to the increasing demands of work, assessing the need for personnel in a team is still not optimal.

BAI07 - Managed IT Change Acceptance and Transitioning						
Purpose	Implement solutions safely and in line with the agreed expectations and outcomes					
Description	Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review					
Align, Plan, and Organize	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	100%	89.49	70.83		
Color Rating	F	F	F	L		

Figure 9 BAI07 Capability Current Level

Based on BAI07 evaluation, there are still weaknesses in the IT change process, which are as follows:

- There was no post-implementation evaluation of the process to determine whether it met the company's expectations or provided the expected benefits.
- Implementation of a new system that makes it difficult for users to use at times, necessitating the use of additional human resources to support these conditions.

BAI09 - Managed Assets						
Purpose	Account for all I&T assets and optimize the value provided by their us					
Description	Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements. Ensure that those assets that are critical to support service capability are reliable and available					
Build, Acquire, Implement	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	100%	72.59			
Color Rating	F	F	L			

Figure 10 BAI09 Capability Current Level

Based on evaluation in BAI09, there are still shortcomings in the IT changes process, which are as follows:

- Identification of the management of software licenses that are owned is not sufficient, so that the requirements and those installed are difficult to measure.
- Identify assets that are no longer used/not in accordance with their needs.
- There has not been any disposal of assets that are not used or needed.

DSS01 - Managed Operations						
Purpose	Deliver I&T operational product and service outcomes as planned					
Description	Coordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services. Include the execution of predefined standard operating procedures and the required monitoring activities.					
Deliver, Service, Support	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	100%	71.53			
Color Rating	F	F	L			

Figure 11 DSS01 Capability Current Level

Based on DSS01 evaluation, there are still weaknesses in the IT change process, which are as follows:

- Monitoring of the data center is insufficient because there are still unorganized and unsafe

room/environment conditions for the data center's devices.

- b) Not every data center has a rise floor and a large separation distance between the data and power cables.

DSS02 - Managed Service Requests and Incidents						
Purpose	Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents					
Description	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents					
Deliver, Service, Support	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100.00%	100.00%	72.96%			
Color Rating	F	F	F			

Figure 12 DSS02 Capability Current Level

Based on DSS02 evaluation, there are still weaknesses in the IT change process, which are as follows:

- There is no record of solutions for incidents that have been successfully handled, so the incident resolution process can be different, resulting in a non-standard process.
- There has been no escalation of incident resolution or resolution to the incident.
- There is no service level agreement for service requests for conditions such as hardening a new PC/laptop or replacing goods or network cables.
- There has been no trend analysis of incidents / requested services in order to find solutions or new service categories.

DSS03 - Managed Problems						
Objective	Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution					
Description	Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements					
Deliver, Service, Support	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	76%				
Color Rating	F	L				

Figure 13 DSS03 Capability Current Level

Based on DSS03 evaluation, there are still weaknesses in the IT change process, which are as follows:

- The problem identification process continues to rely on incident reports, but logs/audit trails have not been used as additional data sources for analysis in order to determine the root cause of problems that arise.

- The problem-solving process has not been documented, so the problem-solving process becomes inconsistent or difficult to repeat if a similar problem arises.
- There is no prioritization or classification of problems dealt with.

DSS05 - Managed Security Services						
Purpose	Minimize the business impact of operational information security vulnerabilities and incidents.					
Description	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring					
Deliver, Service, Support	Capability					
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating (%)	100%	100%	86.31	74.43		
Color Rating	F	F	F	L		

Figure 14 DSS05 Capability Current Level

Based on DSS05 evaluation, there are still weaknesses in the IT change process, which are as follows:

- There has been no evaluation of security information awareness of company staff to determine the level of security understanding that must be considered in the company.
- Not checking User IDs on a regular basis to ensure that all User IDs that are no longer required are removed from the application program to avoid unauthorized access.

Figure 12 shows the outcome of the domain process evaluation and represents the process average between levels 2 and 3.

Kapabilitas						
No	ID Proses	Proses Cobat yang dinilai	Level 0	Level 1	Level 2	Level 3
1	AP007	Pengelolaan Sumber Daya Manusia			59,90%	
2	BAI07	Pengelolaan Perubahan dan Transisi pada sistem IT			70,83	
3	BAI09	Pengelolaan Aset			72,59%	
4	DSS01	Pengelolaan Aktivitas Operasional IT			71,53%	
5	DSS02	Pengelolaan Incident dan Layanan IT			72,96%	
6	DSS03	Pengelolaan Masalah			48,49%	
7	DSS05	Pengelolaan Keamanan			74,43%	

Figure 15 Conclusion Process Current Capability Level

4.6 Gap Analysis

The goal of the IT Governance program is to prioritize increasing the level of IT maturity and control appropriate for each business unit. The process of analysis is carried out in order to increase the level of capability. The target level of IT maturity can be determined not only by looking at the organization's strategic plan, but also by looking at the internal environment or business observations.

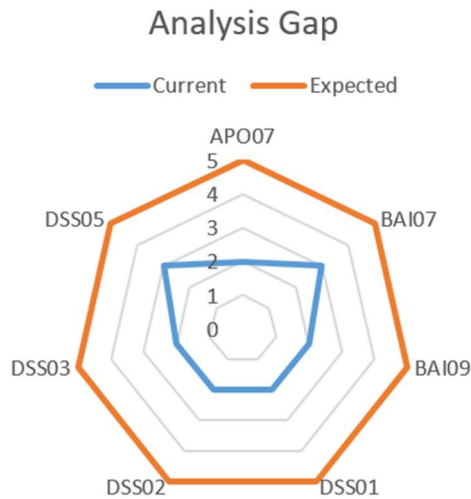


Figure 16 GAP

4.7 Recommendation And Improvement

According to the results of the capability level assessment, no process has met all of the expected targets. As a result, at the outset, it is necessary to implement recommendations for improvement in order for the company's seven priority processes to reach the expected capability level, which are as follows:

a) APO07 - managed human resources

The following recommendations are required to improve the APO07 process so that it can reach the expected level:

- 1) Developing a Learning Management System (LMS) with the following goals:
 - Documentation of training materials to allow employees to access them on their own time and to support the development of skills and competencies.
 - The knowledgebase contains learning resources related to company activities.
 - Employee abilities/skills evaluation
- 2) Conduct manpower planning and job evaluation to determine the number of personnel
- 3) Create an open feedback process and assess employees' abilities/competencies so that they can work to their strengths.

NIST Framework states that managing or training human resources in cybersecurity is necessary to safeguard enterprise systems and data.

The following is the suggestion for human resource activity in cybersecurity:

- 1) In order for employees to carry out their cybersecurity-related activities and responsibilities in accordance with pertinent policies, procedures, and agreements, the organization informs and educates its staff about cybersecurity. Privileged users and physical and cybersecurity workers, for example, are aware of their roles and obligations. Senior executives are also aware of their roles and responsibilities.
- 2) There are methods and procedures to manage the protection of information systems and assets, as well as security policies (that cover purpose, scope, roles, duties, management commitment, and coordination among organizational units).

b) BAI07 - managed it change acceptance and transitioning

The following recommendations are required to improve the BAI07 process so that it can reach the expected level:

- 1) Develop an application for a change management system that seeks to:
 - Document and record all information on changes made such as:
 - Change Date
 - Change PIC
 - Change Implementation
 - Change Summary
 - Category & Priority Change
 - Monitor projects/changes that have not been completed with targets.
- 2) A guide or manual is created on how to use the new system or application, and there is PIC support that assists after implementation.
- 3) Post-implementation monitoring is conducted to assess:
 - The expected outcome has been attained, and business demands have been satisfied.
 - Internal (audit, risk unit, security, and work units) and external (BI, OJK, or regulators) stakeholders' needs have been met.

IT Changes in cybersecurity concern the development and testing environment, which are separate from the production environment, according to the NIST Framework. It is critical to have a separate environment to ensure that information and data are managed in accordance with the organization's risk strategy to protect

information's confidentiality, integrity, and availability.

c) BAI09 - managed assets

The following recommendations are required to improve the BAI09 process so that it can reach the expected level:

- 1) There is an inventory management system that can perform the following functions:
 - Record incoming and outgoing goods assets, as well as the person in charge of the asset's PIC.
 - Streamline the process of verifying the existence of assets for stock taking/reconciliation.
- 2) There is a record of the use of software licenses (both existing and used) and how they are adjusted to the PKS with third parties.
- 3) Assets that are not in accordance with / in line with business needs are monitored and evaluated.
- 4) Periodic monitoring and maintenance of critical assets owned
- 5) There is monitoring of software/operating systems that have reached the end of their support life cycle.

In the NIST framework, asset management is important for identifying assets that a company has so that when a cybersecurity incident occurs, the company (personnel) knows what the impact is and what type of cyber security attack event occurred. These are the activities:

- 1) Hardware and software are identified, inventoried, and managed in accordance with their relative importance to organizational objectives and the risk strategy of the organization.
- 2) Data, time, logs, hardware, and software are prioritized according to their classification, criticality, and business function. The list of dependencies and critical functions is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- 3) All maintenance and repair tasks are completed and recorded.

d) DSS01 - managed operations

The following recommendations are required to improve the DSS01 process so that it can reach the expected level:

- 1) Monitoring the physical environment of the data centre room on a regular basis and cleaning

up the power/data cable lines so that they do not pile up and are not pulled out.

- 2) Preventive maintenance should be performed on equipment such as fire extinguishers, smoke detectors, and water leaks at the data centre/IT site.
- 3) Storing all system activities as an audit trail function that is used to monitor users who access the system.

In NIST, IT operation is the main core for IT cybersecurity, and it must be handled as follows:

- 1) When a cybersecurity incident occurs, the personnel in charge must be aware of the impact of all services, whether internal or external.
- 2) To detect potential cybersecurity events, the physical environment is monitored.
- 3) There are policies and procedures in place to protect physical and remote access, ensuring that all access has been approved and that any access that is no longer needed is deleted.
- 4) Backup activities for information/data are carried out, maintained, and tested. Backup data can be prioritized by the Dependencies and critical function for the delivery of critical services that were previously listed in the identification asset category.
- 5) There are mechanisms in place (for example, failsafe, load balancing, and hot swap) to meet resilience requirements in both normal and adverse situations.

e) DSS02 - managed service requests and incidents

The following recommendations are required to improve the DSS02 process so that it can reach the expected level:

- 1) Developed a system for recording incidents, IT services, and knowledge bases with the goal of:
 - Record incidents that occur, such as the time/summary incident/PIC of the reporter
 - Record the status of the incident being worked on s
 - There is a knowledge base storage related to completed incidents so that if the same conditions occur, it can make it easier for the PIC to resolve
 - Record the IT services requested by the requester as well as the service request approval.
 - Produce reports that stakeholders can see on the handling and progress of incidents/IT services handled and SLA met.

- 2) Create a standard and an escalation mechanism for incidents that do not resolve or exceed the SLA based on the priority/urgency incident classification.
- 3) A trend analysis of IT services/incidents is performed, which can be used to plan improvements or new categories of requested services.

In NIST cybersecurity, incident management plays a critical role in detection, with a focus on activities:

- 1) Every notification and alert is investigated and classified in accordance with its classification.
- 2) The event is being investigated and the incident's significance is recognized.
- 3) Event detection information is shared with authorized personnel or stakeholders.
- 4) During or after a cybersecurity incident, a recovery plan is implemented.

f) DSS03 - managed problems

The following recommendations are required to improve the DSS03 process so that it can reach the expected level:

- 1) Determine the mechanism and classification of the problematic incident so that it can be
- 2) Conducting an analysis of existing root cause problems and seeking permanent solutions to ensure that incidents do not reoccur.

Managing a cybersecurity problem entails conducting a deeper investigation into a cybersecurity event that has occurred in order to ensure that the company has a permanent solution in place to ensure that the same incident does not occur again. According to the NIST Framework, a company can engage in the following activities:

- 1) The impact of events is determined so that if a similar event occurs again, the incident response team will know what to do.
- 2) Cybersecurity forensic analysis is performed to determine what vulnerabilities exist in the company system that can be exploited by hackers.

g) DSS05 - managed security services.

The following recommendations are required to improve the DSS05 process so that it can reach the expected level:

- 1) The existence of SIEM (System Information and Event Monitoring), which records system security logs and can be used as an audit trail to determine who is accessing the system or data.

- 2) Perform hardware update (or patch). This is done to ensure that the equipment / system used is always up to date in order to avoid security flaws.
- 3) Non-used equipment, such as hard drives, is stored in a secure location and immediately destroyed to prevent data theft.
- 4) Determine the classification of documents and always encrypt documents in accordance with their classification.
- 5) User IDs with special abilities, such as (administrator / application admin) are keep it safe.

Managed Security Services is the most important role in cybersecurity because it serves as the company's cybersecurity guideline. The NIST Framework for Security consists of the following activities:

- 1) There are policies, procedures, and personnel in charge of cybersecurity. Roles and responsibilities in cybersecurity are coordinated and aligned with internal roles and external partners.
- 2) All critical asset have been identified and documented.
- 3) Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) in accordance with the transaction's risk (e.g., individual security and privacy risks, as well as other organizational risks).
- 4) The principles of least privilege and separation of duties are used to manage access permissions and authorizations.
- 5) Configuring systems to provide only essential capabilities incorporates the principle of least functionality.
- 6) The network's integrity is safeguarded (e.g., network segregation, network segmentation)
- 7) Furthermore, there is data classification and protection against data leaks. Data is destroyed in accordance with policy.

5. DISCUSSION

Based on calculation that author do, the result of capability the score of capability rate in this IT function is 2.28 and the company has a target for future is to reach max level 5, that about having a Gap Score 2.72. For company to achieve the higher capability the author already make some guideline for company to follow so the capability can be increase to desired result.

6. DIFFERENCE FROM SIMILAR PAPER

Here is the result of similar paper, such as:

1. Evaluation of Information Technology Governance in Banking Companies Using BSC and COBIT 4.1 [11]. The result of comparison from the previous research and my research is the using of method which the previous is 4.1 COBIT and my research using COBIT 2019
2. Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-Edu) [6]. The result of comparison from previous research and my research is the previous study aims to explore the use of COBIT 2019 as an IT Governance Framework to evaluate the maturity level of selected IT processes at institutions in Depok (Indonesia) while the research I conducted for evaluate the capability in banking company especially in IT division
3. [12] Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study.

The result of comparison from the previous research and my research is the scope of case study just using COBIT 5 Framework while the research I Conducted is using COBIT 2019 and NIST Framework for cybersecurity point of view.

7. CONCLUSION & SUGGESTION

This research provides guidance on the implementation of IT Governance, which can be used to measure the level of capability in accordance with the 2019 COBIT guidelines, as well as some recommendations from the NIST cybersecurity framework that can assist companies in protecting themselves from cybersecurity incidents/events. The contribution that this research can make is to increase company productivity by creating alignment between business and IT and the latest innovations from adoption technology from planned IT investments by identifying the requirements of IT Governance activities for continuous improvement, as well as cybersecurity protection or guidelines.

Several conclusions can be drawn from this research discussion of the capability level assessment process and recommendations for improvement. First, the average capability is level 2, which means that the process achieves its goal while remaining complete in terms of the set of activities that can be characterized as performed.

The assessment results show that the process was well organized, achieved its goals, and was well defined, but it still requires improvement in measuring the process's performance and always making improvements to the processes carried out. To compete with other businesses.

The author offers advice and input to the related process.

- 1) It is necessary to improve the culture of documentation of the various activities carried out and the documentation of forms of communication from and to various divisions.
- 2) Create a system to reduce manual paperwork and centralize the process so that it can be monitored in real time.
- 3) Training personnel to improve their skill and competency.
- 4) Begin developing a cybersecurity policy and procedure because data protection will be critical in all businesses in the coming year.

The author hope this research can be contribute for company to achieve the expected level and other author can become a guide for other researcher to know what the important of banking process and the risk for each process.

The suggestion given by author based on evaluation that have been done and need be to reconsidered for to be able to improve the capability level in IT division for the future, namely:

- a. For further research, the author can suggest to see the capability in Domain such as:

Domain		Description
EDM02	Ensure Benefit Delivery	This Domain to measure the delivery for project / service / product for customer
EMD03	Ensure Risk Optimization	This domain is for measure the how company manage the risk
APO14	Managed Data	This Domain for company see that company manage and protect.
BAI01	Managed Program	This domain for company manages the program that build by company or vendor
BAI04	Managed Availability and Capability	This domain for company to manage the resource so the company doesn't run out resource
DSS03	Managed Continuity	This domain for the company measure about system readiness in case of emergency

- b. Project management capability level measurement utilizing the IT Process from COBIT 2019 that has been chosen is still subject to change because it permits the adjustment of Capability Level, Gap, and its Capability Target and must be tailored back to the company's history and purpose.

REFERENCES:

- [1] G. Mangalaraj, A. Singh, and A. Taneja, "IT governance frameworks and COBIT - A literature review," *20th Am. Conf. Inf. Syst. AMCIS 2014*, pp. 1–10, 2014.
- [2] Y. Aprilinda, A. K. Puspa, and F. N. Affandy, "The Use of ISO and COBIT for IT Governance Audit," *J. Phys. Conf. Ser.*, vol. 1381, no. 1, 2019, doi: 10.1088/1742-6596/1381/1/012028.
- [3] M. Rubino, F. Vitolla, and A. Garzoni, "The impact of an IT governance framework on the internal control environment," *Rec. Manag. J.*, vol. 27, no. 1, pp. 19–41, 2017, doi: 10.1108/RMJ-03-2016-0007.
- [4] J. Weill, P., Ross, "IT Governance How Top Performers Manage IT decision Rights for superior result." 2004.
- [5] D. S. Vucek, M. Spremić, and M. P. Bach, "IT governance adoption in banking and insurance sector: Longitudinal case study of cobit use," *Int. J. Qual. Res.*, vol. 11, no. 3, pp. 691–716, 2017, doi: 10.18421/IJQR11.03-13.
- [6] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu)," *2020 3rd Int. Conf. Comput. Informatics Eng. IC2IE 2020*, pp. 236–241, 2020, doi: 10.1109/IC2IE50715.2020.9274599.
- [7] A. Joshi, L. Bollen, H. Hassink, S. De Haes, and W. Van Grembergen, "Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role," *Inf. Manag.*, vol. 55, no. 3, pp. 368–380, 2018, doi: 10.1016/j.im.2017.09.003.
- [8] ISACA, "COBIT Over the Years." <https://www.isaca.org/why-isaca/about-us/isaca-50/cobit-over-the-years>.
- [9] P. . Joao Souza Neto, Ph.D., CRISC, CGEIT, COBIT Certified Assessor, Rafael Almeida, and Miguel Mira da Silva, "Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement," *ISACA website*, 2019. <https://www.isaca.org/resources/news-and-trends/industry-news/2019/defining-target-capability-levels-in-cobit-2019-a-proposal-for-refinement>.
- [10] ISACA, *COBIT 2019 Governance and Management Objectives (ISACA)*. 2018.
- [11] E. Pawan, "Evaluation of Information Technology Governance in Banking Companies Using BSC and COBIT 4.1," *Int. J. Comput. Inf. Syst.*, vol. 2, no. 2, pp. 23–27, 2021, doi: 10.29040/ijcis.v2i2.27.
- [12] Q. A. Al-Fatlawi, D. S. Al Farttoosi, and A. H. Almagtome, "Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study," *Webology*, vol. 18, no. SpecialIssue2, pp. 294–310, 2021, doi: 10.14704/WEB/V18SI02/WEB18073.