The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 6, December 2024
https://doi.org/10.33022/ijcs.v13i6.4527

Enhancing Post-Incident Activities Through Knowledge Management Models: A Systematic Literature Review

Ghina Fitriya[1], Boy Sandi Kritian Sihombing[2] , Fatoumatta Binta Jallow[3], Sofian Lusa[4] , Nadya Safitri[5], Dana Indra Sensuse[6]
ghina.fitriya@ui.ac.id[1], boy.sandi@ui.ac.id[2], fatoumatta.binta@ui.ac.id[3], sofian.lusa12@ui.ac.id[4], nadya.safitri@ui.ac.id[5], dana@cs.ui.ac.id[6]
[1,2,3,4,5,6] Master of Information Technology, Faculty of Computer Science, Universitas Indonesia

Article Information

Received : 22 Nov 2024
Revised : 9 Dec 2024
Accepted : 30 Dec 2024

Keywords

KM model, SLR, incident response, NAT-CSIRT

Abstract

The current condition of Nat CSIRT requires a knowledge management system model to support incident handling, especially in the post-incident stage to accelerate incident handling, especially in repeated incidents. To address these issues, a systematic literature review (SLR) will be conducted to propose a knowledge management model (KMM) for supporting post-incident activities. This research used SLR-PRISMA methodology that consists of 3 steps which are Identification, Screening, and Included. The 22 articles acquired from the SLR-PRISMA process from five databases. Those 22 articles used 12 KMMs and 10 indicators that are used more than once. The 10 indicators were mapped with post incident activities and their best practices based on their correlation event. Eventually 9 best practices and 5 indicators obtained to develop a proposed KMM for NAT-CSIRT to support the post incident activities. The 5 indicators which are knowledge sharing, technology, culture, information, and organizational performance can be used to propose a KM Model for the post incident activities in NAT-CSIRT.

A. Introduction

In contemporary information technology (IT) projects, the handling of cybersecurity incidents is becoming increasingly crucial. According to Villegas-Ch et al. (2021) [1],the frequency, diversity, impact, and disruption of cybersecurity-related attacks have been on the rise. While preventive measures informed by risk assessments can help decrease the occurrence of incidents, not all incidents can be averted. Hence, it is essential for the Computer Security Incident Response Team (CSIRT) to be equipped to promptly detect incidents, minimize losses and damages, address vulnerabilities that have been exploited, and restore IT services [2].

As outlined in BSSN Regulation number 10 of 2020, the CSIRT is a designated body tasked with addressing Cyber Incidents within the specified boundaries. According to Presidential Regulation number 82 of 2022, the CSIRT can be set up at various tiers, including Nat CSIRT at the national level, sectoral CSIRT, organizational CSIRT, and special CSIRT. However, CSIRT implementation can face challenges, including bureaucratic decision-making structures [3], limited resources, and weak authority [4].

To address these obstacles, one effective strategy is to implement scenario-based training, which has been shown to be effective in mitigating socio-technical challenges in incident response [5]. Moreover, fostering greater collaboration between Ministries/Agencies and the Private Sector to tackle cyber threats can be facilitated by establishing a Computer Security Incident Response Team (CSIRT) [6].

The challenges of National Computer Security Incident Response Team (Nat - CSIRT) lie in conducting incident response based on the NIST 800-63 standard. The procedure of this standard undergoes four phases, which are [2]:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident

In the preparation phase, organizations implement protections such as firewalls, intrusion prevention systems, and intrusion detection systems to protect against hacking attempts. The detection and analysis phase involve identifying and assessing potential incidents, using techniques such as statistical process control charts and case-based reasoning to detect anomalies and similarities to known hacking patterns. The containment phase focuses on limiting the impact of the incident and preventing further damage. The phase of eradication and recovery consists of the elimination of threats and the restoration of systems to their normal functioning. Subsequently, the post-incident activity phase entails the examination of the incident, documentation of lessons learned, and the implementation of measures to avert future occurrences [7].

The Regulation number 1 of 2024 by the Head of BSSN regarding cyber incident management enhances the role of Nat CSIRT as outlined in Presidential Regulation 82 of 2022 for executing incident handling at the national level. Nat CSIRT undertakes incident handling by responding to requests for assistance from the CSIRT under its jurisdiction. Based on data from the BSSN Cybersecurity Landscape Report in 2023, there were 29 incidents handled by Nat CSIRT out of a total of 83 requests for assistance received or 35% of the total number with an average completion time of the entire series of incident handling until post-incident

for 20 working days [8]. Based on the results of interviews conducted with the chairman of Nat CSIRT, things that can be improved to shorten incident handling time are information sharing programs. Currently, it is known that the implementation of Nat CSIRT's role in sharing knowledge with the CSIRT below has not been implemented because it does not have a knowledge management system that is in accordance with incident handling procedures. Looking at the current condition of Nat CSIRT, which has not met the target in incident resolution time, namely, there is a delay in handling incidents from the expected time.

This can be concluded that the current condition of Nat CSIRT requires a knowledge management system model to support incident handling, especially in the post-incident stage to accelerate incident handling, especially in repeated incidents.

To tackle these concerns, a systematic literature review (SLR) will be undertaken to propose a knowledge management framework aimed at enhancing post-incident activities. The utilization of a systematic literature review (SLR) serves to present a comprehensive overview of the current state of knowledge in a particular field, allowing for the thorough examination and interpretation of past research endeavors [9]. The present iteration of the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) 2020 method includes guidelines for reporting, such as a flowchart, a 12-point checklist for abstracts, and a 27-point checklist for reporting SLRs. PRISMA enables the assessment of the quality of each literature piece and the scrutiny of the supporting data's significance. Moreover, PRISMA 2020 offers a structured approach for conducting the initial SLR, encompassing the stages of Identification, Screening, and Inclusion [10]. Hence, this study has two research questions:

RQ1: What is the KM Model used in an organization?

RQ2: What are the indicators that can be used to propose a KM Model for the post incident activities in NAT-CSIRT?

This study is organized in 6 sections. Section 1 introduces the state of the art of this study, section 2 explains the related theory about knowledge management, section 3 covers the methodology used in this paper, section 4 discusses about the result, section 5 discusses about the conclusion of this study and in the section 6 will discover the future works regarding this study.

B. Research Method

A Systematic literature review (SLR) was utilized to offer a comprehensive overview of the most advanced knowledge in a particular field, aiming to present, analyze, and elucidate past research in a thorough and transparent manner [11][9]. The updated Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) method of 2020 features specific guidelines for reporting, such as a visual flowchart and a 27-item checklist for SLR documentation [10]. PRISMA allows for quality evaluation of each piece of literature and evaluates the weight of the supporting data. Furthermore, PRISMA 2020 provides a three-steps process for carrying out the original SLR: Identification, Screening, and Included [12].

After the objective of this study was done by creating two research questions, the tactics for seeking the literature were created to respond to the RQ1, “What is

the KM Model that used in an organization?". The three-steps process for conducting the original SLR in this study shown by Figure 1.

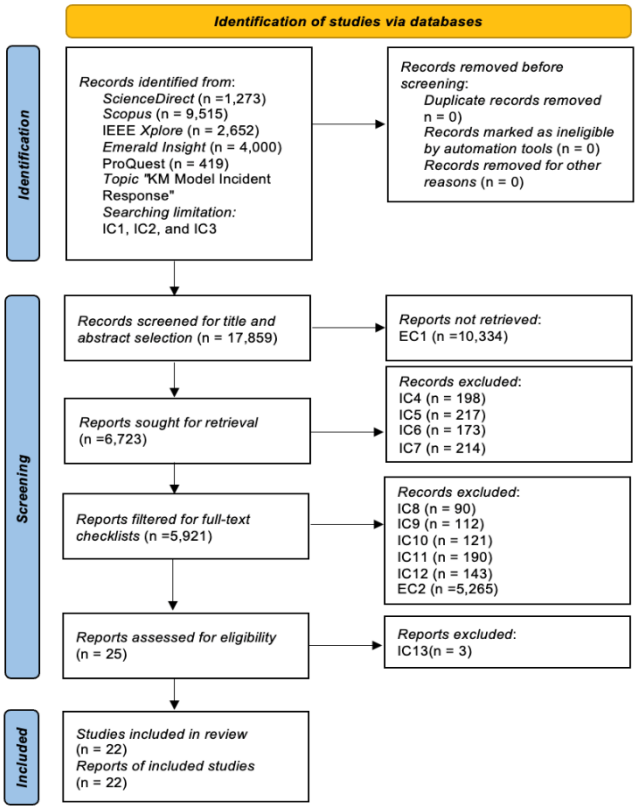

Figure1. SLR Flow Diagram

At the identification stage, a search was conducted using keywords and criteria. Keywords defined "Knowledge Management", "KM Model", "Incident Handling", and "Incident Response". Keywords as a part of the tactics to answer the RQ1 form the literatures. Criteria are defined as "Knowledge Management" AND ("Model" OR "Framework") AND ("Parameter" AND "Standard") AND (("Best Practices" AND "NIST") AND ("Incident Handling" OR "Incident Response")). In addition, there are two searching strategies that used in the stage of identification which are last five years, and the language used is English.

The stage of identification obtained 17,859 articles from five databases: Emerald Insight, IEEE Xplore, ProQuest, ScienceDirect, and Scopus. The results were then checked by following the search strategies attributes shown in Table I which lists the optimum searching techniques to be brought into the stage of screening.

Table 1. Searching Strategies

Stages	Inclusion Criteria	Exclusion Criteria
Initiation	Boolean search (IC1) 2019 – 2023 (IC2) Language: English (IC3)	-
Stage 1 (Title and abstract selection)	- Incident response standards (IC4) - Incident response best practices (IC5) - Knowledge management model (IC6) KM model for incident response (IC7)	Paper SLR /Literature Review /Conference Notes/Speaker Notes (EC1).

Stages	Inclusion Criteria	Exclusion Criteria
Stage 2 (Full-Text Selection)	- Best practices of the post incident activities (IC8) - Best practices for incident response or incident handling standards (IC9) - Post incident activities best practices mapped into KM model/ KM framework (IC10) - Paper should explain best practices for incident response or incident handling standards (IC11) - Paper should use qualitative or mixed method (IC12)	Paper not available at source (EC2)
Stage 3 (Quality Selection)	- Checklist Quality (10 Checklist Statements) using Pareto technic (IC13)	-

The process of the PRISMA consists of 4 stages which are initiation, stage 1, stage 2, and stage 3 used to obtain related articles. Two criteria in the way of optimizing searching techniques are inclusion (IC) and exclusion (EC). There are totally 13 ICs and 2 ECs. In identification stage IC1 to IC3 are used for initiation meanwhile IC4 to IC3 are used in the stage 1, stage 2, and stage 3 under the screening stage. All the 2 ECs are used in the stage 1 and stage 2 under the screening stage.

The number of the articles that acquired in each stage is shown in the Table II. Those 4 stages narrowing the number from the first result of screening which is 17,859 articles eventually become 22 articles.

Table 2. Literature Selection Results

Source	Initiation Stage (Based on search results)	Stage 1 (Title and abstract selection)	Stage 2 (Full text selection)	Stage 3 (Literature Quality Testing Results)
Scopus	9,515	1,048	3	2
Science Direct	- 1,273	1,273	1	1
IEEE Xplore	- 2,652	152	8	8
ProQuest	419	250	10	8
Emerald Insight	4,000	4,000	3	3
Total	**17,859**	**6,273**	**25**	**22**

The result of the literature review included 22 articles for analysis as shown in Table II. In the final step of the research, the literature review results were used to identify indicators that can be applied in composing KMM for Nat-CSIRT Indonesia.

C. Result and Discussion

We conduct Systematic Literature Review from twenty-two papers with topic related to KMM. There are some indicators mentioned in the previous study as shown in table below.

Table 3. Indicators of KM Model from Previous Study

Articles	KMM	Indicators
1_Knowldege Management Practices and Innovation Performance [13]	Inkinen KMM	- Leadership - Strategic Knowledge Management - Knowledge-Based Recruiting Practices

Articles	KMM	Indicators
		- Knowledge-Based Training and Development Practices - Knowledge-Based Performance Appraisal Practices - Knowledge-Based Compensation Practices, - Learning Mechanism - Information Technology Practices - Work Organization Innovation Performance
2_Socio-Technical Systems Cybersecurity Framework [14]	Socio-technical system cybersecurity framework (Revised)	- Join optimization process • Organizational structure • Actors • Technology • Work activities - Joint optimization security controls - maturity indicator levels Continuous capability improvement outcomes
3_Extraction Of Knowledge From Open Government Data [15]	Knowledge iterative value network (KIVN)	- Data - Information Knowledge
4_Individual Knowledge Measurement: Organizational Knowledge Mesured At The Individual Level [16]	Revised Nonaka & Takeuchi	- Tacit Knowledge • Locus • Transfer • Expression • Acquisition process • Source of value • Observability - Codified Knowledge • Locus • Transfer • Expression • Acquisition process • Source of value • Observability - Encapsulated Knowledge • Locus • Transfer • Expression • Acquisition process • Source of value Observability
5_Learning From Near-Miss Events [17]	Propose New Model	- Procedural response - Flexible response - Firm age - Product maturity - Firm size - Environmental dynamism - Frequency of small disruptions - Frequency of near misses - Regulatory pressure

Articles	KMM	Indicators
		Industry pressure
6_An Integrated Approach For Modeling Ontology-Based Task Knowledge On An Incident Command System [18]	TTIPP	- Task analysis - Task ontology - IDFE0 model - Petri net model
7_A Model For Examining The Effect Of Knowledge Sharing And New It-Based Technologies On The Success Of The Supply Chain Management Systems [19]	Propose New Model	- Knowledge sharing • Organizational context • Motivation • Individual character - VANET (vehicular ad hoc network) • Cost • Security • Weather conditions - RFID & NFC Technology • Cost • Motivation & intention • Security - Social Capability of IT using • Social responsibility • Social networks • Organization statue in social media
8_A Conceptual Framework For Measuring Organisational Performance Through Knowledge Managements' Seci Model: *A Mediating Role Of Innovation [20]*	Revised Nonaka & Takeuchi	- Socialization - Externalization - Combination - Internalization - Innovation - Product innovation - Process innovation Organizational Performance
9_Capturing Tacit Knowledge In Security Operation Centers [21]	Revised Nonaka & Takeuchi	- Socialization • Apprenticeship • On-site business trip • Interaction with external contractors - Externalization • Simulation laboratory • Job shadowing reports • Contractor update noticeboard - Combination • Integration into knowledge base - Internalization Direct client action
10_Knowledge Management Capabilities [22]	Hock-Doepgen KMM	- Internal KM capabilities - KM culture - KM structure - KM technology - External KM capabilities - KM acquisition process - KM conversion Process KM application process

Articles	KMM	Indicators
11_Evaluation Model Of Knowledge Management System [23]	Nonaka & Takeuchi KMM	- Socialization - Externalization - Combination Internalization
12_The Performace Evaluation Of Knowledge Management Systems Implementation In The Organization [24]	KMS	- Knowledge sharing Organizational Performance
13_Advancing public sector knowledge management: towards an understanding of knowledge formation in public administration [25]	KMS	- Knowledge sharing - Organizational Performance
14_Knowledge Management In Health Care: An Integrative And Result-Driven Clinical Staff Management Model [26]	Propose KM Model	-Knowledge sharing - Institutional powers -organisational strategies -individuals' sensemaking
15_Research On The Peer Behavior Of Local Government Green Governance Based On Seci Expansion Model [27]	Nonaka & Takeuchi KMM	- Socialization - Externalization - Combination Internalization
16_Project Management In The Development Of Dynamic Capabilities For An Open Innovation Era [28]	KMS	- Knowledge accumulation - Integration - Utilization - Reconfiguration - Sensing Seizing
17_Development Model Of Evaluation Of Knowledge Management Systems Implementation In Government Organization [29]	KMS	- People: employee roles, communication - Process: training, rewards for sharing knowledge, employee's ability to access KMS Technology: Quality features and content of KMS, complexity barriers
18_Unpacking Knowledge Management Practices In China: Do Institution, National And Organizational Culture Matter? [30]	KM process	- Institutional isomorphism - Organizational culture - National culture
19_Knowledge Management Practices: A Public Sector Perspective [31]	Proposed KM Process	- Managers lead the process - Inclusive training - Introduce technology - Include senior and retiring employees as mentors Family oriented culture
20_How To Implement Knowledge Management In Emerging Governments In Africa And Beyond: A Case Study On The South African Government [32]	KMIF	- Culture - People - Content Process

Articles	KMM	Indicators
21_The Development Of Innovation Knowledge Management System In Tangerang Regency [33]	Model Design Regional Innovation Knowledge Management System	- User innovation initiator - Infrastructure - IS Data Innovation - Transaction - Integration Interaction
22_Model Of Knowledge Management Readiness And Initiatives For Improvement In Government Agencies [34]	proposed KMCSF	- The domain of government agencies - Public sector domains - Organizational conditions - Organizational characteristics Culture and regulations

Table III explains there are 12 KMMs used in the 22 articles where Nonaka & Takeuchi has the most frequent to be used with 5 times followed by KMS with 4, Propose New KMM with 3, KM Process with 2, and the rest with 1. The indicator from 4 KMMs that appear more than 1 time then classified to obtain the number of their indicator frequency as per shown by Table IV.

Table 4. Frequently Appears Indicators

No.	Indicator (Ind)	Article (Art)	Frequency (Freq)
1	Technology (Tech)	[13],[22],[29],[31]	4
2	Knowledge Sharing (KS)	[24], [25], [26], [29]	4
3	Organizational Performance (OP)	[20], [24], [25]	3
4	Socialization (S)	[21], [23], [27]	3
5	Externalization (E)	[21], [23], [27]	3
6	Combination (C)	[21], [23], [27]	3
7	Internalization (I)	[21], [23], [27]	3
8	Information (Inf)	[13], [15]	2
9	Organizational (Org)	[14], [30]	2
10	Culture (Cult)	[30], [32]	2

These indicators will be mapped into post incident activities and their best practices based on their correlation event to build the proposed KMM to NAT-CSIRT. The result of mapping is shown in Table V.

Table 5. Mapping Of KMM Indicators Into Post Incident Activities and Their Best Practices

Post Incident Activities	Best Practices	KM Model	Ind	Art	Freq
Lessons learned	How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?	• KMS • Propose KM Model	KS	[24], [25], [26], [29]	4

Post Incident Activities	Best Practices	KM Model	Ind	Art	Freq
	What would the staff and management do differently the next time a similar incident occurs?	• KMS • Propose KM Model	KS	[24], [25], [26], [29]	4
	What precursors or indicators should be watched for in the future to detect similar incidents?	• Inkinen KMM • Hock-Doepgen KMM • KMS • Propose KM Process	Tech	[13], [22], [29], [31]	4
	What additional tools or resources are needed to detect, analyze, and mitigate future incidents?	• Inkinen KMM • Hock-Doepgen KMM • KMS • Propose KM Process	Tech	[13], [22], [29], [31]	4
Using Collected Incident Data	Subjective Assessment of Each Incident.	• KM Process • KMIF	Cult	[30], [32]	2
	Time Per Incident.	• Inkinen KMM • Knowledge iterative value network (KIVN)	Inf	[13], [15]	2
	Number of Incidents Handled.	• Inkinen KMM • Knowledge iterative value network (KIVN)	Inf	[13], [15]	2
	Objective Assessment of Each Incident.	• KM Process • KMIF	Cult	[30], [32]	2
Evidence Retention	Cost.	• Nonaka & Takeuchi • KMS	OP	[20], [24], [25]	3

From Table V, we know that 9 best practices can be supported by 5 indicators which are knowledge sharing, technology, culture, information, and organizational performance. The relation among post incident activities, best practices, and indicators that develop a proposed KMM is shown in Figure 2.

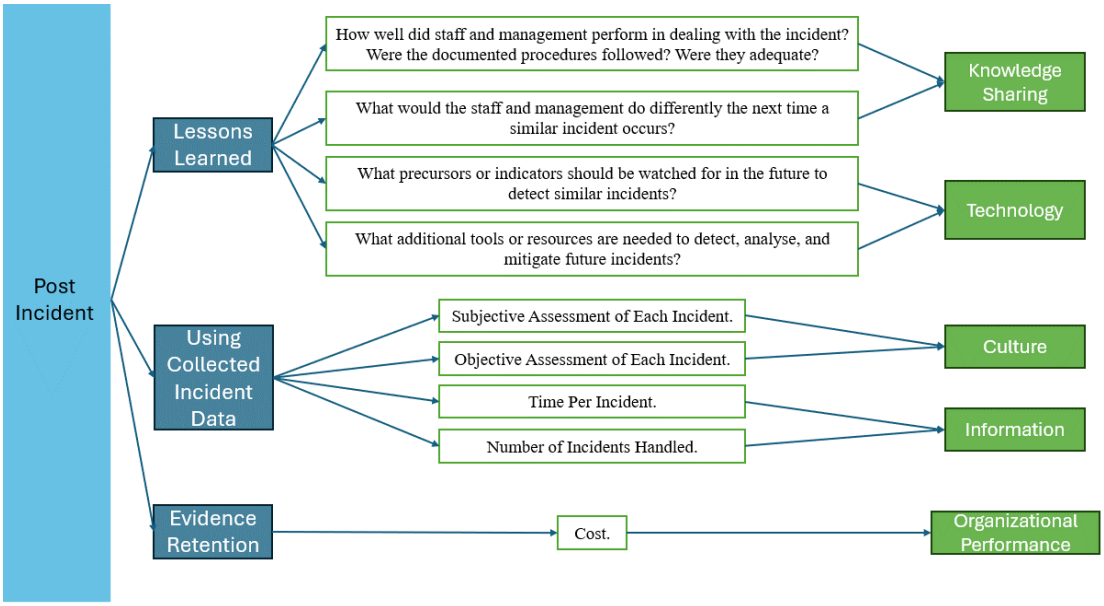

Figure2. Proposed KMM for Nat-CSIRT

This KMM points out the indicators that can be used to be implemented as a recommendation model for NAT-CSIRT in supporting the post incident activities as well as answers the RQ2.

D. Conclusion

The authors successfully procured a total of ten distinct indicators, which encompass the realms of technology, knowledge sharing, organizational performance, socialization, externalization, combination, internalization, information, organizational dynamics, and culture, all of which were meticulously derived from a comprehensive analysis of twenty-two scholarly articles. Subsequently, these ten indicators were systematically mapped in relation to post-incident activities, alongside their corresponding best practices, based on an in-depth examination of their correlations, thus establishing a robust framework for analysis. Ultimately, through this rigorous process, nine exemplary best practices and five pivotal indicators were identified, which collectively serve as the foundation for the development of a proposed Knowledge Management Model (KMM) specifically tailored for the National Computer Security Incident Response Team (NAT-CSIRT), aimed at enhancing the efficacy of post-incident activities. The five critical indicators, which include knowledge sharing, technology, culture, information, and organizational performance, have been meticulously selected and can be utilized to effectively address the research question two (RQ2), which inquires, "What are the indicators that can be employed to propose a Knowledge Management Model for the post-incident activities within the NAT-CSIRT framework?". The findings articulated within this paper contribute substantially to the understanding of the prevailing trends associated with Knowledge Management Models (KMM) and their relevant indicators in the field. However, it is important to note that this paper acknowledges certain limitations, particularly in the context of empirical testing concerning the five indicators that have been proposed within the KMM, which is essential for validating their efficacy in facilitating post-incident

activities within the NAT-CSIRT. Looking ahead, prospective avenues for future research could involve the empirical testing of the proposed KMM utilizing the identified five indicators within the operational framework of the NAT-CSIRT. Furthermore, it is worth highlighting that the proposed KMM has the potential to be adapted and implemented in various organizations on a global scale, thereby extending its applicability beyond the immediate context of NAT-CSIRT.

E. Acknowledgment

This research was supported by a grant from the Ministry of Communication and Digital Affairs of Indonesia. We appreciate their financial assistance, which made this study possible.

F. References

[1] W. Villegas-Ch, I. Ortiz-Garces, and S. Sánchez-Viteri, "computers Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus," 2021, doi: 10.3390/computers10080102.

[2] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," Gaithersburg, MD, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[3] P. Meyer and S. Métille, "Computer security incident response teams: are they legally regulated? The Swiss example Computer Security Incident Response Teams: Sind sie gesetzlich geregelt? Das Schweizer Beispiel," *International Cybersecurity Law Review*, vol. 4, pp. 39–60, 2023, doi: 10.1365/s43439-022-00070-x.

[4] J. Kostrubiec and A. Jarosław Kostrubiec, "The position of the Computer Security Incidents Response Teams in the national cybersecurity system."

[5] A. O'neil, A. Ahmad, and S. B. Maynard, "Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training."

[6] H. Rohman and W. Leksmanawati, "A new decade for social changes Collaboration of ministries/institutions and the private sector in handling cyber threats through the establishment of Computer Security Incident Response Team (CSIRT)," *www.techniumscience.com*, vol. 38, p. 2022, [Online]. Available: https://databoks.katadata.co.id,

[7] E. C. Thompson, "Incident Response Frameworks," in *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*, E. C. Thompson, Ed., Berkeley, CA: Apress, 2018, pp. 17–46. doi: 10.1007/978-1-4842-3870-7_3.

[8] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023," Feb. 2024.

[9] S. Castillo and P. Grbovic, "'The APISSER Methodology for Systematic Literature Reviews in Engineering,' ," *IEEE Access, vol. 10, pp. 23700–23707, 2022, doi: 10.1109/ACCESS.2022.3148206.* .

[10] M. J. Page et al, " 'PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews,' ," *BMJ, vol. 372, 2021, doi: 10.1136/bmj.n160.*.

[11] M. L. Rethlefsen et al, "'PRISMA-S: an extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews,' ," *Syst. Rev., vol. 10, no. 1, p. 39, Dec. 2021, doi: 10.1186/s13643-020-01542-z.*.

[12] M. J. Page et al., "'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews,' ," *BMJ, vol. 372, 2021, doi: 10.1136/bmj.n71.*.

[13] A. I. Susanty, Y. Yuningsih, and G. Anggadwita, "Knowledge management practices and innovation performance: A study at Indonesian Government apparatus research and training center," *Journal of Science and Technology Policy Management*, vol. 10, no. 2, pp. 301–318, Jun. 2019, doi: 10.1108/JSTPM-03-2018-0030.

[14] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Information and Computer Security*, vol. 27, no. 2, pp. 233–272, May 2019, doi: 10.1108/ICS-03-2018-0031.

[15] M. Mohamed, S. Pillutla, and S. Tomasi, "Extraction of knowledge from open government data: The knowledge iterative value network framework," *VINE Journal of Information and Knowledge Management Systems*, vol. 50, no. 3, pp. 495–511, Jun. 2020, doi: 10.1108/VJIKMS-05-2019-0065.

[16] H. A. van den Berg and V. Kaur, "Individual knowledge measurement: organizational knowledge measured at the individual level," *Journal of Knowledge Management*, vol. 26, no. 6, pp. 1409–1437, Jun. 2022, doi: 10.1108/JKM-10-2020-0774.

[17] A. Azadegan, R. Srinivasan, C. Blome, and K. Tajeddini, "Learning from near-miss events: An organizational learning perspective on supply chain disruption response," *Int J Prod Econ*, vol. 216, pp. 215–226, Oct. 2019, doi: 10.1016/j.ijpe.2019.04.021.

[18] K. Fang and S. Lin, "An integrated approach for modeling ontology-based task knowledge on an incident command system," *Sustainability (Switzerland)*, vol. 11, no. 12, 2019, doi: 10.3390/su11123484.

[19] H. Zeraati, H. Molavi, and N. J. Navimipour, "A model for examining the effect of knowledge sharing and new IT-based technologies on the success of the supply chain management systems," *Kybernetes*, pp. 229–251, Jan. 2020, doi: 10.1108/K-06-2018-0280.

[20] K. S. Chib and G. Sehgal, "A Conceptual Framework For Measuring Organisational Performance Through Knowledge Managements' Seci Model: A Mediating Role Of Innovation." [Online]. Available: http://publishingindia.com/ijkmp/

[21] S. Y. Cho, J. Happa, and S. Creese, "Capturing Tacit Knowledge in Security Operation Centers," *IEEE Access*, vol. 8, pp. 42021–42041, 2020, doi: 10.1109/ACCESS.2020.2976076.

[22] M. Hock-Doepgen, T. Clauss, S. Kraus, and C. F. Cheng, "Knowledge management capabilities and organizational risk-taking for business model innovation in SMEs," *J Bus Res*, vol. 130, pp. 683–697, Jun. 2021, doi: 10.1016/j.jbusres.2019.12.001.

[23] W. Sardjono, E. Selviyanti, and W. G. Perdana, "Evaluation model of knowledge management systems implementation using factor analysis and regresion analysis at the corporation," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jun. 2020. doi: 10.1088/1742-6596/1538/1/012027.

[24] E. R. Kaburuan and W. Sardjono, "The performace evaluation of knowledge management systems implementation in the organization," in *2020 8th International Conference on Orange Technology, ICOT 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/ICOT51877.2020.9468735.

[25] H. Laihonen, A. A. Kork, and L. M. Sinervo, "Advancing public sector knowledge management: towards an understanding of knowledge formation in public administration," *Knowledge Management Research and Practice*, 2023, doi: 10.1080/14778238.2023.2187719.

[26] V. Pereira de Souza, R. Baroni, C. W. Choo, J. M. de Castro, and R. R. Barbosa, "Knowledge management in health care: an integrative and result-driven clinical staff management model," *Journal of Knowledge Management*, vol. 25, no. 5, pp. 1241–1262, 2020, doi: 10.1108/JKM-05-2020-0392.

[27] H. Liu, P. Yao, X. Wang, J. Huang, and L. Yu, "Research on the peer behavior of local government green governance based on seci expansion model," *Land (Basel)*, vol. 10, no. 5, May 2021, doi: 10.3390/land10050472.

[28] V. Patrício, R. Lopes da Costa, L. Pereira, and N. António, "Project management in the development of dynamic capabilities for an open innovation era," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 3, Sep. 2021, doi: 10.3390/joitmc7030164.

[29] W. Sardjono, A. Retnowardhani, W. Budianto, and A. Rahmasari, "Development model of evaluation of knowledge management systems implementation in government organization," in *Proceedings of 2021 International Conference on Information Management and Technology, ICIMTech 2021*, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 369–374. doi: 10.1109/ICIMTech53080.2021.9534910.

[30] Y. Liu, C. Chan, C. Zhao, and C. Liu, "Unpacking knowledge management practices in China: do institution, national and organizational culture matter?," *Journal of Knowledge Management*, vol. 23, no. 4, pp. 619–643, May 2019, doi: 10.1108/JKM-07-2017-0260.

[31] D. Pepple, C. Makama, and J. P. Okeke, "Knowledge management practices: A public sector perspective," *J Bus Res*, vol. 153, pp. 509–516, Dec. 2022, doi: 10.1016/j.jbusres.2022.08.041.

[32] L. Barbier and R. K. Tengeh, "How to Implement Knowledge Management in Emerging Governments in Africa and Beyond: A Case Study on the South African Government," *Management Dynamics in the Knowledge Economy*, vol. 11, no. 2, pp. 170–189, Jun. 2023, doi: 10.2478/mdke-2023-0012.

[33] W. A. Yohanitas *et al.*, "The Development of Innovation Knowledge Management System in Tangerang Regency," *Lex Localis*, vol. 21, no. 3, pp. 637–664, Jul. 2023, doi: 10.4335/21.3.637-664(2023).

[34] D. I. Sensuse, D. S. Hidayat, and I. Z. Setyaningrum, "Model of knowledge management readiness and initiatives for improvement in government agencies," *VINE Journal of Information and Knowledge Management Systems*, 2023, doi: 10.1108/VJIKMS-05-2022-0173.