III. 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.
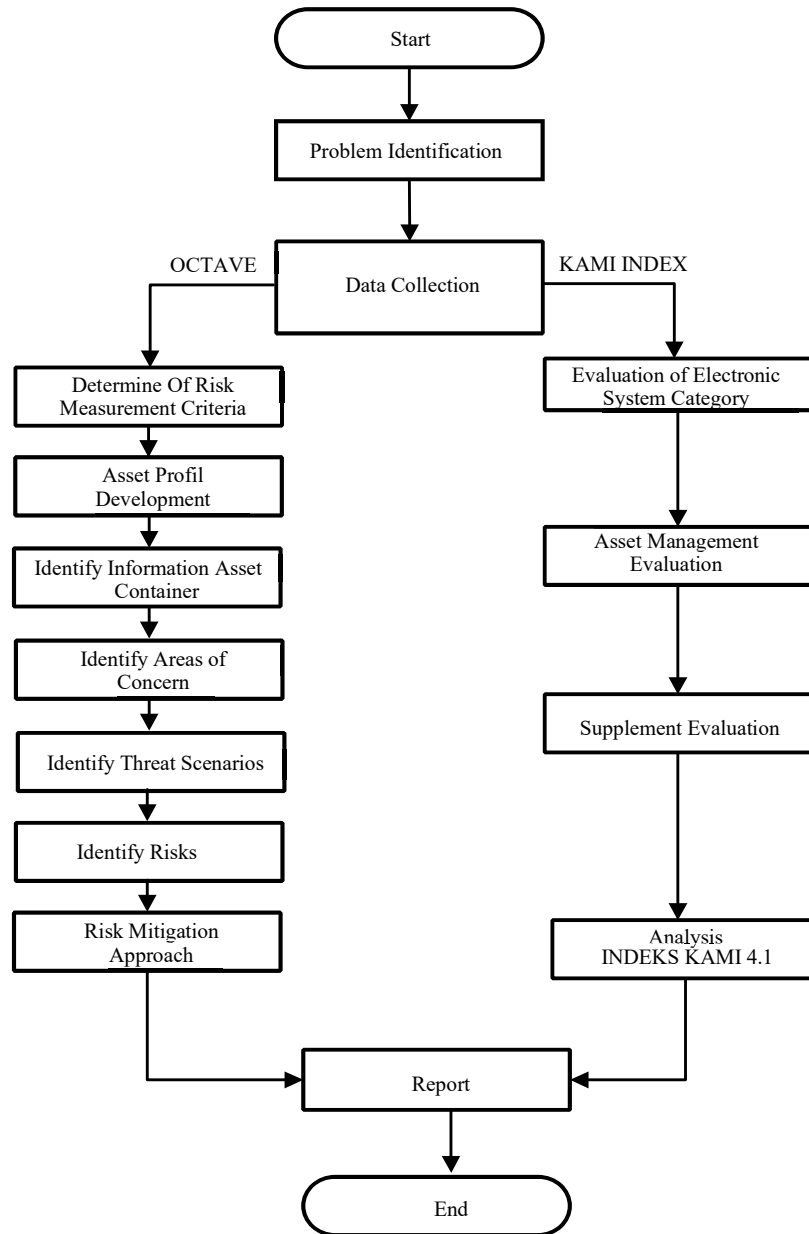

Figure 2. Research flowchart

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:

1. 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.

2. 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.

   a. 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.

   b. 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) .

   c. 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).

   d. 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.

1. 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.

2. 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).

3. 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].

4. 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.

5. 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.

6. 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).

7. 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:

1. 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.

2. 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.

3. 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.

4. 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.