II. LITERATURE REVIEW

2.1. 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 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.

2.2. 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:

a. 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.

b. 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).