Risk Assessment of Electronic Archive Services using Octave Allegro Method (Case Study: SIKN JIKN)

R A Herdianto*1, K Ramli1, Y Suryanto1
1Department of Electrical Engineering, Universitas Indonesia, Indonesia

*Corresponding author: rizal.aditya@ui.ac.id

Abstract. The National Archives Information System (SIKN) and the National Archives Information Network (JIKN) are the government national priority programs that aimed at providing web-based electronic archive treasury information facilities to the public. However, threat and disruption of critical information asset on electronic archives can cause interruption strategic objectives goals, vision, and mission of The National Archives of Indonesia (ANRI) in organizing archives that impact the network node, and the public. Therefore this research aims to analyze and identify risks in the SIKN JIKN electronic archive service and determine the potential risk of threats to important information assets. The OCTAVE Allegro method used to measure information security on five important information assets of the SIKN JIKN electronic archive information service. The results showed 64 areas of concerns analyzed, as many as 40 had to mitigate while the remaining 24 could be deferred or postponed. The conclusion of the risk assessment results in recommendations that must take to manage and protect critical assets in electronic archive services and supporting material for policymaking.

1. Introduction
The emergence of information technology has led to changes in the transformation of archives from conventional to electronic or digital which are increasingly efficient such as reducing physical damage to the original archive, archiving data transmission through a computer network using the metadata archive exchange protocol, assessing archive retention, processing, and storing archives [1]. The National Archives of Indonesia (ANRI) is a government agency with the main task of organizing archives [2]. Archiving services are indispensable for accessing archive information for the public or users and a source of treasures for historians and researchers in health, economy, society, and culture. In the aspect of the health sector, archives have an essential role in preservation, maintenance, and services during the pandemic as well as a media source of information on handling outbreaks about Covid-19 disease for future research [3].

SIKN or The National Archives Information System and JIKN or the National Archives Information Network are a dynamic archive and static archive information service facility that aims to provide electronic records access facilities for the public. The role of SIKN comprehensively collects archived information in the form of archive description. A custody institution manages it at the provincial, district, or city level called the Network Node. JIKN is used to provide archived information for the people gathered from various network nodes [4].
However, threats and disruptions to information technology can interruption the organization's primary business processes in the form of cyber-attacks, loss of electricity resources, damage, or loss of archive data due to negligence by the employees themselves [5,6]. This is a disorder that often occurs, especially in government agencies [7]. The threat of risk to electronic archives is very susceptible to changes in the authentication of the archive information itself [8]. If not appropriately managed, management of risk threats will harm ANRI in archiving services that will impact archive users or the public.

Therefore need a risk assessment method to anticipate threats and disturbances to electronic archive information [9]. This study discusses the formulation of the problems regarding risk assessment of the SIKN JIKN information system. Limitations in this study include two things, namely business processes related to electronic archive information services with the scope of data, applications, IT supporting infrastructure (software and hardware), and employees.

The basis for risk assessment in this study uses the Allegro OCTAVE method to assess a large operational risk environment with better risk assessment results and focus on important information assets that are owned and have an effect on the organization. The importance of information assets for organizations how these assets are used, transferred, processed, and stored as well as how threats, vulnerabilities, and disruptions cause business process obstacles to the organization [6]. The stages of risk assessment are arranged sequentially into four phases, carried out into eight steps. The four phases include the first Establish Driver is the organization developing risk measurement criteria based on the organization's strategic goals, vision, and mission. The second, Profile Assets, is to create and determine critical information assets for the survival of an organization's business. The third, Threat Identification is developing the risk profile of information assets by identifying threats that impact information assets and threat scenarios based on three platforms (technical, physical, and people). Fourth, by identifying risks and determining mitigation approaches from the results of identification and analysis of threats or disturbances to critical information assets and developing strategic steps to overcome the risks that occur.

2. Research Methodology

The research began by conducting interviews with the Head of SJIKN Center, Head of System Development and JIKN, Archivists, and related IT Staff to explore existing problems, policies, hopes, and desires to conduct direct observations to obtain the data needed. Also, interviews were carried out in more depth to explain the importance of information technology risk assessment to the respondent. There are eight steps to the risk analysis and evaluation of the SIKN JIKN system in the risk assessment in the OCTAVE Allegro method.

![Figure 1. Steps for Risk Assessment in the OCTAVE Allegro method [6].](image-url)
3. Results and Discussion

The methodology stage, the following are the results of the analysis of each phase carried out in this study.

3.1. Establish Risk Measurement Criteria

In this first stage consists of two activities in identifying the area of impact of the organization through risk measurement criteria. The first activity is to formulate and qualitatively measure the area of risk impact determined by considering the effect on the organization in the event of threats and disturbances as in table 1. Then, the second activity of the results of the impact area is determined by prioritizing the scale with the most critical value (highest score) to the least important (lowest score) as in table 2. The priority scale of the area of impact will be used in risk assessment to develop a relative risk score that can help the organization decide what mitigation measures to take.

| Impact Area | Low | Medium | High |
|-------------|-----|--------|------|
| Reputation  | Organizational reputation has little effect; no business or small business is needed for repairs. | Organizational reputation is quite bad, and it takes effort and cost to repair. | Organizational reputation has a bad impact, and it takes effort and cost to repair. |
| Customer Confidence | There is user trust to access archived information access through SIKN JIKN. | There is still the confidence of some users who still access archived information through SIKN JIKN. | No user trust accesses archived information through SIKN JIKN. |

| Priority | 5 | 1 | 3 | 4 | 2 |
|----------|---|---|---|---|---|
| Impact Areas | Reputation & Customer Confidence | Financial | Productivity | Safety and Health | Fines and Legal Penalties |

3.2. Develop an Information Asset Profile

In the second stage, the OCTAVE Allegro method has eight activities that are described in the critical information asset form. It starts by identifying groups of information assets that are related to the organization's operational business processes. The second and third activity, consider the real impact of critical information assets that are the main objective and vision and mission of the organization in the event of threats and disturbances and then compiled into the Critical Information Asset Profile form. The fourth activity explains the reasons for selecting critical information assets in this profile. Fifth, make a general description to explain the information assets and identify who owns the information assets. The last activity identifies the potential risk impact of information assets on the most important security requirements.

| Critical Asset | Archival Description |
|----------------|----------------------|
| Rational for Selection | Archival description plays a role in identifying, managing, discovering or searching, explaining the records in question, the context, and the management system of the archives that created them, and supporting the exchange of archive data from different systems. |
| Description | Archival description is information attached to an archive to explain the context and contents that are useful in searching archive information so that it is easily identified, managed, and accessed. It has standard data elements that are used in providing widely structured or semi-structured descriptive information in archives. |
| Owner | Network Node |
**Critical Asset**  
Archival Description

| Security Requirement | Confidentiality | Integrity | Availability |
|----------------------|-----------------|-----------|--------------|
| Confidentiality      | Archival metadata information is vital for network centers, network nodes, and archive users. Only the Archive Manager or Network Node can authorize the archive information. |
| Integrity            | Archival metadata information must be correct following the results of the archive description. It can be changed by archivists and archive managers or network nodes. |
| Availability         | Archival metadata information in open categories must always be available to archive users. |

**Most Important Security Requirement**  
Integrity: Archival metadata information is vital for archive users if there is a change in the archive metadata information. It makes it difficult for archive users to search the source or archival treasures.

3.3. **Identify Information Asset Containers**
This stage identifies by considering three critical issues related to security and the concept of the container of information assets based on the risk environment map such as technical, physical, and people. This container describes how information assets are protected from vulnerabilities or threats to information asset containers are managed internally and externally.

**Tabel 4. Example of Information Asset Risk Environment (Technical) – Archival Description**

| Container Description | Owner(s) |
|-----------------------|----------|
| Inter                 | Development of SJKN |
| Archive metadata stored by the Network Node Admin through the SIKN application and displayed through the National Archives Information Network (JIKN) application. |
| External              | Network Nodes |
| Network Node Admin uses the SIKN Application to store and manage archive metadata, create reporting results from report generate features, store metadata in bulk, synchronize metadata with XML standards. |
| Archive Users          | Archive Users |
| Archive users search archival information based on archive metadata displayed through the JIKN application. |

3.4. **Identify Areas of Concern**
In the fourth step, it starts by developing a risk profile for the SIKN JIKN information assets by conducting interviews with related parties to determine the threat component of the situation and conditions that can threaten the information assets of the archive.

**Tabel 5. Example of an Area of Concern**

| Area of Concern |
|-----------------|
| There is an interruption in the RHV server down impact on the JIKN application so that archive users cannot access the archive metadata. |

3.5. **Identify Threat Scenarios**
In the fifth step, identify a broader threat scenario that has not been accommodated in the Area of Concern through questionnaires. Threat scenarios are arranged in more detail based on the threat of tree structure. Each scenario is identified and described based on the characteristics of the threat property.
### Tabel 6. Example of Information Asset Risk Environment (People) – Incompleted of Information

| Area of Concern | Threat of Properties |
|-----------------|----------------------|
| Errors and incompleteness of archived metadata information cause SIKN Application report results to be inappropriate. | 1. **Actors** Admin SIKN |
|                  | 2. **Means** SIKN admins do not input complete mandatory elements of archive metadata |
|                  | 3. **Motives** Human Error (Accidental) |
|                  | 4. **Outcome** Destruction/Loss |
|                  | 5. **Security Requirements** SIKN admins ensure the mandatory input of mandatory archive metadata elements. |
|                  | 6. **Probability** Medium |

#### 3.6. Identify Risk
In the sixth step, determine the consequences of the threat scenarios developed and the impact on the organization or owner of critical information assets. The results of consequences are measured based on the qualitative value of the impact area and calculate the quantitative score calculated from each of the impact area values and the result of the entirety.

### Tabel 7. Calculate Risk of Impact Area Scores

| Impact Areas                        | Priority | Low (1) | Moderate (2) | High (3) |
|-------------------------------------|----------|---------|--------------|---------|
| Reputation and Customer Confidence  | 5        | 5       | 10           | 15      |
| Financial                           | 1        | 1       | 2            | 3       |
| Productivity                        | 3        | 3       | 6            | 9       |
| Safety and Health                   | 4        | 4       | 8            | 12      |
| Fines and Legal Penalties           | 2        | 2       | 4            | 6       |

#### 3.7. Analyze Risk
The seventh step is about the risk analysis process by giving a quantitative value of how much influence the threat poses to the organization. The first activity starts by considering the risk measurement criteria. The second activity calculates the relative value of risks used to analyze risks and determine the best strategy to reduce the impact of the risk.

### Tabel 8. Example of Properties of Threat – Corrupt Information Archival Descriptions

| Area of Concern | Risk | Consequences |
|-----------------|------|--------------|
| Archived metadata information is corrupt, or data does not appear during the process of changing the archive structure, updating the status of the publication, or the process of mass import through a browser. | The perception of the quality of archive information for archive users gives a negative impression on the organization's services. There are additional IT Staff working hours to analyze, repair, and restore access. As a result of interference, the level of information security on legibility and access to archived metadata is low. |

#### Relative Risk Score 36

| Impact Area                  | Value | Score |
|------------------------------|-------|-------|
| Reputation & Customer Confidence | High (3) | 15    |
| Financial                    | Low (1) | 1     |
| Productivity                 | Moderate (2) | 6     |
| Safety and Health            | High (3) | 12    |
| Fines and Legal Penalties    | Low (1) | 2     |

**Impact Area**

**Value**

**Score**
3.8. Select the Mitigation Approach
At this last stage, it is to sort each risk that has been identified based on the value of risk analysis in step seventh. This sorting activity is carried out to assist the organization in deciding the status of the type of mitigation approach that needs to be done at the risk area of concern.

**Table 9. Relative Risk Score**

| Relative Risk Matrix | 30 to 40 | 16 to 29 | 0 to 15 |
|----------------------|----------|----------|---------|
| Risk Score           | Pool 1   | Pool 2   | Pool 3  |

The calculation of quantitative risk scores is the probability of the area of concern and the consequences to determine one of the status categories such as mitigation, defer, or accept in figure 2.

**Table 10. Determine the Mitigation Approach**

| Mitigation Approach | Mitigate | Defer | Accept |
|---------------------|----------|-------|--------|
| Pool                | Pool 1   | Pool 2 | Pool 3 |

**Figure 2. Mitigation Approach Results.**

4. Conclusion
The results of risk assessment can support material to make risk management policies in preparing strategic planning of important electronic archive information security. It also can be used in developing comprehensive mitigation measures appropriate to the security of information assets that are archive from threats and disturbances that have occurred, are, or will occur. By implementing a risk assessment, SIKN JIKN can maintain and improve information security by knowing the potential threats, disturbances, and vulnerabilities to reduce losses on archives' information assets. Identifying risk assessments from 64 areas of concern resulted in an output in which 40 areas of concern had to mitigate, while 24 areas deferred.

**Acknowledgements**
This research publication was funded by the University of Indonesia's PUTI grant program (contract number: NKB-1079/UN2.RST/HKP.05.00/2020).

**References**
[1] Meng T and Hui L 2017 Application of Information Technology in Digital Archives Management *Proceedings of the 2017 International Conference on Education and E-Learning - ICEEL 2017* the 2017 International Conference (Bangkok, Thailand: ACM Press) pp 81–3

[2] Act No. 43 of 2009 about Archives (Indonesia)
[3] Quintana, A. and Nazar, M., 2020. [online] Ica.org. Available at: <https://www.ica.org/sites/default/files/the_role_of_archives_in_the_covid_19_crisis.pdf> [Accessed 6 July 2020]

[4] Grand Design of SIKN JIKN 2020-2024 (Indonesia)

[5] Bearman D Moments of Risk: Identifying Threats to Electronic Records 32

[6] Caralli R A, Stevens J F, Young L R and Wilson W R 2007 Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: (Fort Belvoir, VA: Defense Technical Information Center)

[7] Mohamad Ramli A A and Kadir Wan Dollah W A 2010 Threats to electronic records in Malaysian government organizations 2010 International Conference on Science and Social Research (CSSR 2010) 2010 International Conference on Science and Social Research (CSSR) (Kuala Lumpur, Malaysia: IEEE) pp 228–33

[8] R. Assessment, “Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools ‘Survey of existing Risk Management and Risk Assessment Methods’) Conducted by the Technical Department of ENISA Section Risk Management,” no. June, 2006

[9] Jouini M, Rabai L B A and Aissa A B 2014 Classification of Security Threats in Information Systems Procedia Computer Science 32 489–96