JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7670

SIMRS RISK ASSESSMENT USING OCTAVE ALLEGRO METHOD AND ISO/IEC 27001:2022 CONTROL STANDARD

Ito Setiawan[1*]; Kharisma Putri Sholekha[1]; Retno Waluyo[1]

Department of Information System[1]
Universitas Amikom Purwokerto, Purwokerto, Indonesia[1]
www.amikompurwokerto.ac.id[1]
itosetiawan@amikompurwokerto.ac.id*, kharismaputricp123@gmail.com,
waluyo@amikompurwokerto.ac.id

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— *Cilacap Regional General Hospital has been using the SIMRS system since 2006 to the present day. however, its use has encountered several challenges, such as human error, lengthy data synchronisation processes and time-consuming application maintenance. Previous studies have analyzed risk assessments regarding application usage, yet there is a gap in the implementation of risk mitigation. The aim of the research is to carry out a risk assessment of the SIMRS using the OCTAVE Allegro method and to propose risk mitigation measures in accordance with ISO/IEC 27001. The novelty of this research lies in the combination of methods used to conduct risk assessment and mitigation utilising the ISO/IEC 27001:2022 control standards. Results of research identify the areas of impact, reputation, finance and productivity. The areas of concern are human error, hardware management and software management. Scenarios were developed based on these areas of concern; according to the calculations, the score for human error was 31, for hardware management 24 and for software management 18. Mitigation, as set out in ISO/IEC 27001:2022, focuses on organisational controls in clauses 5.1, 5.15, 5.24, 5.26, 5.28, 5.33, 5.37. People controls in clauses 6.2, 6.3, 6.5, 6.8. Physical controls in clauses 7.5, 7.7, 7.10, 7.12, 7.13. Technological controls in clauses 8.2, 8.5, 8.7, 8.12, 8.13, 8.20, 8.22, 8.32. The scientific contribution lies in the integration of the OCTAVE Allegro and ISO/IEC 27001:2022 approaches to produce a risk assessment process that is not only capable of identifying and prioritising risks, but also directly provides relevant security controls.*

Keywords*: Information Security, ISO/IEC 27001:2022, OCTAVE Allegro, Risk Assessment, SIMRS.*

Intisari— *RSUD Cilacap sudah menerapkan SIMRS mulai tahun sampai saat ini, namun dalam penggunaan pernah mengalami beberapa kendala seperti human error, lamanya proses sinkronisasi data dan lamanya proses maintenance aplikasi. Studi sebelumnya telah menganalisis penilaian risiko penggunaan aplikasi namun terdapat kesenjangan dalam penerapan mitigasi risiko. Tujuan penelitian adalah melakukan penilaian risiko SIMRS menggunakan metode OCTAVE Allegro dan memberikan mitigasi risiko berdasarkan ISO/IEC 27001. Kebaruan penelitian ini terletak pada kombinasi metode dalam melakukan penilaian dan mitigasi risiko menggunakan standar control ISO/IEC 27001:2022. Hasil dari penelitian menjelaskan area dampak yaitu reputasi, keuangan dan produktivitas kerja. Pada areas of concern yaitu human error, manajemen hardware dan manajemen software. Scenario dibuat berdasarkan areas of concern, berdasarkan perhitungan areas of concern human error skor 31, area manajemen hardware skor 24 dan manajemen software skor 18. Mitigasi mengacu pada ISO/IEC 27001:2022 fokus pada area organizational controls pada poin 5.1, 5.15, 5.24, 5.26, 5.28, 5.33, 5.37, people controls pada poin 6.2, 6.3, 6.5, 6.8 , physical controls pada poin 7.5, 7.7, 7.10, 7.12, 7.13 dan technological controls pada poin 8.2, 8.5, 8.7, 8.12, 8.13, 8.20, 8.22, and 8.32. Kontribusi ilmiah terletak pada integrasi pendekatan OCTAVE Allegro dan ISO/IEC 27001:2022 untuk menghasilkan proses penilaian risiko yang tidak hanya mampu mengidentifikasi dan memprioritaskan risiko, tetapi secara langsung memberikan pengendalian keamanan yang relevan.*

Kata Kunci*: Keamanan Informasi, ISO/IEC 27001:2022, OCTAVE Allegro, Penilaian Risiko, SIMRS.*

INTRODUCTION

Many hospitals have implemented this system in the process of serving patients [1]. Hospital Management Information System (SIMRS) is an information system that has been widely implemented in the health sector [2], [3]. SIMRS has the task of integrating and processing all hospital service flows in the form of administrative procedures, data reporting, coordination networks, and others [4]. SIMRS can improve service quality, supervision, coordination, and time efficiency in hospital work processes [5]. One of the hospitals that has implemented SIMRS is Cilacap Regional General Hospital. Cilacap Regional General Hospital first implemented SIMRS in 2006, initially developing only the basic modules (registration, medical records, personnel, and cashier). This system is still in use today, but its implementation has encountered several obstacles, such as human error, lengthy data synchronization processes, and lengthy application maintenance processes when problems arise.

An organization's dependence on information systems is proportional to the level of threats and risks arising from the use of such systems[6]. Risk is a condition arising from the implementation of something that creates uncertainty for an organization in achieving its goals [7]. In addressing risks that tend to be negative, it is necessary to assess the risks of using information systems [8]. Good risk management can reduce the threats and impacts arising from the use of information technology [9]. Risk assessment is the process of identifying potential threats to an event, analyzing the probability of activities, analyzing the level of damage, and planning mitigation measures [10], [11].

The purpose of risk assessment is to ensure that every risk can be managed properly and to reduce the negative impact it causes [12]. Risk assessment encompasses the process of identifying and evaluating risks related to the integrity, confidentiality, and availability of resources [13]. The assessment process is also tailored to the needs of the existing organization [14]. The results of the assessment will be used as a basis for developing mitigation measures against potential risks [15]. To date, the Regional General Hospital has never conducted a risk assessment related to the use of the Hospital Management Information System.

There are many methods that can be used to assess the risks associated with the use of information systems [16]. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro method is one method for conducting risk assessments [17]. This method has comprehensive sections and well-defined stages for risk assessment based on information security data [18]. The Octave Allegro method can perform more complex risk assessments to produce maximum assessments for organizations [19]. This method was designed by CERT Survivable Enterprise Management with the aim of aligning organizational direction with information security[20]. Another objective is to produce risk assessments more quickly without having to understand risk assessment in depth [21]. The OCTAVE Allegro method focuses on risk assessments related to information capabilities based on the use of storage, distribution, and processing data to develop the right risk reduction strategies [22]. By applying this method, organizations can identify and address threats from the implementation of technology [23].

The risk control process in this study refers to the ISO/IEC 27001:2022 standard. This standard is an international standard created by the non-governmental organization International Organization for Standardization, which functions in the field of information security management [24], [25]. This standard applies the basic principles of an information security management system, namely plan, do, check, and act [26]. This standard provides steps for all organizations in implementing, establishing, maintaining, and continuously improving information security management[27]. The advantage of ISO/IEC 27001 is that it can be used in various types of organizations and is more flexible according to organizational needs, security requirements, and organizational objectives.

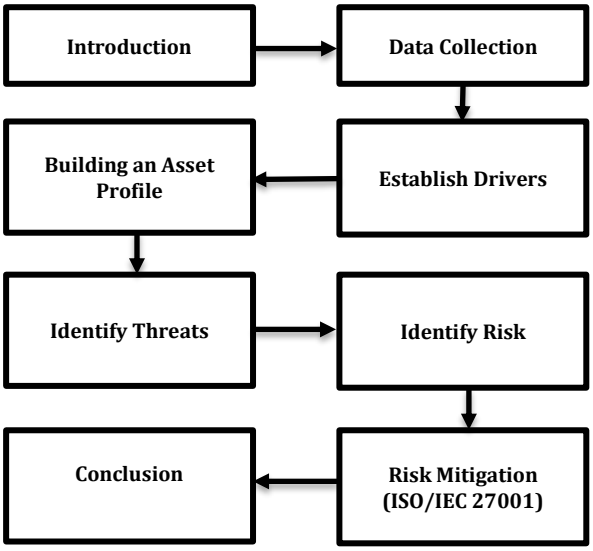
The purpose of this study is to assess the risks associated with implementing a hospital management information system (SIMRS) in order to determine the level of risk involved in using the information system and to provide recommendations for mitigation. A similar study was conducted by [28] using the same methods and controls as this study. Another study by [29] used the same methods and controls as this study, but both studies used ISO/IEC 27001:2013 control. The scientific contribution of this research lies in the integration of the OCTAVE Allegro and ISO/IEC 27001:2022 approaches to produce a risk assessment process that is not only capable of identifying and prioritise risks, but also directly links each risk to the relevant security controls. Previous studies have analyzed risk assessments for application use in organizations, but there are gaps in the implementation of risk mitigation. Risk mitigation implemented has not kept pace with the development of control standard that meet

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7670

organizational needs. Novelty of this research lies in the combination of methods in conducting risk assessment and mitigation using the ISO/IEC 27001:2022 control standard.

MATERIALS AND METHODS



Source: (Research Results, 2026)

Figure 1. Research Flow

Figure 1 shows the stages of the research conducted. The explanation of the research stages is as follows:

1. Data Collection

   This stage involves the collection of data to support the research process. The data collected for this study includes interviews, observations, documentation, questionnaires, and literature studies. Researchers have observed the use of SIMRS, conducted interviews with hospital staff, collected documents such as standard operating procedures for using the application, and distributed questionnaires to the hospital's IT department.
2. OCTAVE Allegro Method

   This method is used to assess SIMRS risks. There are four phases: Define Drivers or Guidelines, Profile Assets, Identify Threats, and Identify & Mitigate [30].
3. ISO/IEC 27001 Method

   This method is employed as a reference for mitigating risks that have been previously analyzed. This method is predicated on its own set of standards for the management of risks arising from the implementation of SIMRS.
4. Conclusion

   Following the completion of the risk assessment and risk mitigation, the subsequent step involves the extraction of conclusions from the identified risks and the formulation of recommendations for the management of existing risks.

RESULTS AND DISCUSSION

1. Establish Drivers

There are three worksheets for establishing risk measurement criteria at Cilacap Regional General Hospital. These worksheets are consistent with the issues at hand and cover indicators of reputation, finance, and productivity. The subsequent table contains explanations of each indicator.

Table 1. Impact Area Prioritization

Allegro Worksheet	Impact Area Prioritization
Priority	Impact Area
1	Reputation
3	Finance
2	Productivity

Source: (Research Results, 2026)

As illustrated in Table 1, the findings of the data entry process concerning the impact of priority areas are presented, with these areas having undergone a systematic prioritization procedure. In accordance with this procedure, reputation indicators were assigned the highest priority, followed by productivity indicators, and finally, financial indicators.

2. Profile Assets

This phase involves identifying a collection of critical assets related to information assets that are important to the company and asset ownership.

Table 2. Critical Asset Inventory

Asset	Critical Asset
Information	Patient Data
	Medication Data
	Financial Data
	Employee Data
	Facilities
	Hospital Assets
Information System	SIMRS
Software	Windows OS, SIMRS, Aplikasi
Hardware	PC (200+)
	Router
	Server (1)
	Application (8)
	Switch/Hub
	Access Point (50+)
	Printer
	Finger Print (40)
	Display
	Internet Network
Human Resources	Director
	Administration Staff
	Medical Record

Asset	Critical Asset
	IT Department
	Physician and Nurse
	Finance Department
	Admissions

Source: (Research Results, 2026)

3. Identify Threats

This stage builds directly on our initial analysis, where we move from those broad concerns to pinpointing specific, actionable threats.

a. Identify Areas of Concern

This phase involves identifying Areas of Concern in the use of SIMRS. Areas of Concern are descriptive statements that explain the conditions or situations that are the main focus of attention and must be addressed in order to minimize and prevent risks to SIMRS.

Table 3. Areas of Concern

Area of Concern	Attack Types Encountered
Data Processing	Human Error
Hardware Management	suboptimal SIMRS
Software Management	SIMRS management failure

Source: (Research Results, 2026)

b. Identify Threats Scenarios

This phase involves expanding each area of concern into threat scenarios that explain how an action or problem could pose a threat to information assets using threat property identification. Below is a table identifying threat properties.

Table 4. Allegro Worksheet Human Error

Allegro Worksheet	Information Asset Risk Worksheet
Data Asset	Hospital Management Information System (SIMRS)
Focus area	Data Processing
Actor	The hospital staff member in charge of that department
Means	The relevant staff member made a data entry or deletion error while using the SIMRS.
Event Chronology	
Motive	Human Error
Reason for the occurrence	
Outcome	
Impact of incident	Modification
Security Requirements	The disciplinary procedure must be formalized and communicated in order to take action against staff and other involved parties who have violated data security policies
Violated regulation	
Probability	High

Source: (Research Results, 2026)

Table 4 describes the human error scenario. This is followed by an explanation of hardware management, as shown in Table 5.

Table 5. Allegro Worksheet Hardware Management

Allegro Worksheet	Information Asset Risk Worksheet
Data Asset	Hospital Management Information System (SIMRS)
Focus area	Hardware Management
Actor	Staff of IT department
Means	suboptimal SIMRS
Event chronology	
Motive	IT staff did not replace the obsolete hardware with new equipment
Reason for the occurrence	
Outcome	Modification
Impact of incident	Interruption
Security Requirements	1. Proper maintenance of equipment is required to uphold data availability, integrity, and confidentiality
Violated regulation	2. Network systems and applications must be monitored for anomalous behavior, and appropriate action must be taken to evaluate the ability to handle data security incidents.
Probability	Medium

Source: (Research Results, 2026)

Table 5 explains the hardware management scenario, followed by an explanation of software management as shown in Table 6.

Table 6. Allegro Worksheet Software Management

Allegro Worksheet	**Information Asset Risk Worksheet**
Data Asset	Hospital Management Information System (SIMRS)
Focus area	Software Management
Actor	Natural disaster / Lightning strike
Vulnerability	
Exploiter	
Means	A lightning strike damaged a critical network switch (or hardware device), resulting in system failure
Event chronology	
Motive	Accidental
Reason for the occurrence	
Outcome	Destruction
Impact of incident	Interruption
Security Requirements	Protection against tangible threats and areas such as natural disasters, as well as other deliberate or unintentional physical threats to infrastructure, must be designed and implemented.
Violated regulation	Backup copies of data, software features, and systems must be maintained and tested periodically, in accordance with the agreed topic-specific backup policy.
Probability	Low

Source: (Research Results, 2026)

So, from what we can see in Table 6, it looks like the issue of old or outdated hardware not being replaced regularly by IT staff or employees

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7670

happened because of some unintentional negligence. This was probably due to a lack of knowledge at the time and some negligence on the part of IT. The consequences of this threat to information system assets were modification or change, and interruption or disruption. In this threat scenario, the likelihood of risk occurring is at a medium level because it results in suboptimal hardware or SIMRS performance.

4. Identify and Mitigate Risks

This stage consists of three phases, which are a continuation of the previous stage: Identify Risk, Analyze Risk, and Select Mitigation Approach.

a. Identify Risk

This phase is a step that will determine how threat scenarios that have been documented in the Information Asset Risk Worksheet can impact the Company. Threat scenarios will also be supplemented by the consequences that may arise.

Table 7. Identify Risk – Scenario

Threats Scenario	Consequences
Input Data Error	Staff are forced to repeatedly re-enter data, a time-consuming process that reduces hospital-wide productivity. This practice also corrupts data and files, requiring constant corrections to the database.
Hardware Management	System performance is degrading, causing significant delays in patient services. This also increases the risk of system failures, which can lead to data loss or costly downtime.
Software Management	Operational downtime and system component failures

Source: (Research Results, 2026)

As outlined in Table 7, the repercussions of data entry and deletion errors made by employees or hospital staff who are responsible for the relevant departments are explained. This will have a negative impact on work productivity in the hospital because it takes a long time to correct these errors, and patients' trust in the hospital will decline.

b. Analyze Risk

This phase entails an evaluation that is informed by the risk criteria that were identified in Phase 1 of Activity 1. The threat scenarios and consequences that have been developed will be examined to determine their impact on the criteria. Furthermore, the impact of the aforementioned factors must be assessed in order to determine whether it is high, medium, or low. Subsequent to this, the impact will be assessed based on the risk criteria and its level. The risk impact will be assigned a value of 3 in cases where the risk impact is high, a value of 2 in cases where the risk impact is medium, and a value of 1 in cases where the risk impact is low. This number will then be multiplied by the risk criteria level in phase 1 of activity 1. The risk criteria level that has been adjusted in phase 1 of activity 1 will be used as a multiplier in the impact value. The multiplication of these values will result in an aggregate total for each risk category. The risk assessment is documented in Table 8.

Table 8. Information Asset Analyze Risk

Allegro Worksheet	Information Asset Risk Worksheet		
Consequences	Security		
Organizational consequences resulting from violations	Severity of Organizational Impact		
	Impact Area	Value	Score
Input Data Error			
Staff are repeatedly forced to re-enter data, a time-consuming	Reputation and Customer trust	High	9
process that hampers productivity across the	Productivity	High	6
hospital.	Finance	High	6
Leading to damaged and loss data	Productivity	Med	4
Performing database repairs	Productivity	High	6
Relative Risk Score			31
	Impact Area	Value	Score
Hardware Management			
	Productivity	High	6
Lower Performance	Productivity	High	6
Growing delays in patient care.	Reputation and Customer trust	Med	6
System failures may occur, causing loss of data or productivity.	Finance	High	6
Relative Risk Score			24
	Impact Area	Value	Score
Software Management			
	Productivity	Med	4
Downtime Operational Requires replacement/upgrade	Finance	High	6
System component failures	Productivity	Low	2
	Finance	High	6
Relative Risk Score			18

Source: (Research Results, 2026)

These findings are consistent with previous research which suggests that human factors are the dominant cause of information security incidents [15].

c. Select Mitigation Approach

Decisions are made when risks are deemed unacceptable or mitigated. At this point, the risks

will be studied again for data collection and evaluation. While the consequences of these risks are not a significant threat to the company, it is important to acknowledge their occurrence. As outlined in the Risk Relative Matrix, the mitigation approach for each area of concern is detailed in Table 9.

Table 9. Area of Concern

Area Of Concern	Risk Relative Matrix	POOL	Mitigation Approach
Human Error	31	1	Mitigate
Hardware Management	24	2	Mitigate
Software Management	18	2	Mitigate

Source: (Research Results, 2026)

Select Mitigation Approach refers to ISO 27001:2022. The following references are provided. Mapping risks to ISO 27001 controls based on area of concern. Several controls are used, such as organizational controls, people controls, physical controls, and technological controls. focusing on the area of organizational controls in points 5.1, 5.15, 5.24, 5.26, 5.28, 5.33, 5.37, people controls in points 6.2, 6.3, 6.5, 6.8, physical controls in points 7.5, 7.7, 7.10, 7.12, 7.13, and technological controls in points 8.2, 8.5, 8.7, 8.12, 8.13, 8.20, 8.22, and 8.32.

Table 10. Select Mitigation Approach.

Mitigation	Information
5.1 Information Security Policies	Information security policies must be established, reviewed and approved by the organization, and implemented by its personnel.
5.15 Controls for Hardware and Software Access	Policies for the access control of hardware and software must be established and adopted by the organization.
5.24 Information Security Incident Management Readiness and Planning	The organization must prepare and plan for information security incident management by establishing, defining, and communicating the roles and responsibilities across all relevant departments.
5.26 Response to Information Security Incidents	Incidents that occur must be handled in accordance with established procedures.
5.28 Evidence Collection	The organization must establish and implement procedures for the collection and identification of evidence related to information security incidents.
5.33 Protection of Procedural Records	Records must be safeguarded against damage, loss, unauthorized access, tampering, and unauthorized disclosure.
5.37 Documentation of Operational Incident Procedures	Documented procedures for information processing must be established and made readily accessible to all relevant personnel.
6.2 Terms and Conditions of Employment	Employment contracts must include a section on information security that outlines the responsibilities of both the individual and the organization.
6.3 Information Security Training, Education, and Awareness	Stakeholders and organizational employees must be willing to participate in relevant information security training. They are required to comply with new information security policies according to their job functions.
6.5 Responsibilities after Change or Termination of Employment	Ongoing information security responsibilities that persist after a role change or employment termination must be enforced, clearly defined, and communicated to all personnel and stakeholders.
6.8 Information Security Event Reporting	The organization must provide a proper and timely mechanism for reporting information security incidents.
7.5 Protection from Environmental and Physical Threats	Infrastructure must be protected by design from environmental and physical threats, including lightning, natural disasters, and intentional or unintentional human acts.
7.8 Secure Positioning and Protection of Equipment	Equipment must be positioned in a protected and secure manner.
7.10 Management of Storage Media	The management of storage media throughout its lifecycle, covering acquisition, use, transportation, and disposal, must comply with the organization's data classification and handling policies.
7.12 Security of Cabling Infrastructure	Data and power cables supporting information services must be safeguarded against interference and physical damage.
7.13 Equipment Maintenance	Equipment must be well-maintained to guarantee information integrity, availability, and confidentiality.
8.2 Information Access Restriction Control	Access to information assets shall be controlled based on the established access control policy.
8.5 Data Security Authentication	Authentication procedures and technologies must be implemented based on the access control policy and information access restrictions.
8.7 Protection Against Malware	Protection against viruses must be supported and reinforced by user awareness.
8.12 Data Leakage Prevention	Measures to prevent data loss must be applied to all networks, systems, and devices responsible for storing, processing, or transmitting sensitive information.
8.13 Information Backup	Regular testing and maintenance of software copies and data backups must be performed as defined by the agreed backup policy.
8.20 Network Security Management	Network devices and providers must be managed, controlled, and secured to safeguard application data.
8.22 Network Segregation	An organization's network must have segmentation between user groups, applications, and information services.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7670

Mitigation	Information
8.32 Change Management Control	Formal change management procedures must be established for any modifications to information system facilities and information processing.

Source: (Research Results, 2026)

CONCLUSION

The results of this study indicate that the priority impact areas are reputation, finance, and work productivity. In the areas of concern, there are three categories of mitigation, namely human error, hardware management, and software management. Scenarios are created based on areas of concern, based on calculations of areas of concern: human error scores 31, hardware management scores 24, and software management scores 18. Mitigation refers to ISO/IEC 27001:2022, focusing on the area of organizational controls in points 5.1, 5.15, 5.24, 5.26, 5.28, 5.33, 5.37, people controls in points 6.2, 6.3, 6.5, 6.8, physical controls in points 7.5, 7.7, 7.10, 7.12, 7.13, and technological controls in points 8.2, 8.5, 8.7, 8.12, 8.13, 8.20, 8.22, and 8.32. The scientific contribution of this research lies in the integration of the OCTAVE Allegro and ISO/IEC 27001:2022 approaches to produce a risk assessment process that is not only capable of identifying and priority risks, but also directly links each risk to the relevant security controls. limitation of this study is that it has not yet assessed the effectiveness of the implementation of the safety controls put in place. Further research can be conducted to evaluate the effectiveness of ISO 27001 control implementation in hospitals. Comparative studies of risk assessment methods are also recommended for more in-depth analysis.

REFERENCE

[1] E. B. Pratama and A. Hendini, "Implementasi Extreme Programming Pada Perancangan SIMRS (Sistem Informasi Manajemen Rumah Sakit)," *J. Khatulistiwa Inform.*, vol. 10, no. 2, pp. 107–112, 2022, doi: 10.31294/jki.v10i2.14159.

[2] R. T. Perkasa and F. Samopa, "Analisa Pengembangan Fitur Lebih Lanjut dengan Pendekatan Requirement Analysis dan Design Thinking," *Kesatria J. Penerapan Sist. Inf. (Komputer Manajemen)*, vol. 5, no. 3, pp. 866–873, 2024, doi: 10.30645/kesatria.v5i3.412.

[3] G. Winarti, "Literature Review: Faktor Keberhasilan Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS)," *Communnity Dev. J.*, vol. 4, no. 1, pp. 486–497, 2023.

[4] I. V. Santosa, M. N. Subekti, G. S. Jagaddhito, and A. D. Susanti, "Analisis Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) dalam Meningkatkan Pengelolaan Rumah Sakit yang Efisien di Rumah Sakit Umum Daerah Surakarta," *Sejah. J. Inspirasi Mengabdi Untuk negeri*, vol. 3, no. 1, pp. 189–197, 2024, doi: 10.58192/sejahtera.v3i1.1716.

[5] Suriani, O. Keteren, and J. Hutajulu, "Studi Penerapan Aplikasi Sistem Informasi Manajemen Rumah Sakit (SIMRS)," *J. Telenursing*, vol. 5, no. 1, pp. 245–253, 2023, doi: 10.26418/justin.v12i4.78493.

[6] M. Suorsa and P. Helo, "Information security failures identified and measured–ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis," *Inf. Secur. J.*, vol. 33, no. 3, pp. 285–306, 2024, doi: 10.1080/19393555.2023.2270984.

[7] T. P. P. Kusuma, I. Setiawan, M. A. Aziz, and B. D. Putranto, "Manajemen Risiko Sistem Informasi Akademik Menggunakan OCTAVE Allegro dan ISO/EIC 27001 di Universitas Perwira Purbalingga," *JUSTIN J. Sist. dan Teknol. Inf.*, vol. 12, no. 4, pp. 592–598, 2024, doi: 10.26418/justin.v12i4.78493.

[8] H. Julianni and E. Rachmawati, "Analisis Persepsi Resiko Terhadap Minat Beli Produk Makanan Online Pada Aplikasi Shopee," *JEMPER (Jurnal Ekon. Manaj. Perbankan)*, vol. 6, no. 2, pp. 120–129, 2024, doi: 10.32897/jemper.v6i2.3309.

[9] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 407–420, 2022, doi: W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," J. Tek. Inform. dan Sist. Inf., vol. 9, no. 1, pp. 407–420, 2022.

[10] P. N. Emmanuel and R. Maulany, "Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House," *Krea-Tif J. Tek. Inform.*, vol. 11, no. 1, pp. 37–52, 2023, doi: 10.32832/krea-tif.v11i1.14179.

[11] R. Zefri, D. A. Wulandari, and Suripin, "Analisis Risiko Kegagalan Bendungan Paselloreng Dengan Metode Pohon Kejadian (Event Tree)," *SIKLUS J. Tek. Sipil*, vol. 8, no. 2, pp. 149–160, 2022, doi: 10.34010/jati.v12i2.6829.

[12] I. P. A. S. Putra and I. K. R. Hendrawan, "Analisis Manajemen Risiko SIMRS pada Rumah Sakit Ganesha Menggunakan ISO 31000," *JATI J. Teknol. dan Inf.*, vol. 14, no. 1, pp. 88–98, 2024, doi: 10.34010/jati.v14i1.
[13] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustain.*, vol. 15, no. 7, 2023, doi: 10.3390/su15075828.
[14] H. Sulaeman, H. P. Utomo, and A. I. Suryana, "Penilaian Risiko Keamanan Informasi Pada Sistem Informasi Akademik (SIAKAD) Dengan Menggunakan Framework NIST-SP 800 30," in *Prosiding Seminar Nasional Teknologi Komputer dan Sains*, 2023, pp. 414–432.
[15] A. Arista and K. N. M. Ngafidin, "An Information System Risk Management of a Higher Education Computing Environment," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 12, no. 2, pp. 557–564, 2022, doi: 10.18517/ijaseit.12.2.13953.
[16] M. Rifial, A. Razak, D. Darmawansyah, I. Indar, and A. Rahman, "Evaluation of the Utilization of the Hospital Management Information System (SIMRS) at Madani Regional General Hospital, Palu," *J. Public Heal. Pharm.*, vol. 5, no. 2, pp. 274–286, 2025, doi: 10.56338/jphp.v5i2.6169.
[17] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *J. Teknol. dan Inf.*, vol. 12, no. 2, pp. 106–117, 2022, doi: 10.34010/jati.v12i2.6829.
[18] Suroso and Wasilah, "Analisis Keamanan Informasi SIMRS dengan Metode Indeks KAMI dan OCTAVE Allegro," *J. Tek.*, vol. 19, no. 3, pp. 795–808, 2025, doi: 10.35446/teknika.v19i3.10705.
[19] S. Alfarisi and N. Surantha, "Risk assessment in fleet management system using OCTAVE allegro," *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 530–540, 2022, doi: 10.11591/eei.v11i1.3241.
[20] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *J. Comput. Inf. Syst.*, vol. 66, no. 1, pp. 123–150, 2026, doi: 10.1080/08874417.2024.2329985.
[21] R. W. Astuti, R. A. Putra, and I. S. Putra, "Penilaian Risiko Penggunaan Sistem Informasi Akademik Pada STIQ Al-Lathifiyyah Palembang Dengan Metode Octave Allegro," *J. Comput. Inf. Syst. Ampera*, vol. 4, no. 1, pp. 44–54, 2023, doi: 10.51519/journalcisa.v4i1.337.
[22] R. F. P. Wahyu, R. G. Utomo, and M. Al Makky, "Analisis Risiko Keamanan Informasi Pada Divisi Penjualan Pt Matahari Department Store Cabang Jogja City Mall Menggunakan Metode Octave Allegro," in *e-Proceeding of Engineering*, 2023, pp. 5073–5079.
[23] H. A. Setia, E. M. Safitri, V. R. Putri, and C. P. Wibowo, "Analisis Keamanan Website Dinas Perhubungan Provinsi Jawa Timur Menggunakan Metode OCTAVE Allegro Dan FMEA," in *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI)*, 2023, pp. 299–308, doi: 10.33005/sitasi.v3i1.554.
[24] A. A. Ipungkarti, "Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta," *J. Media Infotama*, vol. 19, no. 1, pp. 103–110, 2023, doi: 10.37676/jmi.v19i1.3481.
[25] B. Aurabillah, L. A. Putri, N. C. Fadhlilla, and A. Wulansari, "Implementasi Framework ISO 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 454–460, 2024, doi: 10.36040/jati.v8i1.8736.
[26] K. Sari, A. Harnia, S. N. Hidayah, and N. Sri, "Integrated Strategy For Information System Security Assessment Through The Implementation Of ISO 27001 Standards," in *International Conference on Computer Science, Engineering, Social Science, and Multi-Disciplinary Studies (CESSMUDS)*, 2025, pp. 668–671, doi: 10.64803/cessmuds.v1.129.
[27] P. Prasetyo and G. Yudoko, "Information Security Management System Transition Strategy From ISO/IEC 27001:2013 To ISO/IEC 27001:2022 At PT PKT," *Ekombis Rev. J. Ilm. Ekon. dan Bisnis*, vol. 14, no. 2, pp. 2587–2600, 2026, [Online]. Available: https://jurnal.unived.ac.id/index.php/er/indexDOI:https://doi.org/10.37676/ekombis.v14i2
[28] D. Widiyasti, I. Rusi, and F. Febriyanto, "Manajemen Risiko Keamanan Teknologi Informasi Menggunakan Metode OCTAVE Allegro Dan Kontrol ISO/IEC 27001:2013 (Studi Kasus: PLN UP2D Kalimantan Barat)," *CODING J. Komput. dan Apl.*, vol. 11, no. 02, pp. 227–237, 2023, doi:

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7670

10.26418/coding.v11i2.62011.

[29] M. T. Anwar, U. Aryanti, M. Wijana, and D. Atmoko, "Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO / IEC 27001 : 2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x," *Informatics Educ. Prof. J. Informatics*, vol. 9, no. 1, pp. 73–83, 2024, doi: 10.51211/itbi.v9i1.2913.

[30] N. R. Romadhoni, M. S. Hasibuan, and K. Muludi, "Analisis Keamanan Informasi pada Sistem Komputerisasi Terpadu Menggunakan Metode Indeks KAMI dan Octave Allegro," *J. Ilmu Komput. Agri-Informatika*, vol. 12, no. 1, pp. 38–49, 2025, doi: 10.29244/jika.12.1.38-49.