**IJISCS (International Journal of Information System and Computer Science)**
IJISCS, Volume 7, Number 3, December 2023
E ISSN: 2598-246X; P ISSN: 2598-0793, pp. 209-220
**Accredited SINTA 4 Number 79/E/KPT/2023**
https://jurnal.ftikomibn.ac.id/index.php/ijiscs

# OPTIMIZING RISK MANAGEMENT IN THE INSURANCE SECTOR: LEVERAGING THE COBIT 5 FRAMEWORK

**Kenny Pratama[1], Melissa Indah Fianty[2*]**
[1,2]Departement Information System, Faculty of Engineering and Informatics, Universitas Multimedia Nusantara
[1,2]Scientia Boulevard Gading Street, Curug Sangereng, Serpong, Tangerang, Banten, Indonesia

*Corresponding author
melissa.indah@umn.ac.id

**Article history**:
Received October 10, 2023
Revised October 29, 2023
Accepted November 5, 2023

**Keywords:**
Capabilit Level;
COBIT 5;
IT Governance;
Risk Management.

**Abstract**
A vehicle insurance company is grappling with a critical issue amid its efforts to integrate information technology into its operations. The problem revolves around the absence of documented procedures related to IT service management and infrastructure resources, impacting various operational facets, including business processes, staff management, applications, infrastructure, facilities, and vendor relationships. To address these concerns, the company has taken measures, including identification, analysis, control, and mitigation of IT-related risks. However, these measures have proven insufficient for optimal risk management, prompting the need for a comprehensive evaluation of their IT risk management capabilities. This assessment focuses on evaluating the implementation of IT risk management using a qualitative approach within the COBIT 5 framework. Specifically, it assesses the company's performance in two closely related processes: APO 12 (Manage Risk) for identifying IT-related risks and DSS 05 (Manage Security Services) for understanding the role of information security and monitoring security aspects. The assessment results indicate that the company's IT risk management capability is at level 3 (Established) for both processes. However, the company aspires to reach level 4 (Predictable) and improve their risk management. Furthermore, a critical discovery is the absence of Standard Operating Procedures (SOPs) related to data encryption, which is vital for information security. While some monitoring methods for information security service design have been effective, there is a need for enhanced data security through the development of encryption-related SOPs. The company plans to implement improvements based on COBIT 5 framework recommendations to achieve a higher level of risk management capability. These enhancements aim to better align IT-related risk management with the company's business objectives and improve the overall effectiveness of the processes.

## 1.0 INTRODUCTION

One of the significant challenges in today's business world is keeping up with the rapid advancements in Information Technology (IT). IT has become a critical aspect for companies, enabling performance improvement, efficiency, and support for all aspects of business and company growth [1]. However, while reaping the benefits of IT, companies also face various risks associated with its use [2]. Risk management is a key approach required to address these risks. It involves a series of actions aimed at identifying, evaluating, and controlling potential risks that may affect the company [3]. These risks include technology risk, financial risk, human resource risk, marketing risk, and improvement risk. Therefore, risk management is essential to ensure that these risks remain at acceptable levels [4].

Risk management in the Information Technology (IT) division of the company plays a specific role [5]. In addition to ensuring risk management aligns with the Enterprise Risk Management (ERM) framework and company policies, it also involves determining the appropriate level of risk tolerance in line with company objectives [6]. The company acts as an insurance provider, requiring the identification and analysis of IT-related risks and ensuring the necessary controls and mitigation actions are in place. The company faces several critical issues in IT risk management that significantly impact operations and performance. The first issue is the company's inability to conduct comprehensive value analysis related to IT risks. This results in the company's inability to identify the causes of losses and understand internal trends related to IT risks. The impact of this issue is uncertainty in responding to emerging risks, which can lead to financial losses, reputational damage, and operational instability.

Furthermore, the company also faces documentation issues related to dependencies on IT service management processes and unfulfilled IT infrastructure resources. Inadequate documentation affects a wide range of areas, including business process inventory, support personnel, applications, infrastructure, facilities, and vendor relationships. The consequence of this issue is the company's inability to efficiently and effectively manage its IT resources and vulnerability to uncertainty in IT risk management. In a highly competitive and dynamic business environment, these issues can hinder the company's ability to maintain smooth operations and compete in the market. The company faces challenges and issues in information technology, indicating the need for further development in IT risk management. IT risks must be managed effectively to ensure that IT usage has a positive impact on the company. These risks are unpredictable threats that can have a negative impact on the company's objectives and expectations. Therefore, an evaluation is needed to assess the extent to which the company has managed these risks and what needs improvement [7].

The challenges and issues the company faces in information technology emphasize the need for improvements in information technology risk management [8]. IT risks must be well managed to ensure that the use of IT has a positive impact on the company [9]. These risks are unpredictable threats that can have a negative impact on the company's objectives and expectations. Therefore, an evaluation is necessary to assess how well the company has managed these risks and what needs to be improved [10].

This evaluation will help in assessing the current level of IT risk management capability and provide improvement recommendations [11]. One of the frameworks that will be used for the evaluation is COBIT 5, which is a comprehensive guide for IT governance and management [12]. COBIT 5 provides a comprehensive structure to achieve IT governance objectives, optimize risks, and balance resource management [13]. By measuring the level of capability using this framework, the company will be able to evaluate and understand IT risk management and take the necessary actions.

One of the central issues faced by organizations today is the ever-evolving landscape of cyber threats and security breaches. With the rapid expansion of digital systems and data-driven operations, the company is acutely aware of the increasing complexity of IT risks, including cybersecurity threats. Previous research has highlighted the significance of adapting to these modern challenges in risk management. To maintain its competitive edge and protect its sensitive data, the company recognizes the need to bolster its IT risk management strategies and align them with current industry best practices.

The analysis of past research emphasizes that while the company has made strides in managing traditional IT risks, the emerging and dynamic nature of cybersecurity threats requires continuous assessment and adaptation. As the IT environment continually evolves, the

research underlines the necessity of a proactive approach to IT risk management that incorporates real-time threat monitoring, incident response preparedness, and robust cybersecurity protocols. In an era where data breaches and cyberattacks can have far-reaching consequences on a company's reputation and financial stability, the company is committed to staying at the forefront of IT risk management practices. This research aims to assess the company's current IT risk management capabilities in the context of contemporary cybersecurity challenges, providing actionable recommendations to ensure the company remains resilient and secure in the face of ever-evolving IT risks.

## 2.0 THEORETICAL

### 2.1. IT Governance

IT governance is an integrated component of organizational management, encompassing aspects of leadership, data structure, and organizational processes, with the aim of ensuring that the use of IT in the organization supports and advances the organization's strategy and objectives. IT governance involves actions taken by the board of directors, executive management, and IT management teams in planning, implementing, and ensuring alignment between business and information technology [14]. IT governance involves the use of frameworks to allocate data resources and coordinate and control activities within the scope of society or the economy.

### 2.2. COBIT 5

COBIT 5, which stands for Control Objectives for Information and Related Technologies, is a framework that supports organizations and businesses in achieving their business objectives through effective IT governance. This framework provides detailed guidance on various aspects of process management and administration. Within the scope of IT governance, COBIT 5 serves as a tool to assist management in addressing challenges that arise among control requirements, technical issues, and organizational or corporate risks. The framework helps bridge the gaps between these elements [15]. COBIT 5 also represents a set of best practices in IT management developed by the Information System and Control Association (ISACA) and the IT Governance Institute (ITGI). This framework provides process guidance and best practices to managers, auditors, and IT users with the goal of maximizing the benefits that can be obtained through the use of IT and enhancing IT governance and controls within the organization [16].

### 2.3. COBIT 5 Process Assessment Model (PAM)

The Process Assessment Model (PAM) is a framework that involves levels of capability and process dimensions. PAM forms a robust foundation for evaluating the process capabilities within a company. The levels of capability measure the extent to which a process is implemented and executed based on an assessment of the company's processes and practices. The measurement of the processes is divided into several assessment ranges [17]. The levels of capability used in the process evaluation consist of 6 levels, namely:

1) Level 0: An incomplete approach, indicating that the process is not implemented or fails to achieve its strategic objectives.
2) Level 1: The process achieves its goals through the application of incomplete activities, which can be categorized as intuitive and less organized.
3) Level 2: The process achieves its goals through the application of basic, complete activities, and a series of performance-oriented activities.
4) Level 3: The process achieves its goals in a much more organized manner, using organizational resources. Processes are usually well-defined.
5) Level 4: The process achieves its goals and defines its performance well (measurable quantitatively).
6) Level 5: The process achieves its goals, defines its performance well (measurable quantitatively), and engages in continuous improvement.

### 2.4. The COBIT 5 Process Assessment Scale

The rating scale, typically ranging from 0% to 100%, allows organizations to assess their processes and determine their level of achievement based on established criteria. It enables organizations to measure the extent to which their processes align with best practices and industry standards, helping them identify areas for improvement and enhancement [18].

1) N - Not Achieved (0% - 15%): There is no or little evidence supporting the achievement of the attributes specified in the evaluated COBIT 5 process.
2) P - Partially Achieved (15% - 50%): Some evidence supports the attributes or approaches of the assessed COBIT 5 process, but some aspects of the attributes may be challenging to measure.
3) L - Largely Achieved (50% - 85%): There is evidence of a systematic approach and the achievement of the attributes specified in the evaluated process. Nevertheless, there may be some weaknesses in the process.
4) F - Fully Achieved (85% - 100%): There is evidence of a systematic and comprehensive approach, as well as full achievement of the attributes in the evaluated COBIT 5 process, without significant deficiencies.

## 3.0 METHODOLOGY

In the assessment of IT governance management in a company using the COBIT 5 framework, there are several stages as depicted in Figure 1. The initial stage involves the selection of processes to be evaluated based on the company's needs and objectives. Once the processes are chosen, the next step is to assess the level of process capability using a predefined rating scale. The assessment includes an analysis of how well the process is implemented and executed in accordance with COBIT 5 best practices. The assessment results are then used to identify areas where the company can make improvements and enhancements. Subsequently, improvement recommendations can be implemented to ensure that the company's IT governance becomes more effective and aligned with its business objectives [19].

This research comprises five main stages: process selection based on the company's needs and goals, process capability assessment using a predefined rating scale, identification of areas for improvement based on the assessment results, implementation of improvement recommendations, and evaluation of the current IT risk management capability with recommendations. COBIT 5, a comprehensive IT governance and management guide, is used for this evaluation to optimize risk and resource management.

1) Pre-Interview
   During this phase, pre-interviews are conducted with informants from the company's information technology division to obtain an initial overview of the company, identify the challenges faced, and understand the company's objectives. The outcome of this stage is an initial understanding of the existing issues and company information.

2) COBIT 5 Processing
   After obtaining issue data from the pre-interviews, this data will be linked to the company's objectives through further consultations with informants. Following the identification of the company's objectives, the next step is to map these company objectives into IT-Related Goals. Subsequently, these IT-related goals will be integrated into the COBIT 5 framework using the selected IT objectives [20]. In this phase, COBIT 5 processes will be chosen based on primary and secondary priorities. Calculations will be made to determine the most dominant COBIT 5 process, which will be the subject of the audit according to the company's needs. This stage also involves the creation of a RACI Chart and audit documents. The outcomes of this phase include the selection of the COBIT 5 processes to be audited, the RACI Chart, and audit documents.

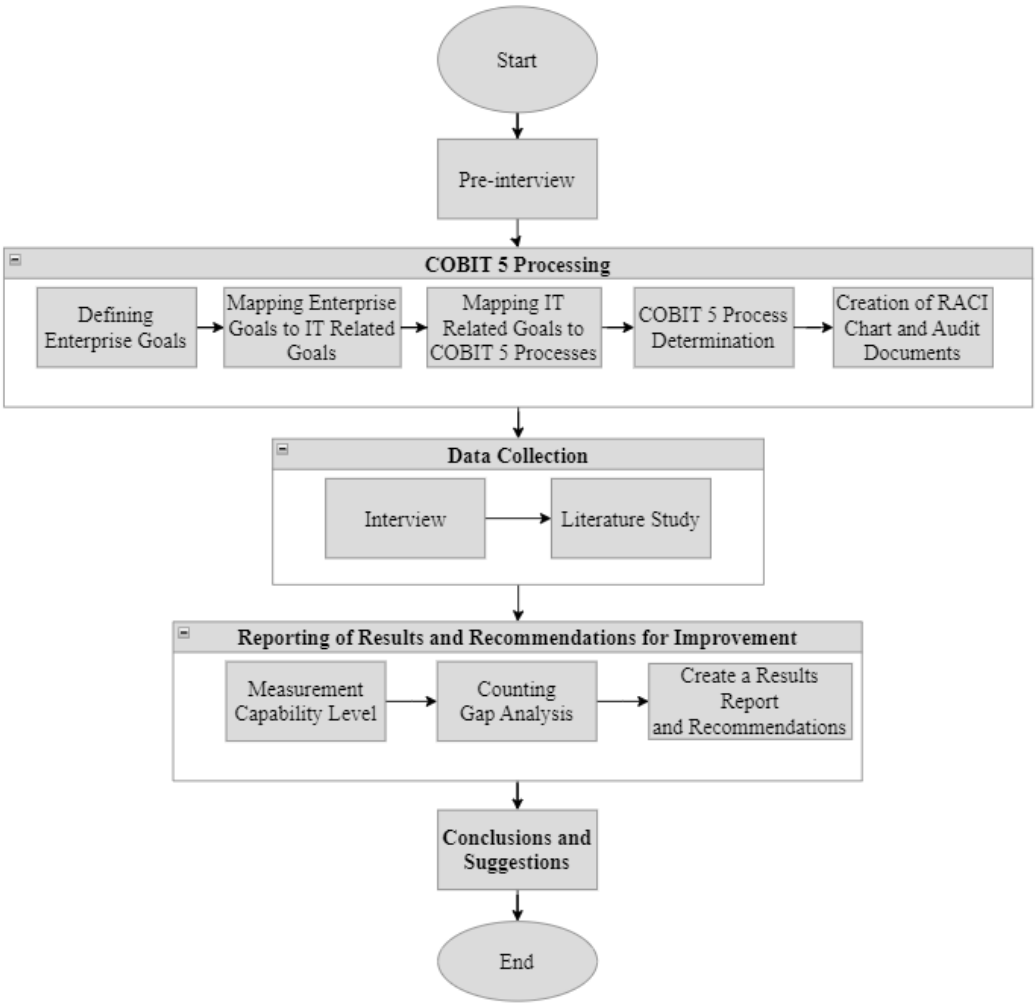


**Figure 1.** Research Flowchart

3) Data Collection

During the data collection phase, information will be gathered through interviews with selected IT and business experts, as well as literature studies based on audit documents created in the previous phase. Interviews and literature studies are conducted to identify company findings and challenges, as well as to assess the existing capability levels for the next phase [21]. The data generated in this phase will be used to evaluate the company based on the activities listed in the audit documents and provide assessments for each activity. The following is the formula that will be used to calculate the capability level based on data obtained from interview results [22].

$$CC = \frac{\sum CLa}{\sum Po} x\ 100\%$$

$CC$ : The value of achieving the level of capability.
$\sum CLa$ : Total value of governance and management.
$\sum Po$ : Total process of governance and management.

4) Reporting of Results

In this phase, the activities listed in the audit documents will be assessed based on the Capability Level according to the selected COBIT 5 process outcomes. After obtaining the Capability Level for each chosen process, the next step is to analyze the gaps between the existing conditions in each selected COBIT process and the company's targets. This is done to identify findings that can be used as recommendations for

improvements within the company when there is a gap between the existing capability levels and the company's expectations. In this phase, an audit report will also be created, including findings, Capability Levels, gap analysis, and improvement recommendations, serving as a guide for the company to implement necessary improvements. Gap analysis is performed by comparing the current situation with the company's expectations or targets. To obtain the results of this gap analysis, a formula as indicated is utilized [23], [24].

$$Gap\ Analysis = expected\ value - current\ value$$

*Gap Analysis* : Expected Value and Current Value in a Situation
*Expected Value* : The target or standard that the company aims to achieve.
*Current Value* : The current unchanged condition.

5) Recommendations for Improvement
In this phase, the results from all the previous stages will be integrated, taking into account key points in each stage. The findings and recommendations obtained from the company's audit process will also be presented [24]. The company can use the existing recommendations and audit results to make improvements and enhancements, thereby improving the governance of information technology within the company as expected and as a reference for future improvements. This phase marks the conclusion of this research.

## 4.0 RESULANTS

### 4.1. Pre-Interview

Through a series of thorough interviews and identification processes with the IT Risk Management Division, essential goals have been established to advance the company's vision. Firstly, the focus is on risk management within the IT Division, aligning it with the company's Enterprise Risk Management (ERM) framework, which includes adapting to the predefined risk appetite and tolerance levels. The objective is to minimize risks while maintaining alignment with the company's goals. Furthermore, through in-depth identification and analysis, we have recognized every threat, vulnerability, and potential impact that might impede the achievement of the company's objectives in the IT environment. This comprehensive understanding of potential risks ensures that the company can effectively prepare for and respond to emerging threats. Lastly, ensuring that each IT Division risk is equipped with suitable controls and mitigations and actively monitoring their implementation is integral to maintaining a proactive and responsive IT risk management strategy. By employing modern approaches to IT risk management that prioritize agility and continuous improvement, the company aims to stay resilient in the face of ever-evolving IT risks and maintain its competitive edge in the digital age.

### 4.2. COBIT 5 Processing

Furthermore, the mapping of the company's goals with COBIT 5 Enterprise Goals is conducted. The company places a priority on Customer, which is the continuity and availability of business services. This is considered a crucial factor in driving the company's business objectives.

1) Defining Enterprise Goals
Next, we proceeded to map the company's goals with COBIT 5 Enterprise Goals. The company prioritized the Customer aspect, focusing on business service continuity and availability, as it was considered a crucial factor in driving the company's business objectives.

**Table 1. Enterprise Goals Results**

| Enterprise Goals COBIT 5 | |
|---|---|
| **BSC Dimension** | **Enterprise Goals** |
| Customer | Business service continuity and availability |

Table 1 represents the results of mapping Enterprise Goals through discussions with the company. The company placed the highest priority on Customer, specifically business service continuity and availability, as it was considered a crucial factor in driving the company's business objectives.

2) Mapping Enterprise Goals to IT Related Goals
Mapping Enterprise Goals to IT-Related Goals, following the guidelines provided in the COBIT 5 framework, is conducted after determining the company's goal priorities.

**Table 2. IT-Related Goals Results**

| Enterprise Goals COBIT 5 | | Priority | IT Related Goals |
|---|---|---|---|
| *Customer* | Business service continuity and availability | 1 | Managed IT-related business risk. |
| | | | Information security, processing infrastructure, and applications. |
| | | | Availability of reliable and useful information for decision-making. |

Table 2 represents the outcomes obtained from mapping Enterprise Goals to IT-Related Goals. Three IT-Related Goals were selected: managed IT-related business risk, information security, processing infrastructure, and applications, as well as the availability of reliable and useful information for decision-making. After identifying these three IT-Related Goals, the appropriate COBIT 5 processes for assessment can be determined.

3) Mapping IT Related Goals COBIT 5 Processes
Mapping to Enabler Goals with the aim of obtaining the COBIT 5 processes to be assessed. The results obtained from mapping IT-Related Goals to Enabler Goals are as follows: for managed IT-related business risk, 15 COBIT 5 processes were selected; for information security, processing infrastructure, and applications, 5 processes were selected; and for the availability of reliable and useful information for decision-making, 6 processes were selected.

4) COBIT 5 Process Determination
The results of mapping IT Pain Points to COBIT 5 processes show that the selected COBIT 5 processes are:

**Table 3. Mapping IT Pain Points with COBIT 5 Processes**

| No | COBIT 5 Process | Scope |
|---|---|---|
| 1 | APO12 (Manage Risk) | Used to continuously identify, assess, and reduce IT-related risks |
| 2 | DSS05 (Manage Security Services) | Used to maintain the role of information security and monitor company security. |

In Table 3, the selection of these two processes has been directed and approved by the company, as the company currently wants to focus on these two processes.

5) Preparation of RACI Chart and Audit Documents
In this step, an RACI Chart is utilized to designate the parties responsible for the information in the chosen domain during the interview process. During the creation of the RACI Chart, it also refers to the distribution of tasks and authorities within the company's environment.

### 4.3. Data Collection

In this stage, data collection is carried out through interviews and literature review. Interviews are conducted with selected informants based on the RACI Chart, specifically those marked with the letter "R." According to the RACI Chart results, two informants are identified, one from the IT division and one from the planning and system development department. The interviews are structured based on the activities of the chosen COBIT 5 process and the

guidelines outlined in the COBIT 5 ISACA framework. The selected informants provide and respond to each activity with a scoring system ranging from 0 as the lowest value to 100 as the highest value.

### 4.4. Reporting of Results and Recommendations for Improvement

Based on the prioritized COBIT 5 processes obtained in Table 3, the next step is to assess the capability level of processes APO12 (Manage Risk) and DSS05 (Manage Security Services).

1) Measurement Capability Level

The APO12 process aims to integrate the management of IT-related business risk with Enterprise Risk Management (ERM) and balance the costs and benefits of managing IT-related business risk.

**Table 4. APO12 Process Calculation Results Level 3**

| Objective process | Total Rating | |
|---|---|---|
| APO12.01 | 82 | |
| APO12.02 | 85,8 | |
| APO12.03 | 83,9 | |
| **Capability Level Results** | **Total** | 261,7 |
| | **Average** | 83,9 |

In Table 4, the results of the measurement for the APO12 process show that it falls under the "Largely Achieved" criteria at Level 3. The percentages for PA 3.1 and PA 3.2 are 82% and 85.8%, respectively, with an average result of 83.9%. Therefore, the capability level achieved for the APO12 process is Level 3 (Established Process).

The DSS05 process also aims to integrate the management of IT-related business risk with ERM and balance the costs and benefits. Here are the results obtained for the capability assessment of the DSS05 process:

**Table 5. DSS05 Process Calculation Results Level 3**

| Objective process | Total Rating | |
|---|---|---|
| DSS05.01 | 79 | |
| DSS05.02 | 86,67 | |
| DSS05.03 | 82,83 | |
| **Capability Level Results** | **Total** | 248,5 |
| | **Average** | 82,8 |

In Table 5, it can be concluded that the measurement results for the DSS05 process in Figure 4.5 fall within the "Largely Achieved" criteria at Level 3. The percentages for PA 3.1 and PA 3.2 are 79% and 86.67%, respectively, with an average result of 82.83%. Hence, the capability level achieved for the DSS05 process is Level 3 (Established Process).

2) Counting Gap Analysis

The next step is the gap analysis, which is necessary to determine the extent of the gap or discrepancy between the current capability level (as is) and the expected capability level (to be) as desired by the company. Based on discussions within the company, the target capability level expected by the company has been determined.

**Table 6. Company's Condition for the APO12 Process**

| Current State | Future State |
|---|---|
| Lack of documentation related to loss data analysis and available trends, both internal and external. | Utilized to identify, assess, and designate the Person in Charge (PIC) to deal directly with loss analysis and documentation creation. |
| Incomplete documentation regarding the dependency on IT service | Designating a Person in Charge (PIC) responsible for managing documentation |

| | |
|---|---|
| management processes and IT infrastructure resources. | of IT service management processes and IT infrastructure resources. |
| Partial implementation of methods to monitor the effectiveness and compliance of risk management design has been running effectively. | Ensuring the monitoring methods for risk management design have been effectively implemented. |

Table 6 shows the current state of the company, which is at level 3 (Established), and the future state at level 4 (Predictable) for the APO12 (Manage Risk) process.

**Table 7. Company's Condition for the DSS05 Process**

| Current State | Future State |
|---|---|
| Absence of Standard Operating Procedures (SOP) related to data encryption. | Creation of SOP for data encryption, using cryptographic algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) for data security. And monitoring when implementing these algorithms. |
| Documentation related to dependencies. Partial implementation of methods to monitor the effectiveness and compliance of information security service design has been effective. | Ensuring that monitoring methods for information security service design are running effectively. |
| Partial implementation of methods to monitor the effectiveness and compliance of risk management design has been effective. | Ensuring that monitoring methods for risk management design are running effectively. |

Table 7 illustrates the company's current status at Level 3 (Established) and the future status at Level 4 (Predictable) for the DSS05 (Manage Security Services) process.

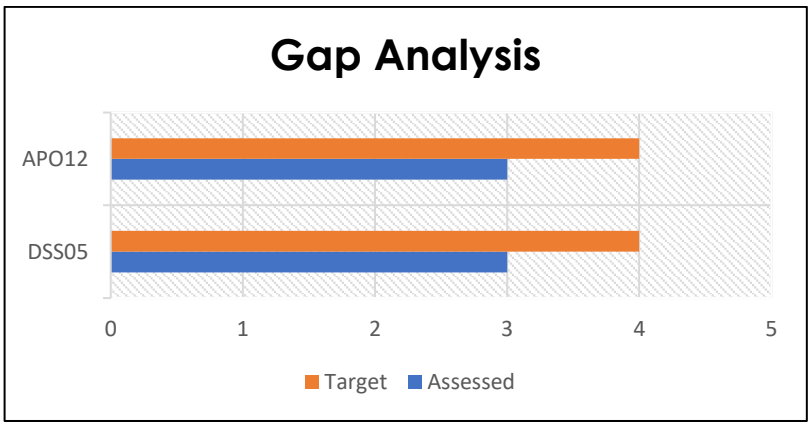


**Figure 2. Gap Analysis Chart**

In Figure 2, the results of the gap analysis for processes APO12 (Manage Risk) and DSS05 (Manage Security Services) reveal that both processes currently operate at Level 3 (Established) but aim to reach Level 4 (Predictable). As a consequence, the identified gap or disparity is found to be at a magnitude of 1. This indicates that there is a specific need for improvement and advancement to bridge the gap and elevate these processes to the desired Level 4 maturity.

3) Recommendations

These recommendations aim to address the findings in the short term. Improvement suggestions for the APO12 and DSS05 processes will be elaborated based on the findings and impacts. To achieve Level 4 (Predictable) in the APO12 and DSS05 processes, these recommendations emphasize the need to enhance data integration

and risk analysis, as well as implement more proactive security solutions. Furthermore, it is essential to strengthen collaboration between the IT division and the planning and development departments. In the short term, these improvements will help reduce uncertainty and enhance efficiency in managing risks and security services. Thus, processes APO12 and DSS05 will be better prepared to achieve the desired maturity level.

**Table 8. APO12 Level 4 Process Improvement Recommendations**

| Process | Recommendations |
|---|---|
| APO12.01 | To ensure the effectiveness of risk management, critical steps need to be taken. These include ensuring that risk management supports business objectives, aligning effectiveness measurements with information needs, setting performance targets, measuring in line with those targets, regularly collecting, analyzing, and reporting measurement results, and evaluating the overall process performance. Thus, risk management can optimally support the company's business objectives. |
| APO12.02 | To ensure the effectiveness of risk management implementation, steps such as defining analysis and control techniques, setting control limits, analyzing measurement data, addressing special causes, and adjusting control limits when necessary are required. This will make risk management implementation more efficient and responsive to changes. |

In Table 8, recommendations for improving the APO12 (Manage Risk) process to Level 4 (Predictable) have been presented to the company. These recommendations are based on the COBIT 5 self-assessment framework, providing a framework for measuring and enhancing process maturity. The recommendations include concrete steps that can be taken to achieve higher maturity levels in risk management, such as improved data integration, deeper risk analysis, and enhanced proactive security solutions. By following the COBIT 5 guidelines, the company can be more effective in achieving its goals and enhancing risk management.

**Table 9. DSS05 Level 4 Process Improvement Recommendations**

| Process | Recommendations |
|---|---|
| DSS05.01 | To ensure the effectiveness of information security services, it's necessary to align service objectives with business needs, set quantitative targets, identify measurement criteria and frequency, and regularly collect, analyze, and report measurement results. Evaluating the performance measurement results of information security services is also essential for process performance characterization. Thus, information security services can be optimized in line with the company's business objectives. |
| DSS05.02 | To ensure the effectiveness of information security services, it is necessary to define analysis and control techniques and set appropriate control boundaries. Analyzing measurement data is required to detect special causes and take corrective action as necessary, as well as adjusting control boundaries afterward. This way, the implementation of information security services will be more responsive to changes. |

In Table 9, recommendations for improving the DSS05 (Manage Security Services) process to Level 4 (Predictable) have been conveyed to the company. These recommendations are based on the COBIT self-assessment framework, providing guidance and a framework for measuring and enhancing process maturity. The

recommendations encompass concrete steps that can be taken to achieve higher maturity levels in managing security services. By following the COBIT guidelines, the company can be more effective in achieving its goals and improving security service management efficiently and responsively to changes.

## 5.0 CONCLUSION

The evaluation of information technology risk management at the company using the COBIT 5 framework, focusing on the APO12 (Manage Risk) and DSS05 (Manage Security Services) processes, has proven that the company has expected capability targets at Level 4 (Predictable) for both processes. However, the measurement results using the COBIT 5 framework standards indicate that the company has only achieved Level 3 (Established) in the execution of the APO12 and DSS05 processes. During the audit process, several critical findings affecting the achievement of capability targets were identified. For example, the lack of effective data integration and in-depth risk analysis in risk management. There is also a need to enhance proactive security solutions in the DSS05 process. In addition to the aforementioned findings, the evaluation of information technology risk management also highlights the importance of improving more effective data integration among related departments. There are challenges in terms of communication and collaboration between teams that affect a comprehensive understanding of information technology risks. Therefore, improvements in inter-departmental communication and collaboration are crucial for better information technology risk management. These findings provide the basis for the improvement recommendations given to address the existing gaps and ensure that the company achieves its established objectives. The goal is to ensure that the company can better meet its business objectives and maintain information security services at the desired level, following the COBIT 5 framework. As a result, appropriate improvement measures can be taken to enhance risk management performance within the company, allowing information technology risks to be managed more effectively and in line with the company's business objectives.

## REFERENCES


[1] F. Salehi, B. Abdollahbeigi, and S. Sajjady, "Impact of Effective IT Governance on Organizational Performance and Economic Growth in Canada," vol. 3, pp. 14–19, Feb. 2021.

[2] I. Scalabrin Bianchi, R. Sousa, and R. Pereira, "Information Technology Governance for Higher Education Institutions: A Multi-Country Study," *Informatics*, vol. 8, p. 26, Apr. 2021, doi: 10.3390/informatics8020026.

[3] W. Santos Castellanos, "Impact of Information Technology (IT) Governance on Business-IT Alignment," *Cuadernos de Gestión*, vol. 2020-12–10, Dec. 2020, doi: 10.5295/cdg.180995ws.

[4] D. Smits and J. Hillegersberg, "The development of a hard and soft IT governance assessment instrument," *Procedia Comput Sci*, vol. 121, pp. 47–54, Jan. 2017, doi: 10.1016/j.procs.2017.11.008.

[5] A. Nurdin and M. Lubis, "The IT Governance Measurement using Cobit 5 Framework in Quality Assurance Department," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 5, p. 80, Mar. 2023, doi: 10.36499/jinrpl.v5i1.7963.

[6] E. Alsaleem and N. Husin, "The Impact of Information Technology Governance Under Cobit-5 Framework on Reducing the Audit Risk in Jordanian Companies," *International Journal of Professional Business Review*, vol. 8, p. e01236, Feb. 2023, doi: 10.26668/businessreview/2023.v8i2.1236.

[7] A. Asmah and M. Kyobe, *Towards an Integrative Theoretical Model For Examining IT Governance Audits*. 2018. doi: 10.1145/3209415.3209423.

[8] A. Nurdin and M. Lubis, "The IT Governance Measurement using Cobit 5 Framework in Quality Assurance Department," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 5, p. 80, Mar. 2023, doi: 10.36499/jinrpl.v5i1.7963.

[9] H. Nugroho, "Proposed IT Governance at Hospital Based on COBIT 5 Framework," *IJAIT (International Journal of Applied Information Technology)*, vol. 1, p. 52, Aug. 2017, doi: 10.25124/ijait.v1i02.875.

[10] D. Putri, J. Juwairiah, and F. Kodong, "Capability Level Analysis of IT Governance Using COBIT 5 on Continuity and Availability Of Services (Case Study: LMS Spada Wimaya)," *Telematika*, vol. 19, p. 283, Oct. 2022, doi: 10.31315/telematika.v19i3.7059.
[11] N. Mutia and R. Nur'ainy, "IT GOVERNANCE: MEASURE CAPABILITY LEVEL USING COBIT 5 FRAMEWORK," *Jurnal Ilmiah Ekonomi Bisnis*, vol. 25, pp. 97–110, Aug. 2020, doi: 10.35760/eb.2020.v25i2.2609.
[12] D. Sanjaya and M. I. Fianty, "Measurement of Capability Level Using COBIT 5 Framework (Case Study: PT Andalan Bunda Bijak)," *Ultima Infosys : Jurnal Ilmu Sistem Informasi*, vol. 13, no. 2, 2022.
[13] A. A. Louis and M. I. Fianty, "Evaluation Human Resources Information System Using COBIT 5 Framework in Technology Insurance Company," *G-Tech: Jurnal Teknologi Terapan*, vol. 7, no. 2, pp. 674–682, Mar. 2023, doi: 10.33379/gtech.v7i2.2393.
[14] Y. Bounagui, A. Mezrioui, and H. Hafiddi, "Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models," *Comput Stand Interfaces*, vol. 62, pp. 98–118, Sep. 2018, doi: 10.1016/j.csi.2018.09.001.
[15] K. Pratama Arthananda, "The Role of COBIT5 as a Reference for Quality Service Quality Improvement Case Study: Private Bank in Indonesia," *Ultima Infosys : Jurnal Ilmu Sistem Informasi*, vol. 12, no. 2, 2021.
[16] A. Amorim, M. Mira da Silva, R. Pereira, and M. Gonçalves, "Using agile methodologies for adopting COBIT," *Inf Syst*, vol. 101, p. 101496, Feb. 2020, doi: 10.1016/j.is.2020.101496.
[17] A. Tantiono and D. Legowo, "Information System Governance in Higher Education Foundation using COBIT 5 Framework," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 2798–2811, Mar. 2020, doi: 10.35940/ijrte.F8192.038620.
[18] F. Muttaqin, M. Idhom, F. Akbar, M. Swari, and E. Putri, "Measurement of the IT Helpdesk Capability Level Using the COBIT 5 Framework," *J Phys Conf Ser*, vol. 1569, p. 022039, Jul. 2020, doi: 10.1088/1742-6596/1569/2/022039.
[19] D. Putra and M. I. Fianty, "Capability Level Measurement of Information Systems Using COBIT 5 Framework in Garment Company," *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 333–346, Mar. 2023, doi: 10.51519/journalisi.v5i1.454.
[20] S. Haes, W. Grembergen, A. Joshi, and T. Huygh, "Enterprise Governance of IT, Alignment, and Value," 2020, pp. 1–13. doi: 10.1007/978-3-030-25918-1_1.
[21] R. Frogeri, D. Pardini, A. Cardoso, L. Prado, F. Pelloso Piurcosky, and P. Portugal Júnior, "IT Governance in SMEs: The State of Art," *International Journal of IT/Business Alignment and Governance*, vol. 10, pp. 55–73, Jan. 2019, doi: 10.4018/IJITBAG.2019010104.
[22] L. Englbrecht, S. Meier, and G. Pernul, "Towards a capability maturity model for digital forensic readiness," *Wireless Networks*, vol. 26, pp. 4895–4907, Oct. 2020, doi: 10.1007/s11276-018-01920-5.
[23] S. Saeedinezhad and A. Naghsh, "Management of IT Services in the Field of Pre-Hospital Emergency Management with the Combined Approach of COBIT Maturity Model and ITIL Framework: A Conceptual Model," 2019.
[24] A. Levstek, T. Hovelja, and A. Pucihar, "IT Governance Mechanisms and Contingency Factors: Towards an Adaptive IT Governance Model," *Organizacija*, vol. 51, pp. 286–310, Dec. 2018, doi: 10.2478/orga-2018-0024.