KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 6, Juni 2023, Hal 765-772
DOI 10.30865/klik.v3i6.848
https://djournals.com/klik

The Implementation of Personal Data Protection Law on Information System Security Risks Using OCTAVE-S

Gita Nurul Aini*, Muhammad Jazman, Angraini, Mona Fronita

Fakultas Sains dan Teknologi, Program Studi Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Indonesia
Email: [1*]gitanurulaini005@gmail.com, [2]jazman@uin-suska.ac.id, [3]angraini@uin-suska.ac.id, [4]monafronita@uin-suska.ac.id
Email Penulis Korespondensi: gitanurulaini005@gmail.com

Abstract−This research focuses on the risk assessment and mitigation of the Hitmi system, an information system used by PT Perkebunan Nusantara (PTPN V) for calculating employee premiums. The study aims to identify and evaluate the risks associated with the system's information technology assets and provide risk mitigation recommendations in accordance with information security practices and the Personal Data Protection Act. The research methodology includes several stages: Planning, Data Collection, Analysis and Data Processing, and Final Phase. In the Planning Stage, the problem is identified through observations and interviews, and the research purpose is defined. The Data Collection Phase involves literature studies, observations, interviews, and the use of OCTAVE-S sheets to collect relevant data. The Analysis and Data Processing stage focuses on analyzing the collected data and processing it for conclusions and problem resolution. The OCTAVE-S framework is used to identify assets, vulnerabilities, and develop security strategies and plans. The results and discussion section presents the mapping of the OCTAVE-S analysis with the Personal Data Protection Act, identifying organizational information, and assessing organizational security practices. The risk impact assessment criteria are used to evaluate the risks, and the assets of the organization are identified. The assessment of security practices reveals areas of improvement and areas where good security practices are already implemented. Based on the findings, recommendations for risk mitigation are provided. These recommendations include security awareness and training programs for employees, improved resource allocation for security activities, regular updates to security policies, and the implementation of access control measures, incident management procedures, and encryption techniques.This research contributes to enhancing information security practices and reducing risks associated with the Hitmi system at PTPN V. The findings can guide the organization in implementing effective security controls, complying with the Personal Data Protection Act, and ensuring the confidentiality, integrity, and availability of sensitive data.

Keywords: Hitmi System; Information Technology Assets; OCTAVE-S; Personal Data Protection Act; Risk Assessment;

1. INTRODUCTION

Information systems generally investigate and discuss the processes in which the system itself is implemented and deployed to ensure that all relevant parties involved in the system can obtain the desired information effectively[1]. Information Systems in general, refers to hardware, digital applications, storage, communication systems, internet utilities, and almost all other aspects of business technology infrastructure, organizations, governments, schools, or other groups that shape the idea of big data[2], [3]. However, the use of information systems has various risks such as electrical failure due to natural factors, human error, system damage due to viruses, fire, data leakage due to hackers and others[4]. In recent times, there have been documented cases of unauthorized disclosure of personal data occurring within institutional and government settings, as well as in private companies, specifically in the realm of fintech start-ups[5].

The protection of personal data is a human right that needs to be given a legal basis to provide security over personal data. This is done to minimize the risk of data leakage on electronic systems. The Government has made the Law on the Protection of Personal Data in the Law of the Republic of Indonesia No.27 of 2022[6]. Information Systems and Information Technology (IT) plays an important role in risk management[7]. Risk management is the recurring process of analyzing, designing, implementing, controlling, supervising strategies and stages to implement security policies[8]. The purpose of risk management is to address a variety of problems such as the inadequacy of business processes, the company's reputation down, financial loss or bankruptcy of the company as well as the security of IT systems that store, process, or transmit information[8], [9]. In a company or organization, risk management refers to the CIA (Confidentiality, Integrity, Authentication) by identifying threats, classifying organization assets, and assessing system vulnerabilities so that effective security controls can be applied[10].

PT Perkebunan Nusantara (PTPN V) is located in Jl. Rambutan No.43, Sidomulyo East, Marpoyan Peace, Pekanbaru City, Riau 28294 is a company that operates in the palm and coconut planting sector in its management. PTPN V is a state-owned enterprise (BUMN) and the largest agribusiness and agro-industrial company of palm and rubber in Riau with the main purpose of serving the public or public interest[11]. In supporting the business processes in the company, PTPN V uses the information system. The information system used is the Hitungan Premi system (Hitmi System). The Hitmi system is a system for calculating employee premiums. The premium is an additional salary given to employees who work in the factory to process palm coconut. Before using the Hitmi System in PTPN V still use manual calculation, so there are some of the following problems: 1) High HPP, premium costs above the budget; 2) Frequently occurring calculation errors and the application of premium terms; 3) Difficult to monitor and evaluate premium calculations.

The development of digital technology transformation in PTPN V as tools supporting then implemented Hitmi system. In the operation of the hitmi system suffered barriers such as human error, where users often enter the data incorrectly. it will affect the instance. Hitmi systems load some sensitive information such as the personal data of employees and employee salary data so it is necessary to investigate so that there is no error input data that can affect the

results of salary calculation. In 2021, the hitmi system was hacked by hackers. the hacker entered the network and replaced index.php with an image resulting in the system being unusable. If the event is ignored by the company, it is concerned that the hacking and the theft of sensitive data will happen again. In order to reduce the occurrence of threats or technological risks, a risk assessment of the existing Hitmi system on PTPN V. The aim is to measure the level of seriousness of risk and develop security controls to reduce losses and get maximum benefits for the agency, as well as to map with the Personal Data Protection Act. It requires a framework to identify information security risks, such as the OCTAVE, FMEA, and ISO frameworks.

The development of digital technology transformation in PTPN V serves as a supporting tool for the implementation of the Hitmi system. However, the operation of the Hitmi system faces certain challenges, such as human error, where users often input data incorrectly, leading to potential issues. The Hitmi system contains sensitive information, including personal employee data and salary information, making it essential to investigate and prevent any data input errors that could impact salary calculations. In 2021, the Hitmi system was hacked by hackers who gained unauthorized access to the network and replaced the index.php file with an image, rendering the system unusable. If this incident is disregarded by the company, there is a concern that hacking and theft of sensitive data could occur again. To mitigate the occurrence of threats and technological risks, a risk assessment of the existing Hitmi system in PTPN V is necessary. The objective is to assess the severity of risks and develop security controls to minimize losses and maximize benefits for the organization, while also aligning with the provisions of the Personal Data Protection Act. This requires the utilization of frameworks like OCTAVE, FMEA, and ISO to identify information security risks.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a method used to identify and evaluate organizational risks that focus on strategic issues related to practices[12], [13]. OCTAVE-S is a simple methodology and supported by the Technology Insertion, Demonstration and Evaluation (TIDE) program at SEI, aimed at small organizations and assumes that such organizations have security involved in the process[14], [15]. OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks[16].

Some previous studies using the OCTAVE Framework research entitled "E-Procurement System Risk Analysis Using OCTAVE-S Method" with system security risk analysis obtained threats with yellow status where the agency needs to improve the security management system to prevent risks that have a major impact and interfere with operational activities[17]. The study entitled "Information Security Planning Based on Information Technology Risk Analysis Using OCTAVE Method and ISO 27001 (Case Study of the IT Field of the Banten Police Region)" was concluded after the analysis process carried out that there are 28 risks that may occur in the IT field of Banten police area with the highest RPN value of 240 to the lowest RPR value of 18. Risk mitigation recommendations can be made with 11 controls contained in ISO 27001[18]. Research with the title IT Risk Management Analysis and Asset Security Using OCTAVE-S Method. The OCTAVE-S method has proven to identify risks and the results of the assessment have been concluded in a category that is very high, high, medium, low, very low. Very high, at this level the researchers had 4 risks with the highest RPN. The ISO 27001 standard can be used as a reference for recommendations for risk mitigation[19].

The following research, entitled Analysis, Evaluation, and Mitigation of Risk of Information Technology Assets Using the OCTAVE Framework and FMEA (Case Study: Unit of Management Technical Information Technology Fan Communication University XYZ) can be concluded that information security can be enhanced by analyzing the assets as well as the risks that occur on such assets using the Octave-S Frameworks. ISO 27001 helps in improving and improving information security in organizations[20]. Research entitled Security Risk Management Analysis System BMKGSOFT Using the OCTAVE-S Method concluded that the method for analyzing assets and risks can be done using the Octave method. Information security can be enhanced by analysing the assets used to manage such information as well as the risks that may occur on those assets[21].

In this study, the OCTAVE-S framework is used to identify the risks associated with the information technology assets used in the service, conduct risk assessments, and provide recommendations for risk mitigation in accordance with information security practices. Subsequently, the results of the OCTAVE-S analysis will be used in the data mapping process, aligning various data sources with the Personal Data Protection Act and integrating them into the main database to bridge any differences.

2. RESEARCH METHODOLOGY

The research methodology refers to the measures taken to achieve the research objectives. The steps involved in this study include: (1) the Planning Stage, (2) the Data Collection Phase, (3) the Data Analysis and Processing Phase, and (4) the Final Phase.

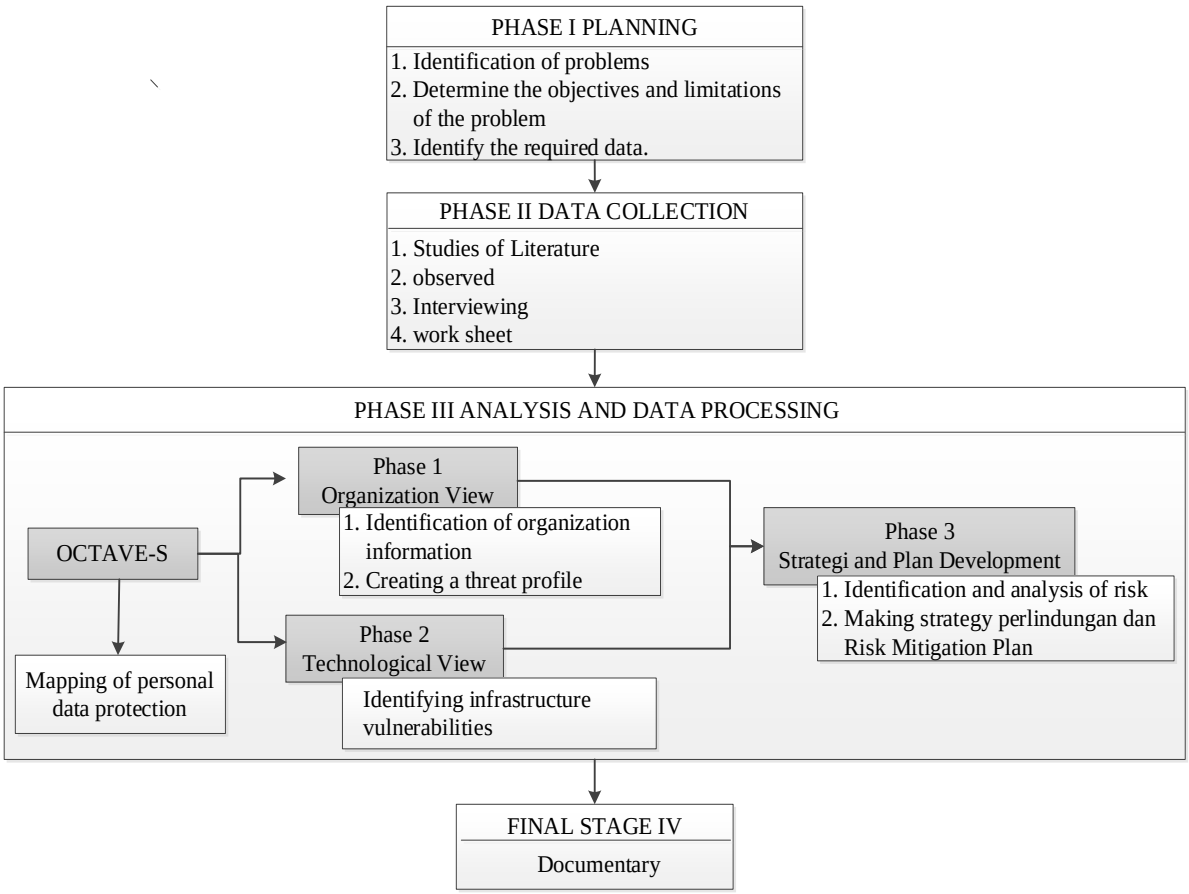

Figure 1. Methodology

2.1 The Planning Stage

The planning stage involves identifying the problem through observations and interviews conducted with PTPN V. Subsequently, the research purpose is determined, and the required data for this study is defined. The outcome of the initial stage is the interview protocol used to conduct a risk analysis on the Hitmi System.

2.2 Stage of Data Collection

The purpose of the data collection phase is to gain a better understanding of the problems to be investigated. There are four processes involved in data collection, including: (1) Literature studies, (2) Observations, (3) Interviews, (4) OCTAVE-S Sheets.

2.3 Analysis and Data Processing

The analysis is conducted to analyze the needs related to the raised problem and how to address it. The purpose of data processing is to transform the obtained raw material into processed information through the analysis process, making it easier to draw conclusions and find solutions to the research problems. The analysis of system security risks based on OCTAVE-S focuses on the initial phase of asset building, specifically the threat profile. This stage involves two processes: identifying organizational information and constructing the expected threat profiles. These activities assist in research and risk assessment, as well as support companies in establishing their vision and mission.

2.3.1 OCTAVE-S

OCTAVE-S is based on three phases:

a. Stage 1: Build Asset-Based Threat Profiles In this phase is the evaluation of organizational aspects. During this phase, the team of analysts defines the impact assessment criteria to be used to evaluate risk, identify the assets of the organization and evaluate the organization's security practices. Finally, the team defines security requirements and defines threat profiles for each critical asset.
b. Phase 2: Identify infrastructure vulnerabilities At this stage is the identification of computing infrastructure, focusing on the extent to which security is considered by infrastructure maintenance. Analyze how people use computing infrastructure to access critical assets, generate key classes of components and who is responsible for configuring andining those components.
c. Phase 3: Develop security strategies and plans The team creates protection strategies for the organization and risk mitigation plans to address risks to critical assets. The OCTAVE-S worksheet used during Phase 3 is highly structured

and closely connected to the OCTAVE practice catalog, enabling the linking of recommendations for improvements with the reference of received safety practices.

2.4 Final Phase

At this stage, the data obtained is collected and processed to become a report.

3. RESULT AND DISCUSSION

3.1 Mapping OCTAVE-S With the Personal Data Protection Act

The personal data protection law regulates a range of provisions, including the types of personal data, processing, and sanctions for misuse of personal data management. According to Article 39, paragraph (1) the controller of personal data is obligated to prevent unauthorized access to personal data. This prevention is supported by paragraph (2) which states that a security system must be implemented for processing personal data using electronic systems reliably, safely, and responsibly.

In Indonesia, there are 30 laws and regulations relating to the collection and management of personal data. Including a number of regulations on the privacy of citizens[22]. Then on 17 October 2022 the Law of the Republic of Indonesia Number 27 Year 2022 on the Protection of Personal Data was approved by the President of Indonesia
This section contains the results of mapping the Personal Data Protection Act and Hitmi System Risk Assessment using OCTAVE-S.

In the context of mapping between the security existing in the OCTAVE-S methodology and the data protection laws, there are some correlations and similarities between the two. Here are some examples of how security in OCTAVE-S can relate to the legal requirements of personal data protection:

Tabel 1. Mapping OCTAVE-S With the Personal Data Protection Atc

No	SAFETY PRACTICE	OCTAVE-S	THE PERSONAL DATA PROTECTION ACT	ARTICLE
1	Security of Data	OCTAVE-S encourages the identification of critical assets and vulnerabilities to threats, including personal data.	Personal data protection laws also require adequate protection of personal data through appropriate safeguards, such as data encryption, access control, and protection against data leakage or misuse.	Chapter VI Duties of the controller of personal data and the processor in processing personal data: Article 32 paragraph 1 Chapter IV Article 12 Paragraph 1 on the right to Chapter VI Chapter 46,47 Chapter XIV Regulations
2	Regulation of access.	OCTAVE-S analyzes existing access policies and controls within the organization, including access to personal data.	The law on the protection of personal data emphasizes the need to regulate appropriate access to personal data, including the exercise of access rights based on the principles of necessity and limitation of access.	Chapter VI Article 13, Article 24, Article 28, Chapter VI: Responsibilities of the controller and processor of personal data in the processing of data: Articles 35-39 on encryption
3	Network and system security.	OCTAVE-S involves vulnerability assessments on infrastructure and systems, which include systems that manage and process personal data.	Personal data protection laws encourage the adoption of adequate network and system security measures to protect personal data from threats and attacks, such as network monitoring, intrusion detection, and protection against malware.	Chapter XVI Transitional Provisions Articles 47 and 75
4	Policy and Procedure	OCTAVE-S involves the evaluation of security-related organizational policies and procedures, including privacy and data security policies.	Personal data protection laws encourage the adoption of transparent and adequate policies and procedures to protect personal data, such as clear privacy policies, notification to individuals regarding data use, and effective incident response procedures.	Chapter VI Obligations of Personal Data Controller and Personal Data Processor in Data Processing, Article 46 on Notification in the event of failure and incident response Chapter V: Data Processing: Article 16 Paragraph 2

5	Monitoring and Reviewing.	OCTAVE-S encourages periodic monitoring and review of existing security measures within the organization.	The Data Protection Act also emphasizes the importance of periodic monitoring and review to ensure compliance with the law and the effectiveness of the security measures implemented.	Chapter XVI Transitional Provisions Articles 74 and 75

It is important to note that the legal requirements for the protection of personal data may vary between countries or jurisdictions. Therefore, the mapping between OCTAVE-S and the data protection laws should be done specifically taking into account the legal requirements applicable in your jurisdiction.

3.2 Identification of Organizational Information

The risk assessment process starts with identifying information from the agency to determine the level of risk that may impact the agency's activities or survival. Data collection is conducted using worksheets.

3.2.1 Establish A Risk Impact Assessment

Data obtained as follows.

Table 2. Work Sheet Filling Data Identifying Risks from Organization Impact Assessment Criteria

No	Criteria of impact	Type / Impact	Level
1	Reputation and	Reputation	Low
	Loss of data	Damage to system	Low
2	financed	Operational costs	Medium
	Productivity	Loss of income	Low
3	Health / Safety	Working hours	Medium
4	Criteria of impact	Health and	Low

Based on Table 2, it can be observed that the System Reputation and Damage Indicators are at a low level. This is attributed to the positive reputation of the Hitmi System, as the existing systems and services are running smoothly. System damage on the Hitmi System occurs primarily during instances when service slows down and employee trust in agents is slightly diminished. As for the Financial Indicators, the impact of operating costs is assessed to be at a moderate level. This is due to the rise in hardware and system maintenance expenses. However, agents do not experience a significant decline in revenue, as indicated by the low risk level of revenue on the agent's criteria. The Productivity Hour indicator reveals that employees encounter a 10% to 30% increase during threats or incidents, placing them at a moderate risk level. In terms of employee health and safety indicators, the potential threats to employee well-being are considered low. Healthcare staff receive health insurance and tailored care based on the severity of their illness.

3.2.2 Identification of Organization Assets

Here is the data obtained from completing the work sheet. The second step involves identifying the assets of the organization, as shown in Table 3, as follows:

Table 3. Data Assets of Human Resources

tem	**Information**	**Applications and Services**	**Other assets**
Hitungan Premi	Stable data premiums	CCTV	PHPstorm (text editor)
System	Employee premiums / salary data every day	Milena	Server windows 2008
	Personal Data of Employees	Intank	MYSQL
	Data Delivery (permit, leave, and sick)	SAP	Code Igniter
	Data extension of the department/employee in other departments	Fossnirs	PKS Online

Table 4. Data Assets of Human Resources

	Human Resource
Departement	Skilled
Programming	Develop, manage, operate, and maintain enterprise system infrastructure, network, server, and database.

3.3 Assessment of Organizational Security Practices

To evaluate aspects of security practices based on the stolight status obtained from the results of filling the worksheet with the following descriptions:

Table 5. Explanation of Assessment

Green	4 indicators very fulfilled
Yellow	3 indicators slightly fulfilled
Red	2 indicators are not met

As for the data obtained from Step 3 on the worksheet that has been filled out against the assessment of security practices that have been implemented by the Hitmi System as follows:

Table 6. Data filling work sheets of security practice agencies

NO	SAFETY PRACTICE	STOPLIGHT		
		RED	YELLOW	GREEN
1	Security Awareness and Training		✓	
2	Security Strategy			✓
3	Security management		✓	
4	Security Policy and Rules		✓	
5	Security and Collaboration Management			✓
6	Contingency Planning			✓
7	Control of physical access		✓	
8	Physical Safety Monitoring and Audit			✓
9	System and network management.		✓	
10	Monitoring and audit of security.		✓	
11	Verification and Authorization		✓	
12	Management of Vulnerability		✓	
13	Encrypted		✓	
14	Design and Security Architecture			✓
15	Management of incidents		✓	

Can be seen in the table 6, there are five security practices are in the status of yellow stoplight which indicates that PTPN V has implemented the security practice but is not good enough and ten security practice is in the state of green stoplight indicating that PTPN V has already implemented that security practice well.

3.4 Recommendations

The results of the risk assessment analysis are as follows:

Table 6. Type of Database

No	Security Practice	Risk action
1	Security Awareness and Training	Training of employees will be the importance of the role and responsibility of employees.
		Routine training for PTPN V employees.
2	Security management	Execute good resource allocation for PTPN V security activities
		Responsibility for PTPN V employees
		Conduct a documented procedure.
		Management should be based on routine reports containing information related to security aspects.
3	Security Policy and Rules	Making policy documentation that is priodically updated
		Conduct a documented process to evaluate whether each employee of the company has the procedures in place.
4	Control of physical access.	Improve physical access control.
		Implement documented policies and procedures towards visitors.
		Implement security measures such as using an ID card and fingerprint scanner in accessing a room and using a password to any sensitive information access.
5	System and network management.	Protect sensitive information in a secure place.
		Make backup data on software and data staff of the company follow the procedure in making changes to username and password.
		Implement documented procedures to protect existing systems.
		Routine inspections of systems and networks.
6	Monitoring and audit of security.	Monitor and audit systems and networks within the company on a regular basis.
7	Verification and Authorization	Implementing Effective Controls in accordance with Existing Policies.
		Enforcing Access Restrictions for Hitmi System Users to prevent unauthorized access to sensitive data or information.

8	Management of Vulnerability	Conduct procedures to manage the level of vulnerability within the company. Evaluate the Hitmi System vulnerability periodically.
9	Encrypted	Implementing Security Controls according to System Requirements. Protecting Sensitive Information. Managing Systems, Routers, and Firewalls.
10	Management of incidents	Conduct procedures documented by the company for the purpose of identifying, reporting, and processing the follow-up of suspected security incidents and breaches.

3.5 Discussion

The research discussed the use of the OCTAVE-S framework to assess the risks and develop security controls for the Hitmi System used by PT Perkebunan Nusantara (PTPN V), a state-owned enterprise in Indonesia. The aim of the research was to identify and mitigate the risks associated with the system, particularly in relation to personal data protection.

The introduction highlighted the importance of information systems in effectively providing desired information to relevant parties. However, the use of information systems also comes with various risks, such as electrical failure, human error, system damage, and data leakage. To protect personal data, the Indonesian government has enacted the Law on the Protection of Personal Data. Information systems and information technology play a crucial role in risk management, addressing problems related to business processes, company reputation, financial loss, and IT system security.

PTPN V uses the Hitmi system for calculating employee premiums, replacing the previous manual calculation method. However, the system has faced challenges such as human errors in data entry and a hacking incident in 2021. Therefore, the research aims to assess the risks associated with the Hitmi system using the OCTAVE-S framework and develop security controls to prevent future incidents and comply with the Personal Data Protection Act.

The research methodology involves four stages: planning, data collection, analysis and data processing, and the final phase. In the planning stage, the problem was identified through observations and interviews with PTPN V, and the research purpose and data requirements were defined. The data collection phase involved literature studies, observations, interviews, and the use of OCTAVE-S worksheets to gather information about the system and its risks. The analysis and data processing stage focused on analyzing the collected data, assessing the risks using the OCTAVE-S framework, and developing security strategies and plans. Finally, the data obtained were processed to produce the research report.

The results and discussion section presents the mapping of the OCTAVE-S framework with the Personal Data Protection Act. It also includes the identification of organizational information, such as the impact assessment criteria and asset identification. The assessment of security practices implemented by the Hitmi System was also discussed, with some practices categorized as yellow (partially fulfilled) and others as green (fulfilled). Recommendations were provided to address the identified risks, including training employees on security awareness, allocating resources for security management, updating security policies, implementing physical access controls, and more.

Overall, this research provides insights into the risks associated with the Hitmi System used by PTPN V and offers recommendations to enhance information security and comply with the Personal Data Protection Act. By applying the OCTAVE-S framework, the study helps identify potential vulnerabilities, assess risks, and develop appropriate security controls. This research contributes to the field of information security and risk management, particularly in the context of organizations handling sensitive data.

4. CONCLUSION

This research focuses on the analysis and mitigation of risks in the Hitungan Premi system (Hitmi System) used by PT Perkebunan Nusantara (PTPN V), a state-owned enterprise operating in the palm and coconut planting sector. The study recognizes the risks associated with information systems, such as human error, system damage, and data leakage. The implementation of risk management, including the OCTAVE-S framework, is crucial to address these risks effectively. The OCTAVE-S framework helps in identifying and evaluating organizational risks, developing security strategies, and implementing risk mitigation plans. The research also emphasizes the importance of aligning the analysis with the Personal Data Protection Act to ensure compliance with data privacy regulations. Through the research methodology, including the planning stage, data collection phase, analysis and data processing, and the final phase, the study provides insights into the risks and security practices within PTPN V. The assessment reveals the impact criteria, organizational assets, and security practices, highlighting areas of improvement and recommendations for risk mitigation. Overall, this research contributes to enhancing information security and protecting personal data in the Hitmi System and provides valuable insights for organizations in similar contexts.

REFERENCES

[1] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Information Processing & Management, vol. 58, no. 1, p. 102397, 2021.

[2] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Computational and Structural Biotechnology Journal, vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

[3] S. Otoum, B. Kantarci, and H. Mouftah, "Empowering Reinforcement Learning on Big Sensed Data for Intrusion Detection," in ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China: IEEE, May 2019, pp. 1–7. doi: 10.1109/ICC.2019.8761575.
[4] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 20, no. 2, pp. 389–396, 2021.
[5] D. Susanto, "URGENSI PENGATURAN DATA DIGITAL/ELEKTRONIK PRIBADI," Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, vol. 2, no. 3, pp. 1140–1148, 2022.
[6] UU No. 27 Tahun 2022. Accessed: Nov. 24, 2022. [Online]. Available: https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022
[7] W. He, Z. J. Zhang, and W. Li, "Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic," International journal of information management, vol. 57, p. 102287, 2021.
[8] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, "The Octave Allegro Method in Risk Management Assessment of Educational Institutions," Aptisi Transactions on Technopreneurship (ATT), vol. 2, no. 2, pp. 167–179, 2020.
[9] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," Nist special publication, vol. 800, no. 30, pp. 800–30, 2002.
[10] R. L. Krutz and R. D. Vines, The CISSP prep guide: mastering the ten domains of computer security. New York: Wiley, 2001.
[11] R. Rosmala, "Fungsi komunikasi korporat Humas PT. Perkebunan Nusantara V Pekanbaru," PRofesi Humas, vol. 5, no. 2, pp. 143–164, 2021.
[12] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2003.
[13] J. S. Suroso and M. A. Fakhrozi, "Assessment of information system risk management with octave allegro at education institution," Procedia Computer Science, vol. 135, pp. 202–213, 2018.
[14] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.
[15] C. Woody, J. Coleman, M. Fancher, C. Myers, and L. Young, "Applying OCTAVE: Practitioners Report," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2006.
[16] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "OCTAVE-S implementation guide, Version 1.0," Manuel électronique. Pittsburg, PA,: Software Engineering Institute, Carbegie Mellon university, 2005.
[17] J. P. SARI, "ANALISIS RESIKO KEAMANAN SISTEM E-PROCUREMENT MENGGUNAKAN METODE OCTAVE-S (Studi Kasus: Unit Layanan Pengadaan Provinsi Riau)," skripsi, Universitas Islam Negeri Sultan Syarif Kasim Riau, 2018. doi: 10/10.%20BAB%20V_2018267SIF.pdf.
[18] F. A. Anshori and A. R. P. Suprapto, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, vol. 2548, p. 964X, 2019.
[19] A. F. Rohman, A. Ambarwati, and E. Setiawan, "Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S," INTECOMS: Journal of Information Technology and Computer Science, vol. 3, no. 2, pp. 298–310, 2020.
[20] R. J. Gagas, I. Syah, and F. Febryanto, "ANALISIS, EVALUASI, DAN MITIGASI RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE DAN FMEA (STUDI KASUS: UNIT PENGELOLA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS XYZ)," Jurnal Khatulistiwa Informatika, vol. 9, no. 2, 2021.
[21] M. Megawati and M. L. Hamzah, "Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S," Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, vol. 8, no. 1, pp. 62–67.
[22] LintangSetianti, "Urgensi Regulasi Perlindungan Data Pribadi di Indonesia - Analisis - www.indonesiana.id," https://www.indonesiana.id/profil/read/68772/urgensi-regulasi-perlindungan-data-pribadi-di-indonesia, Apr. 27, 2019. https://www.indonesiana.id/read/68772/urgensi-regulasi-perlindungan-data-pribadi-di-indonesia (accessed Nov. 24, 2022).