Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8

Hafizhan Irawan[1], Alva Hendi Muhammad[2], Asro Nasiri[3]
[1,2,3] Magister Teknik Informatika Universitas Amikom Yogyakarta,
Jl. Ring Road Utar, Condong Catur, Depok, Sleman, Yogyakarta, Indonesia 55281
E-mail: hfz.irawan@students.amikom.ac.id[1], alva@amikom.ac.id[2], asro@amikom.ac.id[3]

Abstract – Cybersecurity threats are constantly evolving, making it crucial for organizations to maintain a robust and maturing cybersecurity posture. According to the 2022 Annual Report of the Honeynet Project of the National Cyber and Crypto Agency (BSSN), there were 370,022,283 cyber attacks against Indonesia. One of the strategies that can be implemented is to conduct a cybersecurity maturity assessment to determine the organization's current level of cybersecurity implementation. This paper proposes a design for a cybersecurity maturity assessment framework leveraging two established standards: the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1 and the Center for Internet Security (CIS) Controls v8. The proposed framework utilizes a mapping between the NIST CSF v.1.1 subcategories and the CIS Controls v8 subcontrols, enabling a comprehensive assessment of an organization's cybersecurity maturity. The assessment methodology focuses on evaluating the implementation and effectiveness of controls aligned with each NIST CSF function. This approach allows organizations to identify strengths and weaknesses in their cybersecurity posture and prioritize areas for improvement. This research developed a mapping between the NIST CSF framework and CIS Controls v8. The mapping aligns 23 integrated cybersecurity categories from NIST CSF (including 64 subcategories out of a possible 108) with 124 subcontrols from CIS Controls v8 (out of a total 153). This combined framework serves as a tool to help organizations improve their cybersecurity maturity and capabilities.

Keywords – Cybersecurity Maturity, NIST CSF, CIS Controls.

I. INTRODUCTION

Cybersecurity focuses on safeguarding information within computer networks. It's a specific area of information security, which is concerned with protecting all types of information regardless of location. Cybersecurity works to defend information that is processed, stored, or sent electronically against various threats. Efforts to protect information in the context of cybersecurity involve preventing, mitigating, and reducing the impact of system damage [1]. According to the 2022 Annual Report of the Honeynet Project of the National Cyber and Crypto Agency (BSSN), there were 370,022,283 cyber attacks against Indonesia [2]. Just like financial risk and damage to a company's reputation, cybersecurity threats can hurt a company's profits. Cybersecurity issues can increase expenses and decrease sales, making it harder for a company to develop new products and services, and ultimately win and keep customers' trust [3]. One of the strategies that must be implemented is to develop a cybersecurity framework and implement it within organizations. Effective cyber-risk management is essential for all organizations. It involves thorough planning and continuous efforts to identify, assess, and mitigate cyber threats and uncertainties. This proactive approach helps organizations minimize potential damage and achieve their goals [4]. Currently, there are many frameworks available that can measure cybersecurity maturity, such as NIST, ISO, CIS, and other frameworks used by countries and organizations as controls to improve cybersecurity implementation.

Our research builds on existing work in the field. Sulistyowati, et al. had researched about comparative analysis and design of cybersecurity maturity assessment using COBIT, ISO/IEC 27002, NIST CSF and PCI DSS [5]. In other researched, Basofi and Salman had studied about cybersecurity maturity assessment design using NIST CSF, CIS Controls v8 and ISO/IEC 27002 [6]. Both studies have mapped the frameworks they studied, but only up to the category level of the frameworks. Therefore, further research is needed to map the subcategories of the framework activities. Notably, Ashari et al. [7] explored using NIST CSF and COBIT 5 for cyber-risk management in a government agency. Their study provided valuable insights on how NIST CSF can be applied to manage cyber risks and enhance overall cybersecurity capabilities.

This research utilizes the NIST Cyber Security Framework (CSF), which helps identify and prioritize actions to reduce cybersecurity risks. In line with its global popularity, the researchers opted for the NIST Cybersecurity Framework. This choice is supported by the 2019 SANS OT/ICS Cybersecurity Survey which identified it as the most commonly used framework among organizations worldwide [8]. A study by Roy et al. compares NIST CSF and ISO/IEC 27001, highlighting the key differences between the two frameworks and the advantages that NIST CSF offers [9]. The NIST CSF can also be used to manage cybersecurity risks across an organization or can be focused on services that are considered priorities within the organization because of universality and flexibility of NIST CSF as cybersecurity guide for all critical sectors [10]. This research also utilizes CIS Controls, which helps define NIST CSF subcategories into more detail and comprehensive. The basic idea of CIS Controls is that too much information is available on the Internet about information system protection, which is counterproductive, making it less secure [11]. Vinny Fadila, et al. [12] had researched that CIS Controls is succeed to helps organization to calculate the level of cyber security capability of the Pontianak City Communication and Informatics Service. In another research, Fatin Hanifah, et al. [13] used CIS Controls as framework to analyze vulnerabilities in Vulnerable Docker. As the result, 6 controls in CIS Controls v8 succeed to mitigate the risk in Vulnerable Docker. So as Amin Hassanzadeh, et al. [14] with their research. They conclude that CIS Controls offer mechanisms in cybersecurity, including detecting, denying, and deceiving cyber attacks that occur because no single defense mechanism can protect the water and wastewater sector from the threat of cyber attacks.

Based on previous researches above, NIST CSF and CIS Controls v8 can be proven as best practices in measuring cybersecurity maturity in the the organization. The difference between this research and previous research is that in some previous researches used one framework to measure cybersecurity maturity. And in the other researches combined some frameworks but not comprehensively because just combined based on categories or controls. Meanwhile, in this research, researchers map up to the subcategories of NIST CSF to CIS Controls v8. The goal of this study is to create a combined framework that helps to improve cybersecurity risk management and achieve better overall performance more comprehensively.

II. SIGNIFICANCE OF STUDY

A. Systems Security Engineering Capability Maturity Model

The Systems Security Engineering Capability Maturity Model (SSE-CMM) is process-oriented methodology designed to improve the development and implementation of secure systems. It helps organizations assess and enhance their security engineering practices by following a set of best practices.

Developed in the late 1990s, SSE-CMM draws inspiration from the Software Engineering Capability Maturity Model (SEI CMM). It aims to establish security engineering as a defined, mature, and measurable discipline within organizations.

SSE-CMM has five maturity levels. Level 1 known as Initial with security practices are ad-hoc and reactive. Level 2 known as Repeatable, which means basic security practices are documented and repeatable. Level 3 known as Defined, which means security processes are well-defined and standardized. Level 4 known as Managed which means security processes are actively monitored and controlled. And the last is Level 5 known as Optimizing, which means security processes are continuously improved based on quantitative data and feedback [14].

B. NIST CSF

The NIST Cybersecurity Framework (CSF) serves as a guide for cybersecurity activities and integrates cybersecurity risk management into existing risk management processes. Developed to enhance risk management, the NIST CSF is applicable to organizations across all sectors, regardless of size, cybersecurity risk level, or cybersecurity sophistication. Organizations can identify critical cybersecurity activities and prioritize them, enabling effective risk mitigation and management. However, the NIST CSF's focus on technical controls, log analysis, and incident response makes it more suitable for technology-oriented organizations [9]. The NIST CSF adopts a risk-based approach to cybersecurity risk management, comprising three components: Framework Core, Framework Implementation Tiers, and Framework Profile [15].

1. *Framework Core*

   The Framework Core consists of three main components that complement each other to assist organizations in developing, implementing, and strengthening their cybersecurity program. These three components are Identify, Protect, and Detect. Additionally, the Respond and Recover components complete the response and recovery cycle following an attack [15]. All of components has shown in Figure 1.

Figure 1. *NIST CSF Framework Core*

2. *Framework Implementation Tiers*

   The Framework Implementation Tiers is a critical component of the NIST CSF that assists organizations in evaluating their cybersecurity maturity and capability in implementing cybersecurity practices. Framework Implementation Tiers consists of four tiers: Partial, Risk Informed, Repeatable, and Adaptive [15]. Explanation about Framework Implementation Tiers are found at Table I.

TABLE I
FRAMEWORK IMPLEMENTATION TIERS EXPLANATION

Tier	Risk Management Process	Integrates Risk Management Program	External Participation
1 (Partial)	Risk management cyber security not yet formed so it's a priority security activities cyber yet is known.	Awareness regarding risk cyber security still limited.	Organizations don't accept and give information from other parties.
2 (Risk Informed)	Risk management cyber security applied however there is no policy yet	There is awareness regarding risk cybersecurity but not yet done approach to manage things	Organization understands his role in larger scale however delivery and reception information still not running yet well.
3 (Repeatable)	Risk management cyber has applied and there are policies who arranged it. Application cyber security updated regularly periodically.	There is approach to manage risk cyber security. The method used available to respond risk changes effectively.	Organization understands linkages with outside parties so that have a role and each other depending on bigger scale
4 (Adaptive)	Application risk management cyber security based on security activities cyber before and now. Can adapt to that threat changed and respond with quick and precise.	There is approach use policies, processes, and procedures based on risk information to manage and handle cyber security.	Organization understands his role with outside parties and share information directly internal and external.

3. *Framework Profile*

Framework Profile is a customized configuration of cybersecurity categories, subcategories, and practices aligned with the NIST CSF. It reflects an organization's specific cybersecurity objectives, relevant risks, and unique requirements [15]. The Framework Profile helps organizations: adopt a tailored approach to cybersecurity that considers their specific context; identify and prioritize the cybersecurity activities that are most relevant to their needs; develop and implement a cybersecurity program that is aligned with their risk profile and objectives; and track their progress and measure the effectiveness of their cybersecurity efforts. The Framework Profile is a valuable tool for organizations of all sizes and industries that seek to improve their cybersecurity posture and manage cybersecurity risks effectively.

C. CIS Controls v8

The Center for Internet Security created CIS Controls v8 to serve as a guide for organizations and individuals. CIS Controls is not intended to replace existing cybersecurity frameworks such as NIST, ISO 27001/27002, PCI DSS [16]. It prioritizes the most critical cybersecurity measures, helping them take initial steps to defend against cyberattacks [17]. CIS Controls categorize and prioritize cybersecurity activities based on an organization's circumstances. This categorization is known as CIS Implementation Groups (IGs). IGs are self-assessed categories for organizations based on their existing cybersecurity attributes. Each IG identifies a subset of CIS Controls and builds on the previous IG. If an organization is classified

as IG2, the requirements of IG1 must be met. This also applies to IG3, which must fulfill the requirements of IG1 and IG2. This allows organizations to prioritize control implementation based on the determined IG. According to CIS [18], there are three criteria to consider when determining an organization's IG:

1. Size and Complexity:
   a) Small: Organizations with less than 100 employees and limited IT resources.
   b) Medium: Organizations with 100-1,000 employees and some dedicated IT resources.
   c) Large: Organizations with more than 1,000 employees and extensive IT resources.
2. Industry:
   a) Critical Infrastructure: Organizations that provide essential services, such as energy, water, and transportation.
   b) Healthcare: Organizations that provide healthcare services, such as hospitals and clinics.
   c) Financial Services: Organizations that provide financial services, such as banks and investment firms.
3. Risk Tolerance:
   a) Low: Organizations that have a low tolerance for risk and are willing to invest in cybersecurity.
   b) Medium: Organizations that have a moderate tolerance for risk and are willing to invest in some cybersecurity measures.
   c) High: Organizations that have a high tolerance for risk and are willing to invest in minimal cybersecurity measures.

CIS Control v8 provides a proven way to protect information technology systems and data from cyberattacks[19] This approach follows globally recognized security standards and includes 18 main controls with 153 sub controls as more detailed guidelines as shown in Figure 2.

Figure 2. *CIS Controls v8*

D. Research Methods

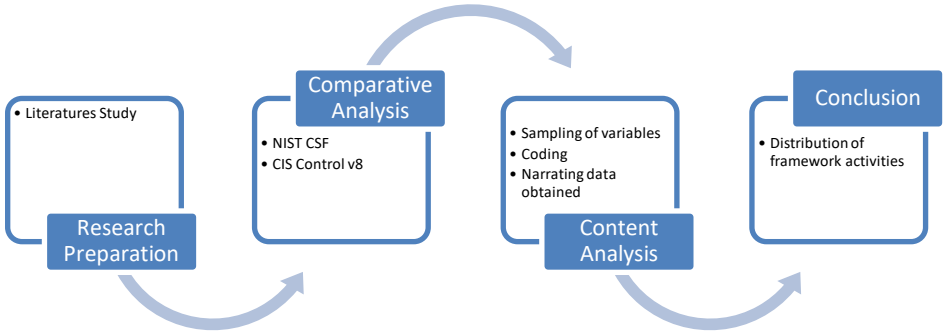

Figure 3. *Research Methods*

This research approach employs qualitative research. Qualitative methodology is a research procedure that produces descriptive data. Qualitative research emphasizes understanding the problem based on the conditions of reality holistically, complexly, and in detail [20]. Based on Figure 3, the research methods used in this study may include the following steps:

1. Research preparation: conducting a comprehensive literature study to understand the concepts and theories related to cybersecurity governance, NIST CSF and CIS Control v8. This literature review will help build the research theoretical foundation and gain an in-depth understanding of relevant cybersecurity frameworks and practices.
2. Comparative analysis: this initial step involves comparing, contrasting, critiquing, synthesizing, and summarizing information from standard data sources and security frameworks. This analysis lays the groundwork for the next stage – identifying the basic framework of activities for further, more in-depth analysis.
3. Content analysis: this subsequent analysis step delves deeper, uncovering the underlying patterns and insights hidden within the data collected in the previous step.
4. Conclusion: conclusion based on distribution of NIST CSF subcategories and CIS Controls v8 subcontrols which is categorized in each functions of NIST CSF.

III. RESULTS AND DISCUSSION

A. Comparative Analysis

A comparative analysis was conducted between the two frameworks, the results of which can be seen in Table II.

TABLE II
COMPARATIVE ANALYSIS

Framework	Function	Categories and Sub Categories
NIST CSF	1. Identification 2. Protect 3. Detection 4. Respond 5. Recovery	Consist of 23 categories and 108 subcategories
CIS Controls v8	Leveraging the experience of individual and corporate communities to improve security through the sharing of ideas, tools, learning, and collective action.	Consist of 18 controls and 153 subcontrols

B. Content Analysis

The next step is subcategories and subcontrols coding. To establish how the two frameworks integrate, the researchers assign codes to the subcategories of the NIST CSF framework (shown in Table III), where 'A' represents NIST CSF, ‘A.1’ represents Asset Management category in NIST CSF and ‘A.1.1’ represents ID.AM-1 sub category in Asset Management category in NIST CSF, and so on.

TABLE III
NIST CSF SUB CATEGORIES CODIFICATION

Categories	Sub Categories	ID
Asset Management	ID.AM-1	A.1.1
	ID.AM-6	A.1.6
Business Environment	ID.BE-1	A.2.1
	ID.BE-5	A.2.5
Governance	ID.GV-1	A.3.1
	ID.GV-4	A.3.4
Risk Assessment	ID.RA-1	A.4.1
	ID.RA-6	A.4.6
Risk Management Strategy	ID.RM-1	A.5.1
	ID.RM-3	A.5.3
Supply Chain Risk Management	ID.SC-1	A.6.1
	ID.SC-5	A.6.5
Identity Management, Authentication and Access Control	PR.AC-1	A.7.1
	PR.AC-7	A.7.7
Awareness and Training	PR.AT-1	A.8.1
	PR.AT-5	A.8.5
Data Security	PR.DS-1	A.9.1
	PR.DS-8	A.9.8
Information Protection Processes and Procedures	PR.IP-1	A.10.1
	PR.IP-12	A.10.12
Maintenance	PR.MA-1	A.11.1
	PR.MA-2	A.11.2
Protective Technology	PR.PT-1	A.12.1
	PR.PT-5	A.12.5
Anomalies and Events	DE.AE-1	A.13.1
	DE.AE-5	A.13.5
Security Continuous Monitoring	DE.CM-1	A.14.1
	DE.CM-8	A.14.8
Detection Processes	DE.DP-1	A.15.1
	DE.DP-5	A.15.5
Response Planning	RS.RP-1	A.16.1

Categories	Sub Categories	ID
Communications	RS.CO-1	A.17.1
	RS.CO-5	A.17.5
Analysis	RS.AN-1	A.18.1
	RS.AN-5	A.18.5
Mitigation	RS.MI-1	A.19.1
	RS.MI-3	A.19.3
Improvements	RS.IM-1	A.20.1
	RS.IM-2	A.20.2
Recovery Planning	RC.RP-1	A.21.1
Improvements	RC.IM-1	A.22.1
	RC.IM-2	A.22.2
Communications systems, victims, other CSIRTs, and vendors).	RC.CO-1	A.23.1
	RC.CO-3	A.23.3

In Table IV the researchers assign codes to subcontrols of CIS Controls v8, where 'B' represents CIS Controls v8, ‘B.1’ represents Inventory and Control of Enterprise Assets control in CIS Controls v8 and ‘B.1.1’ represents Establish and Maintain Detailed Enterprise Asset Inventory subcontrol in Inventory and Control of Enterprise Assets control in CIS Controls v8, and so on.

TABLE IV
CIS CONTROLS V8 SUB CONTROLS CODIFICATION

Controls	Sub Controls	ID
Inventory and Control of Enterprise Assets	Establish and Maintain Detailed Enterprise Asset Inventory	B.1.1
	Use a Passive Asset Discovery Tool	B.1.5
Inventory and Control of Software Assets	Establish and Maintain a Software Inventory	B.2.1
	Allowlist Authorized Scripts	B.2.7
Data Protection	Establish and Maintain a Data Management Process	B.3.1
	Log Sensitive Data Access	B.3.14
Secure Configuration of Enterprise Assets and Software	Establish and Maintain a Secure Configuration Process	B.4.1
	Separate Enterprise Workspaces on Mobile End-User Devices	B.4.12
Account Management	Establish and Maintain an Inventory of Accounts	B.5.1
	Centralize Account Management	B.5.6
Access Control Management	Establish an Access Granting Process	B.6.1
	Define and Maintain Role-Based Access Control	B.6.8
Continuous Vulnerability Management	Establish and Maintain a Vulnerability Management Process	B.7.1
	Remediate Detected Vulnerabilities	B.7.7
Audit Log Management	Establish and Maintain an Audit Log Management Process	B.8.1

Controls	Sub Controls	ID
	Collect Service Provider Logs	B.8.12
Email and Web Browser Protections	Ensure Use of Only Fully Supported Browsers and Email Clients	B.9.1
	Deploy and Maintain Email Server Anti-Malware Protections	B.9.7
Malware Defenses	Deploy and Maintain Anti-Malware Software	B.10.1
	Use Behavior-Based Anti-Malware Software	B.10.7
Data Recovery	Establish and Maintain a Data Recovery Process	B.11.1
	Test Data Recovery	B.11.5
Network Infrastructure Management	Ensure Network Infrastructure is Up-to-Date	B.12.1
	Establish and Maintain Dedicated Computing Resources for All Administrative	B.12.8
Network Monitoring and Defense	Centralize Security Event Alerting	B.13.1
	Tune Security Event Alerting Thresholds	B.13.11
Security Awareness and Skills Training	Establish and Maintain a Security Awareness Program	B.14.1
	Conduct Role-Specific Security Awareness and Skills Training	B.14.9
Service Provider Management	Establish and Maintain an Inventory of Service Providers	B.15.1
	Securely Decommission Service Providers	B.15.7
Application Software Security	Establish and Maintain a Secure Application Development Process	B.16.1
	Conduct Threat Modeling	B.16.14
Incident Response Management	Designate Personnel to Manage Incident Handling	B.17.1
	Establish and Maintain Security Incident Thresholds	B.17.9
Penetration Testing	Establish and Maintain a Penetration Testing Program	B.18.1
	Perform Periodic Internal Penetration Tests	B.18.5

C. Result

The researchers then conducted an analysis of the two frameworks to group CIS Controls v8 subcontrols with NIST CSF subcategories. The grouping was based on the similarity of the objectives of each subcategory and subcontrol. The results of the grouping can be seen in Table V.

TABLE V
ALL SUB CATEGORIES AND SUB CONTROLS MAPPING

Function	Category	NIST CSF ID	CIS Controls v8 ID
IDENTIFY	Asset Management	A.1.1	B.1.1
		A.1.2	B.2.1, B.2.2, B.16.4
		A.1.3	B.3.8
		A.1.4	B.12.4
		A.1.5	B.3.2, B.3.7
		A.1.6	B.14.1
	Business Environment	A.2.1	-
		A.2.2	-
		A.2.3	-
		A.2.4	-

Function	Category	NIST CSF ID	CIS Controls v8 ID
		A.2.5	-
	Governance	A.3.1	B.14.1
		A.3.2	B.15.2, B.17.4
		A.3.3	-
		A.3.4	-
	Risk Assessment	A.4.1	B.7.1, B.7.2, B.7.4
		A.4.2	-
		A.4.3	-
		A.4.4	-
		A.4.5	B.3.7, B.7.6
		A.4.6	-
	Risk Management Strategy	A.5.1	-
		A.5.2	-
		A.5.3	-
	Supply Chain Risk Management	A.6.1	B.15.2
		A.6.2	B.15.1, B.15.3, B.15.5
		A.6.3	B.15.4
		A.6.4	B.15.5
		A.6.5	B.11.1
PROTECT	Identity Management, Authentication and Access Control	A.7.1	B.4.7, B.5.1, B.5.3, B.5.5, B.6.1, B.6.2, B.6.6, B.6.7, B.13.9, B.15.7
		A.7.2	-
		A.7.3	B.4.11, B.6.4, B.6.6, B.12.7, B.13.5
		A.7.4	B.3.3, B.5.4, B.6.8
		A.7.5	B.3.12, B.9.2, B.9.3, B.9.6, B.12.2, B.12.8, B.13.4, B.16.14
		A.7.6	-
		A.7.7	B.6.3, B.6.4, B.6.5, B.12.3, B.12.6, B.12.7, B.13.5
	Awareness and Training	A.8.1	B.14.1, B.14.2, B.14.3, B.14.4, B.14.5, B.14.6, B.14.7, B.14.8, B.14.9, B.16.9
		A.8.2	B.14.9, B.16.9
		A.8.3	B.15.4
		A.8.4	B.14.9
		A.8.5	B.14.9
	Data Security	A.9.1	B.3.11, B.16.11
		A.9.2	B.3.10, B.12.3, B.12.6, B.16.11
		A.9.3	B.1.1, B.3.5
		A.9.4	-
		A.9.5	B.3.13, B.3.13, B.16.14
		A.9.6	B.11.5
		A.9.7	B.16.8
		A.9.8	B.16.14
	Information Protection Processes and Procedures	A.10.1	B.2.7, B.4.11, B.4.2, B.4.3, B.9.1, B.9.4, B.16.7
		A.10.2	B.16.5, B.16.10, B.16.12
		A.10.3	-
		A.10.4	B.11.2, B.11.3
		A.10.5	-
		A.10.6	B.3.1, B.3.5
		A.10.7	B.16.14, B.18.1
		A.10.8	-

Function	Category	NIST CSF ID	CIS Controls v8 ID
		A.10.9	B.11.1, B.17.1, B.17.3, B.17.4
		A.10.10	B.17.7
		A.10.11	B.6.2
		A.10.12	B.7.6
	Maintenance	A.11.1	-
		A.11.2	B.13.5
	Protective Technology	A.12.1	B.8.2, B.8.4, B.8.8, B.8.11
		A.12.2	B.3.9, B.10.3
		A.12.3	B.2.7, B.13.10
		A.12.4	-
		A.12.5	B.11.4
DETECT	Anomalies and Events	A.13.1	B.3.8
		A.13.2	B.8.11
		A.13.3	B.8.2, B.8.5, B.8.6, B.8.7, B.8.8, B.8.12
		A.13.4	-
		A.13.5	B.13.11
	Security Continuous Monitoring	A.14.1	B.8.5, B.13.2, B.13.3, B.13.6, B.13.7, B.13.8
		A.14.2	-
		A.14.3	-
		A.14.4	B.9.7, B.10.1, B.10.2, B.10.4, B.10.5, B.10.6, B.10.7
		A.14.5	-
		A.14.6	B.15.6
		A.14.7	B.1.3, B.1.4, B.1.5, B.2.3, B.2.4, B.2.5, B.2.6, B.9.6
		A.14.8	B.7.5
	Detection Processes	A.15.1	B.17.1, B.17.4
		A.15.2	-
		A.15.3	-
		A.15.4	B.17.5
		A.15.5	-
RESPOND	Response Planning	A.16.1	-
	Communications	A.17.1	B.17.2, B.17.4
		A.17.2	B.17.5
		A.17.3	B.17.5
		A.17.4	B.17.5
		A.17.5	-
	Analysis	A.18.1	B.8.11, B.16.3, B.16.6
		A.18.2	-
		A.18.3	-
		A.18.4	B.17.9
		A.18.5	B.16.2
	Mitigation	A.19.1	-
		A.19.2	-
		A.19.3	-
	Improvements	A.20.1	B.17.8
		A.20.2	B.17.8
RECOVER	Recovery Planning	A.21.1	-
	Improvements	A.22.1	-
		A.22.2	-
	Communications	A.23.1	-
		A.23.2	-
		A.23.3	-

This research analyzed the content of two cybersecurity frameworks, NIST CSF and CIS Controls v8. By mapping the subcategories and subcontrols between the two frameworks, we identified 23 integrated cybersecurity categories. These categories include 64 subcategories from NIST CSF (out of a possible 108) and 124 subcontrols from CIS Controls v8 (out of a total 153) as shown in Figure 4. This combined framework serves as a tool to assess the cybersecurity maturity of organization, which is categorized into each function of NIST CSF, namely Identify, Protect, Detect, Respond, and Recover. All research activities contributed to the development of this integrated cybersecurity maturity framework.

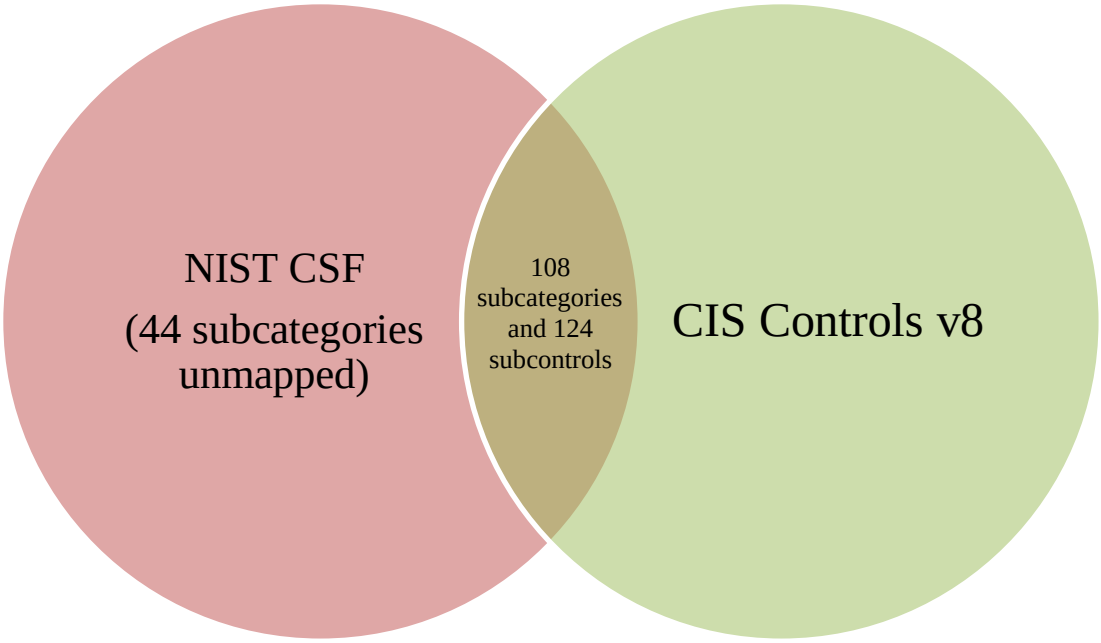

Figure 4. *Distribution of Frameworks Activities*

IV. CONCLUSIONS

Based on the mapping results of NIST CSF to CIS Controls v8, there are 44 subcategories from NIST CSF and 108 subcategories from NIST CSF that are mapped to 124 subcontrols from CIS Controls v8. This integration is categorized into each function of NIST CSF, namely Identify, Protect, Detect, Respond, and Recover. The results of this mapping can be used as points by organizations to determine the tier at which the organization has implemented each subcategory and subcontrol to measure the maturity level of cybersecurity in an organization. The organization can use the result of both frameworks integration to asssest the current tier of IT Unit based on NIST CSF implementation tier by standards that have been set in each subcategories and subcontrols integration. The assessment results can be more comprehensive due to the existence of subcontrols from CIS Controls v8, which are more technical than the NIST CSF which more general. The organization also can set the NIST CSF implementation tier target and measure the gap analysis from the existing organization tier to the desired organizational tier by create action plans. For future research, the latest version of each framework can be used. Even additional frameworks can be used to fill in the NIST CSF sub-categories that CIS Controls v8 has not been able to map.

REFERENCES

[1] Jeremy Straub. *Software engineering: The first line of defense for cybersecurity*. 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS). IEEE. 2020; p. 1-5.

[2] BSSN. *Laporan Tahunan Honeynet Project 2022*. Jakarta. 2022.

[3] CISA. *Cybersecurity Framework Implementation Guide.* United States of America. 2020.

[4] K. Ruan. Chapter 3 - Cyber Risk Management: A New Era of Enterprise Risk Management. Digital Asset Valuation and Cyber Risk Measurement. K. Ruan, Ed., Academic Press. 2019: pp. 49-73.

[5] D. Sulistyowati, F. Handayani and Y. Suryanto. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*. 2020; vol. 4, no. 4: pp. 225-230.

[6] I. Bashofi and M. Salman. *Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002*. 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom). 2022.

[7] R. A. Ashari and O. C. Briliyant. Rencana Penerapan Cyber-risk Management Menggunakan NIST CSF dan COBIT 5. *Jurnal Sistem Informasi*. 2018; vol. 14, no. 2: pp. 83-89.

[8] Filkins, Barbara, Doug Wylie, and A. J. Dely. Sans 2019 state of ot/ics cybersecurity survey. SANS™ Institute. 2019.

[9] Roy P. Prameet. *A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard*. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). 2020; pp. 1-3.

[10] Udroiu, Adriana-Meda, Mihail Dumitrache, and Ionut Sandu. *Improving the cybersecurity of medical systems by applying the NIST framework*. 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE. 2022.

[11] Stjepan Groš. *A Critical View on CIS Controls*. 2021 16th International Conference on Telecommunications (ConTEL). 2021; pp. 122–128.

[12] Viny Fadila, Nurul Mutiah and Renny Puspita Sari. Audit Keamanan Siber Menggunakan Kerangka Kerja CIS CSC, NIST CSF, dan COBIT 2019. *CESS (Journal of Computer Engineering System and Science).* 2023; vol. 8: pp 271-283.

[13] Fatin Hanifah, Avon Budiyono and Adityas Widjajarto. Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan Framework CIS Control. *e-Proceeding of Engineering*. 2021; pp. 8880–8885.

[14] Amin Hassanzadeh et al. A Review of Cybersecurity Incidents in the Water Sector. *ASCE Journal of Environmental Engineering*. 2020.

[15] SSE Project Team. *System Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0*. Technical report, SSE-CMM. 2003.

[16] NIST. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. 2018.

[17] D. P. Prastika, J. Triyono, and U. Lestari. Audit dan Implementasi CIS Benchmark Pada Sistem Operasi Linux Debian Server (Studi Kasus: Server Laboratorium Jaringan Dan Komputer 6, Institut Sains & Teknologi Akprind Yogyakarta). *Jurnal JARKOM*. 2019; vol. 6, no. 1: pp. 1–12.

[18] Amiruddin, Hafizh Ghozie Afiansyah, and Hernowo Adi Nugroho. *Cyber-risk management planning using NIST CSF v1. 1, NIST Sp 800-53 rev. 5, and CIS controls v8*. 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE. 2021.

[19] A. Tedyyana, O. Ghazali, and O. W. Purbo, “Machine learning for network defense: automated DDoS detection with telegram notification integration,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 34, no. 2, p. 1102, May 2024, doi: 10.11591/ijeecs.v34.i2.pp1102-1109.
[20] CIS. *CIS Controls CIS Controls Version 8*. 2021.

ACKNOWLEDGEMENTS

The researchers would like to express sincere gratitude to the institution of "MTI Universitas Amikom Yogyakarta" and all the lecturers for providing the resources and support necessary for the completion of this research.