Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

GOVERNANCE EVALUATION ELECTRONIC SECURITY SYSTEM (Case Study: ABC Central Bank)

[1)]RZ Abdul Aziz, [2)] Anas Ikhsanudin*, [3)]M Said Hasibuan
[1,2,3)]Program Studi Magister Teknik Informatika, Fakultas Ilmu Komputer, IIB Darmajaya, Lampung
[1]rz.azis@darmajaya.ac.id, [2]anas.2221210055@.mail.darmajaya.ac.id , [3]msaid@darmajaya.ac.id

Submitted :Feb 27, 2024 | **Accepted** : Feb 29, 2024 | **Published** : Apr 1, 2024

Abstract: As we know, the role of the security system has a very important role for a state institution to provide security and comfort in carrying out its functions, such as the ABC central bank. A good security system is a security system that is supported by a reliable electronic security system and is composed of several components such as a closed circuit monitoring system, Access Control System, Security Alarm System, and Fire Alarm System. This system is very necessary to provide support for the duties of these state institutions to protect devices, data and electronic infrastructure from potential threats and security risks. The main functions of electronic security systems include prevention, detection, response to incidents, and recovery after disturbances/disasters. For this reason, efforts are needed to provide an evaluation of the system maturity level and information security management as a form of risk management to maintain the continuity of system use. This research uses the INDEKS KAMI 4.1 to map ESS governance maturity and the OCTAVE Allegro method to analyze information security management. From the analysis carried out, it has been concluded that the ESS implementation has been operated well in accordance with the security system requirements andas reached a good level of governance maturity. Information security management analysis carried out using the OCTAVE Allegro method has succeeded in identifying information security management with the result that information security management has been implemented well. This is proven by the existence of indicators, namely video recording data, log systems as information assets that have been managed and distributed according to authority

Keywords: INDEKS KAMI 4.1, OCTAVE Allegro, *Electronic Security System* (ESS), information security, governance, *maturity level*

INTRODUCTION

In order to control macroeconomic stability, a country requires the strategic role of the central bank. This strategic role is realized in the form of a policy mix, including one in terms of managing the stability of the financial system and payment system (Handayani et al., 2021). Central bank ABC as the monetary authority, has carried out its function as the central bank in country XYZ. In its operational activities, ABC central bank has used the electronic security system Electronic Security System (ESS) which functions as a means of controlling and monitoring the security conditions of the ABC central bank office complex because it has a high level of security risk. The implementation of an integrated security system is absolutely necessary so that the system can control security system components and equipment in a comprehensive integrated manner in one interface. This condition will make it easier for ESS operators to monitor, control access to personnel traffic, warn of security disturbances and early warning of fire hazards(Nath, 2021). Security disturbances can take the form of criminal acts of theft, both physical and data and information, which are expected to disrupt the continuity of the institution's duties. The ESS consists of several systems, namely:

CCTV

The CCTV monitoring system acts as a multimedia used to monitor operational activities of the ABC central bank office complex (Rizal et al., 2023). The results of monitoring recording are very useful for reviewing and analyzing operational activities that have been carried out, especially for activities related to payment systems.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Access control

Access control is used to control access for employees and third parties, including guests at office locations. This system functions to control the access rights of all personnel involved in office operational activities in accordance with the established Standard Operating Procedures (SOP). Only personnel who have full authority can enter all rooms. This system is equipped with an alarm system that will provide a warning (alarm) if there is a forced attempt to enter a room that is categorized as restricted and closed, so that this system can replace the role of conventional door locks with a better security system (Najib et al., 2021). The implementation of access control is carried out as a physical protection effort so that several locations that are considered closed and prohibited areas can only be accessed by employees who have received special authorization in accordance with their authority (Azhari & Mukhaiyar, 2021).

Security Alarm System

The security system functions to indicate a security disturbance through equipment installed around the office building, such as passive infrared and perimeter. Other supporting equipment in this system is the emergency button (panic button), foot switch (kick button) which is installed in the money management work area and critical areas such as the leadership room and control room(Hodgkinson et al., 2023). This system will respond when triggered by each installed component and forward the information to the control room to display a camera preview on the monitoring screen in that area. Likewise with the perimeter, this component will provide a warning signal to the main module in the control room if there is movement that crosses the infrared emitting area which is considered an attempt to penetrate the central bank office area (Williams et al., 2016).

Fire Alarm system

Namely an alarm system that can provide an initial warning of the emergence of a fire hazard based on the trigger input of a detector installed at the location where the fire or heat source occurs (Ma et al., 2020). These detectors can be fire detectors, heat detectors, gas detectors and smoke detectors. A trigger occurs when the detector detects changes in the situation around the sensor and continues the trigger to the main panel called the Main Control Fire Alarm (MCFA). The MCFA panel will then provide information to the main module as input for displaying the camera preview on the main screen of the control room. At the same time, in parallel, the MCFA activates an alarm indicating a fire hazard which signals the need for immediate evacuation of office building occupants. Several fire disaster management facilities were also activated along with the emergence of fire warnings such as sprinklers in the work area, fire suppression system in the server area and archive storage (Riyan, 2019).

In previous research, analysis was carried out on the maturity of system governance using Indeks KAMI and information security management using the OCTAVE Allegro method, namely:

Research 1

The OCTAVE Allegro method has been used at PT XYZ to assess the handling of information security management. This was done as risk mitigation against ransomware attacks on PT XYZ's information system which resulted in the company losing critical information such as project data and customer data (Deva & Jayadi, 2022).

Research 2

Research conducted at PT Donarta Hakiki Donarta Surabaya was carried out to analyze the implementation of company information security management. As a company operating in the retail sector, it is necessary to maintain company information assets in the form of customer data, suppliers, inventory data, sales transactions, product purchases, accounts receivable transaction data, and financial transaction data. This data is a critical asset that needs to be maintained to maintain the company's business in a sustainable manner (Saputra et al., 2019).

Research 3

An assessment of the maturity of E-Learning application governance carried out at XYZ University has concluded that E-Learning application governance is running well and in accordance with the expected targets. However, to improve performance, it is still necessary to increase the understanding and skills of E-Learning managers, especially in operating the E-Elearning application. Apart from that, it is necessary to assign special personnel to manage E-Learning so that these personnel do not have multiple duties and multiple positions, so they can focus more on managing E-Learning applications (Patria & Susanto, 2022).

Considering the important role of ESS for the operations of Central Bank ABC, it is necessary to evaluate the maturity level of ESS governance using INDEKS KAMI 4.1 and analysis of information security management using the OCTAVE Allegro method.

LITERATURE REVIEW

INDEKS KAMI 4.1

INDEKS KAMI is an elaboration of ISO/IEC 27001:2013 which can provide guidance for measuring the maturity level of system readiness in supporting the role of the security system. INDEKS KAMI is flexible in all

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

business process contexts and can be used periodically to identify changes in conditions that occur during ESS operations as a result of ABC central bank activities (Paramita et al., 2022).

This method has proven to be effective for analyzing system maturity governance because it involves all users in the system as respondents to participate in assessing the level of ESS reliability in managing the security system. The respondents in question are leaders, ESS application managers, users/operators and employees who act as objects for regulating the ESS security system. The purpose of carrying out the analysis of the ESS is as a form of evaluation of the feasibility of the system governance that has been implemented by the ABC Central Bank in an effort to improve service quality (Gala et al., 2020).

The advantage of using the INDEKS KAMI in assessing the maturity of information system security management is the evaluation of the Information Security Management System (SMKI) which is defined in the capability maturity model for integration (CMMI). The ISMS standard that will be used as a basis for assessment is ISO/IEC 27001:2013, which provides guidelines for maintaining the security of information assets, implementation, system maintenance and continuous system improvement.

The benefits gained from implementing ISMS that are oriented towards ISO/IEC 27001: 2013 are that the Institution has an ESS governance standard that is operated to support the management of the security system.

OCTAVE ALLEGRO

OCTAVE Allegro methodology emphasizes good information security management in agencies or institutions. The governance in question is governance in storing information, processing data into information and distributing it (Sanjaya, 2020). This method, developed by the Carnegie Mellon University Software Engineering Institute (SEI), is often used by companies or institutions, both private and government. This method is quite popular for providing assessments of information system implementation such as storing and distributing information as well as detecting information security threats (Gerardo & Fajar, 2022). Identification of these risks is related to the organization's behavior in carrying out its business processes and provides an assessment of the weaknesses of the systems that have been implemented (Gala et al., 2020). For this reason, it is necessary to evaluate the implementation of information governance in order to obtain ideal conditions for ensuring information security.

Figure 1. Information Security Concept(Iqbal Musyaffa, 2023)

Several aspects assessed through this methodology are information confidentiality, information integrity and information availability. According to research (Iqbal Musyaffa, 2023), the value of information confidentiality is defined by the implementation of a policy that information can only be accessed both within the organization and from outside the organization/institution for individuals or processes in the system whose validity can be trusted. For this reason, it is necessary to identify security vulnerabilities so that they can be overcome and exploited (Al Islami et al., 2016). This can be mitigated by authentication and authorization which are part of the information security protocol, namely:

Authentication

Part of the information security protocol whose role is to determine the identity of system users. Each system user is given a password and techniques for determining identity such as recognizing user identity using body parts (fingerprints), tokens, One Time Password (OTP) and so on.

Authorization

part of the information security protocol, has the function of determining user groups to access modules in the information producing system. Restricting access to this information is intended to maintain the confidentiality of institutional information.

Meanwhile, information integrity is part of the information security method which has the role of ensuring that existing information has a high level of data completeness and data accuracy so that the truth of the information can be trusted (Armadyana et al., 2023). Ease of gaining access is the final part of the information security protocol. This is intended so that authorized users can access information easily without space and time limitations. Apart from that, ease of access is also intended to ensure that data and information are always available when needed (Hermawan et al., 2022).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

METHOD

The ESS governance assessment method is carried out using the INDEKS KAMI, while the evaluation of information security management is carried out using OCTAVE Allegro. In general, the research was carried out according to the following flowchart.

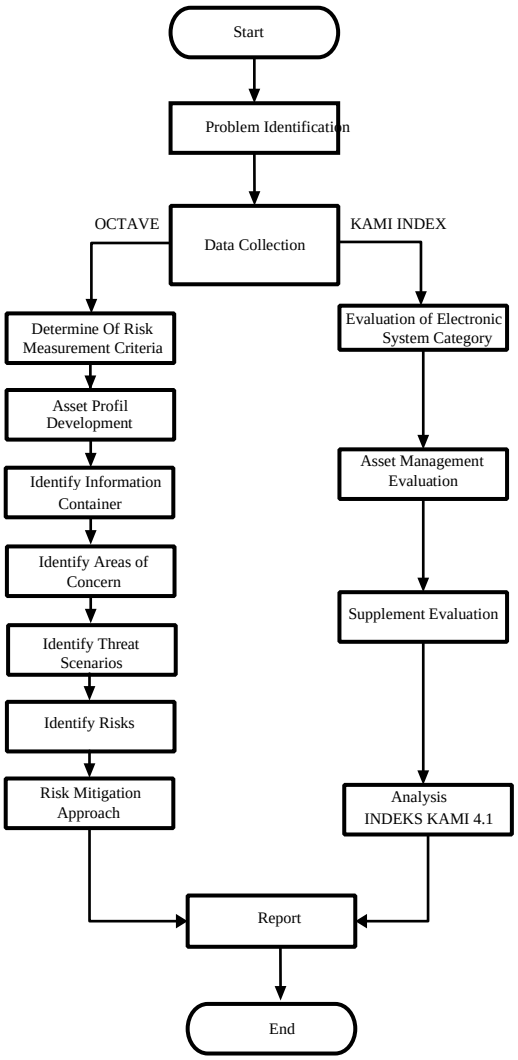

Figure 2. Research flowchart

Based on the flowchart, it can be understood that this research combines two methods and each method has its own framework sequence and produces a final conclusion regarding the maturity of system governance and the maturity of information security management in implementing ESS. The sequence of steps is as follows:

Identify the Problem

This research was carried out to assess the level of maturity of information security management in the use of the ESS system at ABC Central Bank.

Data Collection

In this research the data required is as users, object of observation and setting, security system support equipment, management and application

Obtaining these data was carried out through documentation studies, interviews, observations and filling out questionnaires.

Documentation Study

Collection of several documents related to ESS operations, including leadership policies, SOPs, work instructions, manuals, notes and memorandums related to ESS management and maintenance.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Interview
This activity was carried out to understand the ESS management that has been determined by conducting interviews with the leadership and management of the security system. Interviews are also aimed at finding out policy direction, leadership support and several other aspects related to the field of work (Ayu Setia et al., 2023) .

Observation
Observations were carried out to determine the regulations for the use of ESS in supporting the institution's operational activities, including observing and enforcing operator shifts, enforcing guard tours/physical security patrols (security units) in predetermined areas (Deva & Jayadi, 2022).

Questionnaire
Collecting information through questionnaires aims to obtain data on user awareness of the importance of using ESS by presenting a series of questions asked, both through print and electronic media, for example Google Forms or other applications (Setiya Budi & Tarigan, 2018).
Steps 3 to 9 are used to assess ESS information security management. These steps are included in the OCTAVE Allegro method.

Determination of Risk Measurement Criteria
Determination of risk measurement criteria is based on the scope of the central bank's duties, namely reputation risk, office operational security risk and task continuity risk. Next, an assessment of each criterion is carried out. From the assessment carried out, management direction and area ranking will be obtained based on the level of influence and risk impact on operational activities.

Development of Asset Profile
At this stage, critical information assets are identified which have an important role and greatly influence the continuity of the central bank's duties. The expected output from this stage is a profile of information assets in the critical category (Maya et al., 2020).

Identify Information Asset Containers
At this stage, the scope of information assets is identified based on 3 categories. The classification categories are technical, physical, people.
The three categories of containers are classified using worksheets 9a, 9b and 9c of OCTAVE Allegro [24].

Identify Areas of Concern
Area identification is carried out based on data from the previous stage, namely the information asset container to map potential areas by documenting them based on the Risk Measurement Table.

Identify Threat Scenarios
According to research (Saputra et al., 2019), threat scenario identification is used to determine the type of threat scenario including determining the probabilities that have been created previously.

Identify Risks
At this stage, research is carried out by analyzing previous data acquisition and conclusions will be obtained in the form of anticipatory steps for risks that may occur. In addition, the results of the analysis can be the consequences of threat scenarios that have been previously identified (Haeruddin, 2019).

Risk Mitigation Approach
After identifying risks, the next step will be determining the various risks that will be mitigated based on the results of previous identification. From the results of risk identification (risk measurement criteria), a review will then be carried out to determine mitigation approaches for risks that may occur.
Next, the analysis of the maturity level of ESS governance is carried out using INDEKS KAMI 4.1 in the following order:

Problem Identification and Data Collection
In the initial part of the analysis, problem identification and data collection are carried out as depicted in the flowchart.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Evaluation of Electronic System Reliability
This evaluation was carried out to assess the urgency/level of criticality of using ESS in providing support for the existing security system at ABC Central Bank. This is reflected in the large investment costs and maintenance costs of the ESS as well as the level of confidentiality of the data produced by the system.

Evaluation of Asset Management
This evaluation is used to assess the maturity level of asset management so that asset performance is always in optimal condition to support the security system. This evaluation includes activities to provide a list of assets, defining and level of importance of use asset. Apart from that, the evaluation also assesses the system's flexibility in supporting business processes. Evaluation of configuration settings and identity management (username and password) is also implemented in asset management evaluation.

Evaluate Supplements
Supplemental evaluation includes evaluation of the involvement of third parties as a support system in terms of asset management, incident management including recovery actions after security disturbances and disasters.

RESULT

Evaluation of ESS Governance Reliability

Evaluation of the reliability of ESS governance is carried out using the INDEKS KAMI with three evaluations carried out, namely Electronic System Category Evaluation, Asset Management Evaluation and Supplement Evaluation. Fulfillment of the data that will be evaluated is based on the results of interviews with respondents as follows:

a. The head of the central bank who oversees the ESS operational management unit;
b. ESS operational management;
c. ESS Operator;
d. Employee representatives as objects of monitoring and regulation;
e. Third party carrying out ESS maintenance.

The selection of respondents was carried out with the consideration that the respondents understood the ESS operating mechanism well.

Evaluation of Electronic System Categories

Based on the evaluation carried out, a score of 21 was obtained. This shows that the level of central bank dependence on ESS operations is very high. This is proven by seriousness in managing ESS equipment with indicators, namely:

a. The investment cost for procuring ESS equipment is more than IDR 3,000,000,000.00 (three billion rupiah); Routine maintenance costs for ESS equipment are more than IDR 380,000,000.00 (three hundred and eighty million rupiah);
b. Have a high level of data confidentiality;
c. Has an impact on institutional operations; thus affecting the quality of public services.

Evaluation of Asset Management

The results of the evaluation of ESS system equipment asset management show a score of 168. This shows that ESS asset management has been carried out well as evidenced by the establishment of several standardizations for asset management which are implemented comprehensively in terms of:

a. Providing a list of ESS equipment assets, defining ESS Equipment assets and evaluating the level of importance of information assets;
b. Changes have been implemented to systems, business processes and information technology processes including configuration changes in accordance with central bank business processes;
c. SOPs for the use of computer devices, electronic identity management and authentication processes through usernames and passwords have been implemented, including policies against violations of their use.

Suplement Evaluation
Based on the supplement evaluation that has been carried out, information has been obtained that management of sub contractors and third party services has been carried out with an average score of 3. This shows that:

a. Management of sub contractors/outsourcing to third parties has been running well. This is reflected in the orderly administration of cooperation agreements, performance monitoring and performance evaluation of third parties which have been implemented and well documented.
b. Management of the continuity of third party services related to system operations has been carried out well, including achieving service level targets (service level agreements).

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

c. Asset management procedures with third parties have been managed in good cooperation. This is proven by the establishment of procedures/SOPs for handling ESS equipment assets and information assets.
d. Procedures for handling incidents by third parties as affiliated parties have been established and managed well. This is proven by the existence of standard procedures relating to reporting, monitoring, analysis of incident handling by third parties as maintenance implementers and part of the recovery team after a disruption or disaster (disaster recovery).

Based on the research above, the results of the analysis of the reliability of ESS governance at the ABC central bank have been obtained using KAMI INDEX 4.1, namely that the security system has been operated properly in accordance with the security system requirements. The operated ESS has reached a good level of governance maturity. This is indicated by the seriousness of the ABC central bank in managing and maintaining ESS assets as well as preparing operational supporting factors by involving competent third parties in accordance with established provisions.

Evaluation of ESS Information Security

Information security evaluation for ESS is carried out using the OCTAVE Allegro method which consists of 9 steps, namely:

Identify the problem

This research was carried out to assess the level of maturity of information security management in the use of the ESS system at ABC Central Bank.

Data collection

To assess the maturity of ESS information security management, the data that has been collected is in the form of:

a. Users
There are 4 operator users, 1 administrator user, 2 badging PC users, 2 official users (leaders), each user has a role to run applications for CCTV monitoring applications, control room operator and system administrator.
b. Object of observation
Objects of observation and regulation of ESS include employees, third parties, guests/visitors,management systems.
c. ESS main equipment and supporting equipment
ESS supporting equipment includes hardware (server, CCTV Monitoring PC, Bading PC, leadership monitoring PC, LAN Switch, CCTV camera, Digital Video Recording (DVR), MCFA, access system panel and several fire alarm system supporting devices such as detectors and fire suppression system installed at the control location.
d. Management
Application management consists of a team of employees who are assigned to manage operations, manage maintenance and manage system configuration changes and other system changes.

Determination of Risk Measurement Criteria

Creating risk measurement criteria by conducting interviews with personnel who are the object of regulation and personnel involved in ESS operations.

Table 1. Risk Measurement I

Reputation, Trust and Productivity			
Impact Area	*Low*	*Medium*	*High*
Reputation and trust of employees, third parties and visitors	Trust of employees, third party employees and guests in reliability is very low	Employees, third parties and guests trust the reliability of using ESS	Employees, third parties and guests really trust the reliability of using ESS
Productivity	It does not have a direct impact on organizational performance productivity because ESS is operated to assist the physical security system		

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 2. Risk Measurement II

Finance and Security			
Impact Area	*Low*	*Medium*	*High*
Finance	Increase in operational costs using ESS is less than 2.5%	Increase in operational costs of using ESS is less than 2.5% - 5%	Increase in operational costs of using ESS by more than 5%
Security and Safety	Disruption of personal security and safety	Disruption of security and safety that can disrupt institutional operations	Disruption of security and safety which can disrupt the country's economy

As a follow-up to risk measurement, it is necessary to map priority areas of impact. The area mapping is explained in table 3.

Table 3. Priority Impact Areas

Impact Area	**Priority**
Security and Safety	1
Finance	2
Productivity	3
Reputation and trust of employees, third parties and visitors	4

Development of Asset Profile

At this stage, the evaluation carried out is to inventory critical assets that have a major influence on ESS operations. These assets are part of the information assets that are the object of information security management assessment. The information assets that are the focus for evaluation are CCTV recording data, access control logs, security system logs and fire alarm system logs.

Tabel 4. Asset Information Profile

Critical Asset	CCTV recording data, employee data, incident logs, both security system and fire alarm system logs.	
Rationale for Selection	CCTV recording data, employee data, security system logs and fire alarm systems have an important role in documenting every central bank operational activity.	
Description	CCTV recording data can be used as authentic evidence in carrying out tasks, including currency management. Incident logs also have an important role as a record of security disturbances and fire warnings.	
Owner	*Management ESS*	
Security Requirement	*Confidenciality*	CCTV recording data, employee data, security system logs and fire alarm systems are confidential and are only used for office operational documentation and audit purposes.
	Integrity	CCTV recording data, employee data, security system logs and fire alarm systems must be accessible and utilized by authorized employees for official purposes.
	Availbality	Always maintain the quality of CCTV recording data, CCTV recording data, employee data, security system logs and fire alarm systems so that the recording system can function properly. A log system is needed as a document for tracing every activity when there is a security disturbance and there is a threat of fire.

Based on this table, it can be concluded that CCTV recording data, employee data, security system logs and fire alarm system logs are identified as information assets which are important points in the ESS. This data must be maintained in availability, easy to access and maintain the validity of the data.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Identify Information Asset Containers

Container identification is carried out for the components of the information asset storage system, both internal and external components. These containers are generally divided into 3 categories, namely technical (hardware, software and internal or external), physical (in the form of hardcopy documents) and people (personnel assigned to manage the ESS). In table 5, there is an explanation of the container mapping.

Tabel 5. Asset Container Mapping (Technical)

Allegro Worksheet 9a-Data User	*INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)*
INTERNAL	
CONTAINER DESCRIPTION	*OWNER(s)*
1. Main server and backup server	ESS Management
(Local server used for ESS integration and configuring systems, SAS, ACS, and FAS).	ESS Management
2. NAS (Network Access Storage) Server. Server used to store all CCTV recording data.	ESS Management
3. Internal Network (LAN) Internal network that connects PCs and servers and other system components located outside the control room.	ESS Management
EXTERNAL	
CONTAINER DESCRIPTION	*OWNER(s)*
An external hard disk that is used as a medium for periodically backing up CCTV recordings after the NAS storage period reaches the maximum limit.	ESS Management

Tabel 6. Asset Container Mapping (Physical)

Allegro Worksheet 9b-Data User	*INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)*
INTERNAL	
CONTAINER DESCRIPTION	*OWNER(s)*
1. Operator Movement Book, Control Room Guest Book,	ESS Management
2. ESS maintenance log book Including recording setting changes, changing usernames and passwords, and replacing system components.	ESS Management
3. log book export CCTV recordings	ESS Management

Tabel 7. Asset Container Mapping (People)

Allegro Worksheet 9b-Data User	*INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)*
INTERNAL	
NAME OR ROLE RESPONSIBILITY	*DEPARTEMENT OR UNIT*
1. ESS Management Staff	ESS Management

Identify Critical System Conditions and Situations

At this stage, certain conditions are identified in system operational activities that could pose a threat to ESS information assets. Next, a review of the previous identification data is carried out and the factors that will influence it are well documented quality of established information asset security standards.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 8. System Critical Conditions (User Data)

No	*Area Of Concern -Data user*
1	There was an error when logging in
2	User data is changed by the administrator
3	Loss of user data
4	An unauthorized user attempts to log in to the system

Table 9. Critical System Conditions (CCTV recording data and system logs)

No	*Area Of Concern -Data Rekaman CCTV, Log Akses control, Log SAS dan Log FAS*
1	There is a recording function failure on the DVR and ACS, SAS and FAS
2	There was a failure of the Network Attach Storage (NAS) server and the main server
3	Recordings are lost/deleted accidentally
4	Unauthorized users try to delete CCTV recordings and system logs
5	Unauthorized disclosure or distribution of ESS data
6	Server down
7	Virus attacks (ransomware, malware, etc.)

Identify Threat Scenarios

At this stage, threat scenario identification is carried out by creating detailed threat scenarios by providing a detailed description of the forms of threats that occur.

Table 10. Detailed Threat Conditions

Asset Information	CCTV Recording Data, Employee Data, Incident Logs including Security System Logs, Access Control systems and Fire Alarm Systems.
Area Of Concern	There is a recording function failure on the DVR and ACS, SAS and FAS
	There is a failure of the NAS server and main server
	Recordings are lost/deleted accidentally
	Unauthorized users try to delete CCTV recordings and system logs
	Unauthorized disclosure or distribution of ESS data
	Server down
	Virus attacks (ransomware, malware, etc.)
1-*Actor*	Operators, third party technicians, employees and leaders
2-*Mean*	Sharing critical data intentionally or unintentionally, data affected by ransomware and not carrying out regular data backups, data damaged by virus attacks
3- *Motives*	Lack of understanding of the importance of information security management, lack of attention to server and NAS performance, lack of operator understanding of system operations
4- *Outcome*	[√] *Disclosure* [√] *Modification* [√] *Destruction* [√] *Interuption*
5-*Security Requirement*	Restrict access rights, perform regular data backups, distribute assets via company email, improve IT security features.
6- *Probability*	[√] *High* [ ] *Medium* [ ] *Low*

Identify Risks

After mapping threat scenarios, the next step is to carry out threat scenario analysis (as in Table 8) and identify risk mitigation that may occur and will have an impact on ESS operations.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 11. Calculation of Impact Area Scores

Impact Areas	*Pritority*	*Low* (1)	*Moderate* (2)	*High* (3)
Reputation and trust of employees, third parties and visitors	4	4	8	12
Finance	2	2	4	6
Productivity	3	3	6	9
Safety and health	1	1	2	3

Based on the table data, impact areas that have a high priority get a higher score. The score calculation formula is done by multiplying the priority level by the risk value (value). The results of the multiplication are then added up and a relative risk score value is obtained.

Tabel 12 Threat Probability Mapping

Relative Risk			
Probability	***Risk Score***		
	30 to 45	16 to 29	0 to 15
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

The risk mitigation approach is carried out by classifying each pool.

9. Risk Mitigation Approach

In the final part, a mitigation plan is carried out based on the mitigation approach that has been implemented.

Table 13. Mitigation Categories

Pool	***Mitigation Approach***
Pool 1	*Mitigate*
Pool 2	*Mitigate or Defer*
Pool 3	*Defere or Accept*
Pool 4	*Accept*

Table 14. Mitigation Approach

No	***Area of Concern***	***Prob***	***Risk Score***	***Pool***	***Mitigation Approach***
1	There was an error when logging in	Low	20	Pool 3	*Accept*
2	User data is changed by the administrator	Low	31	Pool 3	*Accept*
3	Loss of user data	Low	45	Pool 1	*Mitigate*
4	An unauthorized user attempts to log in to the system	Med	35	Pool 2	*Mitigate*
5	There is a recording function failure on the DVR and ACS, SAS and FAS	Med	40	Pool 2	*Mitigate*
6	There is a failure of the NAS server and main server	Med	40	Pool 2	*Mitigate*

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13540
e-ISSN : 2541-2019
p-ISSN : 2541-044X

7	Recordings are lost/deleted accidentally	Med	32	Pool 2	*Mitigate*
8	Unauthorized users try to delete CCTV recordings and system logs	Med	25	Pool 2	*Mitigate*
9	Unauthorized disclosure or distribution of ESS data (including user data/access rights)	Med	30	Pool 2	*Mitigate*
10	Server down	Med	40	Pool 3	*Mitigate*
11	Virus attacks (ransomware, malware, etc.)	Med	42	Pool 3	*Mitigate*

Tabel 15. Mitigasi Risiko

Information Assets	Risk	Risk Mitigation Efforts
Hardware (PC, Server, additional devices)	Hardware Damage	Schedule regular checks on hardware
	Theft and loss of important data.	Secure data with a username password policy and data encryption
	Memory Full	Check hard disk capacity and enforce memory space usage policies.
Software (records management, FAS and SAS management)	Software malfunction	Check for software updates and check system functions regularly.
SAS, FAS CCTV Incident Log recording data	Dissemination of data/information by personnel who do not have authority	Implement restrictions on the use of information storage and production devices. Create a licensing and approval mechanism for the distribution of information in stages Use encryption for any information that has been backed up to other media (other than the information generating device).
Network Devices	*Network Failure*	Carrying out network checks to ensure network reliability and readiness.
People (operators, technicians, management)	*Human Error*	Provide understanding by carrying out regular outreach to all teams involved.

DISCUSSIONS

Based on the research above, the results of the analysis of the reliability of ESS governance at the ABC central bank have been obtained using INDEKS KAMI 4.1, namely that the security system has been operated properly in accordance with the security system requirements. The operated ESS has reached a good level of governance maturity. This is indicated by the seriousness of the ABC central bank in managing and maintaining ESS assets as well as preparing operational supporting factors by involving competent third parties in accordance with established provisions.

Information security management analysis carried out using the OCTAVE Allegro method has succeeded in identifying information security management. Information Security has been carried out well, this is based on identification which has been implemented well

and 4 (four) impact areas that need attention have been obtained, namely:

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

1. Reputation and trust of employees, third parties and visitors;
2. Finance;
3. Productivity;
4. Security and safety.

Risk mitigation is carried out based on the Impact Area Score Calculation previously explained. There are 2 categories of risk management, namely mitigate and accept. Risk management in the mitigated category is carried out with the consideration that the area of concern has a large impact so that appropriate treatment/control must be carried out immediately to minimize the risk. There are risks that receive acceptance treatment, taking into account that these risks are risks that can be tolerated and have been anticipated by providing a unique user and password for each user.

CONCLUSION

The use of the INDEKS KAMI 4.1 to assess the maturity of ESS governance has resulted in the conclusion that central banks really need ESS operations to support central bank operations. The use of ESS has met the provisions and can meet the support needs for the security system.

Analysis of information security management carried out using the OCTAVE Allegro method has succeeded in identifying that information security management has been implemented well. CCTV recording data, system logs as information assets have been managed and distributed according to authority. This is characterized by several risk mitigation measures that are carried out related to the malfunction of the ESS system components that play a role information producers, namely CCTV, access control, Fire Alarm System and Security Alarm System.

REFERENCES

Al Islami, F. R., Izatie, S. N., & Destiana, I. (2016). Analisa Kebutuhan Keamanan Sistem Jaringan dan Aplikasi Dengan Metode Square (Studi Kasus PT Tawada Healthcare. *Sisfotek Global*, *06*(01), 30–34.

Armadyana, R., Yasirandi, R., & ... (2023). Analisis dan Penilaian Risiko Keamanan Informasi Menggunakan OCTAVE Allegro (Studi Kasus: PT. XYZ). *EProceedings …*, *10*(3), 3690–3703. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/20684%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/download/20684/19995

Ayu Setia, H., Safitri, E. M., Verina Renata Putri, & Wibowo, C. P. (2023). Analisis Keamanan Website Dinas Perhubungan Provinsi Jawa Timur Menggunakan Metode Octave Allegro Dan Fmea. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), 299–308. https://doi.org/10.33005/sitasi.v3i1.554

Azhari, F. A., & Mukhaiyar, R. (2021). Door Security System Menggunakan Teknologi Biometric Face Recognition. *Ranah Research : Journal of Multidisciplinary Research and Development*, *3*(3), 166–173. https://doi.org/10.38035/rrj.v3i3.397

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi Dan Informasi*, *12*(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

Gala, R. A. P. P., Sengkey, R., & Punusingon, C. (2020). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. *Jurnal Teknik Informatika*, *15*(3), 189–198. https://ejournal.unsrat.ac.id/index.php/informatika

Gerardo, V., & Fajar, A. N. (2022). Academic IS Risk Management using OCTAVE Allegro in Educational Institution. *Journal of Information Systems and Informatics*, *4*(3), 687–708. https://doi.org/10.51519/journalisi.v4i3.319

Haeruddin. (2019). Mapping Information Asset Profile In The Implementation Of Risk Management Information System Using Octave Allergo. *Journal of Information Technology Education: Research*, *3*(1), 67–75. https://doi.org/10.31289/JITE.V3I1.2601

Handayani, M., Talbani Farliani, Riski Fandika, & Indah Islami. (2021). Peran Bank Indonesia Dalam Menjaga Stabilitas Sistem Keuangan Di Tengah Pandemi Covid 19. *Jurnal Penelitian Ekonomi Akuntansi (JENSI)*, *5*(2), 171–182. https://doi.org/10.33059/jensi.v5i2.4515

Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(3), 125–130. https://doi.org/10.30591/jpit.v7i3.3428

Hodgkinson, W., Ariel, B., & Harinam, V. (2023). Comparing panic alarm systems for high-risk domestic abuse victims: a randomised controlled trial on prevention and criminal justice system outcomes. *Journal of Experimental Criminology*, *19*(3), 595–613. https://doi.org/10.1007/s11292-022-09505-1

Iqbal Musyaffa. (2023). *Definisi Keamanan Informasi & 3 Aspek Di dalamnya*. Https://Www.Agus-Hermanto.Com. https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya

Ma, Y., Feng, X., Jiao, J., Peng, Z., Qian, S., Xue, H., & Li, H. (2020). Smart fire alarm system with person

*name of corresponding author

detection and thermal camera. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12143 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-50436-6_26

Maya, E., Sesha, P. S. K., & Ningtias, J. P. (2020). Analisis Penilaian Risiko Pada Keamanan Sistem Informasi: Studi Literatur. *... Dan Sistem Informasi (JIFoSI ...*, *1*(2), 601–607. http://jifosi.upnjatim.ac.id/index.php/jifosi/article/view/87

Najib, A. A., Munadi, R., & Karna, N. B. A. (2021). Security system with RFID control using E-KTP and internet of things. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1436–1445. https://doi.org/10.11591/eei.v10i3.2834

Nath, R. (2021). DigitalCommons @ University of Nebraska - Lincoln Electronic Security Systems (ESSs) in Academic Libraries Electronic Security Systems (ESSs) in Academic Libraries. *Library Philosophy and Practice*, 18. https://digitalcommons.unl.edu/libphilprac%0ANath,

Paramita, S., Siregar, S. A., Damanik, R. A., & Dedi Irawan, M. (2022). Analisis Manejemen Resiko Keamanan Data Sistem InformasiBerdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374–379.

Patria, M., & Susanto, D. A. (2022). Penilaian Tata Kelola E-Learning Di Universitas XYZ Berdasarkan Kombinasi Standar Kuesioner Indeks KAMI Versi 4.0 dan Cobit 5. *Jurnal Tera*, *2*(2), 44–54.

Riyan. (2019). *Komponen Fire Alarm System*. Alatpemadamkebakaran.Co. https://www.alatpemadamkebakaran.co/komponen-fire-alarm-system/

Rizal, C., Iqbal, M., Noor Hasan Siregar, M., & Eka, M. (2023). Smart Home Berbasis Internet of Things (IoT) Dalam Mengendalikan dan Monitoring Keamanan Rumah. *Journal of Information System Research*, *4*(4), 1302–1307. https://doi.org/10.47065/josh.v4i4.3822

Sanjaya, J. (2020). Analisis Risk Assessment Terhadap Perusahaan It Octave Allegro Framework. *Jurnal Teknologi Informasi Dan Komunikasi*, *10*(1), 57–67.

Saputra, R. R., Setiawan, E., Ambarwati, A., & Informasi, J. S. (2019). Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVE Allegro pada PT. Hakiki Donarta Surabaya. *Jurnal Sains, Teknologi Dan Industri*, *17*(1), 1–10.

Setiya Budi, D., & Tarigan, A. (2018). Konsep Dan Strategi Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Dan Evaluasi Kesadaran Keamanan Informasi Pada Pengguna. *Tahun*, *2*(1), 53–64.

Williams, E. A., Cobbina, S. M., & Okrah, S. K. (2016). *Design and Implementation of a Dual Infra-Red Receiver Circuit for Intruder Detection*. *6*(5), 494–497.

*name of corresponding author