
Capability Level Evaluation of Information Security Using COBIT 2019 AP013 and DSS05: A Case Study of the E-Mansinam Safety Patrol System

Asrawati¹, Lorna Yertas Baisa¹, Alex De Kweldju¹

^{1,2,3}University of Papua, Faculty of Engineering, Informatics Engineering, Jl. Gunung Salju, Amban, Manokwari, Papua Barat 98314, Indonesia

Article History

Submitted: 26-06-2026

Revised: 15-07-2026

Accepted: 20-07-2026

Published: 18-09-2026

DOI: 10.32664/j-intech.v14i03.2435

Keywords

AP013; COBIT 2019; Capability Level; DSS05; Information Security Governance; Root Cause Analysis.

***Corresponding Author:**

asrawati658@gmail.com

Abstract

The increasing reliance on digital information systems has made information security governance a critical requirement for maintaining secure and reliable organizational operations. PT Pertamina Patra Niaga Fuel Terminal Manokwari utilizes the Safety Patrol feature within the E-Mansinam Website to support Health, Safety, Security, and Environment (HSSE) activities, including hazard reporting, safety monitoring, and corrective action management. This study evaluates the information security governance capability of the Safety Patrol feature using the COBIT 2019 framework, focusing on the AP013 (Managed Security) and DSS05 (Managed Security Services) domains. A descriptive quantitative approach was employed through observations, interviews, questionnaires, and documentation. The collected data were analyzed using Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA). The results show that the AP013 domain achieved an average capability level of 4.04, exceeding the organization's target of Level 4, whereas the DSS05 domain achieved an average capability level of 3.93, indicating that several operational security service processes require further improvement. The largest capability gap was identified in DSS05.07 with a gap value of 0.44. Root Cause Analysis revealed that inconsistent security monitoring, incomplete documentation, limited periodic evaluations, and varying levels of personnel awareness were the primary factors contributing to the identified capability gaps. Based on these findings, this study proposes practical recommendations to strengthen information security governance and support the continuous improvement of the Safety Patrol feature, particularly in operational security service management.

1. Introduction

The increasing adoption of information technology has transformed how organizations conduct operational activities, manage information, and support strategic decision-making. Information systems enable organizations to improve operational efficiency, facilitate information accessibility, and enhance service quality. However, these benefits can only be fully realized when information technology is governed effectively to

ensure that technology initiatives remain aligned with organizational objectives and generate sustainable business value. Consequently, information technology governance has become an essential element for improving organizational performance and ensuring that IT investments support business strategies, as emphasized by [1].

As organizations become increasingly dependent on digital systems, protecting information assets has become a major challenge. Security threats, including unauthorized access, malware attacks, data leakage, misuse of user privileges, and system failures, may disrupt organizational operations and compromise the confidentiality, integrity, and availability of information. Therefore, organizations are required to continuously evaluate and strengthen their information security controls to minimize security risks and maintain operational reliability. Many organizations still experience weaknesses in implementing information security management, highlighting the importance of continuous monitoring and periodic security evaluation[2].

Information security is particularly critical in the energy sector because operational activities involve high-risk environments where system failures may affect occupational safety, environmental protection, and business continuity. In oil and gas operations, safety management requires systematic monitoring, effective reporting mechanisms, and continuous risk control. Occupational health and safety management within PT Pertamina emphasizes safety supervision, operational risk management, and continuous monitoring to establish a safe working environment[3]. Likewise, organizational safety performance depends not only on safety culture and compliance with operational procedures but also on continuous evaluation processes that support sustainable improvement[4].

PT Pertamina Patra Niaga Fuel Terminal Manokwari supports its Health, Safety, Security, and Environment (HSSE) program through the E-Mansinam Website, an internal information system that facilitates operational reporting and monitoring activities. This study specifically focuses on the Safety Patrol feature within the E-Mansinam Website, which is used to record workplace hazards, unsafe conditions, corrective actions, and follow-up activities. The feature enables safety-related information to be documented systematically while supporting monitoring and operational decision-making processes [5]. Although the E-Mansinam Website operates within the broader organizational information system environment, this research does not evaluate the entire E-Mansinam system or the overall information technology governance of PT Pertamina Patra Niaga Fuel Terminal Manokwari. Instead, the evaluation is limited to information security processes, controls, and practices that are directly related to the operation, management, and protection of the Safety Patrol feature.

Considering the importance of the Safety Patrol feature in supporting operational safety, maintaining the security of its information assets is essential. Information processed within the system must remain confidential, accurate, and continuously available to authorized personnel. Therefore, evaluating the effectiveness of information security governance is necessary to determine the current capability of security processes and identify areas requiring further improvement.

Among the available information technology governance standards, COBIT 2019 is a recognized framework widely used for assessing IT governance capability and information security management. It was developed to provide comprehensive governance objectives and capability assessment mechanisms that enable organizations to evaluate process performance systematically[6].

This study focuses on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains because these domains are the most relevant to the information security requirements and operational characteristics of the Safety Patrol feature within the E-Mansinam Website. The Safety Patrol feature manages safety-related information, including hazard reports, unsafe conditions, corrective actions, and follow-up activities, which require appropriate information security practices to ensure confidentiality, integrity, availability, and reliable operational support. Therefore, APO13 and DSS05 were selected to assess the implementation of information security management processes and operational security controls related specifically to the Safety Patrol feature.

AP013 (Managed Security) aims to establish and maintain an information security management system by ensuring that security policies, practices, and controls are implemented and continuously improved[6]. Meanwhile, DSS05 (Managed Security Services) focuses on protecting enterprise information through operational security services, including identity and access management, security monitoring, vulnerability

management, and protection of information assets. These objectives provide an appropriate basis for evaluating security-related processes that support the operation and protection of the Safety Patrol feature within the E-Mansinam Website.

Although other COBIT 2019 governance and management objectives, such as APO12 (Managed Risk) and DSS01 (Managed Operations), are also related to organizational processes, their primary focus is enterprise risk management and general IT service operations. In contrast, this study specifically evaluates information security management and operational security services associated with the Safety Patrol feature. Therefore, APO13 and DSS05 were selected as the most appropriate domains for assessing the security capability of the selected system component within its operational context.

The expected capability level in this study was established at Capability Level 4 (Predictable Process) based on interviews with relevant organizational stakeholders involved in the management and utilization of the Safety Patrol feature at PT Pertamina Patra Niaga Fuel Terminal Manokwari. The stakeholders indicated that the Safety Patrol feature is expected to operate through information security processes that are measurable, consistently implemented, and effectively controlled to support operational activities and Health, Safety, Security, and Environment (HSSE) objectives. This expectation aligns with the COBIT 2019 Performance Management model[6], which defines Capability Level 4 (Predictable Process) as a process that is quantitatively measured, monitored, and controlled to achieve consistent and predictable performance. Therefore, Capability Level 4 was not assumed as an ideal maturity target, but was determined based on organizational expectations and used as the benchmark for evaluating the current capability level of information security processes related to the Safety Patrol feature.

Several previous studies have demonstrated the effectiveness of COBIT 2019 in evaluating information security governance. The APO13 and DSS05 domains have been shown to effectively measure organizational information security capability while identifying capability gaps that require continuous improvement[7]. Similarly, both domains provide a structured approach for assessing information security management and identifying weaknesses within security processes[8]. Furthermore, periodic security assessments are necessary to ensure the effectiveness of organizational security controls[2].

Despite these contributions, previous studies have primarily focused on assessing information security capability levels and identifying capability gaps within various organizational contexts. Several studies have also applied additional analyses, such as root cause identification, to support the development of improvement recommendations. Therefore, this study does not claim the integration of Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA) as its primary novelty. Instead, the contribution of this research lies in the specific application context, namely the evaluation of information security capability related to the Safety Patrol feature within the E-Mansinam Website at PT Pertamina Patra Niaga Fuel Terminal Manokwari using the COBIT 2019 APO13 (Managed Security) and DSS05 (Managed Security Services) domains. Based on the reviewed literature, previous studies have not specifically examined this operational safety information system component within the context of an energy sector organization. This study extends existing research by assessing the current capability level, identifying capability gaps, analyzing their underlying causes, and formulating improvement recommendations that are tailored to the operational requirements of the Safety Patrol feature.

Accordingly, this study aims to evaluate the information security capability of the Safety Patrol feature within the E-Mansinam Website using the COBIT 2019 framework, focusing on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains. The assessment identifies the current capability levels, measures the gap between existing conditions and the expected Capability Level 4 (Predictable Process), and applies Root Cause Analysis (RCA) to determine the underlying factors affecting capability gaps. Based on these findings, this study formulates improvement recommendations to strengthen information security governance and enhance operational security services for the Safety Patrol feature at PT Pertamina Patra Niaga Fuel Terminal Manokwari.

2. Research Method

This study employed a descriptive quantitative approach to evaluate the information security capability of the Safety Patrol feature within the E-Mansinam Website at PT Pertamina Patra Niaga Fuel Terminal Manokwari. Quantitative research emphasizes the systematic analysis of numerical data to explain research phenomena objectively[9].

The evaluation was conducted using the COBIT 2019 framework, focusing on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains. Data were collected through observations, interviews, questionnaires, and documentation. Respondents were selected using the RACI Chart approach to ensure that the assessment involved stakeholders with appropriate roles and responsibilities related to the Safety Patrol feature. The assessment procedure was adapted from [8].

The collected data were analyzed through Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA). Prior to the capability assessment, the questionnaire instrument was evaluated using validity and reliability tests to ensure the accuracy and consistency of the collected data. The overall research procedure adopted in this study is presented in Figure 1.

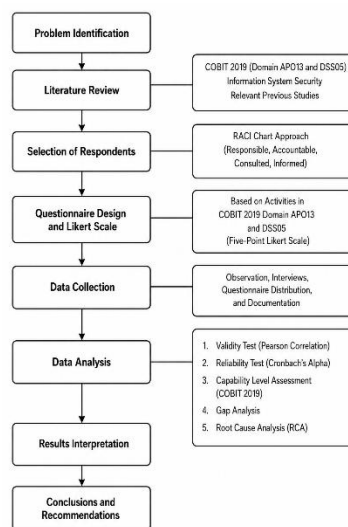


Figure 1. Research Procedure

Figure 1 illustrates the research procedure followed in this study. The process began with problem identification and literature review, followed by respondent selection using the RACI Chart approach. The questionnaire was then designed based on the APO13 and DSS05 domains of COBIT 2019 using a five-point Likert scale. Data were collected through observations, interviews, questionnaires, and documentation. Subsequently, the collected data were analyzed using validity testing, reliability testing, Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA). Finally, the results were interpreted to formulate conclusions and recommendations for improving information security governance.

2.1 Respondent Selection

Respondents were selected using the RACI Chart (Responsible, Accountable, Consulted, and Informed) approach recommended by the COBIT 2019 framework to identify stakeholders directly involved in the governance and management of the Safety Patrol feature within the E-Mansinam Website. The RACI Chart facilitates the identification of stakeholder roles and responsibilities, thereby improving the reliability of capability assessments[10]. Previous studies [11], [12], and [13] also adopted the RACI approach to ensure that respondents possessed relevant knowledge and responsibilities in information technology governance evaluations.

Based on the stakeholder mapping process using the RACI Chart, this study involved 20 respondents representing organizational roles directly associated with the operation, administration, supervision, and

information security management of the Safety Patrol feature at PT Pertamina Patra Niaga Fuel Terminal Manokwari. The respondent composition was determined according to each stakeholder's roles and responsibilities in the implementation and oversight of the Safety Patrol feature rather than by equal representation across organizational positions. The distribution of respondents is presented in Table 1.

Table 1. Distribution of Respondents

No.	Position	Number of Respondents
1	Fuel Terminal Supervisor	4
2	System Administrator	2
3	HSSE Officer	3
4	Security Personnel	10
5	Military Assistance Personnel (BKO TNI)	1
Total		20

Based on the RACI stakeholder mapping, Security Personnel constituted the largest respondent group because they are the primary users of the Safety Patrol feature and are directly responsible for conducting safety patrol activities, reporting workplace hazards, verifying field conditions, implementing corrective actions, and interacting with the system on a daily basis. Consequently, they possess direct operational knowledge of how information security controls are implemented within the Safety Patrol feature.

Although Security Personnel represented 50% of the respondents, the capability assessment was not based solely on their responses. Responses from Fuel Terminal Supervisors, System Administrators, HSSE Officers, and Military Assistance Personnel (BKO TNI), who are responsible for supervision, system administration, policy implementation, and security oversight, were also incorporated into the assessment. The inclusion of respondents from multiple organizational roles was intended to ensure that both operational and governance perspectives were adequately represented, thereby reducing the potential for assessment bias and maintaining consistency with the stakeholder mapping defined through the RACI Chart.

2.2 Data Collection

Data were collected through observations, interviews, questionnaires, and documentation to obtain information regarding the implementation of information security governance within the Safety Patrol feature of the E-Mansinam Website. Observations and interviews were conducted to understand operational processes, governance practices, and information security management practices. In addition, interviews were conducted to identify the organization's expected capability level for information security processes, which served as the benchmark for the capability assessment and gap analysis. Documentation was used to verify and support the information obtained from observations and interviews. Combining multiple data collection techniques improves the reliability and accuracy of COBIT 2019 capability assessments[6]. Similar approaches have also been adopted by [14] and [12] in evaluating information technology governance.

The questionnaire served as the primary instrument for collecting quantitative data. It was developed based on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains of the COBIT 2019 framework and distributed to respondents selected using the RACI Chart approach. The collected data were subsequently used for Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA) to evaluate the current state of information security governance and formulate improvement recommendations.

2.3 Likert Scale

A five-point Likert scale was used to measure respondents' perceptions of the implementation of information security governance within the Safety Patrol feature of the E-Mansinam Website. The Likert scale is widely applied in COBIT 2019-based assessments because it enables respondents to express their level of agreement systematically and facilitates quantitative analysis. Previous studies by [14], [15], and [16] also employed a five-point Likert scale to assess information technology governance capability. The response categories and corresponding scores used in this study are presented in Table 2.

Table 2. Likert Scale

Response Category	Score
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

The questionnaire scores were subsequently used to calculate the capability levels of the APO13 (Managed Security) and DSS05 (Managed Security Services) domains. These results served as the basis for the Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA) conducted in this study.

2.4 Validity Test

The validity test was conducted to determine whether each questionnaire item accurately measured the intended research construct. Questionnaire validity was assessed using the Pearson Product Moment correlation method. An item is considered valid when the calculated correlation coefficient (r_{count}) exceeds the critical value (r_{table}) [9]. The Pearson Product Moment formula used in this study is presented in Equation (1).

$$r_{xy} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{[n\sum X^2 - (\sum X)^2][n\sum Y^2 - (\sum Y)^2]}}$$

where r_{xy} is the correlation coefficient, X is the score of each questionnaire item, Y is the total questionnaire score, and n is the number of respondents.

2.5 Reliability Test

The reliability test was performed to evaluate the internal consistency of the questionnaire using Cronbach's Alpha. An instrument is considered reliable when the Cronbach's Alpha coefficient exceeds **0.70** [9]. The application of Cronbach's Alpha has also been widely adopted in COBIT 2019 studies, including those conducted by [17], and [14]. The Cronbach's Alpha formula is presented in Equation (2).

$$\alpha = \frac{k}{k-1} \left(1 - \frac{\sum \sigma_i^2}{\sigma_t^2} \right)$$

where α represents the Cronbach's Alpha coefficient, k is the number of questionnaire items, σ_i^2 is the variance of each item, and σ_t^2 is the total variance.

2.6 Capability Level Assessment

The capability level assessment was conducted using the COBIT 2019 framework, focusing on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains. Capability levels measure the extent to which governance and management processes achieve their intended objectives, as defined by ISACA [6]. Similar questionnaire-based capability assessment approaches have been adopted by previous studies [18], [19], [20], and [21].

Questionnaire responses were collected using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Each questionnaire item represented governance and management practices within the APO13 and DSS05 domains. The responses were converted into numerical values ranging from 1 to 5, and the average score for each process was calculated using Equation (3).

$$CL = \frac{\sum X}{n}$$

where:

- CL = Average capability score
- $\sum X$ = Total score obtained from respondents
- n = Number of respondents

The resulting average questionnaire score was used to represent the degree of implementation of governance and management practices based on stakeholder perceptions. This questionnaire-based measurement approach has been widely adopted in empirical COBIT 2019 studies to evaluate governance process implementation through stakeholder perceptions [19]–[21]. Accordingly, the capability assessment in this study reflects stakeholders' perceptions of the implementation of governance and management practices rather than a formal COBIT 2019 process capability assessment based on process attribute achievement.

To facilitate interpretation, the average questionnaire scores were first classified according to the interpretation criteria presented in Table 3. These interpretation criteria describe the extent to which governance and management practices have been implemented and were not treated as direct COBIT 2019 capability levels.

The interpreted average questionnaire scores were subsequently compared with the qualitative capability level definitions provided in the COBIT 2019 Performance Management model (Table 4) to determine the capability level that best represented each evaluated governance and management process. Therefore, the capability levels reported in this study represent an interpretation of the implementation status of each evaluated process rather than a direct numerical conversion of Likert-scale scores into COBIT 2019 capability levels.

Table 3. Interpretation Criteria for Average Questionnaire Scores

Average Score	Interpretation	Description
1.00–1.80	Very Low	Governance and management practices are implemented at a very low level and require substantial improvement.
1.81–2.60	Low	Governance and management practices are implemented only to a limited extent and require significant improvement.
2.61–3.40	Moderate	Governance and management practices have been implemented but are not yet consistent and require further improvement.
3.41–4.20	High	Governance and management practices are generally implemented consistently and provide adequate support for organizational objectives, although opportunities for further improvement remain.
4.21–5.00	Very High	Governance and management practices are implemented consistently and effectively, indicating a high degree of process implementation.

The qualitative capability level definitions used as the reference for interpreting the questionnaire results are presented in Table 4.

Table 4. COBIT 2019 Capability Levels

Level	Description
0	Incomplete Process
1	Performed Process
2	Managed Process
3	Established Process
4	Predictable Process
5	Optimizing Process

2.7 Gap Analysis

Gap Analysis was performed to compare the current capability level with the expected capability level established by the organization. Gap Analysis identifies discrepancies between current process performance and organizational objectives [6]. Similar approaches have been reported by [22], [23], and [16]. The gap value was calculated using Equation (4).

$$\text{Gap} = \text{Expected Capability Level} - \text{Current Capability Level}$$

where:

Gap = Difference between the expected and current capability levels

Expected Capability Level = Target capability level established by the organization

Current Capability Level = Capability level obtained from the assessment results

The results were used to identify capability gaps and determine priority areas for improvement.

2.8 Root Cause Analysis (RCA)

Root Cause Analysis (RCA) was conducted to identify the underlying causes of the capability gaps revealed by the Gap Analysis. In this study, the 5-Why analysis technique was employed as the structured RCA method to systematically investigate the factors contributing to capability gaps within the APO13 and DSS05 domains. The 5-Why technique identifies the underlying causes of organizational problems through iterative questioning until the fundamental causes are identified, thereby supporting the development of effective corrective actions [6], [24], [25].

Previous studies by [14], [8], [26], and [27] also applied Root Cause Analysis to identify organizational, procedural, and technical factors affecting information security governance capability and to formulate evidence-based improvement recommendations. In this study, the identified capability gaps were analyzed using interview results, observation findings, and supporting organizational documentation. The resulting root causes were subsequently linked to specific improvement recommendations to support the continuous improvement of information security governance within the APO13 and DSS05 domains. The structured RCA results are presented in Table 5.

Table 5. Root Cause Analysis Results Using the 5-Why Technique

COBIT 2019 Sub-Domain	Identified Capability Gap	Root Cause Identified through 5-Why Analysis	Evidence Source	Improvement Recommendation
APO13.02 – Manage Information Security Risk	Information security risk management has not consistently achieved the expected capability level.	Information security policies and risk treatment procedures are available but are not reviewed and updated periodically to reflect operational changes.	Interview results and organizational documentation.	Conduct periodic reviews of information security policies and update risk treatment procedures based on operational requirements and emerging security risks.
DSS05.03 – Manage Endpoint Security	Endpoint security capability remains below the expected capability level.	Software updates, antivirus management, and vulnerability assessments are not performed consistently across organizational devices.	Observation results and interviews with system administrators.	Establish periodic endpoint maintenance, centralized antivirus management, routine software updates, and vulnerability scanning.

COBIT 2019 Sub-Domain	Identified Capability Gap	Root Cause Identified through 5-Why Analysis	Evidence Source	Improvement Recommendation
DSS05.05 – Manage Physical Access to IT Assets	Physical access management has not consistently achieved the target capability level.	Physical access authorization and visitor control procedures are implemented but are not consistently documented and periodically audited.	Documentation review and interviews with HSSE personnel.	Strengthen physical access control procedures, improve visitor authorization mechanisms, and conduct regular physical access audits.
DSS05.06 – Manage Sensitive Documents and Output Devices	Secure handling of sensitive documents and output devices is not yet fully standardized.	Standard operating procedures for handling sensitive documents are implemented inconsistently and compliance evaluations are conducted infrequently.	Interviews with operational personnel and document review.	Develop standardized document handling procedures and conduct periodic compliance evaluations for sensitive information management.
DSS05.07 – Manage Security Monitoring	Security monitoring recorded the largest capability gap among all assessed sub-domains.	Continuous security monitoring, incident reporting, and security awareness activities have not been implemented systematically, resulting in inconsistent monitoring and delayed identification of security issues.	Interview findings, observation results, and incident documentation review.	Implement continuous security monitoring, strengthen incident reporting procedures, conduct periodic security awareness training for Safety Patrol users, and perform regular evaluations of monitoring activities to support continuous improvement.

3. Result and Discussions

3.1 Respondent Characteristics

A total of 20 respondents participated in this study. All respondents were selected using the total sampling technique because they were directly involved in operating, managing, and supervising the Safety Patrol feature within the E-Mansinam Website. The distribution of respondents is presented in Table 6.

Table 6. Respondent Characteristics

Category	Characteristics	Frequency	Percentage (%)
Position	System Administrator	2	10
	Fuel Terminal Supervisor	4	20
	HSSE Officer	3	15
	Security Personnel	10	50
	Military Support Personnel (BKO TNI)	1	5

Category	Characteristics	Frequency	Percentage (%)
	Total	20	100
Length of Use	< 1 Year	9	45
	1–3 Years	7	35
	> 3 Years	4	20
	Total	20	100

As presented in Table 6, Security Personnel represented the largest respondent group (50%), reflecting their primary responsibility for conducting safety patrol activities and reporting workplace hazards through the Safety Patrol feature. This distribution indicates that the assessment primarily captured responses from personnel who routinely interact with the system during daily operations.

Regarding system experience, 45% of respondents had used the Safety Patrol feature for less than one year, while the remaining respondents had between one and more than three years of experience. Although respondents with shorter system experience constituted the largest proportion of the sample, all participants were selected using the COBIT 2019 RACI stakeholder mapping approach based on their organizational roles and responsibilities rather than the duration of system usage. Consequently, every respondent was directly involved in the operation, supervision, administration, or information security management of the Safety Patrol feature and was therefore considered capable of providing relevant information for the capability assessment.

Nevertheless, this study acknowledges that the relatively small number of respondents (20 participants) and the proportion of respondents with less than one year of system experience constitute limitations of the study. Although the sample size reflects the actual organizational structure and includes all stakeholders directly responsible for the governance and operation of the Safety Patrol feature at PT Pertamina Patra Niaga Fuel Terminal Manokwari, respondents with shorter system experience may have had more limited exposure to certain governance and management practices assessed within the APO13 and DSS05 domains. Therefore, the assessment results should be interpreted within the context of this organizational case study and should not be generalized to other organizations without considering differences in organizational structure and operational context. Future studies involving multiple fuel terminals or larger organizational units with a broader range of respondents are recommended to provide more comprehensive evidence regarding information security capability across similar operational environments.

3.2 Validity Test Results

The validity of the questionnaire was evaluated using the Pearson Product Moment correlation method. A questionnaire item was considered valid when the calculated correlation coefficient (r-count) exceeded the critical value (r-table = 0.444). The results of the validity test are presented in Table 7.

Table 7. Results of the Validity Test

Sub-Domain	Number of Items	r-count	r-table	Result
AP013.01	5	0.770–0.871	0.444	Valid
AP013.02	5	0.777–0.765	0.444	Valid
AP013.03	5	0.860–0.877	0.444	Valid
DSS05.01	3	0.946–0.961	0.444	Valid
DSS05.02	4	0.757–0.759	0.444	Valid
DSS05.03	3	0.925–0.869	0.444	Valid
DSS05.04	3	0.914–0.804	0.444	Valid
DSS05.05	2	0.946–0.951	0.444	Valid
DSS05.06	4	0.880–0.782	0.444	Valid
DSS05.07	4	0.777–0.864	0.444	Valid

As presented in Table 7, all questionnaire items produced r-count values greater than the required r-table value (0.444), indicating that every item satisfied the validity criterion. This result demonstrates that the questionnaire was capable of measuring the intended constructs within the APO13 and DSS05 domains. Similar findings have been reported in previous COBIT 2019 studies by [8] and [28], which confirmed that valid measurement instruments are fundamental for obtaining reliable capability assessment results.

3.3 Reliability Test Results

The reliability of the questionnaire was evaluated using Cronbach's Alpha. An instrument is considered reliable when the Cronbach's Alpha coefficient exceeds 0.70. The reliability test results for each sub-domain are presented in Table 8.

Table 8. Results of the Reliability Test

Sub-Domain	Cronbach's Alpha	Reliability Threshold	Result
AP013.01	0.8505	0.70	Reliable
AP013.02	0.8911	0.70	Reliable
AP013.03	0.8885	0.70	Reliable
DSS05.01	0.9418	0.70	Reliable
DSS05.02	0.8127	0.70	Reliable
DSS05.03	0.8527	0.70	Reliable
DSS05.04	0.9136	0.70	Reliable
DSS05.05	0.8889	0.70	Reliable
DSS05.06	0.8843	0.70	Reliable
DSS05.07	0.8007	0.70	Reliable

As presented in Table 8, the Cronbach's Alpha values ranged from 0.8007 to 0.9418, exceeding the minimum reliability threshold of 0.70 for all sub-domains. These results indicate that the questionnaire demonstrated good internal consistency and produced reliable measurements for evaluating the APO13 and DSS05 processes.

The findings are consistent with previous COBIT 2019 studies by [11], [29], and [26] which reported that Cronbach's Alpha values above 0.70 indicate adequate instrument reliability for capability assessments. Therefore, the questionnaire was considered sufficiently reliable to support the subsequent capability level evaluation.

3.4 APO13 Capability Assessment Results

The capability assessment of the APO13 (Managed Security) domain was conducted to evaluate the implementation of information security management within the Safety Patrol feature of the E-Mansinam Website. The assessment results are presented in Table 9.

Table 9. Results of Capability Assessment Domain APO13

Sub-Domain	Current Capability Level	Target Level
AP013.01	4.15	4
AP013.02	3.93	4
AP013.03	4.05	4
Average	4.04	4

The APO13 domain achieved an average capability score of 4.04, which is slightly above the organization's expected Capability Level 4 (Predictable Process). According to the COBIT 2019 capability model, this result indicates that information security management processes are generally implemented in a predictable and controlled manner. However, the margin above the target is relatively small (0.04), indicating that the achieved capability remains close to the minimum threshold of the expected level rather than substantially exceeding it.

Furthermore, although the overall APO13 domain exceeded the target, the APO13.02 process obtained a capability score of 3.93, which is below the expected level. This finding suggests that not all information security management practices have been implemented consistently across the domain. Therefore, the overall capability score should be interpreted with caution, as it reflects the aggregated performance of all APO13 processes rather than uniformly achieving the target in every sub-process.

The result also needs to be interpreted in light of the respondent composition. Although Security Personnel constituted the largest respondent group because of their direct operational involvement in the Safety Patrol feature, the assessment also incorporated responses from supervisors, system administrators, HSSE officers, and military assistance personnel to include both operational and governance perspectives. Nevertheless, as the assessment was based on stakeholder perceptions collected through questionnaires, the possibility of respondent perception bias cannot be entirely excluded. Therefore, the findings should be interpreted as an indication of the current implementation of information security governance and should be supported by continuous monitoring and periodic evaluations to confirm sustained capability achievement.

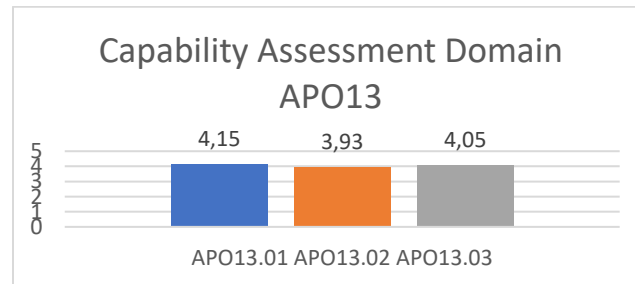


Figure 2. Capability Level Assessment Results for APO13

As illustrated in Figure 2, APO13.01 recorded the highest capability score (4.15), reflecting the effective implementation of information security governance practices. In contrast, APO13.02 obtained the lowest score (3.93), indicating that monitoring and evaluation activities related to information security management have not yet been implemented consistently. Meanwhile, APO13.03 achieved a score of 4.05, demonstrating that security management processes have generally been executed in a controlled and predictable manner.

These findings are consistent with previous studies by [8], [28], and [21], which reported that organizations achieving Capability Level 4 generally demonstrate mature information security governance supported by standardized procedures and effective security controls. Although the overall APO13 domain has achieved the expected capability level, strengthening monitoring and evaluation activities within APO13.02 remains necessary to support continuous improvement and future progression toward Capability Level 5 (Optimizing Process).

3.5 DSS05 Capability Assessment Results

The capability assessment of the DSS05 (Managed Security Services) domain was conducted to evaluate the implementation of information security service management within the Safety Patrol feature of the E-Mansinam Website. The assessment results are presented in Table 10.

Table 10. Results of Capability Assessment Domain DSS05

Sub-Domain	Current Capability Level	Target Level
DSS05.01	4.10	4

DSS05.02	4.09	4
DSS05.03	3.85	4
DSS05.04	4.10	4
DSS05.05	3.93	4
DSS05.06	3.90	4
DSS05.07	3.56	4
Average	3.93	4

The DSS05 domain achieved an average capability score of 3.93, which is slightly below the organization's expected Capability Level 4 (Predictable Process). Although the difference is relatively small (0.07), this result indicates that the implementation of operational security services has not yet consistently achieved the organization's expected capability level. Therefore, further improvements are required before the DSS05 domain can be considered to have fully attained the Predictable Process level.

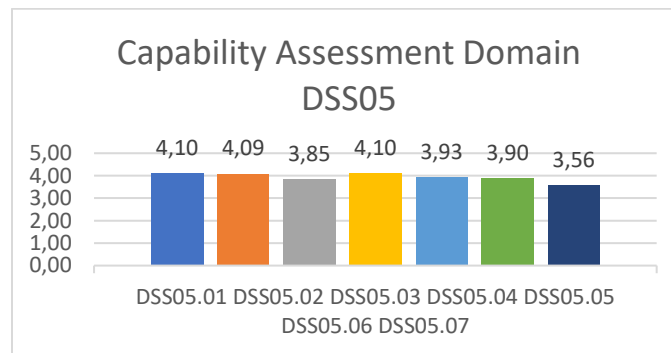


Figure 3. Capability Level Assessment Results for DSS05

As illustrated in Figure 3, DSS05.01 and DSS05.04 recorded the highest capability scores (4.10), followed closely by DSS05.02 (4.09). These results indicate that core security service processes have generally been implemented in a controlled and consistent manner. In contrast, DSS05.07 obtained the lowest capability score (3.56), indicating that security monitoring and operational security management have not yet been implemented consistently across the evaluated processes. Likewise, DSS05.03 (3.85) and DSS05.06 (3.90) also remained below the target capability level, suggesting that several operational security processes still require improvement before the DSS05 domain can consistently achieve the expected Capability Level 4.

These findings are consistent with previous studies by [8], [28], and [30], which reported that operational security processes commonly require continuous monitoring, regular evaluation, and effective incident management to achieve higher capability levels. Although several DSS05 sub-domains have reached or exceeded the expected capability level, the lower performance of DSS05.03, DSS05.06, and particularly DSS05.07 demonstrates that strengthening operational security management should remain the primary focus of future improvements.

3.6 Gap Analysis Results

Gap Analysis was conducted to compare the current capability level with the expected capability level (Level 4 – Predictable Process) established by the organization. The results of the analysis are presented in Table 11.

Table 11. Results of Gap Analysis

No	Sub-Domain	Current Capability Level	Expected Capability Level	Gap
1	APO13.01	4.15	4.00	-0.15
2	APO13.02	3.93	4.00	0.07
3	APO13.03	4.05	4.00	-0.05
4	DSS05.01	4.10	4.00	-0.10
5	DSS05.02	4.09	4.00	-0.08
6	DSS05.03	3.85	4.00	0.15

No	Sub-Domain	Current Capability Level	Expected Capability Level	Gap
7	DSS05.04	4.10	4.00	-0.10
8	DSS05.05	3.93	4.00	0.07
9	DSS05.06	3.90	4.00	0.10
10	DSS05.07	3.56	4.00	0.44

As presented in Table 11, five sub-domains (APO13.01, APO13.03, DSS05.01, DSS05.02, and DSS05.04) exceeded the target capability level, resulting in negative gap values. These results indicate that the corresponding governance and security service processes have been implemented consistently and operate within the organization's expected performance level. Conversely, APO13.02, DSS05.03, DSS05.05, DSS05.06, and DSS05.07 still exhibited positive gap values, indicating that further improvements are required to achieve the target capability level. Among these, DSS05.07 recorded the largest gap (0.44), followed by DSS05.03 (0.15) and DSS05.06 (0.10).

These findings are consistent with previous studies by [22], and [16], which reported that capability gaps are commonly observed in operational security processes due to limitations in continuous monitoring, security control implementation, and process evaluation.

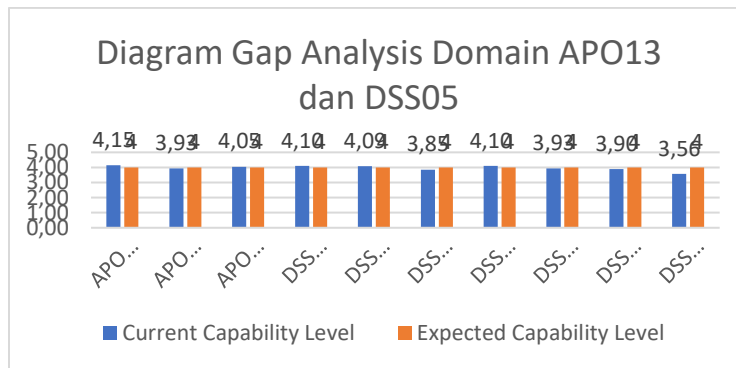


Figure 4. Comparison of Current and Target Capability Levels

Figure 4 provides a visual comparison between the current and expected capability levels for all assessed sub-domains. The figure clearly highlights that DSS05.07, DSS05.03, and DSS05.06 represent the largest capability gaps, indicating that these operational security processes should be prioritized for improvement. In contrast, the APO13 sub-domains generally achieved or slightly exceeded the target capability level, demonstrating stronger performance in information security governance than in operational security service management.

This difference between the APO13 and DSS05 domains indicates that information security governance at PT Pertamina Patra Niaga Fuel Terminal Manokwari is more mature at the policy and management level than at the operational implementation level. The findings suggest that organizational policies, security objectives, and governance mechanisms have generally been established and communicated effectively; however, their implementation in day-to-day operational security activities has not yet been fully consistent across all evaluated processes. This governance–operations gap is commonly reported in information technology governance literature, where organizations often achieve higher capability in governance planning and policy formulation than in the practical execution of operational security controls.

Similar observations indicate that organizations in the oil and gas sector frequently establish comprehensive cybersecurity governance frameworks, while challenges remain in consistently implementing operational security controls due to resource limitations, personnel awareness, and the complexity of industrial operations [31]. Likewise, the NIST Cybersecurity Framework emphasizes that continuous security monitoring, operational control implementation, and regular evaluation are essential to ensure that governance policies are effectively translated into operational practices [32]. Therefore, the lower capability levels observed in several DSS05 sub-domains do not necessarily indicate weaknesses in governance design but rather highlight the need to strengthen the execution and continuous monitoring of operational security services.

These findings indicate that future improvement efforts should prioritize strengthening operational security implementation while maintaining the existing governance practices within the APO13 domain. By reducing the gap between governance and operational implementation, the organization can achieve a more balanced and sustainable level of information security capability.

The identified capability gaps provide the basis for the subsequent Root Cause Analysis (RCA), which aims to determine the underlying factors preventing several DSS05 processes from consistently achieving the organization's expected capability level.

3.7 Root Cause Analysis Results

Root Cause Analysis (RCA) was conducted using the 5-Why analysis technique to identify the underlying factors contributing to the capability gaps identified in the APO13 and DSS05 domains. The analysis focused on the sub-domains that did not achieve the organization's target capability level, namely APO13.02, DSS05.03, DSS05.05, DSS05.06, and DSS05.07. The root causes were identified by integrating evidence obtained from questionnaire responses, interviews, field observations, organizational documentation, and the Gap Analysis results. The detailed RCA findings are presented in Table 5.

The 5-Why analysis revealed that the identified capability gaps were primarily associated with inconsistent implementation of operational security practices rather than the absence of security policies. For APO13.02, information security policies and risk treatment procedures had been established but were not reviewed and updated regularly to reflect operational changes. In the DSS05 domain, the capability gaps were mainly attributed to inconsistent endpoint maintenance, incomplete documentation of physical access controls, non-standardized procedures for handling sensitive documents, and insufficient implementation of continuous security monitoring and incident reporting activities.

Among the evaluated sub-domains, DSS05.07 (Manage Security Monitoring) exhibited the largest capability gap (0.44), indicating that continuous security monitoring and incident management represent the highest priority for improvement. Likewise, the capability gaps identified in DSS05.03 (Manage Endpoint Security), DSS05.05 (Manage Physical Access to IT Assets), and DSS05.06 (Manage Sensitive Documents and Output Devices) indicate that improvements are required in operational security controls, documentation practices, and periodic evaluations to achieve the organization's expected capability level.

These findings indicate that information security governance policies have generally been established; however, several operational security practices have not yet been implemented consistently across the evaluated processes. This pattern suggests that strengthening operational implementation, continuous monitoring, standardized documentation, and periodic evaluations should be prioritized to improve the overall capability of the DSS05 domain.

The findings are consistent with previous COBIT 2019 studies by [8], [26], and [27], which reported that capability gaps are commonly associated with inconsistent process implementation, inadequate documentation, limited monitoring activities, and insufficient continuous improvement mechanisms. Accordingly, addressing these root causes is essential for strengthening information security governance and supporting the achievement of the organization's target capability level.

3.8 Improvement Recommendations

Based on the results of the Capability Assessment, Gap Analysis, and Root Cause Analysis (RCA), several improvement recommendations were developed to address the underlying causes of the capability gaps identified in the APO13 and DSS05 domains. The recommendations were formulated by linking each identified root cause with corrective actions that are considered feasible within the operational environment of PT Pertamina Patra Niaga Fuel Terminal Manokwari. To enhance their practical applicability, Table 12 presents the official COBIT 2019 sub-domain codes and process names together with the identified capability gaps, recommended improvement actions, responsible organizational roles, indicative implementation timelines, and measurable success indicators. This structure provides clear guidance for systematically implementing the proposed improvements within the operational context of the Safety Patrol feature.

Table 12. Improvement Recommendations

COBIT 2019 Sub-Domain	Capability Gap	Improvement Recommendation	Responsible Unit	Timeline	Success Indicator
APO13.02 – Manage Information Security Risk	0.07	Periodically review and update information security policies and risk treatment procedures to ensure alignment with organizational security objectives and operational requirements.	Fuel Terminal Supervisor, HSSE Officer	3–6 months	Updated information security policies and documented periodic risk reviews.
DSS05.03 – Manage Endpoint Security	0.15	Strengthen endpoint protection through regular software updates, antivirus management, vulnerability scanning, and periodic endpoint configuration reviews.	System Administrator	3–6 months	All organizational devices are regularly updated, protected, and periodically monitored.
DSS05.05 – Manage Physical Access to IT Assets	0.07	Improve physical access control procedures, visitor authorization, and periodic audits of access to information technology assets.	HSSE Officer, Security Personnel	3–6 months	Physical access records are maintained and periodically audited.
DSS05.06 – Manage Sensitive Documents and Output Devices	0.10	Establish secure procedures for handling, storing, distributing, and disposing of sensitive documents and output devices, supported by periodic compliance reviews.	System Administrator, HSSE Officer	6–12 months	Secure document management procedures are consistently implemented and periodically evaluated.
DSS05.07 – Manage Security Monitoring	0.44	Implement continuous security monitoring, perform periodic log reviews, strengthen incident reporting procedures, conduct regular security awareness training for Safety Patrol users, and periodically evaluate security incidents to support continuous improvement.	System Administrator, HSSE Officer, Security Personnel	0–6 months (High Priority)	Periodic security monitoring reports are generated, security incidents are documented and reviewed, and security awareness training is conducted at least annually.

These recommendations are consistent with prior findings that organizations in the oil and gas sector require continuous security monitoring, periodic policy reviews, endpoint protection, and personnel security awareness to strengthen cybersecurity governance and maintain operational resilience in safety-critical environments [31]. Likewise, the NIST Cybersecurity Framework emphasizes that continuous monitoring, incident response, and regular security assessments are essential practices for improving cybersecurity governance within critical infrastructure [32]. The improvement priorities identified in this study, particularly for DSS05.07 (Manage Security Monitoring), therefore align with established best practices for enhancing information security governance in high-risk industrial environments while remaining consistent with the governance principles of COBIT 2019 [6].

The proposed recommendations were designed to be directly applicable within the operational environment of PT Pertamina Patra Niaga Fuel Terminal Manokwari. By specifying the responsible organizational units, implementation timelines, and measurable success indicators, the recommendations provide a structured roadmap for systematically improving information security governance within the Safety Patrol feature and supporting the achievement of the organization's target capability level.

4. Conclusions and Future Works

This study evaluated the information security governance of the Safety Patrol feature within the E-Mansinam Website at PT Pertamina Patra Niaga Fuel Terminal Manokwari using the COBIT 2019 framework, focusing on the APO13 (Managed Security) and DSS05 (Managed Security Services) domains. The assessment results showed that the APO13 domain achieved an average capability level of 4.04, indicating that information security management processes have reached the organization's target of Capability Level 4 (Predictable Process). In contrast, the DSS05 domain achieved an average capability level of 3.93, indicating that several operational security service processes have not yet fully achieved the expected capability level.

The Gap Analysis identified DSS05.07, DSS05.03, and DSS05.06 as the sub-domains with the largest capability gaps. Root Cause Analysis revealed that these gaps were primarily associated with inconsistent security monitoring, incomplete documentation, limited periodic evaluations, and variations in personnel awareness of information security procedures. Based on these findings, improvement recommendations were proposed, including strengthening security monitoring activities, standardizing security documentation, conducting regular security evaluations, and implementing continuous security awareness programs.

For future research, the assessment can be extended by including additional COBIT 2019 domains related to governance and risk management, such as EDM03 (Ensure Risk Optimization) and APO12 (Managed Risk), to provide a more comprehensive evaluation of information technology governance. Future studies may also integrate COBIT 2019 with other information security standards, such as ISO/IEC 27001, to obtain a broader perspective on information security management. In addition, future research is recommended to implement the improvement recommendations proposed in this study, particularly those related to security awareness training, continuous security monitoring, documentation standardization, and incident management procedures, and subsequently re-evaluate the APO13 and DSS05 domains. Such a follow-up assessment would enable researchers to measure changes in capability levels after the implementation of the recommendations and evaluate their effectiveness in improving information security governance within the Safety Patrol feature over time.

5. Declarations

Author Contributions

Asrawati : Conceptualization of the research, data collection, data processing and analysis, interpretation of research results, drafting of the initial manuscript, and revision and refinement of the manuscript. Lorna Yertas Baisa: As the primary supervisor, provided academic supervision and guidance on the development of the research concept; offered insights and input regarding the research implementation and methodology; and engaged in in-depth discussions and analysis concerning the research process and results. Alex De Kweldju : As the second supervisor, provided academic supervision and guidance on the implementation of the research and offered input to support the development of the study.

Funding Statement

State the funding source and grant/contract number, or state that the research received no external funding.

Conflict of Interest

The authors declare that there is no conflict of interest related to this research or its publication.

Data Availability Statement

The data supporting the findings of this study are not publicly available because the research involves information related to the internal conditions of the organization and the management of the Safety Patrol feature on the E-Mansinam Website. The data may be made available by the authors upon reasonable request, subject to permission from the relevant organization and applicable confidentiality and privacy requirements.

Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) tools were used to a limited extent in the preparation of this manuscript to assist with language editing and grammatical corrections, as well as to enhance the clarity and readability of the text. AI was not used to generate research data, collect or analyze data, interpret research findings, or make scientific or editorial judgments. The authors retain full responsibility for all data, analyses, interpretations, conclusions, and the content of the manuscript.

Ethical Clearance

This study involved human participants in the data collection process through interviews and questionnaires. The research was conducted in accordance with applicable ethical principles, including voluntary participation, the use of collected information solely for research purposes, and the protection of the confidentiality of information and participant identities. The study did not involve medical intervention, experimental treatment, or procedures that posed significant risks to the participants.

6. References

- [1] S. Suroto and J. Friadi, "Evaluasi Tingkat Capability Keamanan Sistem Informasi PT. CPPI Menggunakan Framework COBIT 2019 (Evaluation of PT's Information System Security Capability Level. CPPI uses the COBIT 2019 framework) Riwayat Artikel," vol. 2, no. 1, pp. 45–60, 2023.
- [2] Y. T. Sepis, "Analisa Keamanan Sistem Informasi Menggunakan Framework Cobit 5 Dengan Domain Dss05 Dan Apo13 Di Pt Xyz," *TeIka*, vol. 12, no. 01, pp. 35–42, 2022, doi: 10.36342/teika.v12i01.2821.
- [3] E. Endrianto and A. Zaelani Adnan, "Sistem Manajemen Keselamatan Kesehatan Kerja (SMK3) Kontraktor Di PT Pertamina EP Asset 3 Jatibarang Field," *Jurnal Kesehatan Tambusai*, vol. 4, pp. 345–350, 2023.
- [4] A. dan N. Hulu, "Evaluation of the Implementation of the Occupational Safety and Health Management System (SMK3)," *Journal of Community Health Provision*, vol. 5, no. 3, pp. 145–162, 2025, doi: 10.55885/jchp.v5i3.773.
- [5] Pertamina Patra Niaga, "Fuel Terminal Manokwari," PT Pertamina Patra Niaga. Accessed: Jun. 08, 2026. [Online]. Available: <https://ftmanokwari.emansinam.com/>
- [6] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL: ISACA, 2018.
- [7] Christiadi & Sutomo, "Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector," *G-Tech : Jurnal Teknologi Terapan*, vol. 7, no. 4, pp. 295–305, 2023.
- [8] Yulita & Tambotih, "Analisis Manajemen Risiko pada PT . XYZ Menggunakan Risk Management Analysis of PT XYZ Using COBIT 2019 with Domain," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 5, pp. 2033–2047, 2024, doi: <https://doi.org/10.32520/stmsi.v13i5.4430>.
- [9] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, Edisi Kedu. Bandung: Alfabeta, 2023.

- [10] ISACA, *COBIT® 2019 Implementation guide : implementing and optimizing an information and technology governance solution*. 2020.
- [11] M. Brian Hardjadinata and J. Wiratama, "Capability Assessment of IT Governance Using the 2019 COBIT Framework for the IT Business Consultant Industry," *International Journal of Science, Technology & Management*, vol. 4, no. 4, pp. 1034–1039, 2023, doi: 10.46729/ijstm.v4i4.902.
- [12] J. Yuan Mambu, Z. Todingdatu, and J. Kondo, "IT Governance Maturity Assessment Using COBIT 2019 for System Enhancement and Strategic Decision Support," *COGITO Smart Journal*, vol. 11, no. 1, pp. 193–206, 2025.
- [13] G. M. W. Tangka and E. Lompoliu, "Optimizing IT Governance in BTS.id: A COBIT 2019-Based Analysis of Design Factors," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 699–710, 2025, doi: 10.57152/malcom.v5i2.1997.
- [14] Hidayat et al, "Evaluation of Information Technology Governance Maturity Using COBIT 2019: A Case Study on the IT Security Industry," *Journal La Multiapp*, vol. 5, no. 4, pp. 286–303, 2024, doi: 10.37899/journallamultiapp.v5i4.1442.
- [15] Y. N. Widasari and N. R. Oktadini, "Capability Level Assessment of IT Governance in the SIAP KOJA Application Using the COBIT 2019 Framework," *Journal of Applied Informatics and Computing*, vol. 9, no. 6, pp. 3706–3715, 2025, doi: 10.30871/jaic.v9i6.11433.
- [16] I. N. S. Saputra, "TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 2019 DENGAN METODE SCOPING GOALS CASCADE DAN DESIGN FACTORS: STUDI KASUS PT . XYZ," *INSERT: Information System and Emerging Technology Journal.*, vol. 6, no. 2, pp. 266–280, 2025.
- [17] M. Khairul Anam, S. D. Putri, D. Yuliana, E. Yumami, and T. P. Lestari, "Application of the COBIT 2019 Framework to Analyse the Security of Academic Information Systems," *Decode: Jurnal Pendidikan Teknologi Informasi*, vol. 3, no. 2, pp. 59–65, 2023, doi: <https://doi.org/10.51454/decode.v3i2.192>.
- [18] A. P. Nugroho and A. Ambarwati, "Analisis Tata Kelola Teknologi Informasi Di Pt. Garam Menggunakan Framework Cobit 2019 Domain, Deliver, Services & Support," *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, vol. 11, no. 1, pp. 48–55, 2025, doi: 10.34010/jtk3ti.v11i1.15782.
- [19] & Y. G. S. Anshari Amry, Yekti Wirani, "Assessment of IT Governance Capability Level Using the COBIT 2019 Framework: A Case Study of XYZ Institution," *JEPIN (Jurnal Edukasi dan Penelitian ...)*, vol. 11, no. 2, pp. 277–286, 2025.
- [20] I. Zufria, "Maturity Assessment at a University IT Center Using COBIT 2019 EDM and APO Domains," *Information Technology Education Journal*, vol. 5, no. 1, pp. 18–40, 2026.
- [21] A. N. Ibrahim and E. Suryani, "Transform IT Governance and Management to Enhance Information Security using COBIT Framework 2019," *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, vol. 7, no. 2, 2026.
- [22] P. Purwadi and H. Santoso, "Comparison of Information Technology Governance Maturity Levels Based on COBIT 2019 at PT Kereta Commuter Indonesia in 2023 and 2024," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 5, pp. 2962–2974, 2025, doi: 10.52436/1.jutif.2025.6.5.5200.
- [23] V. N. Juni, R. D. Amalia, and E. Krisnanik, "Evaluasi Capability Level Tata Kelola TI Berbasis COBIT 2019 untuk Mendukung Transformasi Digital Perguruan Tinggi pengadaan aplikasi atau infrastruktur , tetapi memerlukan tata kelola yang mampu organisasi menyesuaikan ruang lingkup evaluasi berdasarkan," *Jurnal Penelitian Teknologi Informasi Dan Sains*, vol. 4, no. juni, pp. 17–33, 2026.

- [24] M. Barsalou and B. Starzyńska, "Inquiry into the Use of Five Whys in Industry," *Quality Innovation Prosperity*, vol. 27, no. 1, pp. 62–78, 2023, doi: 10.12776/QIP.V27I1.1771.
- [25] A. Ito *et al.*, "Improved root cause analysis supporting resilient production systems," *Journal of Manufacturing Systems*, vol. 64, no. April, pp. 468–478, 2022, doi: 10.1016/j.jmsy.2022.07.015.
- [26] M. D. S. Antariksa, M. P. Angin, and A. P. Widodo, "COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors," *Journal of Renewable Energy, Electrical, and Computer Engineering*, vol. 5, no. 1, pp. 99–105, 2025, doi: 10.29103/jreece.v5i1.19501.
- [27] I. P. S. Almantara, I. N. A. Prabawa, and I. N. A. Prabawa, "Evaluation of Information Technology Governance Using the COBIT Framework in Higher Education in Indonesia : A Literature Study," *NAICE Journal of Next Applied Informatics in Computer Engineering*, vol. 1, no. 1, pp. 25–33, 2026.
- [28] A. Zaki, M. R., & Tirtana, "Implementation of AP012, AP013 and DSS05 Sub-Domains in COBIT 2019 to Improve Information System Security at LAZIS Sabilillah Malang," in *Proceedings of the 1st International Conference on Business, Innovation, Technology & Science (ICoBITS)*, Universitas Bhinneka Nusantara, 2025, pp. 39–44.
- [29] G. B. R. Francolla, G. R. Mandoya, M. D. Walangitan, E. Lompoliu, and J. Y. Mambu, "Information Technology Governance Audit Using the COBIT 2019 Framework at XYZ Institution," *Cogito Smart Journal*, vol. 8, no. 2, pp. 346–358, 2022.
- [30] R. F. Mubarak and M. I. Fianty, "Leveraging COBIT 2019 to Implement IT Governance in Mineral Mining Company," *Journal of Information Systems and Informatics*, vol. 5, no. 3, pp. 1058–1071, 2023, doi: 10.51519/journalisi.v5i3.545.
- [31] A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective," *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 3, pp. 1–27, 2022, doi: 10.1145/3548691.
- [32] K. S. Cherilyn Pascoe, Stephen Quinn, "The NIST Cybersecurity Framework," *National Institute of Standards and Technology*, p. 32, 2024, doi: <https://doi.org/10.6028/NIST.CSWP.29>.