Data and Information Security Analysis in Risk Management Using OCTAVE-S Framework and ISO 27001:2022

Aura sevryan[1], Rini Indriati[2]*, Dwi Harini[3]
UN PGRI Kediri, Kediri, 64112, Indonesia
e-mail: aaurasev@gmail.com, rini.indrianti@unpkediri.ac.id, dwiharini@unpkediri.ac.id
* Corresponding Author

Abstract: *This study examines security policies from a governance perspective within an institution to assess the level of security of assets, data, and information. The results of this study aim to analyse risks and assist the institution in mitigating those risks. This study uses a literature review of previous studies that focus on the OCTAVE-S Framework and ISO27001:2022. The subject of the study is the Academic System, while the object is UN PGRI Kediri University. The method used is based on ISO 27001:2022 and uses the OCTAVE-S framework. The research data was obtained by conducting interviews with university officials, particularly those responsible for the implementation and security of data and information. From the interview results, the assets were then identified, consisting of the categories of system information and applications, and the second was people (human resources). Next, a classification was made containing a description of the risk level, with the aim of conducting a stoplight assessment. The next step was to classify the interview results into 15 types of security practice evaluations and assign them a stoplight rating as defined earlier. Security aspects with a red stoplight rating were used to produce a risk mitigation document referring to ISO 27001:2022.*

Key Words*:* Academic system; ISO 27001 2022; OCTAVE-S; Data and information security.

Introduction

An academic information system is a structure used by educational institutions to facilitate academic administration processes, such as student registration, learning processes, and the management of lecturer and student data (Jamilatulain, 2024). PGRI Kediri University has an academic information system called SIAKAD. This system has been implemented and is actively used at UNP Kediri. SIAKAD not only facilitates administration, but also provides easy access to information for students and teaching staff. SIAKAD serves to support and process all academic information, such as student registration, course schedule selection, and Study Plan Card (KRS) selection.

SIAKAD processes all data and information related to academic activities so that it can be well integrated and support smooth operations and decision-making within the university. Although functionally, the UN PGRI Kediri academic system has been operating well, to date there has been no evaluation of data and information security as part of risk management. Therefore, to reduce the possibility of risks to the academic system, a comprehensive analysis and evaluation of the system is required. This will enable the campus IT department to identify risks and the level of vulnerability of each critical asset. This information will be used to implement appropriate controls for each critical asset based on the level of risk priority as determined by the analysis of the UN PGRI Kediri academic system.

The use of the appropriate framework can reduce information security risks and assist certain institutions in risk mitigation (Putri et al., 2022). Therefore, this study will explore risk management using the OCTAVE-S and ISO 27001:2022 frameworks to improve the security of the UN PGRI Kediri academic system.

The Operationally Critical Threat, Asset, and Vulnerability Evaluation-Small (OCTAVE-S) method is a variation of the OCTAVE method that focuses more on organisations with a smaller scope so that risk analysis and mitigation processes are faster and more targeted (Allen, 2023). The results of the analysis from data processing using OCTAVE-S are used to create risk mitigation based on ISO 27001.

Based on the above explanation, this study focuses on information security analysis in risk management to reduce, assess, and control risks to related systems in order to determine the level of security and provide a reference for risk management (Phirke & Ghorpade-Aher, 2019).

The results of this study are risk management analyses to determine the impact and threats to the system. Furthermore, the analysis is used to create risk mitigation by understanding the threat level to the UN PGRI Kediri academic system. It also provides control recommendations based on ISO 27001:2022 so that it can be used as a guideline document in creating security and information policies.

Method

OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation-Small) is a risk management framework focused on small organisations with fewer than 100 people (Syamsuar, Firdaus, & Lonando, 2023). The process in the OCTAVE-S framework can be seen in Figure 1 below.

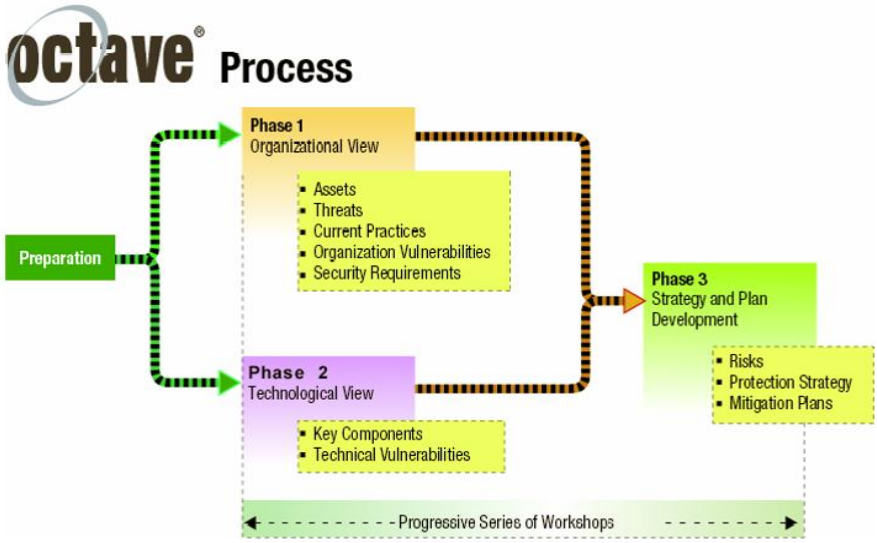

Figure 1. OCTAVE-S Method

OCTAVE-S is designed to help organisations identify and manage data and information security risks using a structured and more easily implemented approach (CIO Wiki, 2022).

The OCTAVE-S framework has three phases, namely:

The first phase consists of two processes, namely organisational information identification and threat profiling. These two processes involve four activities, including identifying organisational information assets, evaluating security practices, selecting critical assets, and identifying threats to previously identified critical assets (Rohman, Ambarwati, & Setiawan, 2020). Critical assets are assets of the organisation that, when experiencing a problem, will have a negative impact on the organisation. These impacts can include operational disruptions, financial losses, damage to reputation, and even legal violations (Rido Butar Butar et al., 2023).

The list of assets at PGRI Kediri University in managing the SIAKAD system, based on interviews with service and system managers, is as follows:

Table 1. Asset Identification

No	Categories	Assets
1	Information, Systems, and Applications	• SIAKAD System • Servers, network infrastructure, and databases • Standar Operasional Prosedur (SOP)
2	People	• Leaders/Heads of units • System Development Coordinators • Data and Network Infrastructure Coordinators

The next step is to create a risk level description containing values between 1 and 5 with levels and level descriptions. This risk level is used to assess the evaluation of security practices. The results of the risk level description are as follows:

Table 2. Risk Level Description

Impact Value	Level	Description
1	Green (Low)	No corrective action is required in the near term.
2-3	yellow (Medium)	There are corrective actions and plans for improvement within a specified time frame.
4-5	Red (High)	There is a strong need for corrective action.

After mapping threats based on their level of risk, the author continued by compiling a list of more structured and targeted questions. These questions were prepared as a guide for the interview process so that the information obtained could provide a comprehensive picture of the system's security status (Setiawan, 2020). The main focus of the questions was to understand how each threat could impact the system, the extent to which controls had been implemented, and how the relevant parties assessed their readiness to deal with risks.

The list of questions was then used in interviews with those responsible for managing the SIAKAD system and services. The answers provided are then collected, analysed, and processed systematically to produce more objective conclusions. The results of the analysis

form the basis for determining the stoplight category, which is an indicator that shows the status or level of security readiness in each part of the system, thus providing a clear picture of the priorities for improvement that need to be addressed.

Table 3. Evaluation of Security Practices

No	Security Aspects	Stoplight
1	Security Awareness and Training	Yellow
2	Security Strategy	Green
3	Security Management	Green
4	Security Policies and Regulations	Red
5	Collaborative Security Management	Green
6	Contingency Planning/Disaster Recovery	Red
7	Physical Access Control	Green
8	Monitoring and Auditing Physical Security	Red
9	System and Network Management	Green
10	Monitoring and Auditing IT Security	Yellow
11	Authentication and Authorization	Green
12	Vulnerability Management	Yellow
13	Encryption	Green
14	Security Architecture and Design	Green
15	Incident Management	Red

Based on the results of the organisation's security practice evaluation, there are four stoplights with red status, which means that the organisation or agency has not implemented the security practices documented in the rules or SOPs, three with yellow status, which means that the organisation or agency has implemented some of the security practices and therefore requires minor improvements, and eight with green status, which means that the organisation or agency has implemented the security practices and no corrective action is required. The security aspects with red status are used to develop mitigation measures (Setiawan, 2020).

The second phase is the identification of vulnerabilities in the organisation's infrastructure. Based on interviews and the results of the security practice evaluation, the security practices and threats are represented in the following table.

Table 4. Safety Aspects with Red Traffic Lights

No	Security Aspects	Threats
1	Security Policies and Regulations	No formal documents governing security policies and procedures.
2	Contingency Planning or Disaster Recovery	No documented plans for disaster recovery or system rollback.
3	Monitoring and Auditing Physical Security	No documentation of maintenance performed.
4	Incident Management	No written procedures governing incident management.

Critical assets refer to data, information, and resources that are important to an organisation. Critical assets in academic systems can include the following aspects:

a. Systems for learning processes, such as places for delivering material, examinations, and journal publications
b. Academic administration systems, such as student registration, lecture schedules, and transcripts
c. Data and network infrastructure containing servers and databases.
d. Responsible actors who have knowledge and expertise regarding the academic system, have access rights, and have control in making decisions.

A threat profile refers to an overview of potential threats to an organisation's assets. Developing a threat profile provides a clear understanding of the threat risks faced by the organisation, enabling it to take appropriate mitigation measures.

The third phase is to develop a security strategy and control recommendations based on a risk mitigation plan that complies with ISO 27001:2022 for previously defined threats. The results of the control recommendations are as follows:

Table 5. Control Recommendations

No	Security Aspects	Controls According to ISO 27001:2022	Recommendations
1	Security Policy and Regulations	1) A.5.1 Policies for information security	1) Information security policies and specific topic policies must be established, approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and when significant changes occur
		2) A.5.36 Compliance with policies, rules and standards for information security	2) Compliance with the organisation's information security policies, specific topic policies, rules and standards must be reviewed periodically
2	Contingency Planning or Disaster Recovery	A.8.26 Application security requirements	Information security requirements must be identified, defined and agreed upon when developing or acquiring applications.
3	Monitoring and Auditing Physical Security	1) A.8.16 Monitoring activities	1) Networks, systems and applications must be monitored for anomalous

				behaviour and appropriate action taken to evaluate potential information security incidents.
		2)	A.5.22 Monitoring, review and change management of supplier services	2) Organisations must periodically monitor, review, evaluate and manage changes in suppliers' and service providers' information security practices.
4	Incident Management	1)	A.5.24 Information security incident management planning and preparation	1) Organisations should plan and prepare for information security incident management by defining, establishing and communicating the processes, roles and responsibilities for information security incident management.
		2)	A.6.8 Information security event reporting	2) There are no written procedures governing incident management.
		3)	A.5.26 Response to information security incidents	3) Information security incidents must be responded to in accordance with documented procedures
		4)	A.5.27 Learning from information security incidents	4) Knowledge gained from information security incidents must be used to strengthen and improve information security controls

Results and Discussion

Based on the control recommendations, four security aspects were identified as requiring attention due to their status with red stoplight and need for immediate improvement. These security aspects received nine control points and recommendations based on ISO 27001: 2022.

Conclusion

The OCTAVE-S framework successfully mapped critical assets, security aspects, and threat identification, and provided risk mitigation recommendations based on ISO 27001:2022. The results are accurate and can be used as guidelines for creating formal documents related to standard operating procedures for working with and securing data and information.

References

Allen, C. (2023). Threat Modeling Methodology: OCTAVE. Retrieved November 28, 2024, dari https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies#:~:text=OCTAVE%2DS,(less%20than%20100%20people).

CIO Wiki. (2022). OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation). Retrieved November 28, 2023, dari https://cio-wiki.org/wiki/OCTAVE_%28Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation%29?form=MG0AV3

Geograf. (2023, November 28). Pengertian Keamanan Data: Definisi dan Penjelasan Lengkap Menurut Ahli, dari https://geograf.id/jelaskan/pengertian-keamanan-data/?form=MG0AV3

Jamilatulain. (2024). Pengertian Sistem Akademik. Retrieved November 28, 2024, dari https://redasamudera.id/pengertian-sistem-akademik/?form=MG0AV3

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. NUANSA INFORMATIKA, 18, 46-54.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. Dalam TQM Journal (Vol. 33, Nomor 7). https://doi.org/10.1108/TQM-09-2020-0202

Galih, A. P. (2020). Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas. AL Maktabah, 5(1). https://doi.org/10.29300/mkt.v5i1.3086

Kurniawan. (2013). MANAJEMEN RISIKO TEKNOLOGI INFORMASI.

Kurniawan, A. N., & Hanggara, B. T. (2020). Penerapan Manajemen Risiko Teknologi Informasi menggunakan Metode OCTAVE-S pada UPT Pusat Komputer Politeknik Negeri Malang. Pengembangan Teknologi Informasi dan Ilmu Komputer, 4(6).

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). Coding Jurnal Komputer dan Aplikasi, 10(02). https://doi.org/10.26418/coding.v10i02.54972

Setiawan, I., Sutopo, M., & Azis, A. (2020). Manajamen Risiko SIMRS Menggunakan Metode OCTAVE-S dan Standar Pengendalian ISO/EIC 27001. 7(3), 593–600. http://jurnal.mdp.ac.id

Supriyo. (2017). MENEJMEN RISIKO DALAM PERFEKTIF ISLAM . 5, 130–142.

Syamsuar, D., Firdaus, A., & Lonando, P. T. (2023). ANALISIS MANAJEMEN RISIKO IT PADA IKEST MUHAMMADIYAH PALEMBANG MENGGUNAKAN METODE OCTAVE – S. Journal of Information System Management (JOISM), 5(1). https://doi.org/10.24076/joism.2023v5i1.1077

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 3). https://doi.org/10.35940/ijrte.B1128.0782S319

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik

Kalimantan Barat). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02). https://doi.org/10.26418/coding.v10i02.54972

Rido Butar Butar, F., Saputra, E., Marsal, A., Hamzah, M. L., Fronita, M., Studi, P., … Riau, K. (2023). Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data Accurate Menggunakan Metode OCTAVE-S. *Jurnal Sains Komputer & Informatika (J-SAKTI*, *7*(2).

Rohman, A. F., Ambarwati, A., & Setiawan, E. (2020). ANALISIS MANAJEMEN RISIKO IT DAN KEAMANAN ASET MENGGUNAKAN METODE OCTAVE-S IT RISK MANAGEMENT ANALYSIS AND ASSET SECURITY USING OCTAVE-S METHOD. *Journal of Information Technology and Computer Science (INTECOMS)*, *3*(2).

Setiawan, I. (2020). Risk Management SIMRS using OCTAVE-S Method and ISO/EIC 27001 Control Standards. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(3). https://doi.org/10.35957/jatisi.v7i3.336

Syamsuar, D., Firdaus, A., & Lonando, P. T. (2023). ANALISIS MANAJEMEN RISIKO IT PADA IKEST MUHAMMADIYAH PALEMBANG MENGGUNAKAN METODE OCTAVE – S. *Journal of Information System Management (JOISM)*, *5*(1). https://doi.org/10.24076/joism.2023v5i1.1077