The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4609

Reformulation of the Vulnerability Management Cycle for Enhancing Indonesia's Critical Information Infrastructure Protection: An International Comparative Study

Muhammad Azza Ulin Nuha[1], Muhammad Salman[2], Nur Annisa Kadarwati Febriyani[3], Eka Hero Ramadhani[4]
muhammad.azza21@ui.ac.id[1], muhammad.salman@ui.ac.id[2], nur.annisa22@ui.ac.id[3] , eka.hero@poltekssn.ac.id[4]
[1,2,3] University of Indonesia, Depok, Indonesia
[4] National Cyber and Crypto Polytechnic, Bogor, Indonesia

Article Information

Received : 4 Jan 2025
Revised : 12 Jan 2025
Accepted : 1 Feb 2025

Keywords

CII, NSOC, Vulnerability Management, Gartner's Cycle

Abstract

This research conducts an analysis of vulnerability management practices in three countries— the United States, Australia, and the United Kingdom— to serve as a benchmark for the National Security Operation Center (NSOC) for protecting Critical Information Infrastructure (CII) in Indonesia. The methodology employed is a document study of standards, regulations, and publications related to vulnerability management in these three countries. The analysis results are classified into Gartner's Cycle, producing 38 vulnerability management activities. The mapping of these activities to the CII Protection Framework in Indonesia demonstrates alignment with 35 sub-categories of the framework, resulting in a vulnerability management cycle that can be proposed to NSOC for the protection of CII in Indonesia.

A. Introduction

In the present era, technology is advancing rapidly, bringing various implications, such as the dissolution of borders between nations, interconnection with diverse systems, and ease of access to information through digitalization [1]. The diversity of these technologies, however, can also trigger negative impacts, including an increase in cyber threats, necessitating that all stakeholders remain vigilant and equipped with robust cybersecurity practices [2]. Critical Information Infrastructure (CII) is one of the key domains that must be protected due to its essential functions, encompassing sectors such as government, energy, telecommunications, transportation, finance, healthcare, food, information technology, and defence [3], [4]. The operation of CIIs is increasingly directed towards digitalization, interconnection, and computerization, making them highly vulnerable to cyberattacks [5]. Any disruption in these infrastructures could have significant consequences for the nation and society that depend on them [6].

To support the protection of CII, Indonesia has established regulations, notably Peraturan Presiden Nomor 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. This regulation outlines measures for protection, prevention of disruptions, and enhanced preparedness in addressing cyber incidents targeting CIIs [7]. The protective measures for CIIs, as stipulated in the regulation, are further elaborated in the Peraturan Badan Siber dan Sandi Negara Nomor 8 tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital. This framework serves as a reference for implementing CII protection based on the core cybersecurity domains: identification, protection, detection, response, and recovery [8]. Adequate CII protection requires specialized organizations dedicated to providing cybersecurity support [9]. In Indonesia, the protection of CIIs is carried out by the National Security Operation Center (NSOC), which functions as the national-level Security Operation Center (SOC). CII is one of the primary areas of focus for NSOC protection, alongside internet service providers, central and regional government institutions, and other SOC providers in Indonesia [10].

In 2023, Indonesia recorded over 403 million cyberattacks targeting various CII sectors. Data breaches, defacements, malware attacks, and vulnerability findings in electronic systems within CII sectors accounted for a significant number of these incidents [11]. Cyber threats to CIIs are not limited to technical aspects but also extend to information indirectly related to critical infrastructure [12]. Additionally, security gaps in various electronic systems are often inadequately addressed, leading to cyber incidents such as online gambling defacements [13] and ransomware attacks on critical assets, such as the temporary national data center. Therefore, improved policies for addressing vulnerabilities and threats in CII are urgently needed.

Vulnerability management is a preventive action that can be implemented to mitigate the impact of security gaps in electronic systems [14]. Prompt action on identified vulnerabilities and threats can help prevent more significant incidents at an earlier stage [15]. The urgency of implementing vulnerability management in protecting CIIs lies in its role in safeguarding critical assets and sensitive information [16]. The implementation of vulnerability management can leverage

the synergy between people, processes, and technology as a foundational framework for SOC operations tailored to the functions it supports [17].

In terms of standards or guidelines, the NSOC currently lacks a specific framework for implementing vulnerability management to protect CIIs. Several countries have adopted comprehensive vulnerability management measures supported by government agencies specializing in cybersecurity, such as CISA in the United States, ACSC in Australia, NCSC in the United Kingdom, and other nations with high cybersecurity indexes. Each country has its standards and practices, which can be analyzed as references for developing a vulnerability management framework. The results of such analysis can be adapted to align with Indonesia's regulatory framework and cybersecurity practices.

This study analyze the implementation of vulnerability management in three countries: the United States, the United Kingdom, and Australia. These countries possess comprehensive guidelines and implementation measures for cybersecurity [18]. The research methodology involves a document study of standards, regulations, and publications related to vulnerability management activities in each country, as well as coding activities based on Gartner's general vulnerability management cycle. This cycle consists of the stages of Preparation, Assess, Prioritize, Act, Reassess, and Improve [19], [20]. Gartner's management cycle was chosen due to its broad yet inclusive stages, covering all activities in vulnerability management. The study's outcome is a benchmarking map of vulnerability management activities in these three countries against the CII Protection Framework as a reference for the NSOC in carrying out CII protection [8]. This mapping can serve as a proposed implementation of vulnerability management for the NSOC to enhance the security of CIIs in Indonesia.

B. Literature Review

1. Vulnerability Management

Vulnerability management is a critical component in ensuring the security of information technology assets. Several studies have implemented vulnerability management within the CII sector. Dissanayake et al. utilized the vulnerability management steps outlined in NIST SP 800-40 to address delays in vulnerability remediation within healthcare sector software. Their findings highlighted the need for improved coordination in disseminating remediation information and suggested applying vulnerability management to other sectors [21]. Sotiropoulos et al. implemented vulnerability management in Cyber-Physical Systems to minimize the numerous vulnerabilities within this sector [22]. Li et al. developed a vulnerability management platform for the transportation sector, which is characterized by complex and vulnerable IT networks [15]. Chhillar and Shrivastava proposed a vulnerability management framework for the academic sector [23]. Nikolaou et al. established vulnerability management processes, including incident management, identification, and information sharing, within the energy sector [24]. Meanwhile, Avadanei et al. developed a predictive model for vulnerability management in the telecommunications sector [25].

2. Security Operation Center

A Security Operation Center (SOC) is an organization equipped to implement protection for CII. Several studies have explored the role of SOCs in delivering security services. Fysarakis et al. examined the urgency of establishing centralized SOCs as a means of enhancing national cybersecurity, fostering collaboration across various sectors, and safeguarding critical infrastructure in the European Union [26]. Kassim et al. investigated operational practices and challenges within MyCERT and proposed improvements, including the need for a platform for information exchange between CSIRTs and a framework for operational support for CSIRTs [27]. Hore et al. suggested the application of vulnerability management to assets within internal SOCs [28]. Farris et al. proposed methods for managing and prioritizing vulnerabilities, emphasizing the importance of monitoring vulnerabilities within internal SOC operations [29].

3. Gartner's Cycle

The cycle proposed by Gartner provides a comprehensive overview of the implementation of vulnerability management [19], [20]. This cycle consists of one initial stage and five main stages, as illustrated in Figure 1. The implementation of vulnerability management begins with the Preparation stage. This stage involves the formulation of policies and procedures for executing vulnerability management. The main stages consist of Assess, Prioritize, Act, Reassess, and Improve, and are carried out continuously. These stages encompass key activities for managing vulnerabilities, such as asset identification, risk assessment, patching, verification of fixes, and monitoring and evaluating the implementation process.

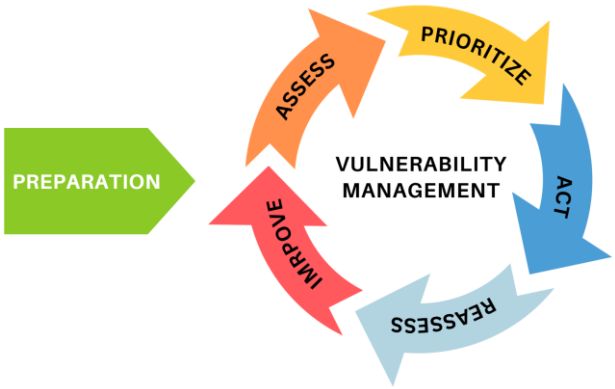

Figure 1. Gartner Vulnerability Management Cycle

4. CII Protection Framework

The Critical Information Infrastructure (CII) Protection Framework is derived from Peraturan Presiden Nomor 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. In accordance with the mandate in this regulation, the BSSN (National Cyber and Crypto Agency) issued a framework consisting of four domains: Identification, Protection, Detection, Response, and Recovery [8]. Each domain encompasses various categories, sub-categories, and controls that can be applied as needed, as well as detailed implementation steps. When used for CII protection, this framework serves as a guide for planning, implementing, and evaluating security activities.

C. Research Method

1. Document Study

In the document study, an in-depth analysis was conducted on the implementation of vulnerability management in three countries. The selection of these countries was based on the analysis of cybersecurity implementation frameworks from the United States, the United Kingdom, and Australia [18]. This research provides an overview of the differences in the implementation of cybersecurity frameworks in each country, allowing for the identification of gaps in those frameworks. However, there has been no comparison at the practical application level, suggesting the need for further research exploring comparisons of cybersecurity practices, such as vulnerability management. Standards, regulations, and publications related to vulnerability management in these three countries will be analyzed to gather insights into the vulnerability management practices carried out by each country.

2. Coding Activity

In the coding activity, the analysis of vulnerability management implementation in the three countries was coded by identifying and classifying them into the steps of vulnerability management based on Gartner's cycle. This coding activity is helpful in mapping the steps in the vulnerability management cycle to relevant activities in the three countries. This methodology is similar to the framework categorization performed by Azmi et al. [30]. The outcomes of the coding activity will highlight the vulnerability management activities of each country based on Gartner's cycle, making them easier to understand and use as a reference.

3. Activity Mapping

After the coding activity, the activity mapping is used to map the activities within the vulnerability management cycle of each country to the CII Protection Framework in Indonesia. This mapping is intended to provide an overview of the vulnerability management cycle based on benchmarking from the United States, the United Kingdom, and Australia, in accordance with the standards applicable in Indonesia, so that it can be applied to protect CII. The NSOC can implement this vulnerability management framework as the national-level SOC, which is responsible for protecting CII.

D. Result and Discussion

1. Vulnerability Management Analysis

This phase involves conducting an in-depth analysis of the standards, regulations, and publications related to vulnerability management practices in these three countries.

a. Vulnerability Management in the United States

The United States (US) has a standard related to the implementation of vulnerability management, namely the CRR Supplemental Resource Guide Vulnerability Management Version 1.1, which is the result of research collaboration between the Cybersecurity and Infrastructure Security Agency (CISA) and Carnegie Mellon University [31]. Broadly, the implementation of

vulnerability management is carried out through four main stages, which are explained as follows:

1) Define a Vulnerability Analysis and Resolution Strategy
   In this stage, the strategy for implementing vulnerability management in alignment with the organization's objectives is determined. This stage includes activities such as gathering information and support from stakeholders, defining the scope of the vulnerability management program, determining the methods to be used in the vulnerability assessment process, and documenting all activities that will be carried out in the vulnerability management process. Through this stage, it is expected that the organization will have all the necessary information for the subsequent stages.
2) Develop a Plan for Vulnerability Management
   All the strategic information collected is compiled into a plan that includes the rules and procedures related to the vulnerability management program. This planning phase involves preparing planning documents, determining the effectiveness standards for the program, identifying training needs, selecting appropriate tools, identifying sources of vulnerability information, defining roles and responsibilities, and identifying the involvement of other stakeholders.
3) Implement the Vulnerability Analysis
   This stage focuses on the implementation of the prepared vulnerability management program plan. Activities in this stage include providing training for end-users and personnel involved in the vulnerability management program, conducting vulnerability assessments, recording identified vulnerabilities, categorizing and ranking vulnerabilities, managing identified vulnerabilities to ensure proper handling, assessing the effectiveness of the vulnerability remediation efforts, and conducting root cause analysis for vulnerabilities.
4) Assess and Improve the Capability
   As an organization, sustainability and continuity are critical when implementing a program, given that cybersecurity is constantly evolving, and organizations must remain adaptive in facing emerging challenges. Therefore, this stage is used to assess the program's condition and make improvements. The activities in this stage involve determining the current status of the program, gathering and analyzing information about the program's condition, and enhancing the capabilities of the vulnerability management program.

b. Vulnerability Management in Australia

Australia has a government organization that plays an active role in coordinating national cybersecurity practices and formulating guidelines related to cybersecurity: the Australian Cyber Security Centre (ACSC). ACSC has developed various cybersecurity guidelines, which are documented in the Information Security Manual [32]. These guidelines are intended for both government and private organizations in Australia to implement protection for their information technology and operational technology from cyberattacks. Within the Information

Security Manual, there are several guidelines related to the implementation of vulnerability management, such as the Guidelines for System Management, Guidelines for System Monitoring, and Guidelines for System Hardening.

These guidelines provide detailed steps for managing vulnerabilities. The Guidelines for System Management describe system patching procedures, including developing procedures for patch management, inventorying software assets in a register, conducting vulnerability scans, mitigating vulnerabilities, and deactivating assets that no longer receive security support. For vulnerability monitoring, the Guidelines for System Monitoring are used to regulate event logging and centralized monitoring, ensuring that it is detailed and includes retention periods. The Guidelines for Cyber Security Incidents provide procedures for handling security gaps, which include vulnerability detection, developing a vulnerability response plan, documenting identified vulnerabilities, implementing an insider threat program, and reporting vulnerabilities to asset owners and the public. Specifically, the Guidelines for System Hardening detail steps for hardening various components, including the Operating System (OS), applications, servers, authentication mechanisms, and virtualization systems. Recommendations for the timeframe for addressing vulnerabilities are provided in the Guidelines for Assessing Security Vulnerabilities and Applying Patches to ensure that patching is performed promptly according to the criticality of the vulnerability in the asset [33]. The Guidelines for Continuous Monitoring Plan further support ongoing vulnerability monitoring efforts.

In addition to ACSC, the government of South Australia has guidelines that detail vulnerability management, specifically in the South Australian Cyber Security Framework – Vulnerability Management and Patching. The steps for vulnerability management outlined in this framework are as follows [34].

1) Identifying Security Vulnerabilities
   This step involves identifying assets using an asset register, identifying vulnerabilities from various sources, conducting vulnerability assessments, and performing penetration testing.
2) Assessing Security Vulnerabilities
   This step involves assessing the risk of vulnerabilities using the Common Vulnerability Scoring System (CVSS) and determining the priority for handling vulnerabilities. High-risk vulnerabilities will be prioritized for remediation.
3) Mitigating Security Vulnerabilities
   This step involves applying patches to vulnerable assets. If patches are unavailable or cannot be applied, alternative measures are implemented to reduce the risk of vulnerabilities in the assets.
4) Reporting Vulnerabilities and Patching Compliance
   This step ensures that patching has been effectively applied and the results are documented. These documents serve as reports and provide valuable insights for future learning.

c. Vulnerability Management in the United Kingdom

In the United Kingdom (UK), the national authority responsible for cybersecurity services is the National Cyber Security Centre (NCSC). This

organization is a government entity that is part of the UK's intelligence services. Its cybersecurity services cover protection for Critical National Infrastructure (CNI), handling cyber incidents, and enhancing cybersecurity resilience.

NCSC guides vulnerability management implementation through publications available on its web platform. This guidance is intended for organizations of all sizes, public sector entities, and professionals. The stages of vulnerability management, as recommended by NCSC, are as follows [35].

1) Put in place a policy to update by default
   This stage recommends that organizations implement a policy to update software by default when updates are available. Good communication preferences are needed to ensure that security updates are received promptly. The updates must be tested to ensure they do not cause issues in the assets. If a cybersecurity incident arises requiring a faster update process, policies for handling incidents should be developed so that exploitable vulnerabilities can be mitigated quickly.
2) Identify your assets
   This stage involves identifying and cataloguing assets across various platforms, such as systems, services, cloud infrastructure, mobile devices, hardware, and software, along with assigning responsibility for those assets. Obsolete assets are categorized and explicitly handled. The identified assets undergo configuration management to ensure they are securely configured according to cybersecurity standards.
3) Carry out assessments by triaging and prioritising
   This stage is implemented when updates or mitigation measures have not sufficiently reduced the impact of vulnerabilities. It involves triaging and prioritizing, which includes monthly scanning of all assets. Organizations may also develop a vulnerability disclosure program to receive reports from researchers. Identified vulnerabilities are categorized to facilitate prioritization. For each vulnerability, three actions are selected:
   - Fix - Implementing patching or other mitigation measures based on the highest impact vulnerabilities.
   - Acknowledge - Accepting the current risk of the vulnerability.
   - Investigate - Further investigation is conducted before mitigation or acceptance.
4) The organisation must own the risks of not updating
   If the organization cannot apply remediation or fix the vulnerability, the risks must be accepted by the organization. This stage advises organizations to consider their risk appetite when accepting the risks associated with not addressing a vulnerability.
5) Verify and regularly review your vulnerability management process
   This stage involves verifying that vulnerabilities have been appropriately handled. Regular reviews are also needed to ensure that the vulnerability management process aligns with the organization's evolving needs and standards.

2. Classification of Vulnerability Management Based on the Gartner's Cycle

Based on the analysis of vulnerability management practices in the United States, Australia, and the United Kingdom, coding was performed on the activities carried out in these countries. This coding process involved classifying the vulnerability management activities of each country according to the stages of the Gartner vulnerability management cycle in order to provide a comprehensive overview of the entire vulnerability management cycle, as detailed in Table 1.

Table 1. Classification of Vulnerability Management Activities According to the Gartner's Cycle

Phase	Country	Activities
Preparation	United States	1. Prepare the necessary documents and information for the planning and implementation of vulnerability management. 2. Define the scope of the vulnerability management program (assets, services, and operational scope). 3. Determine the method to be used in the vulnerability assessment. 4. Designate responsibility for assets and budgeting in the execution of the program. 5. Develop a document outlining the plan for executing the vulnerability management program. 6. Establish roles and responsibilities for the implementation of vulnerability management. 7. Determine the effectiveness of the vulnerability management program as a basis for program evaluation. 8. Plan and execute training for end-users and program staff involved in vulnerability management. 9. Identify the tools to be used in the vulnerability management process.
	Australia	1. Develop policies related to vulnerability management to enhance the success of the program implementation
	United Kingdom	1. Develop policies related to default updates through good communication references to ensure timely receipt of updated information 2. Develop policies for handling cybersecurity incidents that require immediate patching. 3. Conduct testing on the applied patches
Assess	United States	1. Identify sources of vulnerability information, including asset identification and external sources of vulnerability information. 2. Conduct vulnerability scanning, either independently or through third-party services. 3. Perform vulnerability assessments (penetration testing) to obtain a more detailed understanding of the vulnerabilities. 4. Log identified vulnerabilities into a repository.
	Australia	1. Identify systems and assets using asset registers. 2. Perform hardening on assets, including Operating Systems (OS), applications, servers, authentication, and virtualization.

		3. Identify vulnerabilities from public vulnerability sources and vulnerability monitoring activities, documenting them in a cybersecurity incident register. 4. Implement centralized event logging for monitoring potential vulnerabilities. 5. Apply retention periods to logs. 6. Conduct vulnerability scanning to identify vulnerabilities and misconfiguration tools. 7. Perform penetration testing to identify vulnerabilities through real-world attack simulations. 8. Run an insider threat mitigation program. 9. Report vulnerability findings to asset owners.
	United Kingdom	1. Identify assets and compile them into an asset catalogue. 2. Classifying obsolete assets to facilitate easier identification. 3. Implement configuration management for assets to meet security standards. 4. Conduct regular scanning of all assets at least once a month. 5. Run a vulnerability disclosure program to receive vulnerability reports from researchers.
Prioritize	United States	1. Categorize the vulnerabilities that have been found, considering the relevance and the responsible parties for the affected assets. 2. Prioritize the categorized vulnerabilities. 3. Determine the classification of remediation actions for the identified vulnerabilities.
	Australia	1. Conduct vulnerability assessment using a vulnerability scoring system. 2. Determine the prioritization of vulnerability remediation based on the highest risk.
	United Kingdom	1. Categorize vulnerabilities based on specific categories. 2. Determine risk mitigation steps, such as fix, acknowledge, or investigate
Act	United States	1. Conduct testing of remediation. 2. Implement remediation. 3. Ensure that the results of remediation implementation are recorded in a repository for evaluating the outcomes of the remediation implementation
	Australia	1. Apply patching to workstations or servers to mitigate the impact of vulnerabilities. 2. Apply patching by following the correct guidelines to ensure the patching functions properly. 3. Apply relevant vulnerability mitigation measures if no patches are available. 4. Implement a deadline for remediation based on the risk impact of the vulnerability. 5. Deactivate assets that are no longer in use or no longer receive security support.
	United Kingdom	1. Implement patching and mitigation for identified vulnerabilities. 2. Accept the risks and impacts of vulnerabilities if they align with the organization's risk appetite.
Reassess	United States	1. Evaluate the results of the remediation implementation.

		2. Repeat the remediation process if necessary to ensure vulnerabilities have been adequately addressed. 3. Conduct a Root Cause Analysis to identify the underlying cause of the vulnerabilities and develop appropriate remediation updates, which also serve to update the vulnerability repository. 4. Monitor the results of remediation from the Root Cause Analysis.
	Australia	1. Implement monitoring of the patching process to ensure its proper application. 2. Conduct regular scanning to identify new vulnerabilities and applicable patches. 3. Assess the effectiveness of the applied patching in addressing vulnerabilities.
	United Kingdom	1. Conduct verification to ensure that the vulnerabilities have been closed.
Improve	United States	1. Regularly update the vulnerability repository. 2. Evaluate the ongoing vulnerability management program to identify shortcomings or assess the effectiveness of the program (which is documented in a report). 3. Develop a strategy for improving the vulnerability management program based on the evaluation results. 4. Implement improvements based on the developed strategy.
	Australia	1. Provide reports on trends in security vulnerabilities, risks, and patching. 2. Continuously monitor new vulnerability findings.
	United Kingdom	1. Conduct periodic reviews of the vulnerability management process to align with organizational needs.

3. Generalization and Mapping of Activities

Vulnerability management activities in the United States, Australia, and the United Kingdom can be classified into the vulnerability management stages from Gartner. After classification, the stages of each country can be generalized based on similar or different activities, resulting in a comprehensive vulnerability management stage from the three countries. If this is to be used as a benchmark for NSOC in carrying out vulnerability management to protect CII, mapping the generalization into the CII Protection Framework can be conducted. NSOC can use the results of this mapping to apply the CII Protection Framework within the context of vulnerability management implementation.

The results of the generalization and mapping into the CII Protection Framework are outlined in Table 2. This generalization results in 38 vulnerability management activities, with nine activities in the Preparation phase, nine activities in the Assess phase, four activities in the Prioritize phase, seven activities in the Act phase, five activities in the Reassess phase, and four activities in the Improve phase. All these activities are relevant and can be mapped into 35 sub-category points of the CII Protection Framework.

Table 2. Generalization and Mapping of Vulnerability Management Activities

Phase		Activities	CII Protection Framework
Preparation	1	Develop policies related to vulnerability management	1.2.1 2.4.2
	2	Develop a program implementation plan for vulnerability management	1.2.2 2.4.2
	3	Define the scope and limitations of the vulnerability management program	1.1.2
	4	Establish roles and responsibilities in implementing vulnerability management	1.1.3 4.1.4
	5	Identify tools and methods to be used in the vulnerability management process	2.4.2 3.3.5
	6	Formulate the effectiveness level of the program implementation as a benchmark for evaluation	1.2.2
	7	Develop policies for incident handling that require immediate patching	1.2.3 4.1.1
	8	Develop a training plan for vulnerability management implementers	2.6.2
	9	Conduct testing on the routine patching process	2.2.2 4.4.1
Assess	10	Identify assets and organize them into an asset catalogue	1.3.1
	11	Classify obsolete assets	1.3.4
	12	Perform hardening on assets	2.4.1
	13	Implement configuration management to ensure asset security standards	2.4.1
	14	Implement centralized event logging and log retention periods	2.5.6
	15	Run an insider threat mitigation program	3.3.2 2.6.1
	16	Implement a vulnerability disclosure program to receive vulnerability reports from external sources	1.4.2
	17	Conduct vulnerability scanning to identify vulnerabilities and misconfigurations	3.3.5 1.4.1
	18	Perform penetration testing to gain a detailed understanding of vulnerabilities through real-world attack simulations	1.4.1 3.3.5
Prioritize	19	Group or categorize vulnerabilities based on relevance, risk, or specific categories	1.4.1 1.4.4
	20	Assess vulnerabilities using a vulnerability scoring system	1.4.4
	21	Determine risk management actions	1.4.5 4.3.1
	22	Prioritize vulnerability handling based on the highest risk levels	1.4.5 1.4.7
Act	23	Execute patching or mitigation of vulnerabilities according to risk response	1.4.8 4.4.1
	24	Apply other relevant mitigation steps if patching is unavailable	4.3.3 4.4.3
	25	Set patching or mitigation deadlines based on the vulnerability's risk level	1.4.1 4.4.2
	26	Test the effectiveness of remediations performed	3.3.5 2.5.4

	27	Disable assets that are no longer in use or lack security support	3.3.5
	28	Accept vulnerability risks if they align with the organization's risk appetite	1.4.8 4.4.1
	29	Document remediation results in the catalogue for evaluation purposes	4.3.3 4.4.3
Reassess	30	Evaluate and verify remediation implementations to ensure vulnerabilities are adequately addressed	1.4.8 4.4.1
	31	Conduct Root Cause Analysis (RCA) to understand the underlying causes of vulnerabilities	4.3.3 4.4.3
	32	Use RCA results to update the vulnerability catalogue and formulate remediation updates	1.4.1 4.4.2
	33	Conduct continuous monitoring to ensure the effectiveness of patching implementations	3.3.5 2.5.4
	34	Perform periodic scanning to detect new vulnerabilities or further patching needs	3.3.5
Improve	35	Regularly update the vulnerability catalogue and remediation actions	1.4.1 4.4.2
	36	Conduct periodic reviews of the vulnerability management program implementation in line with organizational needs	1.4.8 4.4.1
	37	Develop improvement strategies based on the evaluation of vulnerability management implementation	1.2.2 4.4.1
	38	Publish information related to trends in vulnerabilities, risks, and patching of electronic assets	3.1.4

E. Conclusions

This research proposes the implementation of vulnerability management at the NSOC to protect CII in Indonesia. The activities within this framework can be determined based on benchmarking standards, regulations, and vulnerability management publications from three countries: the United States, Australia, and the United Kingdom, as well as mapping them into the CII Protection Framework as a reference for implementing CII protection in Indonesia. The vulnerability management practices in the United States, the United Kingdom, and Australia are explained in a comprehensive and structured manner, originating from government agencies responsible for cybersecurity practices. There are several similarities and differences in the activities, which can be classified into the Gartner vulnerability management cycle. The generalization and mapping of vulnerability management activities from these three countries resulted in 38 relevant activities across 35 sub-categories in the CII Protection Framework. The results of this mapping can serve as a proposal for NSOC to implement effective vulnerability management in protecting CII in Indonesia.

F. References

[1] D. Perwej, S. Qamar Abbas, J. Pratap Dixit, N. Akhtar, and A. Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security," *International Journal of Scientific Research and Management*, vol. 2021, no. 12, pp. 669–710, 2021, doi: 10.18535/ijsrm/v9i12.ec04ï.

[2] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327–350, Sep. 2023, doi: 10.3390/jcp3030017.
[3] L. C. Herrera and O. Maennel, "A comprehensive instrument for identifying critical information infrastructure services," Jun. 01, 2019, *Elsevier B.V.* doi: 10.1016/j.ijcip.2019.02.001.
[4] P. A. W. Putro and D. I. Sensuse, "Threats, Vulnerabilities and Security Functions in Critical Information Infrastructure," in *2021 8th International Conference on Information Technology, Computer and Electrical Engineering, ICITACEE 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 113–117. doi: 10.1109/ICITACEE53184.2021.9617515.
[5] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178–188, Mar. 2019, doi: 10.1016/J.FUTURE.2018.09.063.
[6] H. P. Beckvard, "Protecting Critical Infrastructure and Critical Information Infrastructure," *CONTEMPORARY MILITARY CHALLENGES*, vol. 24, no. 2, pp. 15–28, Jun. 2022, doi: 10.33179/bsv.99.svi.11.cmc.24.2.1.
[7] Presiden Republik Indonesia, "Peraturan Presiden No. 82 tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital," 2022.
[8] BSSN, *Peraturan Badan Siber dan Sandi Negara Republik Indonesia No. 8 tahun 2023 tentang Kerangka Kerja Perlindungan Infrastruktur Informasi Vital*. Jakarta, 2023. Accessed: Dec. 28, 2024. [Online]. Available: https://jdih.bssn.go.id/peraturan/d/426
[9] C. H. Han, S. T. Park, and S. J. Lee, "The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system," *International Journal of Critical Infrastructure Protection*, vol. 26, Sep. 2019, doi: 10.1016/j.ijcip.2019.100312.
[10] Pusat Operasi Keamanan Siber Nasional, *Grand Desain NSOC - National Security Operation Center*. Jakarta: BSSN, 2021.
[11] BSSN, "Lanskap Keamanan Siber Indonesia 2023," 2023. Accessed: Dec. 28, 2024. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf
[12] H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, no. 4, pp. 332–340, Dec. 2019, doi: 10.1049/iet-cps.2018.5079.
[13] F. A. Pratama, "'Wabah' Iklan Judi Online Masih Bercokol di Situs Pemerintah." Accessed: Dec. 26, 2024. [Online]. Available: https://tirto.id/sempat-turun-masih-banyak-iklan-judi-online-di-situs-pemerintah-gYtY
[14] G. M. K. Magnussen, M. Pettersen, and M. I. Niemimaa, *A Comprehensive Framework for Patching and Vulnerability Management in Enterprises An Exploratory Study of How Enterprises Facilitate Patching and Vulnerability Management*. University of Agder, 2023.
[15] W. Li, K. Tian, and W. Wang, "Research and Practice on Network Security Vulnerability Management Methods in the Transportation Industry," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2023, pp. 318–322. doi: 10.1145/3661638.3661699.

[16] V. A. Mehri, P. Arlos, and E. Casalicchio, "Automated Context-Aware Vulnerability Risk Management for Patch Prioritization," *Electronics (Switzerland)*, vol. 11, no. 21, Nov. 2022, doi: 10.3390/electronics11213580.
[17] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3045514.
[18] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries," *Information and Computer Security*, vol. 27, no. 3, pp. 373–392, Jun. 2019, doi: 10.1108/ICS-10-2018-0122.
[19] C. Lawson, "Gartner's Strategic Vision for Vulnerability Management," 2020.
[20] R. Maués, "Vulnerability Management Process, what is it? – Conviso AppSec." Accessed: Dec. 21, 2024. [Online]. Available: https://blog.convisoappsec.com/en/vulnerability-management-process-what-is-it/
[21] N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, "An Empirical Study of Automation in Software Security Patch Management," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2022. doi: 10.1145/3551349.3556969.
[22] P. Sotiropoulos, C. M. Mathas, C. Vassilakis, and N. Kolokotronis, "A Software Vulnerability Management Framework for the Minimization of System Attack Surface and Risk," *Electronics (Switzerland)*, vol. 12, no. 10, May 2023, doi: 10.3390/electronics12102278.
[23] K. Chhillar and S. Shrivastava, "Vulnerability Scanning and Management of University Computer Network," in *IEMECON 2021 - 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/IEMECON53809.2021.9689207.
[24] N. Nikolaou, A. Papadakis, K. Psychogyios, and T. Zahariadis, "Vulnerability Identification and Assessment for Critical Infrastructures in the Energy Sector," *Electronics (Switzerland)*, vol. 12, no. 14, Jul. 2023, doi: 10.3390/electronics12143185.
[25] A. Avadanei, L. Nitescu, I. Constantin, and C. P. Sultanoiu, "Predictive Model for Software Vulnerability Management in Telecommunication Infrastructures," in *2021 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2021*, Institute of Electrical and Electronics Engineers Inc., May 2021. doi: 10.1109/BlackSeaCom52164.2021.9527768.
[26] K. Fysarakis, V. Mavroeidis, M. Athanatos, G. Spanoudakis, and S. Ioannidis, "A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness," in *Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 2601–2609. doi: 10.1109/BigData55660.2022.10020736.
[27] S. R. B. M. Kassim, S. Bin Shamsuddin, S. Li, and B. Arief, "How National CSIRTs Operate: Personal Observations and Opinions from MyCERT," *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, 2022, doi: DOI:10.1109/DSC54232.2022.9888803.

[28] S. Hore, A. Shah, and N. D. Bastian, "Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework," *Expert Syst Appl*, vol. 221, Jul. 2023, doi: 10.1016/j.eswa.2023.119734.
[29] K. A. Farris, A. Shah, G. Cybenko, R. Ganesan, and S. Jajodia, "VULCON: A system for vulnerability prioritization, mitigation, and management," *ACM Transactions on Privacy and Security*, vol. 21, no. 4, Jul. 2018, doi: 10.1145/3196884.
[30] R. Azmi, W. Tibben, and K. T. Win, "Review of cybersecurity frameworks: context and shared concepts," *Journal of Cyber Policy*, vol. 3, no. 2, pp. 258–283, May 2018, doi: 10.1080/23738871.2018.1520271.
[31] CISA, "CRR Supplemental Resource Guide Vulnerability Management Version 1.1," 2016. Accessed: Dec. 28, 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf
[32] ACSC, *Information Security Manual*. Canberra: Australian Cyber Security Centre, 2024. Accessed: Dec. 28, 2024. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2024-12/Information%20Security%20Manual%20%28December%202024%29.pdf
[33] ACSC, "Assessing Security Vulnerabilities and Applying Patches," 2021. Accessed: Dec. 29, 2024. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Assessing%20Security%20Vulnerabilities%20and%20Applying%20Patches%20%28October%202021%29.pdf
[34] Government of South Australia, "SACSF Guideline – Vulnerability management and patching," Oct. 2024. Accessed: Dec. 28, 2024. [Online]. Available: https://www.security.sa.gov.au/documents/documents/SACSF-G11.0-Vulnerability-management-and-Patching-Guideline-.pdf
[35] NCSC, "NCSC Vulnerability Management - NCSC.GOV.UK." Accessed: Dec. 29, 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/vulnerability-management