Jurnal Darma Agung
Volume: 31, Nomor: 4, (2023), Agustus: 674 - 686
https://dx.doi.org.10.46930/ojsuda.v31i4.3236
P-ISSN:0852-7296
E-ISSN:2654-3915

INFORMATION SECURITY RISK ASSESSMENT USING FACTOR OF ANALYSIS INFORMATION RISK (FAIR) IN THE HEALTHCARE SECTOR: SCOPING REVIEW

Iman Pribadi Sudarsana [1)], Kalamullah Ramli [2)]
Magister Program of Information Network Security Management, Dept. of Electrical Engineering, University of Indonesia Jakarta, Indonesia [1)]
Dept. of Electrical Engineering, Faculty of Engineering, University of Indonesia Jakarta, Indonesia [2)]
Corresponding Author: iman.pribadi@ui.ac.id [1)], k.ramli@eng.ui.ac.id [2)]

Abstract

Risk assessment is an effective way to reduce information technology risks in healthcare facilities by determining the severity of potential dangers and weaknesses affecting each vital data element. This enables appropriate actions to be taken by prioritizing data with the highest risk. However, there is still a lack of research on information security risk assessment using Factor Analysis of Information Risk (FAIR) in healthcare information systems, necessitating further studies to understand its implementation in Indonesia. A 21,939 articles were found in four databases, but only three met the inclusion criteria from Indonesia, Japan, and the United States. These studies focus on risk assessment and management in the healthcare sector, including ISO 27005, cloud ecosystem risk analysis, cybersecurity standards, and IoT risk management for COVID-19. The review stresses the significance of risk assessment and management in the health sector to sustain health facilities amidst policy changes, technological advancements, and globalization. FAIR is vital in determining the likelihood and potential consequences of events that can affect organizations, particularly in the competitive healthcare industry where a secure health information system is necessary for business continuity. Hence, studies must develop methods to reduce information security risks in Healthcare services information systems.

Keywords: ***Information Security Risk Assessment, FAIR, Healthcare Sector***

INTRODUCTION

Information systems are an integral part of daily business activities, it can even be said that business processes and decision-making strategies are now heavily dependent on information systems. One of the companies that depend on information systems is healthcare service facilities. Healthcare service facilities become primary needs for everyone, not only for service nor action that can influence the comfort of the patients but also for management with an organized healthcare information system. (Indrajit, 2000; Sudjiman & Sudjiman, 2018)

Healthcare information systems in healthcare service facilities are a breakthrough in the healthcare world. This system functions to manage processes, making healthcare

History:
Received : 25 Mei 2023
Revised : 10 Juni 2023
Accepted : 23 Juni 2023
Published: 23 Agustus 2023

Publisher: LPPM Universitas Darma Agung

service facility data management more accurate, secure, and effective. The rise in the prevalence and widespread adoption of the internet, as well as the Internet of Things (IoT) and the latest iteration of healthcare-focused technology known as the Internet of Medical Things (IoMT) or Internet of Healthcare Things (IoHT), poses a significant security risk, particularly in terms of cyber-attacks. Information security risk assessment in information systems allows for minimizing and addressing various information technology risks in healthcare service facilities. Additionally, the healthcare industry's staff is usually inexperienced with remote work and lacks planning skills for this transition, creating a weak spot for potential cyberattacks to target the sector.(Boddy et al., 2017; Jalali et al., 2020; Offner et al., 2021) Likewise, after assessment, the magnitude of threats and vulnerabilities is known for each critical data segment, leading to appropriate action by prioritizing data with the highest risk. (Chotimah, 2022)

One approach to information security risk assessment is the Factor Analysis of Information Risk (FAIR) method. FAIR is a risk analysis framework that concentrates on analyzing risk information and identifying assets, threats, and vulnerabilities that lead to risk. This standard is predominantly based on quantitative concepts and provides a practical and innovative approach to analyze risks by gathering information. By using this methodology, organizations can communicate their risk information and align with their enterprise's needs by assessing the risk scenarios and determining Loss Event Frequency and Loss Magnitude. In short, FAIR provides a comprehensive risk analysis approach that helps enterprises manage their risks efficiently. (Josey, 2014)

To establish a reliable and expandable network infrastructure for healthcare information systems, it is necessary to perform research to evaluate the potential security risks that these systems may face. While there is some research on assessing the security risks of healthcare information systems, it is still insufficient. Therefore, this scoping review was overseen to identify the role and application of Information Security Risk Assessment on Information Systems in the healthcare sector, to provide an overview of healthcare facilities in Indonesia on mitigating information security risks in healthcare information systems. (Hasanah, 2019; Jayadi et al., 2022)

a. *Research Problem*

   Although FAIR is a commonly acknowledged and adopted technique for evaluating and controlling information security risks, its efficiency in the healthcare industry has not been extensively studied.

b. *Research Focus*

   This scoping review will focus on identifying and evaluating the key factors analyzed in FAIR for information security risk assessment in the healthcare sector. The research will also evaluate the strengths and limitations of using FAIR in information security risk assessment in the healthcare sector. By identifying the gaps in the literature regarding the use of FAIR in the healthcare sector, this scoping review will highlight areas for future research and improvement.

c. *Research Aim and Research Questions*

The research will aim to to identify and analyze the existing literature on information security risk assessment using the Factor Analysis of Information Risk (FAIR) model in the healthcare sector. The review aims to explore the current state of knowledge, identify research gaps, and suggest avenues for future research in this area. The Research Questions: (1) What is the current state of research on information security risk assessment using the Factor Analysis of Information Risk (FAIR) model in the healthcare sector? (2) What are the key factors analyzed in the FAIR model for assessing information security risks in healthcare organizations? (3) How effective is the FAIR model in identifying and mitigating information security risks in healthcare organizations? (3) What are the challenges and limitations of using the FAIR model for information security risk assessment in healthcare organizations? (4) What are the best practices for implementing the FAIR model in healthcare organizations for effective information security risk management? (5) How can healthcare organizations leverage the FAIR model to achieve regulatory compliance and enhance patient data protection? (6) What are the future research directions for information security risk assessment in the healthcare sector using the FAIR model?

RESEARCH METHODOLOGY

A. General Background

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) is a methodological framework that provides guidelines for conducting scoping reviews.(Tricco et al., 2018) A scoping review is a type of literature review that aims to map the key concepts, evidence sources, and research gaps in a particular field.

In the case of the proposed research on information security risk assessment using the Factor Analysis of Information Risk (FAIR) model in the healthcare sector, the PRISMA-ScR framework can be used to guide the review process. The framework includes several steps, such as identifying the research question, searching for relevant literature, screening and selecting articles, extracting data, and summarizing and reporting the findings.

In addition to the PRISMA-ScR framework, the Population Concept Context (PCC) model can also be used to guide the scoping review. By using the PCC model, the scoping review can ensure that the search strategy is focused on the relevant literature and that the review findings are applicable to the specific population and context of interest.(Peters et al., 2015)

B. Sample of Eligible Document Criteria

The search strategy will involve searching electronic databases such as Scopus, IEEE Xplore, ProQuest, and ScienceDirect using a combination of keywords related to the population, concept, and context which comes to Information Systems, Healthcare, Information Security Risk, and Information Security Risk Assessment that is summarized in Table 1. Including the keyword combination used is: "Information Systems" AND "Health". Alternative keywords are also used such as "Information Systems" AND "Information Security Risk" AND "Information Security Risk Assessment", "Healthcare" AND "Factor Analysis of Information Risk". The articles selected were full-text Indonesian and English articles published in the last 5 years. Into the bargain, a search was also done on the list of references to articles that met the inclusion criteria to find out whether other related studies related to this research.

C. Instrument and Procedures

The PRISMA-ScR framework provides guidelines for developing inclusion and exclusion criteria to ensure that the scoping review is focused on relevant literature. The following are some instruments and procedures for developing inclusion and exclusion criteria.

The criteria for inclusion in this scoping review are: (1) The article is original research and has been reviewed and written in Indonesian and English; (2) Articles published within the last 5 years (2017-2022); (3) Studies accomplished in health services; (4) Research contains information security risk assessment on Health Information Systems.

Exclusion criteria used: (1) Articles that are not related to the problem in the research; (2) Articles that cannot be downloaded in full-text version; (3) The article is in the form of a scoping review.

D. Data Analysis

Below are methods for analyzing data in a scoping review focused on using the FAIR model for information security risk assessment in the healthcare sector.

Screening and Selection, the first stage of data analysis involves screening and selecting relevant articles. This process will involve an initial screening of titles and abstracts to identify potentially relevant articles, followed by a full-text screening of the selected articles to determine whether they meet the inclusion criteria. The PRISMA-ScR framework recommends using a standardized screening and selection form to record the reasons for inclusion or exclusion of each article.

Data Extraction, the second stage of data analysis involves extracting data from the selected articles. This process will involve identifying key information such as the author, publication year, study design, study population, intervention or exposure, outcome measures, and results. The PRISMA-ScR framework recommends using a standardized data extraction form to record the relevant data from each article.

Data Synthesis, the third stage of data analysis involves synthesizing the data from the selected articles. This process will involve organizing and summarizing the

extracted data in a way that addresses the research questions. The PRISMA-ScR framework recommends using a narrative synthesis approach, which involves summarizing the findings in a descriptive and interpretive manner. The synthesized data can be presented in tables, charts, and graphs to help visualize the results.

Reporting the Findings the final stage of data analysis involves reporting the findings of the scoping review. The PRISMA-ScR framework recommends reporting the findings in a structured and transparent manner. The scoping review report should include a clear description of the search strategy, inclusion and exclusion criteria, screening and selection process, data extraction and synthesis, and limitations of the study. The report should also provide a summary of the key findings and their implications for future research and practice.

RESEARCH RESULTS

In order to carry out the research, we reviewed a total of 21,939 articles using pre-determined keywords until December 31, 2022, through online databases such as ProQuest, SpringerLink, ScienceDirect, and Oxford journals. After manually filtering the search results using Microsoft Excel and removing duplicate articles, three articles were selected based on their title, abstract, and full text to meet the inclusion criteria. This process is illustrated in Figure 1 and summarized in Table 2.

Out of the seven reviewed studies, the articles comprise both quantitative and qualitative research and were produced in the United States, Indonesia, Japan, Lithuania, Italy, England, and Tunisia. Table 1 summarizes the main methods and findings of the reviewed articles. The first study run in Indonesia focuses on the Risk Assessment of Puskesmas Management Information System Data and Assets Using ISO 27005. (Jonny et al., 2021)

The second study overseen in Japan discussed the Risk Analysis and Modeling of Cloud Healthcare Ecosystems, using the FAIR approach and focusing on the Arterys™ case study on AWS. (Mariam Traore, 2022) Meanwhile, the third study in the United States is about creating a standard risk assessment framework for health information technology. There is also another article from the United States that includes the seventh study on cybersecurity standards, which will allow IoHT systems to automatically adapt to cyber threats using quantitative analysis and standards such as FAIRTM and DoCRA to optimize health outcomes. (Sparrell, 2019; Suzanna, 2021)

The article in Italy discusses Interdisciplinary research that opens up innovative solutions in healthcare, the platform proposes innovative solutions on how personal healthcare data can be processed and analyzed, protecting user privacy(Lepore, 2023) Articles in Tunisia discuss Security Risk Management in e-Health Systems. Researching e-health systems and their security challenges, especially for IoMT applications due to data sensitivity, rapid context changes, and aging ICT infrastructure. (Ksibi, 2022)

Another article in England discusses the Cyber Risk of Using IoT Devices to Manage COVID-19. Current findings indicate that medical IoT solutions are not being adequately evaluated for cyber risk, especially with the increased use of such solutions in Covid-19 management. (Radanliev, 2021)

Table 1. ***PCC Framework***

Population (P)	Health Information System
Concept (C)	Information Security Risk Assessment using FAIR Model
Context (C)	Types of Information Security Risk Assessment to be applied in the Healthcare Sector

Figure 1. ***PRISMA-ScR Research Diagram***

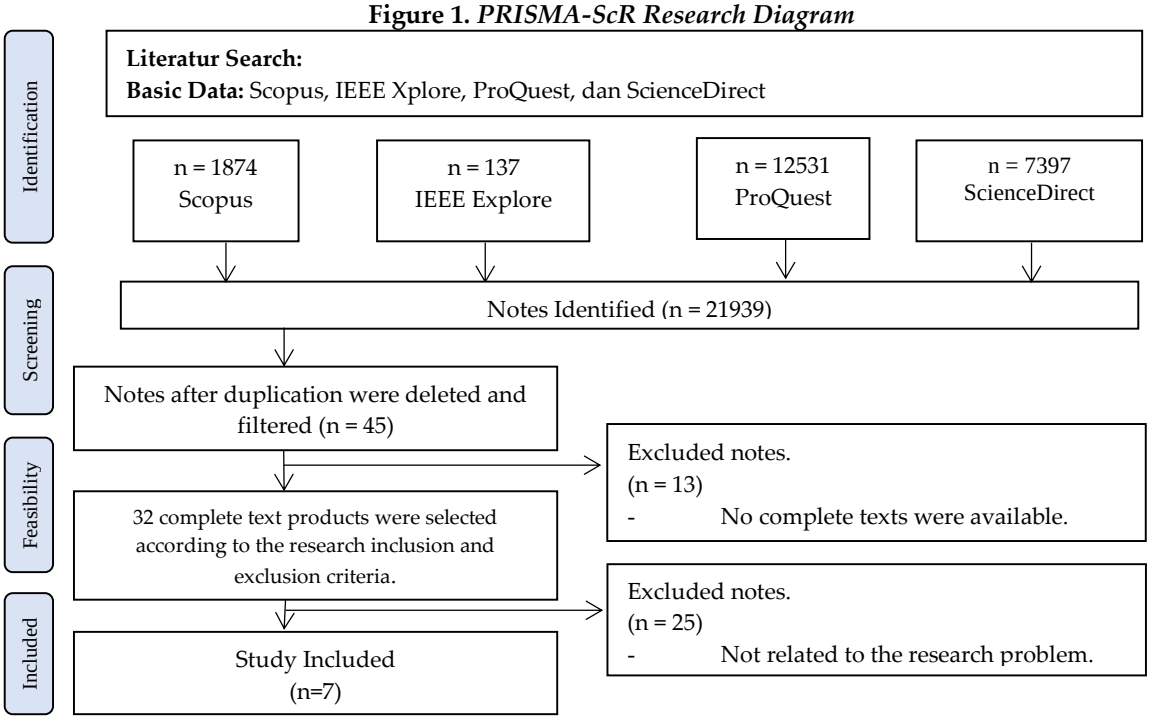

Table 2. Characteristics of the research used

Main Researcher/ Year/ Location	**Title**	**Research methods**	**Results**
Jonny, Awalludiyah Ambarwati, Cahyo Darujati/ 2021 / Indonesia	Risk Assessment of Health Center Management Information System Data and Assets Using ISO 27005	Quantitative and qualitative analysis, involving observation and interviews, to determine the category of risk impact and the probability of	Even though the standard documents do not give a detailed explanation of the risk assessment methodology as a process to achieve the objectives in the Information Security Management System (ISMS) control, an operational approach called Factor Analysis Information Risk (FAIR) is used to evaluate risks. The FAIR method makes it easier to conduct the risk assessment process required by Clause 6 of the ISO 27001:2013

Main Researcher/ Year/ Location	Title	Research methods	Results
		occurrence of threats to information security	ISMS standard, as defined in ISO 27005:2018. The average risk analysis result shows that the potential threat of medium and high-risk is still relatively low in terms of likelihood, as the services are still running normally.
Mariam Traore, Prof. Shuichiro Yamamoto/ 2022/ Japan	Healthcare CloudEcosystem Risk Analysis and Modeling: A FAIR Approach (A Case Study of Arterys™ on AWS)	Quantitative	Discussing the effectiveness of the FAIR method in cloud risk analysis and its relationship with ArchiMate elements. However, there are still many unanswered questions, especially regarding the impact of cloud risk analysis in the healthcare field. Future research will measure and model security risks using the FAIR and ArchiMate methods and analyze the ability of cloud services such as AWS to address security risks in the healthcare sector.
Suzanna Schmeelk / 2021 / United States	Risk in Healthcare Information Technology: Creating a Standardized Risk Assessment Framework	Qualitative, Descriptive.	Proposing a new open-source standard risk management framework library to improve coordination and communication of management components. Adopting such a standard risk center framework would benefit the healthcare industry. Furthermore, using the FAIR method, the paper discusses the importance of risk assessment in developing budgets for side effects and ensuring that financial resources are kept in line with uncertain probabilities to pay for patient identity protection. In summary, this scientific publication highlights the urgent need for healthcare service organizations to address information technology risks and implement standard risk management frameworks.
Dominique Lepore/2023/ Italia	Interdisciplinary Research Unlocking Innovative Solutions in Healthcare	Qualitative, Descriptive.	The platform proposed an innovative solution that aimed to process and analyze personal healthcare data while safeguarding user privacy. Its main strength lies in the use of an interdisciplinary approach via the triple-helix model, which incorporated different academic fields, institutions, companies, and researchers. Additionally, the output of the threat risk assessment in the

Main Researcher/ Year/ Location	Title	Research methods	Results
			TRM framework's second stage was utilized to facilitate advanced risk assessment based on the FAIR ontology. From this perspective, the paper accentuated the possible advantages of integrating IoT and ML models while also emphasizing the key challenges that remained to be tackled.
Sondes Ksibi /2022/Tunisia	A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach	Quantitative	The study examines e-health systems and security challenges, specifically those related to IoMT applications, which are affected by data sensitivity, rapidly changing contexts, and outdated ICT infrastructure. The FAIR method, a quantitative approach to risk assessment that establishes standard references and promotes commercial software, is discussed as one of the Trust-risk awareness methods in this paper. Examples of software promoted by FAIR, such as RiskLens and CyVaR, are based on a quantitative assessment approach but may have reliability and consistency issues as black box tools. A highly detailed risk management approach comprising three distributed agents and an orchestrator module is proposed by the authors, aimed at assessing risks related to devising zones, network areas, and storage infrastructure. Further exploration of IoMT risks and the development of an AI-based intelligent management approach is planned by the authors.
Duncan Sparrell /2019/ United States of America	Cyber-Safety in Healthcare IoT	Qualitative	In the future, IoHT systems will be able to adjust themselves to cybersecurity threats in real time, thanks to the current development of cybersecurity standards. The adaptation will be based on a quantitative analysis of practical mitigation measures that will optimize overall health outcomes economically. To achieve this, quantitative risk analysis will be done using standards such as FAIRTM and DoCRA. Automation will be driven by standards such as SBoM, STIXTM, TAXIITM, OpenC2, and CACAO.
Petar Radanliev	Cyber-Risks from	Qualitative,	The paper concludes that medical IoT

Main Researcher/ Year/ Location	Title	Research methods	Results
/2021/ England	Using IoT Devices for Managing Covid-19	Descriptive	solutions are not appropriately evaluated for cybersecurity risks, particularly in their usage for Covid-19 management. The use of third-party solutions can lead to significant losses for healthcare providers. Thus, it is essential to employ quantitative cybersecurity risk models like FAIR, which require a similar quantitative approach to estimate the risk of IoT systems used in Covid-19 management. However, this approach must be adjusted to account for the fast spread rate and other pandemic conditions related to Covid-19. To achieve this, the authors recommend an approach that uses AI in risk analytics for medical IoT solutions, which will result in stronger system resilience and the protection of patients' medical data, secure predictive analytics outputs, and integration of these solutions into fog computing security.

CONCLUSIONS

a. Discussion

The development of business in the health sector currently requires innovation that must be continuously updated to maintain the continuity of business activities in the health sector. Changes in various aspects such as government policies, the discovery of new technologies, and globalization have driven the sector of health to continue updating the system information on health facilities and mitigating possible risks that might appear in information systems. (Kemala Hayati & MT, n.d.; Sisca et al., 2021)

Broadly speaking, Information Security Risk Assessment is a technique used to calculate the level of risk that may occur. In this case, the risk is the possibility of an event occurring and the consequences that may arise that can affect the organization. (Hardani & Ramli, 2022; Kemala Hayati & MT, n.d.; Rohmani & Wibisono, 2016)

Some of the articles found in this scoping review demonstrate the importance of Information Security Risk Assessment in the health sector. In the first-level facility information system in this study, operated in community health centers, the results of the risk analysis showed that the average potential threat risk and high-risk threats were still relatively low in terms of the possibility of threats because the services were still running normally. (Jonny et al., 2021)

Furthermore, the security risk assessment on the Health Ecosystem Cloud demonstrates the effectiveness of the FAIR method in cloud risk analysis and its

relationship to ArchiMate elements. However, there are still many unanswered questions, especially regarding the impact of cloud risk analysis on health, it is still very difficult to determine risk from the enterprise architecture of a cloud system. The probability of technology risk occurrence is very uncertain by the diversity and complexity of facilities and structures. (Mariam Traore, 2022)

Security Risk Assessment on Healthcare Information Technology in the United States shows that Patients should be aware of the risk of identity theft if their personal information is compromised and sold on online marketplaces. The use of technology in healthcare is becoming more commonplace and society needs to establish standard procedures for managing and responding to privacy and cybersecurity risks. By adopting a framework for dealing with actual privacy and security breaches, the healthcare industry can be more effective to communicate and reduce risk, which is especially important in situations where human lives are at stake. (Suzanna, 2021)

Information Security Risk Assessment on the Health Platform proposes innovative solutions on how personal healthcare data can be processed and analyzed, protecting user privacy. The main strength of this platform is the interdisciplinary approach used in the triple-helix model, which involves various institutions, companies, and researchers from various academic fields. From this perspective, this paper shows the potential offered by the integration of IoT and ML models and the main challenges that still need to be overcome. (Lepore, 2023)

Later studies in Tunisia examined e-health systems and their security challenges, especially for IoMT applications due to data sensitivity, rapidly changing contexts, and aging ICT infrastructure. The authors propose a highly detailed risk management approach consisting of three distributed agents and an orchestrator module, which aims to assess risks associated with device zones, network areas, and storage infrastructure. They plan to further explore IoMT risks and develop an intelligent management approach based on artificial intelligence techniques. (Ksibi, 2022)

Cybersecurity in Health IoT The standards developed today will enable future IoHT systems to adapt to cybersecurity threats automatically and in real-time, based on quantitative analysis of reasonable mitigations triage to economically optimize overall health outcomes. Risk analysis uses standards such as FAIRTM and DoCRA. Automation will be driven by standards such as SBoM, STIXTM, TAXIITM, OpenC2, and CACAO. (Sparrell, 2019)

Cyber Risk of Using IoT Devices to Manage COVID-19 currently shows that medical IoT solutions are not being adequately evaluated for cyber risk, especially with the increased use of such solutions in Covid-19 management. Third-party medical IoT solutions used in Covid-19 monitoring may provide inadequate protection for large healthcare providers, which may result in maximum loss scenarios. To address this issue, an approach is proposed using AI in the risk analytics of medical IoT solutions, which can create stronger system resiliency through cognition in its physical and digital

dimensions. The goal is to protect the integrity of patient medical data while securing predictive analytics output and integrating the solution into fog computing security. (Radanliev, 2021)

Several articles relevant to the research purpose indicate that Information Security Risk Assessment can assist healthcare services in providing recommendations to reduce information system risks in the healthcare sector. In the realm of healthcare services, FAIR is highly feasible to be considered for implementation in the process of assessing information system risks of a healthcare institution. In healthcare services, all business stakeholders are involved in designing how the organization will operate with a secure Health Information system when accessing healthcare services. This will not only produce good results for patients but also improve the efficiency and effectiveness of the system. (Arina, 2020; Hadikaryana & Sasongko, 2019; Hardani & Ramli, 2022; Kemala Hayati & MT, n.d.; Rohmani & Wibisono, 2016)

The utilization of Information Security Risk Assessment in the broader healthcare sector can clarify customer needs, offer better value-added, and create and capture more value for healthcare service providers and the patients they serve.(Mauluddani et al., 2021; Rangkuti, 2017)

The weakness of this scoping review is the limited literature available on the assessment of information security risks using the FAIR method in the healthcare sector.

b. Conclusions and Implications

The healthcare sector can overcome security threats and stay ahead of the competition with the advancement of information systems. Developing a secure healthcare information system is a challenging task, but implementing the FAIR model in security risk assessments can help ensure success in each service sector. While finding articles that focus on information security risk assessments using the FAIR model in healthcare services may be challenging, there are opportunities to focus on the development plan of information systems in healthcare services and conduct further studies on information security risk assessment models to ensure that the FAIR model prevails.

REFERENCES

Arina, emilia dkk. (2020). Strategi dan tantangan dalam meningkatkan cakupan vaksinasi covid-19 untuk herd immunity. *Jurnal Medika Hutama*, *02*(01), 402–406. http://www.jurnalmedikahutama.com/index.php/JMH/article/view/264/179

Boddy, A., Hurst, W., Mackay, M., & Rhalibi, A. El. (2017). A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 1–7.

Chotimah, S. N. (2022). Implementasi Sistem Informasi Kesehatan di Fasilitas Pelayanan Kesehatan Indonesia: Literature Review. *Jurnal Rekam Medis & Manajemen Infomasi Kesehatan*, *2*(1), 8–13.

Hadikaryana, O., & Sasongko, A. (2019). Penilaian Resiko Keamanan Informasi Pada Infrastruktur Kritis Sistem Scada Area Pengatur Beban Xxx Berdasarkan Panduan Nist Sp 800-82. *Syntax Lit. J. Ilm. Indones*, *4*(4), 131–145.

Hardani, M. S., & Ramli, K. (2022). Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30. *JURIKOM (Jurnal Riset Komputer)*, *9*(3), 591–599.

Hasanah, U. (2019). *Pengaruh Audit Operasional, Pengendalian Internal Dan Sistem Informasi Manajemen Terhadap Kualitas Pelayanan Jasa Transportasi Pada PT. Hiba Group*. Sekolah Tinggi Ilmu Ekonomi Indonesia (STEI) Jakarta.

Indrajit, R. E. (2000). Manajemen sistem informasi dan teknologi informasi. *Jakarta: PT Elex Media Komputindo*.

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: investigation in hospitals. *Journal of Medical Internet Research*, *22*(1), e16775.

Jayadi, P., Sarwono, P., & Nanda, M. D. (2022). Pengukuran Kinerja Teknologi Informasi di Indonesia dalam General Control: Literature Review. *JIMP (Jurnal Informatika Merdeka Pasuruan)*, *7*(1).

Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005. *Sistemasi: Jurnal Sistem Informasi*, *10*(1), 13–25.

Josey, A. (2014). *The Open FAIR™ Body of Knowledge: A Pocket Guide (Security Series)* (First edit). Van Haren Publishing, Zaltbommel, www.vanharen.net.

Kemala Hayati, S. T., & MT, I. P. M. (n.d.). *Sistem Manajemen Klaim Berbasis Sistem Informasi*.

Ksibi, S. (2022). *Sebuah Pendekatan Kuantitatif Komprehensif untuk Manajemen Risiko Keamanan dalam Sistem e-Health.*

Lepore, D. (2023). *Penelitian Interdisipliner membuka Solusi Inovatif dalam Perawatan Kesehatan*.

Mariam Traore, P. S. Y. (2022). *Analisis dan Pemodelan Risiko Cloud Ekosistem Kesehatan: Pendekatan FAIR (Studi kasus dari Arterys ™ pada AWS)*.

Mauluddani, D. N., Abdurrahman, L., & Santosa, I. (2021). Analisis Risiko Dan Perancangan Kontrol Keamanan Informasi Pada Sistem Informasi Manajemen Rumah Sakit Modul Aset Menggunakan Metode Octave Allegro (studi Kasus: Rumah Sakit Khusus Ibu Dan Anak Bandung). *EProceedings of Engineering*, *8*(2).

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2021). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review

of recent trends, threats and mitigation. *Health Security Intelligence*, 92–121.

Peters, M. D. J., Godfrey, C. M., McInerney, P., Soares, C. B., Khalil, H., & Parker, D. (2015). *The Joanna Briggs Institute reviewers' manual 2015: methodology for JBI scoping reviews*.

Radanliev, P. (2021). *Risiko Siber dari Penggunaan Perangkat IoT untuk Mengelola COVID-19*.

Rangkuti, F. (2017). *Customer care excellence: meningkatkan kinerja perusahaan melalui pelayanan prima plus analisis kasus jasa raharja*. Gramedia Pustaka Utama.

Rohmani, A., & Wibisono, M. G. (2016). Strategi Mitigasi Resiko Keamanan Informasi Berdasarkan Analisa Return On Investment Pada Badan Pusat Statistik Daerah Kota Semarang. *Techno. Com*, *15*(2), 140–150.

Sisca, S., Simarmata, H. M. P., Grace, E., Purba, B., Dewi, I. K., Silalahi, M., Fajrillah, F., Sudarso, A., & Sudarmanto, E. (2021). *Manajemen Inovasi*. Yayasan Kita Menulis.

Sparrell, D. (2019). *Keamanan Siber dalam IoT Kesehatan*.

Sudjiman, P. E., & Sudjiman, L. S. (2018). Analisis sistem informasi manajemen berbasis komputer dalam proses pengambilan keputusan. *TeIKa*, *8*(2), 55–66.

Suzanna. (2021). *Risiko dalam Teknologi Informasi Layanan Kesehatan: Membuat Kerangka Penilaian Risiko Standar*.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., & Weeks, L. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Annals of Internal Medicine*, *169*(7), 467–473.