Infoman's : Jurnal Ilmu-ilmu Informatika dan Manajemen

Vol. 19 No.1 May (2025)

DOI: 10.33481/infomans.vxxixx

Optimization of Information Security Standard Operating Procedures for The Academic Information System at Sebelas April University

[1]Eka Hidayat, [2]Hadi Prasetyo Utomo, [3]Wiwin Suwarningsih
[1]Teknik Informatika, Universitas Langlangbuana
[2]Teknik Informatika, Universitas Langlangbuana
[3]Badan Riset dan Inovasi Nasional, BRIN
[1,2,3]Indonesia
email : [1]ekahidayat19@gmail.com

ABSTRACT
The Academic Information System at Sebelas April University housed various essential data, including student information, faculty information, and academic records. These data were susceptible to cybersecurity threats, data breaches, and unauthorized access, potentially disrupting academic processes and tarnishing the university's reputation. This study aimed to enhance the security of UNSAP's Academic Information System by optimizing the Standard Operating Procedures for information security. A descriptive qualitative research method was employed to analyze the current information security conditions and formulate recommendations for improving the Standard Operating Procedures. The Octave Allegro approach and the ISO 27001:2022 standard served as frameworks in this study. The analysis revealed that the existing Standard Operating Procedures for information security were inadequate. Consequently, new, more comprehensive Standard Operating Procedures were developed, encompassing access control, data management, incident handling, and data backup. These new Standard Operating Procedures were expected to bolster the security of UNSAP's Academic Information System and assist UNSAP in complying with applicable information security standards.

Keywords **-** Information security, Academic Information System, Octave Allegro, ISO 27001:2022, Standard Operating Procedure.

1. Introduction

Digitalization had become a necessity for universities in Indonesia to enhance efficiency, effectiveness, and transparency in academic management. Universitas Sebelas April (UNSAP), a private university in Sumedang, West Java, also took this strategic step by implementing digitalization in various aspects of its operations, especially in academic management. The core of this digitalization initiative was the Academic Information System (SIAKAD), which served as a comprehensive platform to manage academic data and information. SIAKAD not only handled academic administration tasks such as student registration, class scheduling, and grade recording, but also facilitated data reporting to the Higher Education Database (PD-Dikti) [1]. PD-Dikti was a national information system mandated by the government to collect, manage, and analyze higher education data throughout Indonesia.

Although digitalization offered many benefits, the implementation and management of SIAKAD at UNSAP faced several challenges. One major challenge was information security. UNSAP had not conducted a comprehensive security evaluation based on internationally recognized standards, thus posing risks to the confidentiality, integrity, and availability of academic data [2]. Confidentiality meant ensuring that information was only accessible to authorized parties. Integrity meant maintaining the accuracy and completeness of information and preventing unauthorized changes. Availability meant ensuring that information was available and accessible to authorized parties when needed.

Moreover, UNSAP did not have complete and well-documented standard operating procedures (SOPs) for information security [3]. Information security policies and SOPs were essential to provide guidance for SIAKAD users in protecting academic data and information. Another challenge was the low awareness of the importance of information security among SIAKAD users. Lack of awareness could lead to risky behavior that could jeopardize information security.

This study used a descriptive qualitative approach to analyze information security conditions and formulate recommendations for optimizing information security SOPs. A qualitative method was chosen because this study aimed to gain an in-depth understanding of the information security phenomenon at UNSAP, including the factors that influenced it and its impact on academic processes. Descriptive research aimed to describe the condition of SIAKAD information security at UNSAP systematically and factually, without manipulating or controlling variables.

This study aimed to improve the information security of SIAKAD at UNSAP. The academic information system was a very important asset for every university because it stored various data and academic information that was crucial in nature. Therefore, the security of the academic information system was a very important thing to consider. The OCTAVE Allegro method was used in this study to identify and analyze information security risks [4]. This method was chosen because it involved the active participation of various stakeholders at UNSAP, thus it was expected to produce a comprehensive risk analysis that was in accordance with the context at UNSAP. The application of the ISO 27001:2022 standard could assist universities in building a comprehensive and effective information security management system, so as to protect data and academic information from various threats [5].

The novelty of this research lied in the comprehensive approach that integrated OCTAVE Allegro-based risk analysis with the ISO 27001:2022 standard in optimizing SIAKAD information security SOPs. This research was expected to produce recommendations that were applicative and easily understood by various disciplines, so that they could be implemented effectively at UNSAP to improve SIAKAD information security.

2. Research Method

This study aimed to gain an in-depth understanding of SIAKAD information security at UNSAP, including individual experiences, social processes, cultural contexts, interactions, meanings, and dynamics. To achieve this goal, this study employed a descriptive qualitative method [6]. The qualitative method was chosen because the focus of this research was to explore and understand the complex meanings, processes, and contexts related to information security, which could not be measured quantitatively [7]. Descriptive research aimed to describe existing phenomena systematically and factually, without manipulating or controlling variables [8]. This methodology was chosen because it was considered relevant to the purpose and context to analyze and evaluate the information security system at SIAKAD in UNSAP.

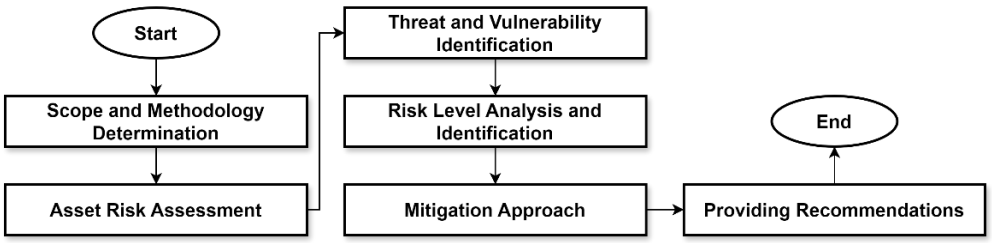

Figure 1. Research Methodology

DOI: 10.33481/infomans.vxxixx

This research was conducted through several main stages. First, the determination of scope and methodology. This stage included defining the research focus and selecting the appropriate method, namely the modified ALLEGRO framework. Second, asset risk assessment. This stage included the identification and analysis of risks to UNSAP SIAKAD assets, such as hardware, software, and data. Third, threat and vulnerability identification. At this stage, various potential threats and vulnerabilities that could endanger the system were identified. Fourth, risk level analysis and identification. The impact of each risk was analyzed and categorized based on its severity level. Fifth, mitigation approach. This stage determined strategies to reduce the impact of risks. Sixth, providing recommendations. Based on the analysis results, recommendations for improving UNSAP SIAKAD security were formulated.

3. Result and Analysis

a. Determination of Scope and Methodology

The determination of scope and methodology was a crucial initial step in this research. The scope of the research was focused on SIAKAD, specifically related to the management of PD-Dikti. This focus was chosen based on the vital role of SIAKAD in managing academic data and information, as well as the importance of SIAKAD integration with PD-Dikti as a national integrated information system.

The framework utilized in this study was the modified ALLEGRO framework. This modification was carried out to adapt the ALLEGRO framework to the specific needs and characteristics of UNSAP SIAKAD. The ALLEGRO framework was chosen due to its comprehensive and structured nature, enabling systematic identification and analysis of information security risks. Furthermore, ALLEGRO was also aligned with the principles in ISO 27001:2022, the international standard for information security management that served as a reference in this study.

b. Identifikasi dan Analisis Aset

At this stage, it was necessary to identify all information assets, both physical and digital, as these assets formed the foundation of the SIAKAD system and its operations. This comprehensive identification ensured that no critical component was overlooked in the subsequent risk assessment and security enhancement efforts. These assets included hardware components like servers and computers, software elements like the SIAKAD application itself, and the crucial data and information managed by the system.

Table 1. Asset Identification

No	Category	Asset
1	Hardware	Servers, computers, network devices, and storage devices.
2	Software	Operating systems, SIAKAD applications, and other supporting applications.
3	Data and Information	Student data, lecturer data, academic data, financial data, and employee data.

c. Risk Analysis

After the assets were identified, the next stage was risk analysis, a critical process of evaluating potential threats and vulnerabilities that could compromise the SIAKAD system. This analysis involved a thorough examination of each asset, identifying potential risks such as unauthorized access, data breaches, and system failures. By understanding these risks, UNSAP could take proactive steps to mitigate them and ensure the continued security and integrity of the SIAKAD system.

Table 2. Risk Analysis

No	Asset	Threat
1.	Server	Hardware damage
2.	Network Devices	Hardware failure
3.	Server Rack	Lack of physical security around the server rack
4.	Server Operating System	Operating system vulnerabilities
5.	SIAKAD Application	XSS attacks
....	...	...
74.	Student Data	Data leakage
75.	SIAKAD Users	Phishing

d. Determination of Risk Severity Level

After conducting a thorough risk analysis, the subsequent stage involved determining the severity level of each identified risk, a crucial step in prioritizing mitigation efforts. This determination considered both the likelihood of the threat materializing and the potential impact it could have on the SIAKAD system, allowing for a nuanced understanding of the risks. By assigning severity levels, UNSAP could effectively allocate resources and develop targeted strategies to address the most critical threats to their academic information system.

Table 3. Risk Level

No	Asset	Threat	Threat Score	Impact Score	Risk Level
1.	Server	Hardware damage	4	4	16
2.	Network Devices	DoS attack	2	2	4
3.	Server Rack	Lack of physical security around the server rack	3	2	6
4.	Server Operating System	Operating system vulnerabilities	4	4	16
5.	SIAKAD Application	XSS attacks	3	3	9
.....	...	...	...	...	...
74.	Student Data	Data leakage	3	4	12
75.	SIAKAD Users	Phishing	3	4	12

The risk level was categorized into 5 levels, namely very high (score 16-25), high (score 12-15), medium (score 8-11), low (score 4-7), and very low (score 1-3).

e. Mitigation Approach

The mitigation approach aimed to reduce the likelihood and impact of risks that had been identified in UNSAP SIAKAD, focusing on proactive measures to enhance the system's security posture. This involved a multifaceted strategy that included strengthening technical controls, improving user awareness and training, and establishing robust security policies and procedures. By implementing these mitigation approaches, UNSAP could effectively minimize the potential for security breaches and protect the integrity of its academic information system:

- Critical Attention Areas

  Critical attention areas were areas that had the potential for significant impact on SIAKAD information security, demanding focused attention and robust mitigation strategies. These areas represented key vulnerabilities or weaknesses in the system that, if exploited, could lead to severe consequences, such as data breaches, system disruptions, or reputational damage. Identifying these critical areas was essential in developing a targeted and effective information security management system for UNSAP SIAKAD.

Vol. 19 No.1 May (2025)
DOI: 10.33481/infomans.vxxixx

Table 4. Critical Attention Areas

No.	Area of Attention
1.	Vulnerabilities in Applications
2.	Data Security
3.	User Awareness and Compliance
4.	Physical and Environmental Security
5.	System and Operations Management
6.	Service Continuity
7.	Integration Between Systems
8.	Access Rights Management

- Threat Scenarios

Threat scenarios described how threat actors could exploit vulnerabilities to compromise assets, providing a detailed narrative of potential attack vectors and their impact on the SIAKAD system. These scenarios served as valuable tools for understanding and visualizing potential security breaches, enabling UNSAP to develop proactive mitigation strategies and strengthen their overall security posture. By analyzing these scenarios, UNSAP could better anticipate and defend against potential attacks, protecting the confidentiality, integrity, and availability of their academic information.

Table 5. Threat Scenario Identification

No	Area Perhatian	Skenario Ancaman	
1.	User Awareness and Compliance	**Aktor**	Users, Administrators, Operators
		Means	Negligence, Lack of information security awareness, and Social engineering
		Motive	Accidental, Ease, and Influenced by other parties
		Consequences	Data input errors, Leakage of sensitive information, and Misuse of access rights
		Security Requirements	- Confidentiality: Ensuring that only authorized parties can access data. - Integrity: Ensuring data accuracy and unauthorized modification. - Availability: Ensuring system and data availability when needed. - Accountability: Ensuring all actions can be tracked and audited. - Non-Repudiation: Ensuring users cannot deny actions taken
		Likelihood	High

- Impact Identification

Impact identification was a crucial step in the risk assessment process, as it involved determining the potential consequences that could arise if identified threats successfully exploited vulnerabilities in the SIAKAD system. This process involved a comprehensive evaluation of various potential impacts, ranging from data breaches and financial losses to disruptions in academic activities and damage to the university's reputation. By understanding the potential impacts, UNSAP could prioritize mitigation efforts and allocate resources effectively to safeguard their critical assets and ensure the continuity of academic processes

Table 6. Impact Identification

Area of Attention	Impact
Vulnerability in Applications	Data theft, unauthorized data changes, service disruption (DoS), damage to the university's reputation
Data Security	Data theft, data leakage, unauthorized data changes, data deletion
User Awareness and Compliance	Data input errors, leakage of sensitive information, abuse of access rights
Physical and Environmental Security	Hardware damage, data loss, service disruption
System and Operations Management	Service disruption, data theft, unauthorized data changes
Service Continuity	Service disruption, data loss
Integration Between Systems	Data inconsistency, data errors
Access Rights Management	Unauthorized access to data and systems, unauthorized data changes, data theft

- Impact Value Identification

Impact value identification was a crucial step in quantifying the severity of potential consequences, providing a numerical representation of the impact each threat could have on the SIAKAD system. This involved assigning a specific value to each impact based on predefined criteria, such as the affected area, the extent of damage, and the recovery time. By quantifying the impact value, UNSAP could gain a clearer understanding of the potential consequences of security breaches, facilitating informed decision-making and prioritization of mitigation efforts.

Table 7. Impact Analysis

Area Perhatian	Dampak			
User Awareness and Compliance	**Consequences**	Data input errors, leakage of sensitive information, misuse of access rights		
	Severity Level	**Area of Attention**	**Value**	**Score**
		Reputation	High	15
		Finance	High	12
		Productivity	High	9
		Safety	Low	2
		Legal and Regulatory	Medium	2
		Relative Risk Score		**40**

- Mitigation Selection

Mitigation selection involved utilizing the Relative Risk Matrix [9] as a crucial tool for categorizing and prioritizing risks based on their likelihood and potential impact on UNSAP SIAKAD. This matrix provided a structured framework for evaluating each risk, facilitating informed decision-making regarding appropriate mitigation strategies. By employing this approach, UNSAP could effectively allocate resources and prioritize efforts to address the most critical threats to their academic information system.

Table 8. Relative Risk Matrix

Likelihood	Risk Score		
	30 - 45	**16 - 29**	**0 - 15**
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

 ISSN : 1978-3310 | E-ISSN : 2615-3467

Vol. 19 No.1 May (2025)
DOI: 10.33481/infomans.vxxixx

To determine the appropriate mitigation strategy, the approach involved carefully evaluating each identified risk and selecting the most suitable action: Risk Reduction, Risk Reduction or Postponement, Risk Postponement or Acceptance, or Risk Acceptance. This decision-making process considered the likelihood and potential impact of each risk, ensuring that UNSAP could effectively allocate resources and prioritize mitigation efforts. By selecting the appropriate mitigation strategy for each risk, UNSAP could proactively address security concerns and enhance the overall security posture of their SIAKAD system.

Table 9. Mitigation Approach

POOL	Mitigation Approach
POOL 1	Risk Reduction: Risks with high likelihood and impact. Must be addressed immediately.
POOL 2	Risk Reduction or Postponement: Risks with moderate likelihood or impact. Handling is more flexible, can be reduced or postponed.
POOL 3	Risk Postponement or Acceptance: Risks with relatively low likelihood and impact. Handling can be postponed or accepted.
POOL 4	Risk Acceptance: Risks with very low likelihood and impact, so they can be accepted without mitigation actions.

To summarize the specific mitigation strategies selected for each risk that had been identified, UNSAP could utilize a Specific Mitigation Strategy table, providing a clear and concise overview of the chosen actions for each risk. This table served as a valuable tool for documenting and communicating the mitigation plan, ensuring that all stakeholders understood the strategies in place to address potential threats to the SIAKAD system. By following this structured mitigation selection process and documenting the strategies in a clear and accessible format, UNSAP could effectively manage and mitigate risks to their academic information system

Table 10. Specific Mitigation Strategy

Area of Attention	Relative Risk Score	Likelihood	POOL	Mitigation Approach
Vulnerability in Applications	35	High	POOL 1	Risk Reduction
Data Security	37	Medium	POOL 2	Risk Reduction or Postponement
User Awareness and Compliance	40	High	POOL 1	Risk Reduction
Physical and Environmental Security	39	Medium	POOL 2	Risk Reduction or Postponement
System and Operations Management	35	Medium	POOL 2	Risk Reduction or Postponement
Service Continuity	25	Medium	POOL 2	Risk Reduction or Postponement
Integration Between Systems	32	Low	POOL 3	Postponement or Acceptance of Risk
Access Rights Management	36	Low	POOL 3	Postponement or Acceptance of Risk

f. Recommendations

Based on the research and analysis conducted, there were several recommendations that could be provided to improve the information security of SIAKAD at UNSAP. These recommendations covered eight main areas, namely: application vulnerabilities, data security, user awareness and compliance, physical and environmental security, system and operations management, service continuity, integration between systems, and access rights management. Addressing these areas comprehensively would

significantly enhance the security posture of SIAKAD and protect UNSAP's critical academic information and processes. These recommendations covered eight main areas, namely:

1) Application Vulnerabilities: It was necessary to ensure that the SIAKAD and Neo Feeder applications were secure and protected from attacks. This meant that UNSAP had to routinely check applications for weaknesses and immediately fix them if problems were found.
2) Data Security: It was necessary to maintain the security of important data and information, such as student and lecturer data. This meant that UNSAP had to restrict who could access the data and store copies of the data in a safe place.
3) User Awareness and Compliance: It was necessary to inform all SIAKAD users on how to maintain information security. This meant that UNSAP had to provide training and guidance on best practices for cybersecurity.
4) Physical and Environmental Security: It was necessary to protect the server room and SIAKAD equipment from unauthorized access and other hazards. This meant that UNSAP had to restrict physical access to the area and have security systems such as CCTV.
5) System and Operations Management: It was necessary to ensure that SIAKAD computer systems and software were always updated and secure. This meant that UNSAP had to regularly update software and operating systems and use security software such as antivirus.
6) Service Continuity: It was necessary to develop a structured and tested disaster recovery plan, as well as provide a backup power system to ensure the availability of SIAKAD services.
7) Integration Between Systems: It was necessary to ensure that the SIAKAD system could work well with other systems. This meant that UNSAP had to test new systems to ensure they were compatible with SIAKAD.
8) Access Rights Management: It was necessary to control who was allowed to access SIAKAD and what they were allowed to do. This meant that UNSAP had to have a system for managing user accounts and access permissions.

4. Conclusion

This study showed that UNSAP SIAKAD needed to improve its information security. Several security gaps were found, such as unauthorized access, unauthorized data modification, and data theft. The risk analysis identified several issues, such as malware attacks, phishing, social engineering, and data leaks. Several areas needed improvement, including vulnerabilities in the SIAKAD and Neo Feeder applications, data security, user awareness and compliance, physical and environmental security, system and operations management, service continuity, integration between systems, and access rights management. Some of the vulnerabilities found included weak data access controls, weak passwords, lack of data encryption, lack of data change controls, lack of audit trails, lack of data backups, lack of data recovery mechanisms, and poor physical and electronic security. To address these issues, comprehensive information security improvement recommendations were compiled. These improvement recommendations needed to be implemented and evaluated periodically.

The results of this study could be further developed by implementing the compiled information security SOPs and conducting regular monitoring and evaluation to ensure their effectiveness. In addition, it was necessary to conduct socialization and training for all SIAKAD users regarding the importance of information security and how to implement the compiled SOPs. The development of an integrated information security monitoring system was also necessary to facilitate monitoring and early detection of security threats.

Vol. 19 No.1 May (2025)

DOI: 10.33481/infomans.vxxixx

References

[1] D. Cahyono, Rasid, L. O. M. A. Ardyawan, E. Lestari dan M. Bayu, "Upgrading Tata Kelola Perguruan Tinggi Baru di ITBK Muhammadiyah Muna Barat Sulawesi Tenggara," *Jurnal Abdi Masyarakat Indonesia (JAMSI),* vol. 3, no. 1, pp. 355-360, 2023.

[2] E. Novianto, E. H. H. Ujianto dan Rianto, "Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia," *RABIT : Jurnal Teknologi dan Sistem Informasi Univrab,* vol. 8, no. 1, pp. 10-15, 2023.

[3] E. Riana, M. E. S. Sulistyawati dan O. P. Putra, "Analisis Maturity Level Dan PDCA Dalam Penerapan Proses Audit SMKI (Information Security," *Informatics For Educators And Professionals,* vol. 7, no. 1, pp. 39-50, 2022.

[4] B. S. Deva dan R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI) ,* vol. 12, no. 2, pp. 106-117, 2022.

[5] A. I. Mafiana, L. Hanun, H. M. Ilmi dan S. Febriliani, "Implementasi Manajemen Keamanan Informasi Berbasis ISO 27001 Pada Sistem Informasi Akademik," *Journal of Digital Business and Innovation Management,* vol. 2, no. 2, pp. 139-163, 2023.

[6] J. W. Creswell dan J. D. Creswell, Fifth Edition Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, California: SAGE Publications, 2018.

[7] E. Werdiningsih dan A. Hamid, "Lima Pendekatan dalam Penelitian Kualitatif," *LIKHITAPRAJNA Jurnal Ilmiah,* vol. 24, no. 1, pp. 39-50, 2022.

[8] Rusandi dan M. Rusli, "Merancang Penelitian Kualitatif Dasar/Deskriptif dan Studi Kasus," *Education And Islamic Studies,* vol. 2, no. 1, pp. 1-13, 2022.

[9] R. R. A dan R. Bisma, "Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik," *Journal of Emerging Information Systems and Business Intelligence,* vol. 2, no. 2, pp. 17-23, 2021.

Nida, S. N. S. S. (2024). Readiness Measurement of Integrated Stunting Prevention System Users (SIMPATI) Using Technology Readiness Index (TRI). *Infoman's: Jurnal Ilmu-ilmu Informatika dan Manajemen*, *18*(2).