**International Journal of Engineering and Information Systems (IJEAIS)**
**ISSN: 2643-640X**
**Vol. 6 Issue 6, June - 2022, Pages: 77-88**

# Audit of Finance Application using COBIT 5 Framework (Case Study in Banking)

**Kevin Christianto, Honni, Julia Gunadi, Rendy Ferdinal, Tjhin Felix Hendrawan**

Department of Information Systems,
Faculty of Design and Technology,
Bunda Mulia University, Jakarta, Indonesia.
E-mail: kevin.hikoza@gmail.com

***Abstract***—*In this research, we will discuss how XCZ Bank IT governance, particularly in financial information systems. Bank XCZ is the largest private bank in Indonesia. Founded in 1957, Bank XCZ has continued to grow and become what it is today. The main operational activities that have been run by Bank XCZ are mostly online based, including the finances. The finance information system expects to be a means to produce an accurate, reliable, on time and accountable finance report, to create an excellent financial information system. A capability test can be performed using the COBIT 5 framework. COBIT 5 itself is a framework that is often used by auditors, especially information system auditors. It is because COBIT 5 provides us with a comprehensive framework service so that it can be used as a tool to created better IT governance for the company. In this research, we use the COBIT framework to review the financial application process used in banking industry to see the level of evaluation in the industrial banking system. Focus domain that the authors use at this research is EDM02, EDM03, DSS01. The results of the capability level of EDM02 domain is 3 and located at establish process, EDM03 average capability level is 2,4 so the capability level of this domain is 2 located at managed process, DSS01 average capability level is 2,6 so the capability level of this domain is 3, established process, DSS03 capability level is 3 located at established process.*

**Keywords:** Audit information system, Bank, COBIT 5, financial information system

## 1. INTRODUCTION

Information technology plays an important role in a company, over the years it's transitioned the provision of transaction support to an advantage for the organization. IT is very important to a company because it's provides the agility needed to respond to markets and competition [1].

Information about the relative importance of various IT control and security processes is important for CIOs in large organizations that are responsible for IT governance and maintaining and managing the organization's IT infrastructure [2]. Claims that information technology (IT) applications bring benefits when aligned with business goals [3].

In today's era, information technology (IT) is very helpful for companies and organizations in the security field. There is no doubt that security, privacy and trust are complex issues with multi-dimensional factors. Many of them have transcended the traditional physical market and entered the electronic market. In addition, although each online bank has a different reputation and provides different service quality, the reputation of the bank is the most important factor in choosing online banking services, and the quality of online banking services has a great impact on customer satisfaction [4].

Information technology (IT) has developed rapidly, making it easier for many people to carry out activities without having to go out, such as opening new accounts and conducting transactions through online banking. IT provides new opportunities for banks to organize product development, delivery, and marketing. Although IT has been used to improve conventional banking operations, such as speeding up transactions and database management, the threat of using IT for illegal activities (especially money laundering) has become a practical issue and research focus. Both IT scholars and financial researchers recognize that the use of IT in banks may bring security risks. The introduction of IT infrastructure (such as the network) increases the possibility of external access to the bank's confidential and proprietary information [5]. Applying IT to business processes will improve the accuracy and efficiency of working hours [6].

The improvement of information technology (IT) application efficiency shows that the performance of information technology is consistent with the realization of the company's business strategy. Considering the importance of information technology to the company, it is necessary to evaluate the company's information technology governance to measure maturity, and to look for problems in business processes to increase maturity, and to look for problems in business processes, information technology analysis (IT) Use COBIT framework 5. The Control Objective of Information and Related Technology (COBIT) addresses the need for management and control of information and related IT. COBIT is a method for managing and controlling information and IT risks and vulnerabilities. COBIT recognized that the effective management of information and related IT is essential to the success and survival of the organization. COBIT is also one of the important ITG frameworks and supporting tools. It enables IT managers to communicate

and bridge the gap between business risks, control requirements, value creation and technical issues. COBIT was created by the Information Systems Audit and Control Association (ISACA) [7]. COBIT provides best practical steps that can be taken and is more focused on control, which is further explained in the phase and process framework [8]. In addition to helping, they use resources, COBIT also helps business professionals and managers use the benefits of IT to maintain a balance between expected benefits and risks. The COBIT framework has changed its focus on its development path [9]. The domain involved in information technology security is the DSS domain. Domain DSS (Delivery, Service and Support) is a domain used in information technology analysis in management areas with multiple processes [10].

The problem discussed here is how to evaluate data through information technology governance audits to determine the level of maturity based on the COBIT 5 framework and provide security system recommendations according to the COBIT 5 framework standards.

## 2. LITERATURE REVIEW

### 2.1 Audit Information System

Auditing plays an essential part in the development and strengthening of the global economy and business companies. This is an important strategy for conducting audits in a company to identify security measures. The results of the audit will help determine whether they are suitable for this situation. The main purpose of the audit is to ensure that the correct measures are taken to prevent vulnerabilities. Auditing is a preventive measure that can be deployed after something has happened [11]. Business organizations accept different types of audits for different purposes. The most general is external (financial) audits, internal audits, and fraud audits. IT audit is based on the computer-based aspects of the organization's information system; and modern systems use a lot of technology [12].

There are several methodologies and standards that solve this issue: COBIT, ITIL, ISO 27002 (ex ISO 17799) and ISO 9000. [13].

### 2.2 COBIT 5

ISACA launched a new fourth edition of COBIT in 2005, with a clear focus on IT governance. Another version of this framework is COBIT 4.1 released in 2007, which accepts common frameworks such as "IT Infrastructure Library (ITIL)", "ISO 27000 Series" and "Functional Maturity Model® Integration (CMMI)". The current version of framework, COBIT 5, was released in 2012 [14]. COBIT 5 is a comprehensive framework that can help companies create maximum value from IT by maintaining a balance between realizing benefits, optimizing risk levels, and resource usage [15]. COBIT supports clear policy formulation and best practice steps that can be taken to control the information technology of all companies [16]. COBIT 5 enables information and related technologies to be fully managed in the end-to-end business and functional responsibilities of the entire enterprise, considering the IT-related interests of internal and external stakeholders. The COBIT 5 principles and enabling factors are universal and are useful for businesses of all sizes, whether it is a commercial enterprise, a non-profit organization, or the public sector [17].

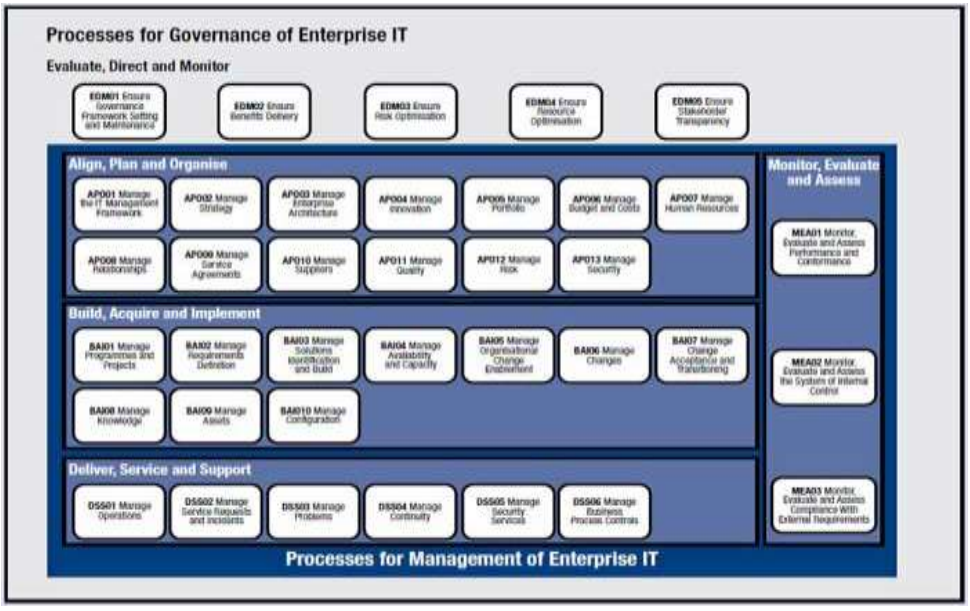

**Figure 1**: COBIT 5 Process references model [18].

## 3. METHODOLOGY

The methodology used in this research starts from initiation, planning, briefing, data collection, data validation, and attribute level processes, then we collect or obtain data from interviews conducted. shown in the research flow chart in Figure 2.

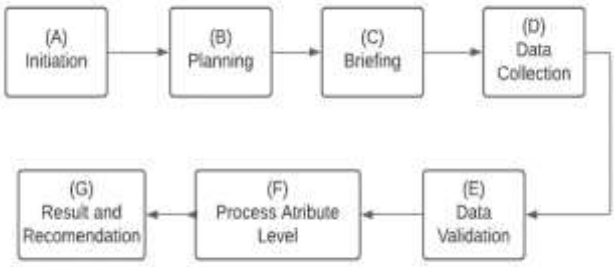


**Figure 2:** Research Flow-chart [19].

The process is carried out starting from planning until it can be drawn from research on auditing using COBIT5.

## 4. RESULT AND DISCUSSION

In this chapter, we will analyze general controls using the COBIT 5 framework approach. The author will analyze the environment that occurs in the financial information system at Bank XCZ. The business processes at this Bank are computerized, including the financial system. In the Financial Information System, computers and other supporting tools to cooperate in the task of recording, calculating, summarizing, classifying and reporting banking activities that occur at XCZ Bank, the authors will discussing the results of audits that have been carried out in the EDM02, EDM03, DSS01 and DSS03 domains. In the COBIT framework 5. Data collection was carried out using interviews, and then the data obtained were used to analyze the level of capability. According to the sources we interviewed, a financial information system audit is needed by Bank XCZ so that the employees always follow existing procedures in the company, then Bank XCZ has not had any problems in the IT audits they carry out because the audit is carried out by experienced resources in their fields, the main objective of the banking business run by Bank XCZ has been fulfilled by the financial information system audit process they are running, because previously unknown problems can be found and resolved quickly.

### 4.1 EDM02 Ensure Benefit Delivery

Optimize the value to the business from business processes IT services and IT assets generate from investments made by IT at reasonable cost as well as producing proper and reliable information and supporting business effectively and efficiently.

#### 4.1.1 EDM02.01 Evaluate value optimization

Continuous evaluation of IT support investment portfolio, services, and assets to determine the likelihood of achieving company goals and provide value at an acceptable cost. Identify and make judgments about the changes and direction that need to be given to management to optimize value creation. Audit results, in this sub domain, the authors analyze that there is already an evaluation process for IT investments, services and assets to determine the likelihood of achieving goals and provide value with reasonable resources to the organization's financial information system, we also find that evaluation is to assess the effectiveness of integration. organization with IT in the analysis results show that the value of the capability level of this process is 3, because the process has been going well in the process arrangement and work results are defined, controlled, and maintained appropriately, carried out using the specified process and its achievements. the result.

This domain's capability level is 3, the defined process. Activities:

- Understand strategic IT issues, technical insights, and functions of stakeholders' actual and potential implications for IT corporate strategy.
- Understand the value composition of the company’s current emerging technologies and optimize the value created from these opportunities
- Understand what constitutes corporate value, and consider the extent to which it is communicated, understood and applied throughout the enterprise process.
- Assess the degree of integration and consistency of the enterprise and IT strategy in the enterprise's value delivery goals.

- Understand and consider current emotional roles, responsibilities, responsibilities and how decision-making agencies ensure value management and financial management practices.
- Evaluate the portfolio of investment, services and assets for alignment with the enterprise strategics objectives, business process alignment, effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health.

### 4.1.2 EDM02.02 Direct value optimization

Direct value management principles and practices to realize optimal value realization from IT-enabled investments throughout their full economic life cycle. The results of the audit on this sub domain, we analyze that the process of directing principles and practices to produce optimal IT investment realization has been carried out, according to the answers given by our sources, in our company we find that the process of determining requirements for investment related to corporate risk and funding risk has been carried out. implemented properly in the management of processes and work results that are determined, controlled and maintained. appropriately, implemented using defined processes and achieved results. Therefore, we find that the capability level of this domain is 3.

The capability level of this domain is 3, established process. Activities:

- Define and communicate portfolios and investment types, categories, criteria, and relative weights to standards to achieve overall relative value scores.
- Define stage-gates requirement and other reviews of the significance of the investment to the enterprise, associated risk, programme schedules, funding plans, the delivery of key capabilities and benefits and ongoing contribution to value.
- Direct management to consider potential innovative uses of IT that enable the enterprise and responding to new opportunities or challenges.
- Directing required changes in the assignment of accountabilities and responsibilities for executing the investment portfolio and delivering value from business processes.
- Define and communicate enterprise-level value delivery goals and result metrics to achieve effective monitoring.
- Directing the necessary changes in the investment and service portfolio to match the current and expected goal constraints of the company.
- Recommended to consider potential innovations, organizational changes or operational improvements that may drive IT-based programs to add value to the enterprise.

### 4.1.3 EDM02.03 Monitor value optimization

Monitor the key goals and metrics to specify the extent to which the business is delivering the expected value and benefits to the company from IT-enabled investments and services. Identify significant issues and consider corrective actions. The audit result is in this sub-domain, we analyze that the company has monitored the main objectives and metrics on risk management in the financial information system processes that are currently running within the company, identified, monitored and reported so that improvements are made, in the company we found that after reviewing the audit report were there any corrective actions taken by management. Through answers given by our sources, it is found that Capability level value is 3, because the process has been going well and start to have SOPs, policies, or regulations that have standard implementation and are under the responsibility of experienced resources in their fields.

The capability level of this domain is 3, established process. Activities:

- Define a balanced set of performance goals, indicators, indicators and benchmarks. Metrics should cover activity and outcome measures, including leading and lagging indicators of outcomes, and an appropriate balance of financial and non-financial measures. Review and reach an agreement with IT and other business functions and other relevant stakeholders
- Collect relevant, timely, complete, credible and accurate data to report the progress of achieving value according to the target. Obtain a brief, high-level, holistic view of the portfolio, planning, and IT (technical and operational capabilities) performance to support decision-making and ensure the desired results are achieved.
- Get regular and relevant product portfolio, plan and IT (technical and functional) performance reports. Review the progress of the company in achieving the established goals, as well as the extent to which the planned goals are reached, the deliverables obtained, the performance goals reached and the risks reduced.
- After reviewing the report, take appropriate management measures as needed to ensure that the value is optimized.
- After reviewing the report, make sure that appropriate management corrective actions are initiated and controlled.

**Table 1.** Result of EDM02 Ensure Benefit Delivery

| No | Sub-Domain | Capability Level | Expected level |
|---|---|---|---|
| EDM02.01 | Evaluate value optimisation | 3 | 4 |
| EDM02.02 | Direct value optimisation | 3 | 4 |
| EDM02.03 | Monitor value optimisation. | 3 | 4 |

### 4.2 EDM03 Ensure Risk Optimization

Ensure that the enterprise's risk taste and tolerance are understood, expressed, and communicated and that the enterprise value risks associated with the use of IT are identified and managed.

#### 4.4.1 EDM03.01 Evaluate risk management

Continually examine and make a judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the risk tolerance of the company is appropriate and the impact of the risk on the value of the company and identify and manage information related to IT usage. The audit result is in this sub-domain, we analyze that checking and assessing the effect of present and future risks due to the use of IT, in the company we found that there's already an assessment of the alignment of IT strategies and risks with company strategies and risk, in this financial information system it has passed the process at level 2, so we determine that the capability level of this sub-domain is 3 The process is managed and has SOPs run by adequate resources for the company.

The capability level of this domain is 3, established process. Activities:

- Determine the level of IT-related risk that the company is willing to take to achieve its goals (risk appetite).
- Evaluate and approve the recommended IT risk tolerance thresholds based on the enterprise's acceptable level of risk and opportunity
- Determine the degree of consistency between the IT risk strategy and the corporate risk strategy.
- Proactively assess IT risk factors before pending strategic corporate decisions and ensure that risk-conscious corporate decisions are made.
- As described in relevant international and national standards, determine appropriate risk assessments and assessments for IT use.
- Evaluate risk management activities to ensure that it is consistent with the company's IT-related loss capability and the leader's tolerance.

#### 4.4.2 EDM03.02 Direct risk management

Guide the establishment of risk management practices to reasonably ensure that IT risk management practices are appropriate to ensure that actual IT risks do not exceed the risk tolerance of the board of directors. The audit result is in this sub-domain we analyze that XCZ Bank has created a good practice in risk management to provide assurance that the risk management made does not exceed the risk appetite of the company, in the company, there's a culture of being aware of IT risks and empowering organizations to proactively identify IT risks, opportunities and potential in the financial information system, the process in this domain has been running and has passed the existing process at level 1 and It has been managed so that we get the capability level value of this sub-domain is 2.

The capability level of this domain is 2, managed process. Activities:

- Promote a culture of IT risk awareness that enables companies to proactively identify IT risks, opportunities and potential business impacts.
- Guide the integration of IT risk strategy and operation with corporate strategic risk decision and operation.
- Guide the development of risk communication plans (covering all levels of the enterprise) and risk action plans.
- With the support of the agreed escalation principles (report content, time, location and method), directly implement appropriate mechanisms to quickly respond to changing risks and immediately report to the appropriate management level.
- Instruct that anyone can identify and report risks, opportunities, problems, and concerns at any time. Risks should be managed according to published policies and procedures and reported to relevant decision makers.

- Determine the key objectives and indicators of the risk governance and management process to be monitored, and approve the methods, methods, techniques, and processes used to capture and report measurement information.

#### 4.4.3 EDM03.03 Monitor risk management

Monitoring the key purpose and metrics of the risk management processes and establish how deviations or problems will be identified, tracked, and reported for remediation. The audit result is in this sub-domain, we analyze that the monitoring process on the main objectives and metrics as well as how problems will be properly identified, monitored and reported so that improvements can be made immediately and optimally, especially in the financial information system section of this company, this organization already doing a review conducted by key stakeholders regarding the progress of the organization, in the sub- In this domain, the process that occurs at level 2 has been fulfilled properly so that the capability level of this domain is 3.

The capability level of this domain is 3, established process. Activities:

- Monitor the extent to which the risk profile is managed within the risk appetite threshold.
- To monitor the key objectives and indicators of the risk management and management process, analyze the causes of deviations, and take remedial measures to solve the root causes.
- Enable key stakeholders to review the progress of the company in achieving the established goals.
- Report any risk management issues to the board of directors or executive committee.

**Table 2.** Result of EDM03 Ensure Risk Optimisation

| No | Sub-Domain | Capability Level | Expected level |
|---|---|---|---|
| EDM 03.01 | Evaluate risk management | 3 | 4 |
| EDM 03.02 | Direct risk management. | 2 | 4 |
| EDM 03.03 | Monitor risk management. | 3 | 4 |

### 4.3 DSS01 Manage Operation

This point coordinates and implements the activities and operational procedures required to provide internal IT services and outsourcing, including the implementation of predefined standard operating procedures and the necessary monitoring activities.

#### 4.4.1 DSS01.01 Perform operational procedures

Reliable and consistent maintenance and execution of operational procedures and operational task, audit results is in this sub-domain we discuss the maintenance of operational procedures that support the running of the business, the management and implementation of related activities or activities in accordance with predetermined schedules and standards. According to the sources we interviewed, in this financial information system, anyone who accesses it can be recorded, there is also an SOP that controls the operation of this financial information system, so that the capability level achieved is 3.

The capability level of this subdomain is 3, established process. Activities:

- Develop and maintain operational procedures and related activities to support all the services provided.
- Supervise the schedule of operational activities, carry out activities, and manage the performance and throughput of scheduled activities.
- Verify that all data expected to be processed have been received and processed in a complete, accurate and timely manner. Give a suitable result.
- To the needs of the company. Support restart and reprocessing needs. Ensure that users receive the correct output in a safe and timely manner.
- Ensure that applicable security standards are met for the reception, processing, storage, and output of data in a manner that meets the company's objectives, company security policy and regulatory requirements.
- Plan according to Schedule, take, and record backups according to established policies and procedures.

#### 4.4.2 DSS01.02 Manage outsourced IT services

Manage the operation of outsourced IT services to maintain the protection of enterprise information and reliability of service delivery The audit result is in this sub-domain, we will discuss how to manage relationships with service providers related to existing financial information systems, in this financial information system it can be ensured that there has been an independent audit to ensure

that the services provided by the outsourced party are in accordance with the SOP, This process has been running well enough so that in its implementation the process has been carried out and well managed, so that the capability level value of this domain is 3.

The capability level of this subdomain is 3, established process. Activities:

- Ensure that company requirements for information processing security are executed in accordance with the contract and the third SLA parties that organize or provide services.
- Ensure that the company's business operations and IT processing requirements and priorities to provide the complied with services comply contracts and SLAs with third parties that host or provide services.
- Combine critical internal IT management processes with an outsourced service provider, which includes, for example, performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and process performance monitoring and reporting.
- Plan for independent audits and assurance of the outsourcing provider's operational environment to ensure that agreed requirements are being met handled adequately.

#### 4.4.3 DSS01.03 Monitor IT infrastructure

Monitor the IT infrastructure and related events. Store sufficient chronological information in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations. The audit result is in this sub-domain, we will analyze the infrastructure monitoring process and related matters such as historical information storage and operation logs to allow reconstruction, review and inspection of the operation timeline and other supporting activities. This company has carried out the existing process, but it has not been manager zed so that the capability level of this sub-domain is 1.

The capability level of this subdomain is 1, performed. Activities:

- Event log, identifying the level of information to be recorded based on risk and performance considerations.
- Identify and maintain a list of infrastructure assets that require monitoring based on criticality of services and relationships between configurations goods and services that depend on it.
- Define and apply rules that identify and record threshold violations and event conditions. Find the balance between the minor events and the events that caused the error, so that the event log is not overwhelmed with unnecessary information.
- Create a log of events and keep it for a suitable period to help with future investigations.
- Establish procedures for monitoring event logs and conducting regular reviews.
- Ensure that incident tickets are generated in a timely manner when monitoring identifies deviations from the specified threshold levels.

#### 4.4.4 DSS01.04 Manage the environment

Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment. The audit result is in this sub-domain, we discuss how a company maintains a list of infrastructure assets and logs activity or event logs related to the current financial information system. In this company, we found that the company already has a special place that is arranged in such a way as to protect the facilities that support the financial information system running from disasters, so it is found that the capability level value of this sub-domain is 3.

The capability level of this subdomain is 3, established process. Activities:

- Identify natural and man-made disasters that may occur in the area where the IT facility is located. Assess the potential effect on IT facilities.
- Identify how IT equipment, including mobile and off-site equipment, is protected from environmental threats. Ensure that the policy restricts or does not include eating, drinking, and smoking in sensitive areas, and prohibits the storage of stationery and other equipment that could cause a fire hazard inside computer room.
- Locate and build IT facilities to limit and reduce vulnerability to environmental threats.
- Regularly supervise and maintain devices that detect environmental threats (e.g., fire, water, smoke, humidity).
- Respond to environmental alarms and other notifications. Test documents and procedures, which should include alarm and contact priority with local emergency response authorities, and train personnel in these procedures.
- Compare emergency measures and plans with insurance policy requirements and report results. Address non-compliance points in a in a timely fashion.
- Ensure that IT sites are built and designed to reduce the impact of environmental risks (for example, theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, and explosives). consider specific security zones and / or fireproof cells (for example, locating remote production and development environments / servers from one person to another) Keep IT

sites and server rooms always clean and in a safe condition (e.g., no clutter, no paper or cardboard boxes, no filled bins, no chemicals, or flammable materials).

### 4.4.5 DSS01.05 Manage facilities

Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines. The audit result is, In this sub-domain, we will analyze how companies manage their facilities and check their compliance with applicable regulations and laws. In this company, we found that the cables in this XCZ bank had been placed securely and were not visible and prevented unwanted access. The process had been carried out and well managed, so we analyzed that the capability level that the financial information system had in this company is 2.

The capability level of this subdomain is 2, managed process. Activities:

- Check IT facility requirements for protection against fluctuations and power outages, related to other business continuity planning with requirements. Obtain suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.
- Regularly test the uninterruptible power supply mechanism and ensure that power can be switched to the power supply without a significant effect on business operations.
- Ensure that the facility that houses the IT system has more than one source for the dependent utility (e.g., electricity, telecommunications, water, gas). Separate physical entrances to each utility.
- Confirm that the external cable to the IT site is located underground or has suitable alternative protection. Determine that the wiring is inside the IT site in secure drains, and cable cabinets have limited access to authorized personnel. Protect cables properly from damage caused by fire, smoke, water, interception, and disturbance.
- Ensure that the cabling and physical patching (data and telephone) is structured and orderly. Cable and conduit structures shall be documented (for example, blueprint building plans and wiring diagrams).
- Analyze the facility's high-availability residential system for redundancy and fail-over cable requirements (external and internal).
- Ensure that sites and IT facilities continuously comply with relevant health and safety laws, regulations, guidelines and vendor specifications.
- Educate personnel regularly about health and safety related laws, regulations, and guidelines. Educate personnel about fire and rescue drills for ensure knowledge and action taken in the event of a fire or similar incident.
- Record, monitor, manage and resolve facility incidents in accordance with the IT incident management process. Provide a facility report incident where disclosure is required in terms of laws and regulations.
- Ensure that the IT site and equipment are maintained according to the supplier's recommended service intervals and specifications. Care should be carried out only by authorized personnel.
- Analyze physical changes to IT sites or premises to reassess environmental risks e.g., fire or water damage). Report the results of this analysis to business continuity and facilities management

**Table 3.** Results of DSS01 Manage Operations

| No. | Sub Domain | Capability Level | Expected Level |
|---|---|---|---|
| DSS 01-01 | Perform Operational Procedures | 3 | 4 |
| DSS 01-02 | Manage Outsourced IT Services | 3 | 4 |
| DSS 01-03 | Monitor IT Infrastructure | 1 | 4 |
| DSS 01-04 | Manage The Environment | 3 | 4 |
| DSS 01-05 | Manage Facilities | 2 | 4 |

### 4.4 DSS03 Manage Problems

Identify and classify problems and their root causes and provide timely explanations to prevent recurring incidents. Provide recommendations for improvements.

#### 4.4.1 DSS03.01 Identify and classify problems

Define and implement standards and procedures for reporting problems found, including problem classification, classification, and priority. The audit results in this sub-domain will discuss how the company establishes the criteria and procedures for reporting problems that have been identified. In this company, every problem that occurs in the financial information system already has formal handling with relevant access, the process has been running well and is well managed so that the value of the capability level is obtained namely 2.

The capability level of this subdomain is 2, managed process. Activities:

- Identify issues according to incident reports, error logs, and other problem identification resources. Set priority levels and categorizations to solve issues in a timely way based on business risk and service definitions.
- Resolve all issues formally with access to all relevant data, including information from change management systems and IT configuration/assets and incident details.
- Determine the right support groups to help identify problems, analyze root causes, and determine solutions to support problem management. Define support groups based on previously defined categories, such as hardware, networking, software, applications, and support software.
- Determine priority levels through consultation with businesses to ensure that problem identification and root cause analysis are handled in a timely way in accordance with the agreed SLA. Basic priority level on business impact and urgency.
- Report the status of the identified issue to the service desk so that customers and IT management can continue to be notified.
- Maintain a single problem management catalog to register and report identified issues and to implement audit traces of the problem management process, including any issues.

#### 4.4.2 DSS03.02 Investigate and diagnose problems

Investigate and diagnose problems using relevant subject management experts to assess and analyze root causes. The audit results in this dub-domain, we will investigate and diagnose the problem using the relevant subject to assess and link the root of the problem, within the company, we find that there is already a routine report generation to communicate the problem-solving process, the process has been carried out and has also been managed well and have a defined process and achieve process results. So that the level of capability obtained is 3.

The capability level of this subdomain is 3, established process. Activities:

- Identify issues that may be known errors by comparing incident data with known error databases and classifying the issue as a known error.
- Associate all affected configuration items with defined/known errors.
- Generate reports to communicate progress in resolving problems and to monitor the ongoing impact of unsolved problems. Monitor the status of the troubleshooting process throughout its lifecycle, including input from change management and configuration.

#### 4.4.3 DSS03.03 Raise known errors

Once the root cause of the problem is discovered, create a record of known errors and appropriate solutions, and identify potential solutions. The audit result is, In this sub-domain we will discuss how Bank XCZ recorded errors identified and the right solution after finding the problem then provided a timely resolution by taking into account the cost-benefit and impact on the running of the financial information system processes that are running within the company, from the answers given by interviewees, Bank XCZ will immediately forward the problems found to the problem recording and solutions, the process has been carried out and has also been managed properly and has a defined process and achieves process results. So that the capability level obtained is 3.

The capability level of this subdomain is 3, established process. Activities:

- Once the root cause of the problem is identified, create a known error record and develop the appropriate solution.
- Identification solutions, evaluations, priorities, and processes for known errors based on a business case that benefits costs and impacts and business urgency.

#### 4.4.4 DSS03.04 Resolve and close problems

Identify and initiate a sustainable solution to the root cause, and if the error needs to be resolved, then make a change request through the established change management process. Ensure that the affected people are aware of the actions taken and the plans made to prevent future incidents. The audit results in this sub-domain, we will discuss how XCZ bank makes sustainable solutions to deal with the problems found, then from the results of the interviews we conducted with the informants we have found that there has been

a review process and confirmation of the successful resolution of the problem., The process It has been executed properly with a defined process so that the results of the process are obtained, so that from this sub-domain, we get a capability level value of 3.

The capability level of this subdomain is 3, established process. Activities:

- Close the issue record after confirmation of the successful removal of known errors or after an agreement with the business on how to handle the issue alternatively.
- Inform the service desk about the closing schedule of the problem, for example, the schedule to correct known errors, possible solutions or the fact that the problem will remain until the changes are implemented, and the consequences of the approach taken. Maintain information that matches affected users and customers.
- During the completion process, get regular reports from change management about progress in resolving problems and errors.
- Continuously monitor the impact of ongoing issues and known errors on the service.
- Monitor and confirm the success of major problem resolution.
- Make sure the knowledge learned from reviews is included in service review meetings with business customers.
- Make sure the knowledge learned from reviews is included in service review meetings with business customers.

### 4.4.5 DSS03.05 Perform proactive problem management

Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment. The audit result is, in this domain, we will analyze the way XCZ Bank collects and analyzes operational data to identify things that might cause problems, according to the answers given by our sources, in XCZ Bank there are monitoring actions carried out to monitor the use of costs that have caused by problems, according to our source, the process at level 3 has been carried out with defined boundaries to produce process results. So that the capability level value is achieved, namely 4.

The capability level of this subdomain is 4, Predictable process. Activities:

- Capture information on issues related to IT changes and incidents and communicate to key stakeholders. These communications can be reports to and periodic meetings between owners of incident management processes, issues, changes, and configurations to consider the latest issues and potential corrective actions.
- Make sure owners and process managers of incidents, issues, changes, and configuration management meet regularly to discuss known issues and future planned changes.
- Enable the company to continuously monitor the total cost of the problem, capture the change efforts resulting from the problem management process activities (e.g., fixes for known problems and errors) and report them.
- Generate reports to continuously monitor troubleshooting against business requirements
- And SLAs. And make sure the escalation of the problem is appropriate, for example, escalating to a higher management level according to the agreed criteria, contacting an external vendor, or referring to the change advisory board to increase the priority of urgent change requests (RFC) to implement temporary solutions.
- Optimize resource usage and reduce solutions, track problem trends.
- Identify and initiate sustainable solutions addressing the root causes and increasing demand for change through a defined change management process.

**Table 4.** Results of DSS03 Manage Problem

| No | Sub Domain | Capability Level | Expected Level |
|---|---|---|---|
| DSS03-01 | Identify and classify problems. | 2 | 4 |
| DSS03-02 | Investigate and diagnose problems. | 3 | 4 |
| DSS03-03 | Raise known errors. | 3 | 4 |
| DSS03-04 | Resolve and close problems. | 3 | 4 |
| DSS03-05 | Perform proactive problem management. | 4 | 5 |

### 4.5 Gap Analysis

Results of current capability analysis (as is) and expected capability targets (to-be) for each existing process. The report analysis can be seen in table 5, then it can be seen in Figure 3.

**Table 5.** Gap Analysis

| No | Proses | Gap analysis | | |
|---|---|---|---|---|
| | | As-is | To-be | Gap |
| 1 | EDM-02 | 3 | 4 | 1 |
| 2 | EDM-03 | 2,6 | 4 | 1,4 |
| 3 | DSS-02 | 2,4 | 4 | 1,6 |
| 4 | DSS-03 | 3 | 4 | 1 |

From the gap analysis carried out, a graph of the process capability gap level can be made as a figure. 3 of the following:

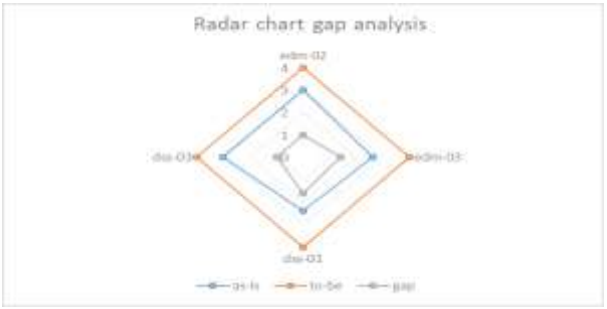


**Figure 3**: Radar Chart of Gap Analysis.

### 5. CONCLUSION

Based on the research that has been done, the conclusion can be obtained that XCZ bank has it governance process, good corporate governance, the whole process has been running well and effectively according to the standards. The conclusions of the capability level analysis are as follows:

- In the EDM02 Ensure Benefit Delivery process reaching level 3 established process, all sub-domains in EDM02 have reached level 3 established process.
- In the EDM03 Ensure Risk Optimization process the average capability level is 2.6, most sub-domains in EDM03 get a level 3 established process.
- In the DSS01 Manage Operations process the average capability level is 2.4, most sub-domains on DSS01 get a level 3, established process.
- In the DSS03 Manage Problems process the average capability level is 3, some sub-domains in DSS03 get a level 3 established process.

## 6. 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]** D. S. Kerr and U. S. Murthy, "The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey," Inf. Manag., vol. 50, no. 7, pp. 590–597, 2013, doi: 10.1016/j.im.2013.07.012.

**[3]** H. Tanuwijaya and R. Sarno, "Comparation of COBIT Maturity Model and Structural Equation Model for Measuring the Alignment Between University Academic Regulations and Information Technology Goals," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 10, no. 6, pp. 80–92, 2010, [Online]. Available: http://paper.ijcsns.org/07_book/201006/20100611.pdf%5Cnhttp://paper.ijcsns.org/07_book/html/201006/201006011.html.

**[4]** S. M. Huang, W. C. Shen, D. C. Yen, and L. Y. Chou, "IT governance: Objectives and assurances in internet banking," Adv. Account., vol. 27, no. 2, pp. 406–414, 2011, doi: 10.1016/j.adiac.2011.08.001.

**[5]** R. Ø. Skotnes, "Information & Computer Security Article information :," Inf. Comput. Secur., vol. 23, no. 3, pp. 302–316, 2015.

**[6]** S. Mukaromah and A. B. Putra, "Maturity level at university academic information system linking it goals and business goal based on COBIT 4.1," MATEC Web Conf., vol. 58, 2016, doi: 10.1051/matecconf/20165803009.

**[7]** A. Abu-Musa, "Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study," Inf. Manag. Comput. Secur., vol. 17, no. 2, pp. 73–95, 2009, doi: 10.1108/09685220910963974.

**[8]** M. Rubino and F. Vitolla, "Internal control over financial reporting: Opportunities using the cobit framework", Managerial Auditing Journal, vol. 29, no. 8. 2014.

**[9]** L. Al Omari, P. H. Barnes, and G. Pitman, "Optimising COBIT 5 for IT Governance : Examples from the Public Sector," Appl. Theor. Inf. Syst. Res., pp. 2–14, 2012.

**[10]** N. M. Alramahi, A. I. Barakat, and H. Haddad, "Information Technology Governance Control Level in Jordanian Banks Using : Control Objectives for Information and Related Technology ( COBIT 5 )," Eur. J. Bus. Manag., vol. 6, no. 5, pp. 194–206, 2014.

**[11]** R. Valverde, M. Wolden, R. Valverde, and M. Talla, "ScienceDirect The effectiveness of COBIT 5 Information Security Framework for reducing Cyber of Attacks The effectiveness COBIT Information for reducing Cyber Attacks on Supply Management System," IFAC-PapersOnLine, vol. 48, no. 3, pp. 1846–1852, 2015, doi: 10.1016/j.ifacol.2015.06.355.

**[12]** K. Budiarta, A. P. Saputra Iskandar, M. Sudarma, "Audit Information System Development using COBIT 5 Framework," International Journal of Engineering and Emerging Technology, vol. 1, no. 1, pp. 3–7, 2016.

**[13]** D. Radovanović, T. Radojević, D. Lučić, and M. Šarac, "IT audit in accordance with Cobit standard," MIPRO 2010 - 33rd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. Proc., no. May 2014, pp. 1137–1141, 2010.

**[14]** J. F. Andry, "Audit of IT Governance Based on COBIT 5 Assessments: A Case Study," J. Nas. Teknol. dan Sist. Inf., vol. 2, no. 2, pp. 27–34, 2016, doi: 10.25077/teknosi.v2i2.2016.27-34.

**[15]** A. K. Setiawan and J. F. Andry, "IT Governance Evaluation Using Cobit 5 Framework on the National Library," J. Sist. Inf., vol. 15, no. 1, pp. 10–17, 2019, doi: 10.21609/jsi.v15i1.790.

**[16]** H. Pratama and J. F. Andry, "IT Governance at financial Technology company using cobit 4. 1 Framework and balanced scorecard perspective," Int. J. Open Inf. Technol., vol. 7, no. 6, pp. 4–8, 2019.

**[17]** W. Gunawan, E. P. Kalensun, A. N. Fajar, and Sfenrianto, "Applying COBIT 5 in Higher Education," IOP Conf. Ser. Mater. Sci. Eng., vol. 420, no. 1, 2018, doi: 10.1088/1757-899X/420/1/012108.

**[18]** J. F. Andry, Hartono, and A. Chakir, "Assessment IT Governance of Human Resources Information System Using COBIT 5," International Journal of Open Information Technologies, ISSN: 2307-8162 vol. 8, no.4, 2020 Assessment.

**[19]** L. N. Amali, M. R. Katili, S. Suhada, and L. Hadjaratie, "The measurement of maturity level of information technology service based on COBIT 5 framework," Telkomnika (Telecommunication Comput. Electron. Control., vol. 18, no. 1, pp. 133–139, 2020, doi:10.12928/TELKOMNIKA.V18I1.10582.