IV. RESULT

4.1. 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.

A. 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:

1) 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);
2) Have a high level of data confidentiality;
3) Has an impact on institutional operations; thus affecting the quality of public services.

B. 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:

1) Providing a list of ESS equipment assets, defining ESS Equipment assets and evaluating the level of importance of information assets;
2) Changes have been implemented to systems, business processes and information technology processes including configuration changes in accordance with central bank business processes;
3) 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.

C. 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:

1) 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.
2) 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).
3) 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.
4) 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.

4. 2. Evaluation of ESS Information Security

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

A. 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.

B. Data collection

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

1) 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.

2) Object of observation

Objects of observation and regulation of ESS include employees, third parties, guests/visitors,management systems.

3) 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.

4) 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.

C. 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		

Table 1. 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

D. 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.

Table 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.

E. 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.

Table 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 Attached 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

Table 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

Table 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

F. 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.

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.)

G. 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*

H. 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.

Table 11. Calculation of Impact Area Scores

Impact Areas	*Pritority*	*Low*	*Moderate*	*High*
		(1)	(2)	(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.

Table 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.

I. 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*
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*

Table 15. Risk Mitigation

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.