JOISTECH: Journal of Information System and Technology
ISSN 3063-9778 (Media Online)
Vol 01, No 02, Desember 2024, Hal 82-87

Comparative Analysis of Cybersecurity Maturity Frameworks: NIST-CSF and C2M2

Faishal Wafiq Zakiy[1*], Nisa Dwi Angresti[2]

[1]Faculty of Science and Technology, Software Engineering, Darunnajah University, Jakarta, Indonesia
[2]Faculty of Information Technology, Information Systems, Andalas University, Padang, Indonesia

Email: [1]zakiy@darunnajah.ac.id, [2]nisadwi@it.unand.ac.id

Abstract– Cybersecurity maturity assessment is crucial for organizations implementing information technology. Various methods and frameworks are currently available to facilitate such assessments. This analysis focuses on two popular frameworks published by recognized legal entities in the United States: NIST-CSF and C2M2. These frameworks were developed in collaboration with relevant stakeholders. While they share some similarities, each framework has distinct characteristics. Employing either one is preferable to not conducting a cybersecurity maturity assessment at all. Alternatively, using both frameworks together can yield more comprehensive assessment results.

Keywords: Cybersecurity Maturity Model; NIST-CSF; C2M2

1. INTRODUCTION

Cybersecurity maturity assessment is crucial for organizations implementing information technology (IT) (Jauhari et al., 2024). This assessment must be carried out by professional teams knowledgeable in cybersecurity maturity (Sakinah & Setiawan, 2014). They are responsible to stakeholders for conducting audits of the organization (Aminudin et al., 2024). The audit results will determine the organization's level of cybersecurity maturity (Tinungki et al., 2021).

Audit teams will find it easier to work with the guidance of a cybersecurity maturity framework (Valavanis, 2024). Over time, advancements necessitate higher standards of cybersecurity maturity, making it essential to update previously established standards (Marican et al., 2023).

Cybersecurity maturity standards are more accountable when issued by legally recognized entities such as government institutions and formally established organizations. In this analysis, the authors selected two frameworks published by official institutions in the United States. The authors compare the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF) from NIST with the Cybersecurity Capability Maturity Model (C2M2) from the U.S. Department of Energy and NIST (NIST | NCCoE, 2023).

The cybersecurity maturity assessment methods from both institutions can generally be applied across various fields (Sugara et al., 2019). However, some fields may specifically benefit more from one of the cybersecurity maturity assessment methods (Sama et al., 2021). This comparative analysis aims to evaluate the two methods selected by the authors (Safitri & Kabetta, 2023).

2. RESEARCH METHODOLOGY

2.1 Cybersecurity Maturity Model

The cybersecurity maturity model serves as a framework to measure the maturity of security programs, providing guidance on how to reach the next level (Jauhari et al., 2024). This framework offers organizations an approach to understand the state of their cybersecurity maturity, whether they are at the crawling, walking, or running stage, as well as their pace of progress (Tinungki et al., 2021). Organizations can also identify the necessary steps to advance to a higher stage (J. Christopher, 2021).

2.2 National Institute of Standards and Technology Cyber Security Framework

National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) for information technology security is a product of NIST, first published in February 2014 following Executive Order 13636 issued by the President of the United States in February 2013, aimed at enhancing government information security (President et al., 2012). At the time, the U.S. President recognized the need for standards to protect critical and strategic infrastructure in the country. NIST has revised the NIST-CSF twice, in 2017 and 2018 (National Institute of Standards and Technology, 2018).

This framework emphasizes encouraging businesses to guide their cybersecurity activities while considering cybersecurity risks as part of organizational risk management (National Institute of Standards and Technology, 2018). The NIST-CS consists of three components:

a. **Framework Core**: A set of cybersecurity activities and common references across sectors and critical infrastructure, organized based on desired outcomes (J. D. Christopher et al., 2014). It provides detailed guidance for developing a Profile (National Institute of Standards and Technology, 2018)

b. **Framework Profile**: A framework that helps organizations identify, align, and prioritize current cybersecurity activities with target objectives according to their business/mission requirements, risk tolerance, and available resources (National Institute of Standards and Technology, 2018). It also represents the outcomes achieved or intended to be achieved by the organization according to Categories and Subcategories (DOE, 2014).
c. **Implementation Tiers**: A mechanism for organizations to review and understand the characteristics of their approaches to managing cybersecurity risks, helping them prioritize and achieve their cybersecurity goals (National Institute of Standards and Technology, 2018).

2.3 Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2) was first published in February 2014 by the U.S. Department of Energy (DOE) in collaboration with NIST and the U.S. Department of Homeland Security (DHS), producing a guidance document that highlights the interoperability between NIST-CSF and C2M2 (J. D. Christopher et al., 2014). This framework focuses on process domains, goals, and practices used in the electricity, gas, and oil industries. However, the model ensures adaptability to an organization's cybersecurity environment, making C2M2 applicable to businesses of any size or industry (Homeland Security, 2015).

C2M2 is structured around three Maturity Indication Levels (MILs). The model is designed to measure the strength of processes within specific areas and assess maturity by considering organizational process improvement broadly. The ES-C2M2 is divided into 10 functional domains, each comprising several objectives (Homeland Security, 2015). The C2M2 domains are as follows: risk management; asset, change, and configuration management; identity and access management; threat and vulnerability management; situational awareness; information sharing and communications; event and incident response, continuity of operations; supply chain and external dependencies management; workforce management; and cybersecurity program management (Curtis & Mehravari, 2015).

NIST-CSF and C2M2 share many core elements. For example:
a. **C2M2 Practices** include elements of the Framework Core and Tier characterizations, addressing the sophistication of cybersecurity programs and the culture or institutionalization that supports them (DOE, 2014).
b. **C2M2 Maturity Indicator Levels (MILs)** represent the measure of progress within the C2M2 domains as cybersecurity programs evolve, correlating with elements of the Framework Tiers. Each C2M2 MIL domain score incorporates risk management characteristics of the Tiers (DOE, 2014).
c. **C2M2 Score Card** highlights the maturity level across C2M2 domains, closely resembling the concept of the Framework Profile, both in its current state and target state (DOE, 2014).

3. RESULT AND DISCUSSION

The NIST-CS and C2M2 frameworks have several differences and similarities, as C2M2 was developed based on NIST-CS through collaboration between the U.S. Department of Energy and NIST (Garba et al., 2020) (Sulistyowati et al., 2020). As a result, they share common outlines. However, each framework has its own unique characteristics.

3.1 Framework Core

Both frameworks are structured into three separate levels: Functions, Categories, and Subcategories. These frameworks include five Functions: Identify, Protect, Detect, Respond, and Recover. The Identify, Protect, and Detect Functions provide a strategic view of organizational cybersecurity risk management (National Institute of Standards and Technology, 2018)(DOE, 2014). The identification of Categories and Subcategories underpins each Function, aligning them with Informative References in the form of standards, guidelines, and practices (DOE, 2014).

The framework operates on three levels of coordination: Executive, Business/Process, and Implementation/Operations. A comparison of the core structure of the NIST-CSF and C2M2 frameworks is illustrated in Figure 1.

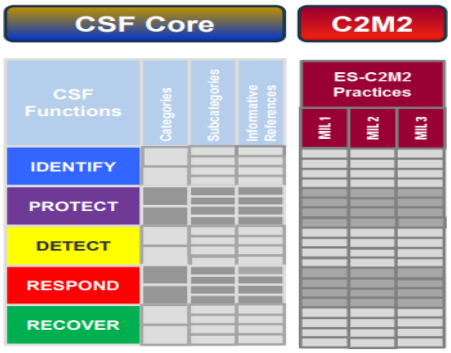

Figure 1. Core Structure of NIST-CSF and C2M2

3.2 Maturity Levels

The NIST-CSF framework addresses maturity levels more accurately than C2M2 (Garba et al., 2020). However, it is more informal and only provides a general discussion in Section 2.2, whereas C2M2 offers more detailed descriptions. The NIST-CSF framework starts numbering from 1 (one), while C2M2 begins numbering from 0 (zero) (*Revision 06 Cybersecurity Capability Maturity Model (C2M2) Version 2.0 July 2021*, 2021). An overview of the maturity levels in the NIST-CSF and C2M2 frameworks is presented in Table 1 and further illustrated in Figure 2.

Table 1. NIST-CS Levels and C2M2 Maturity Indicators (MILs)

NIST-CS Levels	C2M2 Maturity Indicators (MILs))
	0 – Incomplete
1 – Partial	1 – Initiated
2 – Risk Informed	2 – Performed
3 – Repeatable	3 – Managed
4 – Adaptive	

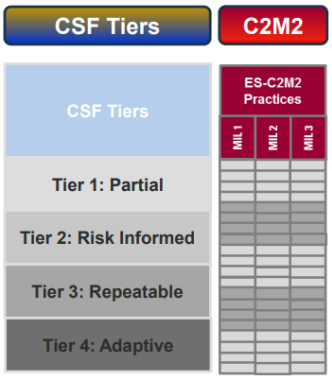

Figure 2. NIST-CS Levels and C2M2 Indicators (MILs)

3.3 Functions and Categories

The NIST-CS framework uses the terms *function* and *category*, where each category is a collection of subcategories (Krumay et al., 2018). This comparison remains too general compared to the terminology used by C2M2. A clearer depiction of the differences can be seen in Table 2.

Table 2. Comparison of Layouts Between NIST-CS and C2M2

NIST-CS	C2M2
Function	Domain
Category	Objectives
Subcategory	Practices

Each concept between NIST-CSF and C2M2 is still comparable but uses different approaches in its delivery (Sulistyowati et al., 2020). C2M2 is more specific and focuses on maturity levels, while NIST-CSF only defines objectives and leaves the identification of maturity levels to individual organizations. (J. D. Christopher et al., 2014) A comparison of the content of these two frameworks is illustrated in Figure 3 and Figure 4.

1. Detect Cybersecurity Events

MIL1	a.	There is a point of contact (person or role) to whom cybersecurity events are reported
	b.	Cybersecurity events are detected and reported
	c.	Cybersecurity events are logged and tracked
MIL2	d.	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)
	e.	There is a repository where cybersecurity events are logged based on the established criteria
MIL3	f.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features
	g.	Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RISK-2j) and threat profile (THREAT-1d) to help detect known threats and monitor for identified risks
	h.	The common operating picture for the function is monitored to support the identification of cybersecurity events

Figure 3. Maturity Indicator Level (MIL) in C2M2

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established

Figure 4. Functions, Categories, and Subcategories in NIST-CS

3.4 Assessment Results

The C2M2 toolkit produces a graphical summary of results divided by C2M2 domains and MIL levels, along with detailed results and analysis provided for each domain, as shown in Figure 5.

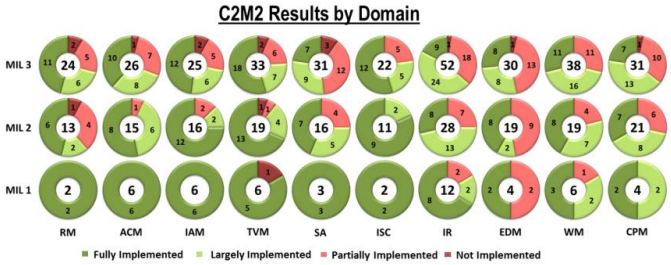

Figure 5. Example of Maturity Indicator Level (MIL) assessment results using C2M2

Meanwhile, NIST-CSF uses a matrix table to illustrate assessment results, as shown in Figure 6.

		MIL 1	MIL 2	MIL 3	TOTALS
Identify	Fully Implemented	24	23	24	71
	Largely Implemented	1	14	23	38
	Partially Implemented	2	8	14	24
	Not Implemented	2	0	3	5
	Subtotals:	29	45	64	138
Protect	Fully Implemented	50	28	10	88
	Largely Implemented	3	26	32	61
	Partially Implemented	3	16	30	49
	Not Implemented	0	0	1	1
	Subtotals:	56	70	73	199
Detect	Fully Implemented	20	2	8	30
	Largely Implemented	1	22	10	33
	Partially Implemented	1	2	14	17
	Not Implemented	0	0	3	3
	Subtotals:	22	26	35	83
Respond	Fully Implemented	10	4	3	17
	Largely Implemented	0	9	9	18
	Partially Implemented	0	6	6	12
	Not Implemented	0	0	0	0
	Subtotals:	10	19	18	47
Recover	Fully Implemented	1	0	1	2
	Largely Implemented	0	0	3	3
	Partially Implemented	0	3	4	7
	Not Implemented	0	0	0	0
	Subtotals:	1	3	8	12
	TOTALS	118	163	198	479

Figure 6. Example of cybersecurity maturity assessment results using NIST-CSF

4. CONCLUSION

Cybersecurity maturity assessment is not entirely objective, as determining maturity levels depends on each organization, even when using frameworks such as NIST-CSF or C2M2. Consequently, some parties may object to the use of such frameworks. However, this approach is better than conducting no assessment at all. Future developments in cybersecurity will inevitably modify these models to ensure they remain usable for those who need them. This assessment is only the beginning, as every organization must consider the next steps, including improving its maturity level. The definition of "progressing" differs at each level. Regardless of the framework chosen, organizations must align their programs accordingly.. Organizations can conduct cybersecurity maturity assessments using the NIST-CSF or C2M2 frameworks. Additionally, they may opt to use both frameworks together for more comprehensive results.. Cybersecurity maturity models facilitate organizations in assessing their current position. These models provide a foundation for enhancing organizational cybersecurity efforts and serve as a communication bridge between management teams and technical teams.

REFERENCES

Aminudin, A., Supriyanto, A., Semarang, U., & Artikel, R. (2024). *Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001 : 2013 (Studi kasus : Bapenda Provinsi Jawa Tengah)*. *21*(2), 210–229.

Christopher, J. (2021). *The Cybersecurity Maturity Model: A Means To Measure And Improve Your Cybersecurity Program*. FORBES. https://www.forbes.com/councils/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., Curtis, P., & Dolan, T. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, *February*, 1–76. https://apps.dtic.mil/sti/citations/AD1078768%0Ahttps://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0%0Ahttps://www.energy.gov/sites/prod/files/2019/08/f65/C2M2 v2.0 06202019 DOE for Comment.p

Curtis, P. D., & Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1–6. https://doi.org/10.1109/THS.2015.7225323

DOE. (2014). *Use of the NIST Cybersecurity Use of the NIST Framework & DOE C2M2*. https://energy.gov/sites/prod/files/2014/02/f7/Use-of-NIST-Cybersecurity-Framework-DOE-C2M2.pdf

Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An explanatory review on cybersecurity capability maturity models. *Advances in Science, Technology and Engineering Systems*, *5*(4), 762–769. https://doi.org/10.25046/AJ050490

Homeland Security. (2015). Energy Sector Cybersecurity Framework Implementation Guidance. *Department of Homeland Security*, *1*, 40.

Jauhari, M. A., Wardijono, B. A., & Hegarini, E. (2024). *Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan Framework Center for Internet Security Controls yang telah dilakukan . Perusahaan ini dalam bentuk infeksi ransomware yang menyebabkan kerugian besar termasuk mengenkripsi ata*. *14*(1), 72–83.

Krumay, B., Bernroider, E. W. N., & Walser, R. (2018). *Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework* (pp. 369–384). https://doi.org/10.1007/978-3-030-03638-6_23

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*, 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf%0Ahttps://doi.org/10.6028/NIST.CSWP.04162018

NIST | NCCoE. (2023). *Cybersecurity Capability Maturity Model to NIST Cybersecurity Framework Mapping*. Announcements. https://www.nccoe.nist.gov/news-insights/cybersecurity-capability-maturity-model-nist-cybersecurity-framework-mapping

President, T., Critical, I., & Cybersecurity, I. (2012). Presidential Documents. *Presidential Documents*, *78*(33), 11739–11744. https://doi.org/10.4324/9780203122273

Revision 06 Cybersecurity Capability Maturity Model (C2M2) Version 2.0 July 2021. (2021). *July*.

Safitri, E. H. N., & Kabetta, H. (2023). Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, 332–338. https://doi.org/10.1109/ICoCICs58778.2023.10277652

Sakinah, F., & Setiawan, B. (2014). *Manajemen Keamanan Layanan TI*. *3*(2), 2–7.

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). Studi Komparasi Framework Nist Dan Iso 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *6*(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Sugara, V. I., Syahrial, H., & Syafrullah, M. (2019). Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute of Standards and Technology (Nist) Cybersecurity Framework. *Komputasi: Jurnal Ilmiah Ilmu Komputer Dan Matematika*, *16*(1), 203–212. https://doi.org/10.33751/komputasi.v16i1.1591

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV : International Journal on Informatics Visualization*, *4*(4), 225–230. https://doi.org/10.30630/joiv.4.4.482

Tinungki, A. C. D., Sentinuwo, S. R., & Karouw, S. (2021). Analisa Tingkat Kematangan Penerapan Keamanan Informasi Pemerintah Kota Bitung Menggunakan Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika …. *Repo.Unsrat.Ac.Id*, 1–8. http://repo.unsrat.ac.id/2963/

Valavanis, S. (2024). Understanding Cybersecurity Maturity in Practice. *Journal of Information Systems*, *38*(3), 1–5. https://doi.org/10.2308/ISYS-2024-026