E-ISSN: 2988-585X (Online)

Journal of Elektronik Sistem Informasi (JESII)

Volume 3 No 1 June 2025

DOI: 10.31848/jesii.v3i1.4041

Audit of the Security of the Attendance Application in the Human Resource Management System Using the Cobit 5 Framework

Acep Saepuloh[1], Titan Parama Yoga[2], Züleyha Yılmaz Acar[3]

[1,2]Information Systems Study Program, Indonesian University of Informatics and Business

[3]Selcuk University, Turkey

Article Info

Article history:

Received Apr 22, 25
Revised Jun 29, 25
Accepted Jun 30, 25

Keywords:

Application Audit
COBIT 5
APO13
DSS05
Human Resource Management

ABSTRACT

Information system security is very important in supporting company operations, especially in employee data management. PT. Dekatama Centra uses a face verification-based attendance application to record employee attendance, but this application has potential security risks that need to be evaluated. This study aims to analyze the security level of HRMS presence applications using the COBIT 5 framework, focusing on the domains APO13 (Manage Security) and DSS05 (Manage Security Service). The methods used include interviews, observations, and questionnaires to assess the level of security maturity based on the COBIT 5 assessment model. The audit results show that the current maturity level is at Level 1 (Performed), which means that security processes have been implemented but have not been systematically documented. Some of the weaknesses found include a lack of adequate access control, suboptimal malware protection, and the lack of an effective security monitoring system. This study recommends the implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001, improved data encryption, and cybersecurity training for employees. The implementation of these recommendations is expected to improve employee data protection, strengthen systems from cyber threats, and ensure the sustainability of the company's operations safely and efficiently.

Corresponding Author:

Titan Parama Yoga,
Information Systems Study Program, Faculty of Technology and Informatics, Indonesian University of Informatics and Business.
Jln. Soekarno Hatta No.643 Bandung, West Java, Indonesia. 40285
Email: titanparama@unibi.ac.id

1. INTRODUCTION

In today's all-digital era, information technology has a crucial role in supporting the activities of a company. The Human Resource Management System is one of the technology systems that is starting to be widely used to manage various human resource activities, including managing employee attendance [1]. However, behind the benefits of this technology there is a security risk of information systems. Cybercrimes, misconfigurations, or weak internal controls that can result in very serious losses for the company, such as employee data theft, and disruption of employee absenteeism activities [2][3].

PT. Dekatama Centra is a manufacturing company engaged in the garment industry and has implemented an employee attendance system using the Human Resource Management System (HRMS) application [4]. This application makes it easier for employees to be present with the face verification feature through personal phones [5]. In addition, the HRMS application also provides a feature for applying for permits for employees who are unable to

work. But like any other system, this application still has potential risks that must be considered. Therefore, it is necessary to conduct an audit to evaluate the security level of the application using the right framework [6].

To address these challenges, organizations require a well-structured framework to manage and evaluate application security. COBIT 5 is one such framework that offers both strategic and operational approaches for assessing information systems [7]. It not only covers technical aspects but also includes governance, management, risk assessment, and alignment between IT processes and business objectives [8][9].

This study concentrates the audit on two specific COBIT 5 domains: APO13 (Manage Security) and DSS05 (Manage Security Services). These domains were selected due to their direct relevance to information system security. APO13 focuses on security planning and policy formulation, while DSS05 deals with technical implementation aspects such as data protection, access control, and incident response. By narrowing the audit scope to these two domains, the evaluation becomes more focused and in-depth, aligning closely with the primary objective of this research: to assess the current security level of the company's Human Resource Management System (HRMS) [10].

This research is important to be carried out because it is related to the security of information systems in the application which is a vital aspect in supporting the continuity of the company's operations, especially for PT. Dekatama Centra which utilizes an HRMS system based on the presence application in managing employee data. Employee data theft or cyberattacks are security risks that can have a significant impact on the company's credibility and efficiency [11].

With the COBIT 5 framework, the implementation of this application security audit not only provides an evaluation of the effectiveness of the security controls implemented in HRMS applications, but also provides measurable and standardized recommendations in improving the security of enterprise presence applications [12].

2. METHOD

This study uses a qualitative descriptive approach to audit the security of presence applications in the Human Resource Management System (HRMS) by referring to the COBIT 5 framework. This approach was chosen because it is able to provide an in-depth understanding of the security level of the application through detailed and in-depth data analysis. Data in this study was collected through interviews, questionnaires, and observations, which focused on important aspects related to application security. The following are the steps taken in this study:

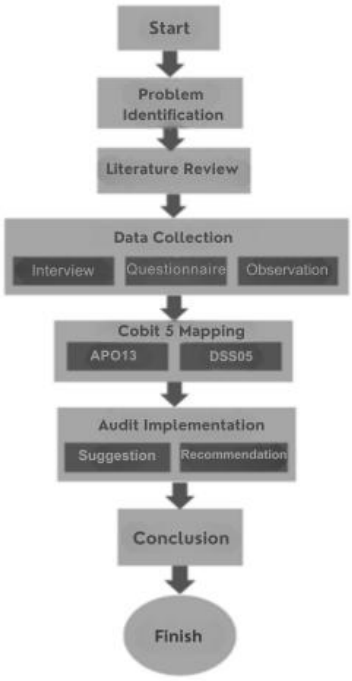


Figure 1. Research Stages

The study began by identifying potential vulnerabilities in the HRMS attendance system used by PT Dekatama Centra. Once the risks were recognized, the researchers defined the goal of the study: to assess the system's security level using the COBIT 5 framework, with particular emphasis on the APO13 and DSS05 domains.

To obtain relevant data, three techniques were employed: conducting interviews with system administrators, distributing questionnaires aligned with COBIT 5 metrics, and performing on-site observations of the system in operation [13]. Following data collection, the evaluation was structured according to the COBIT 5 framework, with a focused analysis on APO13—which deals with planning and security policies—and DSS05, which involves the execution and operational control of IT security services [14].

The next stage was the conduct of the audit, which consisted of measuring the capability level of the system based on the process attributes in COBIT 5, as well as developing relevant improvement recommendations based on the analysis and findings. After all the data is analyzed, the researcher draws up a conclusion from the audit that includes the current state of the security level and areas that need improvement [15].

3. RESULT AND DISCUSSION

3.1. Audit Preparation

Thorough audit preparation is the foundation for identifying audit objectives, setting scope, and identifying IT processes and IT Goals. Therefore, the researcher made preparations before the audit was carried out.

3.1.1. Determination of the Audit Scope

The scope of audit in this study focuses on the evaluation of the security of the HRMS attendance application used by PT. Dekatama Centra. The audit was conducted using the COBIT 5 framework, especially in the domains APO13 (Manage Security) and DSS05 (Manage Security Service), which were selected based on relevance to the company's strategic needs in developing a safe, reliable, and effective presence. The limitations in this audit cover the security aspects of the application, without covering other systems or infrastructure outside of HRMS. This research is expected to be the first step in improving the efficiency and reliability of the attendance system through a standards-based audit approach.

3.1.2. Identify IT Processes

The IT process identification stage is carried out by mapping IT objectives with existing IT processes. This step aims to understand and identify the processes that are carried out within the organization. The results of the mapping between IT objectives and IT processes can be seen in the following table:

Table 1. IT Goal Mapping and IT Processes

IT Objectives	IT Process
Maintain the integrity of the entire information security system to maintain a level of security. Establish and manage user access rights, as well as supervise the security of operational information.	APO13
Ensure the protection of IT services and information from security threats by maintaining the confidentiality, integrity and availability of data. Minimize risks to IT services through effective management and security, including mitigating the impact of threats and vulnerabilities, and proactively managing security incidents to prevent disruption to business operations.	DSS05

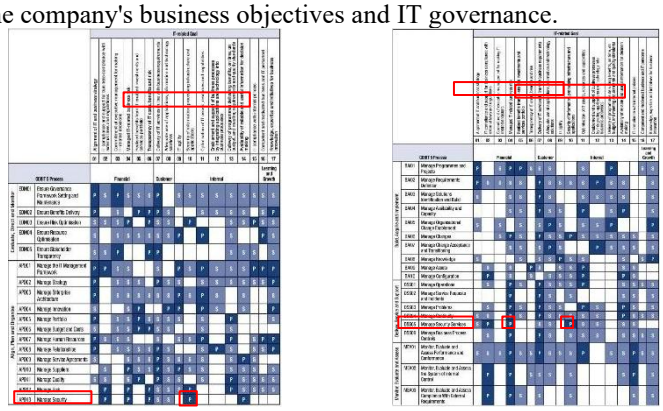
The table above is the result of a mapping between IT processes and IT objectives, showing the IT processes that have been identified. The results of this mapping are then adjusted to the supporting processes in the COBIT 5 framework. This mapping is also the basis for the preparation of a questionnaire to measure the level of maturity. The function of this questionnaire is to find out the level of importance of each IT process contained in the COBIT 5 framework.

3.2. Audit Implementation

The purpose of this audit is to assess security controls in the APO 13 (Manage Security) and DSS05 (Manage Security Service) domains by referring to the COBIT 5 framework. This audit process includes data collection, mapping IT objectives with IT processes, and evaluating security controls. In the APO13 domain, it focuses on information security risk management, ISMS monitoring, and risk management. Meanwhile, the DSS05 domain focuses on malware protection, network security management, and user access control. The results of this audit will be included in a report containing findings, recommendations, and assessments of the system's compliance with applicable security standards, in order to support the strategic and operational improvement of the security of attendance applications.

3.2.1. Assessment Process Activities COBIT 5

This study applies the Initiation stage in Assessment Process Activities based on the COBIT 5 framework to determine the scope of the security audit of the HRMS attendance application at PT. Dekatama Centra. This stage begins with the identification of information security issues which are then mapped into the domains APO13 (Manage Security) and DSS05 (Manage Security Service), with a focus on monitoring system security operations. Its primary objective is to ensure the application of confidentiality, integrity, and availability (CIA) principles, while minimizing IT service risks and mitigating security threats. This stage also supports the achievement of the Enterprise Goals of COBIT 5, such as regulatory compliance, IT service reliability, and security risk management. Thus, Initiation becomes the strategic foundation of the audit, ensuring that the evaluation is carried out in a systematic, structured and aligned manner with the company's business objectives and IT governance.



Picture 2. COBIT Process (Mapping COBIT 5 IT-related Goals to to Processes APO13 and DSS05)

Based on the results of the COBIT 5 mapping, this study focuses on two domains, namely APO13 (Manage Security) and DSS05 (Manage Security Service), where each is related to IT-related goals in column 10 (information security, infrastructure, and applications). DSS05 is also related to column 4 (IT-related business risk management), which shows its role in mitigating security risks.

APO13 focuses on strategic aspects, such as the formulation of security policies and procedures in the organization. Meanwhile, DSS05 plays a more operational role, namely to manage security services and ensure effective policy implementation and monitoring. While both domains support IT and data infrastructure protection, DSS05 has a broader scope as it covers business risk management.

This study uses these two domains to evaluate the application of security practices in the HRMS attendance application at PT. Dekatama Centra. This audit is expected to provide an overview of the level of system security maturity and mitigation recommendations needed to better protect employee data and be ready to face future security challenges.

3.2.2. Audit Data Collection Using COBIT 5

The audit data examination process refers to the COBIT 5 framework, starting with the evaluation of a questionnaire compiled based on the domains APO13 (Manage Security) and DSS05 (Manage Security Service). After the data is collected, validation is carried out to ensure the accuracy and correctness of the respondents' answers. This validation is important so that the audit findings reflect real conditions, so that the recommendations provided are on target and relevant to the needs in the field.

Table 2. Categories and Collections of APO13 Domains

Process Number	APO13
Name	Managing Security
Description	Determine the operation and monitoring of systems for information security management
Purpose	Keeping the impact and occurrence of information security incidents in accordance with the company's risk tolerance level
Data Collection	PA 1.1 - Process performance
Achievement	**Result of Full Achievement of the Attribute**
PA 2.1 - Performance Management	1. Definition of objectives for process performance. 2. Monitoring and planning of process performance. 3. Adjustment of process performance to meet the plan. 4. Definition, assignment and communication of responsibilities and authority to carry out the process. 5. Definition, allocation and use of the resources and information necessary to carry out the process. 6. Communication between the parties involved is managed to ensure effective communication and clarity of responsibility assignments. 7. Definition of objectives for process performance. 8. Monitoring and planning of process performance. 9. Adjustment of process performance to meet the plan.

Process Number	APO13
Name	Managing Security
Description	Determine the operation and monitoring of systems for information security management
Purpose	Keeping the impact and occurrence of information security incidents in accordance with the company's risk tolerance level
Data Collection	PA 1.1 - Process performance
Achievement	Result of Full Achievement of the Attribute
	10. Definition, assignment and communication of responsibilities and authority to carry out the process. 11. Definition, allocation and use of the resources and information necessary to carry out the process. 12. Communication between the parties involved is managed to ensure effective communication and clarity of responsibility assignments.
PA 2.2 Work Product Management	1. Definition of requirements for the working product of the process. 2. Definition of requirements for documentation and control of work products. 3. Identification, documentation and proper control of work products. 4. The review of work products is in accordance with the planned arrangement and adjusted as necessary to meet requirements. 5. Definition of requirements for the working product of the process. 6. Definition of requirements for documentation and control of work products. 7. Rapid identification, documentation and control of work products. 8. The review of work products is in accordance with the planned arrangement and adjusted as necessary to meet requirements.
PA 3.1 - Process Definition	1. A standard process definition that can describe the fundamental elements that must be included in a process. 2. Determination of the sequence and interaction of standard processes with other processes. 3. Definition of the competencies required and roles to carry out the process as part of the standard process. 4. Identification of the necessary infrastructure and work environment to carry out the process as part of the standard process. 5. Determination of suitable methods to monitor the effectiveness and suitability of the process.
PA 3.2 - Process Deployment	1. The selection and/or adjustment of the processes identified Questionnaire is placed based on appropriate process standards. 2. Definition, assignment and communication of the roles, responsibilities and authorities required to carry out the process. 3. Definition of the competencies of personnel who carry out the process on the basis of education, training and experience 4. Definition, allocation, and use of the necessary resources and information necessary to carry out the process. 5. Definition, management and maintenance of the necessary infrastructure and work environment to carry out processes. 6. Appropriate data is collected and analyzed as a basis for understanding the behavior of the process to demonstrate suitability and effectiveness, as well as evaluating the continuous improvements the process can make.
PA 4.1 - Process Measurement	1. The process information needed supports relevant business objectives. 2. The purpose of process measurement comes from the need for process information. 3. Quantitative objectives for process performance in support of relevant business objectives are set. 4. The measurement action and frequency are identified and defined in line with the process measurement objectives and the quantitative objectives for the process performance. 5. Collection, analysis and reporting of measurement results to monitor the extent to which quantitative objectives for process performance are being met. 6. The measurement results used describe the performance of the process.
PA 4.2 - Process Measurement	1. Determination and application of analysis and control of applicable techniques. 2. Setting variation control limits for normal process performance. 3. Analysis of measurement data for specific causes of variation. 4. Corrective action to address specific causes of variation 5. Re-erection (if required)
PA 5.1 - Process Innovation	1. The impact of all proposed changes is assessed against the objectives of the identified process and the standard process. 2. Management of approval of the implementation of all changes to ensure that any disruption to process performance is understood and acted upon. 3. Based on actual performance, the effectiveness of the change process is evaluated against the product requirements and the process objectives applied to determine whether due to general or specific causes.
PA 5.2 - Process Optimization	1. The impact of all proposed changes is assessed against the objective questionnaire of the defined process and the standard process. 2. Management of approval of the implementation of all changes to ensure that any disruption to process performance is understood and acted upon.

Process Number	APO13
Name	Managing Security
Description	Determine the operation and monitoring of systems for information security management
Purpose	Keeping the impact and occurrence of information security incidents in accordance with the company's risk tolerance level
Data Collection	PA 1.1 - Process performance
Achievement	**Result of Full Achievement of the Attribute**
	3. Based on actual performance, the effectiveness of the change process is evaluated against the product requirements and the process objectives set for the determination of the outcome whether due to general or special causes.

Table 3. DSS05 Domain Categories and Collections

Process Number	DSS05
Name	Managing Security Services
Description	Protect company information to keep the level of information security risk within limits acceptable to the company in accordance with the security policy. Establish and maintain information security roles and access rights, as well as conduct security monitoring.
Purpose	Minimize the business impact of operational information security vulnerabilities and incidents.
Data Collection	PA 1.1 - Process performance
Achievement	**Result of Full Achievement of the Attribute**
PA 2.1 - Performance Management	1. Definition of objectives for process performance. 2. Monitoring and planning of process performance. 3. Adjustment of process performance to meet the plan. 4. Definition, assignment and communication of responsibilities and authority to carry out the process. 5. Definition, allocation and use of the resources and information necessary to carry out the process. 6. Communication between the parties involved is managed to ensure effective communication and clarity of responsibility assignments.
PA 2.2 - Work Product Management	1. Definition of requirements for the working product of the process. 2. Definition of requirements for documentation and control of work products. 3. Identification, documentation and control of work products. 4. The review of work products is in accordance with the planned arrangement and adjusted as necessary to meet requirements.
PA 3.1 - Process Definition	1. Definition of the required competency processes and roles to conduct the process as part of the standard process. 2. Determination of the sequence and interaction of standard processes with other processes 3. Definition of the competencies required and roles to carry out the process as part of the standard process. 4. Identification of the necessary infrastructure and work environment to carry out the process as part of the standard process. 5. Determination of suitable methods to monitor the effectiveness and suitability of the process.
PA 3.2 - Work Product Management	1. The selection and/or adjustment of defined processes is placed based on precise process standards. 2. Definition, assignment and communication of the roles, responsibilities and authorities required to carry out the process. 3. Definition of the competencies of personnel who carry out the process on the basis of education, training and experience. 4. Define, allocate and use the necessary resources and information necessary to carry out the process. 5. Definition, management, and maintenance of the necessary infrastructure and work environment to carry out the process. 6. Appropriate data is collected and analyzed as a basis for understanding the behavior of the process to demonstrate suitability and effectiveness, as well as evaluating the continuous improvements the process can make.
PA 4.1 - Process Measurement	1. Process information needs are set to support relevant business objectives. 2. The purpose of process measurement is derived from the need for process information. 3. Quantitative objectives for process performance are set to support relevant business objectives. 4. The size and frequency of measurements are identified and determined according to the process measurement objectives and quantitative objectives for process performance. 5. Measurement results are collected, analyzed, and reported to monitor the extent to which the quantitative objectives of process performance are being achieved 6. The measurement results are used to characterize the performance of the process.
PA 4.2 - Process Control	1. Analysis and control techniques are determined and applied where relevant. 2. Variation control limits are set to ensure normal process performance. 3. The measurement data is analyzed to identify specific causes of variation. 4. Control limits are reset (if necessary) after corrective action has been taken.
PA 5.1 - Process Innovation	5. Process improvement goals are set to support relevant business objectives. 6. Appropriate data is analyzed to identify common causes of variations in process performance. 7. Based on actual performance, the effectiveness of the change process is evaluated against the product requirements and the process objectives set for the determination of the outcome whether due to general or special causes.

Process Number	DSS05
Name	Managing Security Services
Description	Protect company information to keep the level of information security risk within limits acceptable to the company in accordance with the security policy. Establish and maintain information security roles and access rights, as well as conduct security monitoring.
Purpose	Minimize the business impact of operational information security vulnerabilities and incidents.
Data Collection	PA 1.1 - Process performance
Achievement	**Result of Full Achievement of the Attribute**
	8. Appropriate data is analyzed to identify best practice and innovation opportunities. 9. Opportunities for improvement gained from new technologies and process concepts are identified. 10. Implementation strategies are set to achieve process improvement goals.
PA 5.2 – Process Optimization	1. The impact of all proposed changes is assessed against the objectives of the defined process and the standard process. 2. Management of approvals for the implementation of all changes to ensure that any disruption to process performance is understood and given Action. 3. Based on actual performance, the effectiveness of the change process is evaluated against the product requirements and the process objectives set for the determination of the outcome whether due to general or special causes.

3.3. Verification of Data and Audit Results

Verification of data and audit results aims to ensure the accuracy, reliability, and conformity of the system with security and risk management standards. Referring to the APO13 (Manage Security) and DSS05 (Manage Security Service) domains in the COBIT 5 framework, this process includes important aspects that support the improvement of the quality of the application security system at PT. Dekatama Centra.

3.3.1. Outcome Process APO13

Process Number APO13 has several derived processes that are used to determine the results as follows:

Table 4. Outcome of Process APO13

Outcome	Description
APO13.01	A system is placed in place that is considered effective to handle the company's information security requirements.
APO13.02	A security plan has been formed, accepted and communicated throughout the company.
APO13.03	Information security solutions are implemented and operated consistently across the company.

Total achievement/outcome is used to determine the final value of total achievement at the PA1.1 level and rating by criteria for the APO13 domain. The percentage of achievement of each outcome is calculated based on the average of the percentage of achievements/components that make up it. The components of each outcome are explained as follows:

Table 5. Components of each outcome in Process APO13

Outcome	Component	Number	Description
APO13.01	Work Product Output	APO13-WP1	SMKI Policy.
		APO13-WP2	Statement of the scope of SMKI.
		APO13-WP5	SMKI audit report.
		APO13-WP6	Recommendations for improvement to improve SMKI.
	Base Practice + Work Product Input	APO13-BP1	Build and maintain an information security management system (SMKI).
		APO13-BP3	Monitor and review SMKI.
APO13.02	Work Product Output	APO13-WP3	Plan for the treatment and handling of information security risks.
		APO13-WP4	Information security business case.
	Base Practice + Work Product Input	APO13-BP2	Determine and manage information security risk management plans.
APO13.03	Work Product Output	APO13-WP5	SMKI audit report.
		APO13-WP6	Recommendations for improving SMKI.

	Base Practice + Work Product Input	APO13-BP3	Monitor and review SMKI.

The process components obtained from the total number of "Y" answers divided by the total number of questions for each component are presented in the following table:

Table 6. Tabulation of audit assessment of process number APO13

Number	Description	Achievement / Component	Achievement / Component	Outcome	Total Achievement PA 1.1 (APO13)
APO13-WP1	SMKI Policy.	75%	$\frac{(75\% + 92\%)}{2} = 84\%$	APO13-01	$\frac{(84\% + 47\% + 80\%)}{3} = 70\%$
APO13-WP2	Scope statement.				
APO13-WP5	SMKI.				
APO13-WP6	SMKI audit report.				
APO13-BP1	Recommendations to improve SMKI.	92%			
APO13-BP3	Build and review SMKI.				
APO13-WP3	Information security risk treatment plan.	50%	$\frac{(50\% + 43\%)}{2} = 47\%$	APO13-02	
APO13-WP4	Information security business case.				
APO13-BP2	Define and manage risk treatment plans.	43%			
APO13-WP5	SMKI audit report.	100%	$\frac{(100\% + 60\%)}{2} = 80\%$	APO13-03	
APO13-WP6	Recommendations to improve SMKI.				
APO13-BP3	Monitor and review SMKI.	60%			

The table above shows the tabulation results of the audit assessment for the APO13 (Manage Security) domain. The value of each component was obtained from the average results of the respondents. For APO13-WP1, WP2, WP-5, and WP6, the average value is 75%. Meanwhile, APO13-BP1 and BP3 each obtained 92%. The combined values of WP1-WP6 and BP1-BP3 resulted in an APO13-01 score of 83%.

For APO13-WP3 and Wp4, a score of 50% was obtained, while APO13-BP2 obtained 43%. The average of the three resulted in an APO13-2 score of 46%.

Furthermore, APO13-WP5 and WP6 obtained a score of 100%, while APO13-BP3 obtained 63%, resulting in an APO13-03 score of 80%.

The final value of Process Attribute PA1.1 for APO13 was calculated on the average of the three outcomes (APO13-01, APO13-02, APO13-03), namely ((83%+46%+80%/3), resulting in a final score of 70%.

3.3.2. Outcome Process DSS05

Process Number DSS05 has several derived processes that are used to determine the following results:

Table 7. Outcome of Process DSS05

Outcome	Description
DSS05-01	Network and communication security meet business needs.
DSS05-02	Information is processed, stored, and transmitted, by a protected endpoint device.
DSS05-03	All unique users are identified and have access rights according to their business roles.
DSS05-04	Physical measures have been put in place to protect the information from unauthorized access, damage and interference while it is being processed, stored, or transmitted.
DSS05-05	Electronic information is completely guaranteed when it is stored, transmitted or destroyed.

The sum of the Achievement/Outcome percentage determines the value of the Total Achievement PA 1.1 and Rating By Criteria for DSS05. However, the Achievement/Outcome percentage of each Outcome is determined based on the percentage of Achievement/Component. The components of each result are as follows:

Table 8. Components of each outcome in Process DSS05

Outcome	Component	Number	Description
DSS05-01	Work Product Output	DSS05-WP1	Malicious software prevention policies.
		DSS05-WP2	Evaluate potential threats.
		DSS05-WP10	Characteristics of security incidents.
		DSS05-WP11	Security event logs.
		DSS05-WP12	Security incident tickets.
		DSS05-WP13	Inventory of sensitive documents and devices.

		DSS05-WP14	Access rights.
	Base Practice + Work Product Input	DSS05-BP1	Protects malware.
		DSS05-BP2	Manage network security and connectivity.
		DSS05-BP7	Monitor infrastructure for security-related events.
DSS05-02	Work Product Output	DSS05-WP3	Connectivity security policies.
		DSS05-WP4	Penetration test results.
		DSS05-WP5	Security policies for endpoint devices.
	Base Practice + Work Product Input	DSS05-BP1	Protects against malware.
		DSS05-BP3	Manage endpoint security.
DSS05-03	Work Product Output	DSS05-WP6	User access rights are approved.
		DSS05-WP7	Review results from user accounts and privileges.
	Base Practice + Work Product Input	DSS05-BP4	Manage user identity and logical access.

The process component is obtained by dividing the total number of "Y" answers by the total number of questions for each component, as shown in the following table:

Table 9. Tabulation of audit assessment of process number DSS05

Number	Description	Achievement / Component	Achievements / Component	Outcome	Total Achievement PA 1.1 (APO13)
DSS05-WP1	Malicious software prevention policies.	57%	66% $\frac{(57\% + 75\%)}{2}$	DSS05-01	75% $\frac{(66\% + 70\% + 94\% + 46\% + 100\%)}{5}$
DSS05-WP2	Evaluate potential threats.				
DSS05-WP10	Characteristics of security incidents.				
DSS05-WP11	Security event logs.				
DSS05-WP12	Security incident tickets.				
DSS05-WP13	Inventory of sensitive documents and devices.				
DSS05-WP14	Access.				
DSS05-BP1	Protects against malware.	75%			
DSS05-BP2	Manage network and device security.				
DSS05-BP7	Monitor infrastructure.				
DSS05-WP3	Connectivity security policies.	67%	70% $\frac{(67\% + 73\%)}{2}$	DSS05-2	
DSS05-WP4	Penetration tests.				
DSS05-WP5	Security policies for endpoint devices.				
DSS05-BP1	Protects malware.	73%			
DSS05-BP3	Manage endpoint security.				
DSS05-WP6	The user's permissions are approved.	100%	94% $\frac{100\% + 88\%)}{2}$	DSS05-3	
DSS05-WP7	Review results from user accounts and privileges.				
DSS05-BP4	Manage user identities and login access.	88%			
DSS05-WP8	Approve access requests.	50%	46% $\frac{(50\% + 43\%)}{2}$	DSS05-04	
DSS05-WP9	Access logs.				
DSS05-BP5	Manage physical access to IT.	43%			
DSS05-BP6	Manage sensitive documents and output devices.	100%	100%	DSS05-05	

The tabulation results of the audit assessment of the DSS05 domain showed that each component value was obtained from the average respondents' answers. For the DSS05-01 Outcome, the DSS05-WP1, WP2, WP10 to WP14 components obtained an average score of 57%, while the DSS05-BP1, BP2, and BP7 components reached 75%. The combined average of the two resulted in a DSS05-01 final score of 66%. Furthermore, in Outcome DSS05-02, the average score from DSS05-WP3 to WP5 was 67%, while DSS05-BP1 and BP3 obtained 73%, making the final score 70%. For DSS05-03, DSS05-WP6 and WP7 obtained 100%, while DSS05-BP4 obtained 88%, resulting in a final score of 94%. In DSS05-04, DSS05-WP8 and WP9 obtained 50%, while DSS05-BP5 obtained only 43%, with a final result of 46%. Lastly, DSS05-05 only consists of DSS05-BP6 which gets 100% perfect. Thus, the total PA1.1

achievement in the DSS05 domain is calculated from the average of all outcomes, i.e. ((66% + 70% + 94% + 46% + 100%) / 5), which results in a final value of 75%.

3.3.3. Total Achievement for Each Domain

The total PA 1.1 achievements of each domain are entered into the following format to facilitate analysis and comparison of evaluation results. This format is used to present data in a systematic manner, making it easier to interpret and understand the level of achievement of each audited domain:

Table 10. Rating Domain APO13

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
APO13	**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
Rating by Criteria	70%	71%	100%	70%	71%	75%	85%	80%	33%
Rating	L	L	F	L	L	L	L	L	P
Capability Level Achieved	1	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

Based on Table 4.10, the results of the capability level assessment in the APO13 domain show that in PA 1.1 a rating by criteria of 70% was obtained with the category of Largely Achieved (L) at Level 1. For PA 2.1 at Level 2, the rating value of 71% was also categorized as L, but it was stopped (Stop!) because it had not met the threshold to proceed to the next level. Meanwhile, PA 2.2 reached 100% and was categorized as Fully Achieved (F), but it was still given a STOP! mark because PA 2.1 was not fully completed. The same thing happened with PA 3.1 (70%) and PA 3.2 (71%) at Level 3, both of which received an L rating with an achieved status but were also marked STOP!. At Level 4, PA 4.1 gets 75% and PA 4.2 gets 85%, both of which are in the L category and given STOP! status. At Level 5, PA 5.1 gets 80% (L) and PA 5.2 only 33% with a Partially Achieved (P) rating, which indicates that the process has not fully met the criteria. Overall, although some processes get high scores, achievement stalls at Level 1 because the COBIT principle requires all attributes in a level to be completed before moving to the next level.

Table 11. Rating Domain DSS05

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
DSS05	**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
Rating by Criteria	75%	96%	75%	80%	83%	67%	80%	100%	83%
Rating	L	F	L	L	L	L	L	F	L
Capability Level Achieved	1	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

Table 4.11 shows the results of the capability level assessment for the DSS05 domain. In PA 1.1 (Level 1), a rating by criteria of 75% was obtained with the category of Largely Achieved (L), which placed DSS05 at Capability Level 1. At Level 2, PA 2.1 obtained a score of 96% with the Fully Achieved (F) category, but the process was discontinued (STOP!) because PA 2.2 only reached 75% with the L category. Furthermore, at Level 3, PA 3.1 recorded a score of 80% and PA 3.2 of 83%, both in the L category with achieved status, but still marked STOP! because the consistency of completeness at the previous level has not been met. At Level 4, PA 4.1 got a score of 67% and PA 4.2 of 80%, both of which are also in the L category with achieved and STOP! statuses. At Level 5, PA 5.1 obtained a perfect score of 100% with category F, and PA 5.2 was 83% (L), but achievement at this level was also stopped (STOP!). Thus, despite some high achievements, the process in DSS05 is also held back at Capability Level 1 due to the COBIT assessment principle which requires the completeness of all attributes at one level before moving on to the next.

The results of rating by criteria are used as a reference in determining the ratings obtained based on:

A. N (Not Achieved)

   The Not Achieved category occurs when, the range obtained from the rating by criteria ranges from 0%-15%.

B. P (Partially Achieved)

   The Partially Achieved category occurs when, the range obtained from the rating by criteria ranges from 15%-50%.

C. L (Large Achieved)

   The Large Achieved category occurs when, the range obtained from the rating by criteria ranges from 50%-85%.

D. F (Fully Achieved)

The Fully Achieved category occurs when, the range obtained from the rating by criteria ranges from 85%-100%.

3.4. Assessment of Existing Results

The ratings obtained from each domain have been determined. The next step is to conduct an assessment of the existing results, which includes the following aspects:

A. Existing condition of APO13

The results obtained from the existing condition of APO13 include:

1. Companies already have basic mechanisms in place to manage application security, but they have not been formally and thoroughly documented.
2. The company has already carried out risk identification and assessment, but it is still reactive and not fully based on a systematic risk analysis.
3. Firewalls and encryption systems have been implemented, but there is still room for optimization in threat detection and prevention.
4. There is a monitoring mechanism for application security, but it is not entirely based on measurable metrics.
5. Roles and responsibilities in security management have been defined and communicated, but security training for employees is still limited.

Some resources for system security have been provided, but they are still insufficient for long-term needs.

B. Existing DSS05 condition

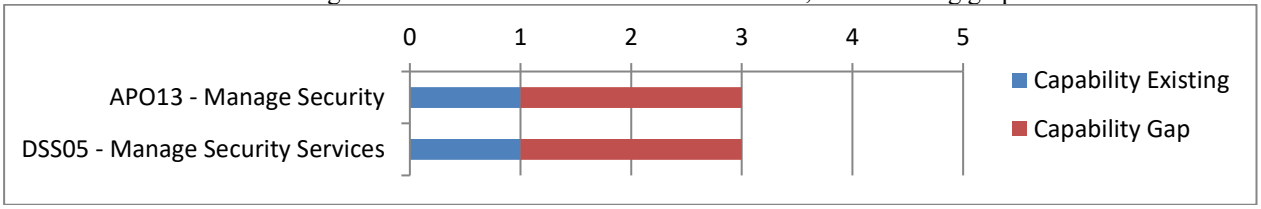
The results obtained from the existing conditions of DSS05 include:

1. A network security system has been implemented, but there is no integration with an automated monitoring system.
2. Security incident handling is already in place, but it is still reactive and does not yet have well-documented standard procedures.
3. Access and authorization rights have been implemented by user level, but Multi-Factor Authentication has not yet been implemented.
4. System security testing has not been conducted regularly, so potential security gaps may not have been fully identified.
5. Data from the system has been analyzed to understand security patterns and determine mitigation measures.

This research initially aimed to thoroughly evaluate each COBIT 5 domain using its process attributes. Upon analysis, the DSS05 domain demonstrated slightly stronger performance than APO13, particularly in areas related to operational execution such as access control and device protection. In contrast, the APO13 domain was found to be less developed, especially regarding the formalization of security policies and the formulation of long-term strategic plans. This suggests that the company shows greater maturity in technical operations (DSS05) than in strategic governance (APO13), highlighting a tendency to emphasize practical security measures over establishing a robust and structured security policy framework.

3.5. GAP

Gap is the difference between the target level that is to be achieved and the capability level that has been achieved. Based on the existing results for the APO13 and DSS05 domains, the following graph is obtained:



Picture 3. Existing Capability and Capability Gap Graph

The gap graph shows that the company wants level 3, but in reality the level of capability of the Human Resource Management System presence application used by PT. Dekatama Centra is still at level 1.

Both APO13 and DSS05 at Level 1 indicate that organizations have begun to implement application security practices and security services, but are still in their early stages and do not yet have robust standards. To upgrade to Level 2 onwards, organizations need to document, standardize, and integrate their security processes more formally.

3.6. Recommendations

Based on the results of APO13 and DSS05, there need to be several recommendations so that the level achieved can be achieved according to the company's wishes. Here are the resulting recommendations:

A. APO13 Recommendations
   1. Develop a more structured security policy document with clear operational guidance.
   2. Implement a more proactive risk mitigation strategy with the use of automated tools for threat analysis.
   3. Optimize end-to-end data encryption systems to ensure the security of user data.
   4. Implement Security Information and Event Management (SIEM) for real-time threat detection and monitoring.
   5. Implement attack simulations (Phishing test, penetration testing, etc.) so that users are better prepared to face real threats.

B. DSS05 Recommendations
   1. Improve the log monitoring system so that every activity in the system can be monitored and traced easily.
   2. Develop well-documented incident handling procedures to ensure a prompt response to threats.
   3. Implement Multi Factor Authentication (MFA) to improve the security of access to the system.
   4. Schedule penetration testing (pentest) every 6 months to identify possible security gaps.
   5. Conduct periodic assessments of employee compliance in implementing security policies.

4. CONCLUSION

Based on the security audit of the HRMS attendance application at PT. Dekatama Centra using the COBIT 5 framework in the APO13 and DSS05 domains, concluded that the system is at Capability Level 1 (Performed), which means that the security process is running but has not been well documented and is still reactive. The evaluation showed weaknesses in access management, activity monitoring, and incident response, even though some basic controls such as User ID, Password, and encryption were already in place.

To improve capabilities, in the APO13 domain, companies need to develop structured security policies, implement proactive risk mitigation, adopt SIEM, and routinely conduct threat simulations such as phishing tests and pentests. In the DSS05 domain, it is necessary to improve log monitoring, incident handling procedures, MFA implementation, and periodic security audits. The implementation of these recommendations is expected to encourage improved system security and achieve higher levels of capability on a sustainable basis.

ACKNOWLEDGEMENTS

We would like to express our gratitude to the Leadership of PT. Dekatama Centra who has given us the opportunity to conduct research, especially to Muhammad Syamroni as the IT project manager of PT. Dekatama Centra and Novianti Rahayu as Human Resource Development (HRD) who assisted us in filling out an assessment questionnaire for the security audit of the human resource management system attendance application using the Cobit 5 framework.

REFERENCES

[1] Lie Elke Melvinda Christian and Lina Sinatra Wijaya, “Analisis Strategi Komunikasi Human Resources Terhadap Penerapan Presensi Fingerprint,” *PRecious Public Relations J.*, vol. 1, no. April, pp. 158–176, 2021.

[2] B. A. Permana, “Aplikasi Presensi Online Menggunakan Validasi Jarak Lokasi Pengguna Berbasis Android,” *J. Inform. dan Rekayasa Perangkat Lunak*, vol. 3, no. 1, pp. 86–92, 2022, doi: 10.33365/jatika.v3i1.1865.

[3] A. Fajri, N. H. Safaat, and M. Affandes, “Analisis Manajemen Risiko TI Menggunakan Framework COBIT 5 Domain APO12 dan EDM03,” *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 3, pp. 1523–1530, 2023, doi: 10.30865/klik.v4i3.1396.

[4] J. Sidabutar, A. T. Zy, F. Juliarta, P. Nutug, and J. Barat, “Analisa Sistem Manajemen Keamanan Informasi (

SMKI) Organisasi Menggunakan Indeks KAMI Analysis Organization Information Security Management System (ISMS) Using Indeks KAMI," pp. 50–56, 2024, doi: 10.32938/jitu.v4i2.7747.

[5] M. W. Septyanto, H. Sofyan, H. Jayadianti, O. S. Simanjuntak, and D. B. Prasetyo, "Aplikasi Presensi Pengenalan Wajah Dengan Menggunakan Algoritma Haar Cascade Classifier," *Telematika*, vol. 16, no. 2, p. 87, 2020, doi: 10.31315/telematika.v16i2.3182.

[6] H. Honni, F. S. Lee, M. F. Isputrawan, I. I. Limawal, and J. F. Andry, "Audit Aplikasi Presensi Pada Perusahaan Industri Kosmetik Menggunakan Cobit 5," *Infotech J. Technol. Inf.*, vol. 9, no. 1, pp. 19–30, 2023, doi: 10.37365/jti.v9i1.153.

[7] M. Muthmainnah, S. Safwandi, M. Jannah, and V. Ilhadi, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Proses Dss03 Dan Mea01 Di Universitas X," *Sisfo J. Ilm. Sist. Inf.*, vol. 5, no. 1, pp. 1–12, 2021, doi: 10.29103/sisfo.v5i1.4848.

[8] ISACA, *Cobit 5 Business Framework*, vol. 23, no. 3. 2019.

[9] T. P. Y. Titan, R. Y. Rakhman Alamsyah, and S. Silkillah Adwa, "Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastika," *J. Account. Inf. Syst.*, vol. 6, no. 1, pp. 75–88, 2023, doi: 10.32627/aims.v6i1.680.

[10] 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.

[11] N. D. Ramadhani, W. H. N. Putra, and A. D. Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 5, pp. 1490–1498, 2020, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7259

[12] A. Rahman, I. Ahmad, and A. F. Oktaviansyah, "Perancangan Sistem Informasi Administrasi Penduduk Untuk Validitas Data Kependudukan Menggunakan Framework Codeigniter 4 (Studi Kasus: Desa Branti Raya, Natar)," *J. Teknol. dan Sist. Inf.*, vol. 3, no. 4, p. 3, 2022, [Online]. Available: http://jim.teknokrat.ac.id/index.php/JTSI

[13] R. Hidayat, K. Imtihan, and M. Ashari, "Penerapan Kerangka Kerja Cobit 5 Untuk Audit Sistem," vol. 7, pp. 195–203, 2024.

[14] B. Gunawan Sudarsono, V. R. Ananda, and M. R. Kardi, "Audit Aplikasi Keuangan Menggunakan Framework Cobit 5.0 Domain Dss Studi Kasus Perusahaan Peralatan Tambang Audit of Financial Applications Using the Cobit 5.0 Domain Framework Case Study of Mining Equipment Companies," *J. Bus. Audit Inf. Syst.*, vol. 6, no. 1, pp. 23–36, 2023, [Online]. Available: http://journal.ubm.ac.id/index.php/jbase

[15] C. Hanifurohman and D. D. Hutagalung, "Analisis Statis Menggunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E-Commerce Berbasis Android," *Sebatik*, vol. 24, no. 1, pp. 22–28, 2020, doi: 10.46984/sebatik.v24i1.920.