International Journal of Engineering & Technology, 9 (3) (2020) 779-784

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cybersecurity capability maturity models review and application domain

Adamu Abdullahi Garba [1] *, Aliyu Musa Bade [1], Muktar Yahuza [1], Ya'u Nuhu [2]

[1] Department of Computer Science, Yobe State University Damaturu, Nigeria
[2] Department of Computer Science, The Federal Polytechnic Damaturu, Nigeria
**Corresponding author E-mail: adamugaidam@gmail.com*

Abstract

Cybersecurity is a way of protecting organization critical assets, through the identification of cyber threats that can compromise the information stored, it involves the protection, identification, and responding to threats. The main aim of this article is to conduct an ample review of the published cybersecurity capability maturity models using a systematic review of published articles from 2014 to 2019. Features of Hal- vorsen and Conradi's taxonomy were adopted to explain the models identified. The results indicated adopting a model to a certain organization is not feasible. However, modification is required before implementation, as the cost of implementation is not available when conducting this research.

Keywords: *Cybersecurity Model; Maturity Model; Information Security; Cybersecurity.*

1. Introduction

The emergence of cybersecurity is mature as the transition of the computer, any information that is transmitted through the internet is at risk of getting compromised without the knowledge of the sender. The emergence of cybersecurity is subjected to the advancement of the cyber domain in the 1950s. Any information stored in cyber-space is subjected to intrusion, it includes financial, military, government, and individual. Security breaches occur as a result of the new development of either hardware or software. This new device results in new vulnerabilities. The field of cybersecurity emerged as a result of Robert Morris testing the worlds' network vulnerability in 1980 when he uses a virus he created to test the size of the internet, to protect organization assets, an organization needs to improve their cybersecurity practices. Many industries use cybersecurity capability maturity models that are used to assess the capability of cybersecurity in an organization and to position them at different levels. Most organizations have developed their maturity model to respond to their unique needs, therefore, capability maturity models are more specific than generic. This paper intends to answer the following objective:

- To identify currently available cybersecurity capability maturity models available for this study from 2014 to 2019.
- To identity the application of the cybersecurity capability maturity models among organizations.

The sections of the following paper include, section 1 as the introduction of the research objectives, also the review protocol applied during the research. Section 2 is the literature review, section 3 is the methodology adopted when conduction the research, section 4 critical review on the identified cybersecurity capability maturity, section 5 result, and analysis of the review, section 6 is the conclusion of the research and section 7 is the future research direction.

1.1. Review method

The systematic review has a repeatable process that provides all document studies relevant to a topic area or a particular research question [1]. SR is conducted to summarise existing evidence about a technology or a treatment or to support the creation of a novel hypothesis. However, [2], [3] provided, and approach for gaining a comprehensive way or method to answer questions of a broad field, relevant topic within this field of maturity models. Also [4], [5] advised mapping studies that are a method of conducting a systematic literature review. According to [1] SR involves some distinct activities which are: (i) formulate a review protocol, (ii) identify inclusion and exclusion criteria, (iii) illuminate the research strategy process; (iv) study the selection area, (v) quality consideration, (vi) use data extraction and synthesis. All the above mention distinct activates will be explained in the following section. The criteria of inclusion and exclusion for the researchers to follow when doing the study. This research considers the following articles (journal, conference, white paper, and workshops) published in English, also published from 2014 to 2019 in the digital database. Any article that doesn't fall under this range of years will not be included. Table 1 shows a summary of these criteria.

Copyright © Adamu Abdullahi Garba et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Table 1: Inclusion and Exclusion Criteria

Included article	Excluded article
Available text	Uncompleted Studies
Published within from 2014 – 2019	Outside range of the year
English journal	Non-English journal
Cybersecurity Model	Were outside domain
White papers	Not related to objectives

2. Literature review

The cybersecurity Capability maturity model (C2M2) has arisen from the capability maturity model been design from the quality management field in the 1930s. it becomes popular in the 1990s when it was first developed by software engineering institutions [6]. The model is later being adapted into many fields of studies to identify or measure the maturity level of an organization or process or even product quality as the widely known model called capability maturity model (CMM) which was for software industries which describes the key elements of an effective software development process[7]. Today all these models are basic on this basic model, the model has a set of a structured set of operations and activities that improve over time [8]. the model consists of a basic 5 process maturity level called, initial, repeatable, defined, managed, and optimizing [9]. Likewise [10] conducted a study regarding the capability maturity models in 2006, this research identified and compares many maturity models for software domain and product quality. The model was designed for software products as guidance as well as for management excellence in producing quality software[11]. Nevertheless, The C2M2 seeks to help support the cybersecurity capabilities of organizations and to help them efficiently measure their cybersecurity capabilities. The C2M2 is intended to be used by any organization to assess its cybersecurity capabilities dependably, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. [12]. "A Cybersecurity maturity model offers a framework for assessing the maturity of a security program and guidance on how to reach the next level." [13]. The cybersecurity maturity model provides a pathway that enables the organization to measure where they are along that path. This can be a valuable tool not only for improving Cybersecurity efforts but also for collaborating with upper management and getting the support needed to enhance Cybersecurity culture in organizations. There are many Cybersecurity Maturity Models from which to choose, Based on the systematic review performed regarding the currently available peculiar to Cybersecurity models published to the knowledge of the author from 2014 to 2019 are; Cybersecurity Capability Maturity Model (C2M2), Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), National Initiative for Cybersecurity Education-Cybersecurity Capability Maturity Model (NICE-C2M2), African union maturity model for cybersecurity (AUMMCS) and Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC- CMM).

3. Methodology

After conducting the review, the author has identified the following: C2M2, ES-C2M2, NICE-C2M2, FFIEC- CMM, and AUMMCS models. The author adapted 10 features from Halverson and Conradi taxonomy of software process improvement, (2001), this taxonomy consists of 21 features peculiar to software process and are grouped into 5 categories: general, process, organization, quality, and result. Each category refers to:

- General: this feature describes the overall attribute of improvement.
- Process: this feature explains the way the organization uses the features.
- Organization: this explains the relationship between the features and organization and how they work simultaneously.
- Quality: this explains the feature related to the quality dimension.
- Result: this explains the feature of the results as the result of using the environment, the cost of achieving the result.

In this paper, only adopted general, process, organization, and results as the other one has no relation to Cybersecurity Capability Maturity Models. The features that fall under each category is modified to suit Cybersecurity terms as shown in table 2 below.

Table 2: Halverson and Conradi Taxonomy

Category	Feature
General	Origin
	Purpose
	Maturity level
Process	Field Applicable
	Depth of assessment
	Assessment
Organization	Organization
	Organization Environment
Result	Implementation cost
	Validation

The features related to General group are defined below:

- Origin: this feature tells us which state, organization, the university that design the model
- Purpose: This feature explains the synopsis of the model design purpose
- Maturity level: this feature explains how many levels of maturity each model constitute

The features related to the process group are defined below:

- Field Applicable: this feature explain which environment the model is implemented
- Assessment: this feature helps us to know what the model is assessing in the implemented environment
- Depth of Assessment: this feature helps us to know whether the model is complex or simple based on the maturity level

The feature related to the organization group as defined below

- Organization Size: this feature helps us to understand the nature of the model in terms of size to know which organization will be applied to
- Organization Environment: this feature explain if the model is for the whole organizational activities or specific to the unit or department.

The feature related to result, the group is defined below

- Validation Method: this feature explain the method used for validating the model before release, and after to see it impact
- Implementation Cost: this feature shows the cost variation in implementing the model

The paper uses the following criteria to evaluate some of the define features above:

- Origin: this shows the country, lab, organization that created or design the model e.g. the US
- Maturity Level: the criteria identify the level of maturity for each model number 1- 5 are used, the more level a mode is the more level of the maturity increases
- Field Applicable: the criteria explains where the model is applicable criteria include: organization, paper lab. University
- Organization Size: the measure the size of the organization for appropriate adaption, criteria used here are: large, medium, small or all
- Organization Environment: the criteria "whole" is used if the model focuses on the entire organization while " Specific" if the model is on a specific unit or department in the organization
- Assessment: the feature is explained by the name of a process to be assessed in the organization e.g. risk, maturity.
- Validation Method: the criteria identifies the method of validation of the identified.
- Implementation Cost: this identified the budget for implementing the model in the organization.

4. Cybersecurity capability maturity models review

This section explains the maturity models based on their focus on cybersecurity and their structures. The identified models from the review are C2M2, ES-C2M2, NICE-C2M2, FFIEC-CMM, and AUMMCS models.

4.1. Cybersecurity capability maturity model (C2M2)

The Cybersecurity Capability Maturity Model was designed by Carnegie Mellon University in association with the US Department of Energy in 2014 [14]. The model consist of ten domains and each domain is a grouping of cybersecurity practices. Also, many objectives are grouped to be in one domain which represents achievements the model contains ten domains with grouped objectives and Maturity level of C2M2. Table 3 depicts the model domains and table 4 depicts the maturity level

Table 3: C2M2 Domain and Objectives

Domains	Grouped Objectives
Asset, Change and Configuration Management	Manage Asset inventory Manage Asset configuration Manage changes to Asset Management Activities
Cybersecurity Program Management	Established Cybersecurity Program Strategy Sponsor Cybersecurity Program Established And Maintain Cybersecurity Architecture Perform Secure Software Development Management Activities
Event and Incident Response, Continuity of Operation	Detect Cybersecurity Events Escalate Cybersecurity Events And Declare Incidents Respond To Incident And Escalated Cybersecurity Events Plan Continuity Management Activities
Identify and Access Management	Established And Maintain Identities Control Assess Management Activities
Information Sharing and Communications	Share Cybersecurity Information Management Activities
Risk Management	Established Cybersecurity Risk Management Strategy Manage Cybersecurity Risk Manage Activities
Situational Awareness	Perform Logging Perform Monitoring Established And Maintain A Common Operating Picture Management Activities
Supply Chain and External Dependencies Management	Identify Dependencies Manage Dependency Management Activities
Threat And Vulnerability Management	Identify And Respond To Threats Reduce Cybersecurity Vulnerabilities Management Activities
Workforce Management	Assign Cybersecurity Responsibilities Control The Workforce Life Cycle Develop a Cybersecurity Workforce Increase Cybersecurity Awareness Management Activities

Table 3: C2M2 Maturity Level Description

Maturity indicator level MIL	Level description
Level 0	This level has no practices or processes defined. There is no stable environment for activities. MIL 0 is given as a result of the domain objective not achieved.
Level 1	This level contains a set of initial practices. This level activities are usually ad hoc and chaotic. MIL 1 is scored if there is an initial practice performed

Level 2	This level has more stable practice compared to MIL, more confidence is achieved at this level as the result of the performance and is sustained over time.
Level 3	At MIL 3 policy is applied to the practices to further stabilize the operations in the organization and is guided by top- management directives. Also, the staff s' are fully trained and fully funded.

4.2. Electricity subsector cybersecurity capability maturity model (ES-C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model was developed by the department of energy USA for the protection of the electricity subsector from any form of cybersecurity attacks. [15]. This model was designed as a subsector of the C2M2 i.e. Independent guidance. Both models' general purpose is almost the same, which is to improve cybersecurity capabilities by allowing continuous Benchmarking. The ES-C2M2 threat and vulnerability incident are reported to electricity sector information sharing and analysis centers specifically [15]. The model was made for electricity sector organizations. Table 4 shows the model domain and it description.

Table 4: ES-C2M2 Domain Description

Domain	Description
Process and Analytics	This domain describes activities of the workforce planning as well as how those steps are integrated with other processes in the organization.
Integrated Governance	This represents activities linked to establishing a governance structure, guidance and driving decision making
Trained Professionals and Enabling Technology	This domain shows the activities related to creating a professional cadre of workforce planners in the organization, using technology to represent activities and use of data systems.

Table 5: ES-C2M2 Maturity Level

Maturity Level	Description
MIL 0 " Not Performed"	This level describes the domain has achieved nothing.
MIL 1 " Initial"	This level shows only initial practices are performed
MIL 2 "Performed"	The level is characterized by having well-documented practices, stakeholders' involvement, and provision of standards or guidelines for practice implementation.
Mil 3 "Managed "	This level shows all practices and activities are fully guided by policy, also practice is only assigned to adequate skills personal. The formed policy are periodically evaluated for improvement

Table 6: Nice Domain Description

Domain	Practices
Risk	Risk Assessment
Assets	Asset, Change, and Configuration Management
Access	Identity and Access Management
Threat	Threat and Vulnerability Management
Situation	Situational Awareness
Sharing	Information Sharing And Communication
Response	Event And Incident Response, Continuity Of Operations
Dependences	Supply Chain And External Dependencies Response Management
Workforce	Workforce Management
Cyber	Cybersecurity Program Management

4.3. National initiative for cybersecurity education capability maturity model (NICE)

The NICE model was designed under the directives of the then US President George Bush under the directive of national security in 2008, [16]. The model was designed specifically to select the staff with cybersecurity background

Table 7: Nice Maturity Level

Maturity level	Description
Limited level	This level shows an organization's cybersecurity capability is in the initial stage, having few established processes less guidance, less or no structural data, and method of analysis. Marcelo et al., (2018).
Progressing level	This level describes certain infrastructures are established and workforce planning have been fully performed
Optimized level	This level is associated with fully developed workforce planning, and are united organization other business processes. Workload analysis is carryout which assists in decision making in the organization regarding cybersecurity

4.4. Federal financial institute of examination council capability maturity model (FFIEC-CMM)

The Federal Financial Institute of Examination Council Capability Maturity Model was made available to direct them in creating the complexity of the cyber risk landscape. The model is considered as an assessment tool to help managers assess their institution's cybersecurity readiness, evaluate its risk, and determine what risk management practices and controls are needed to attain the desired state. This tool has two-part as shown below.

- The Inherent Risk Profile: these are risks posed to the organization by technologies and connection types, delivery channels, online and mobile products, and other external threats.
- Cybersecurity Maturity: this helps the organization to measure the level of risk and corresponding controls. The level starts from baseline to innovation. The model contains five domains and some assessment factors.

4.5. African union maturity model for cybersecurity (AUMMCS)

The African union maturity model for cybersecurity was made available in 2014 by the center for the cyber Security University of Johannesburg on security and protection of personal data, at the convention of African member states, this model covers three sections: electronic

transactions, personal data protection and promoting cybersecurity and combating cybercrime [17]. The model was future to help member states of the African Union to assess their cybersecurity status against a specific part of the convention. This model can be utilized in two ways: one as a self-assessment by a specific country against the specification of the convention, two as an evaluation by the AU between different member states in other to see how they compare as far as the requirements are concerned. Also, it covers the promotion of cybersecurity and combating cybercrime[17].
The model has four objectives.

- A national culture of cybersecurity does exist.
- A national Cybersecurity policy does exist
- Public-private partnerships, initiated by the government, do exist

Cybersecurity capacity building on all levels, driven by the government, does exist.

Table 8: AUMMCS Maturity Decryption

Maturity levels	Description
ML0	Nothing Exists At All
ML1	Very Basic Position
ML2	Progressed Position
ML3	Stable Position

5. Results and analysis

This section shows a well and detailed evaluation on the models in form of comparisons using the adopted taxonomy features from Halverson and Conradi's taxonomy of software process improvement, these features are used to determine how the models are made up of and also how they can be used in an organization and what organization can use them. Table 9 shows the identified model and the features select from the Halverson and Conradi's taxonomy.

Table 9: Comparative Review on Cybersecurity Models

Model / Features	C2M2	ES-C2M2	NICE-C2M2	FFIEC- CMM	AUMMCS
Origin	USA	USA	USA	US Federal Financial Institute Of Examination Council	Centre For Cyber Security At The University of Johannesburg
Maturity level	4	3	3	5	4
Purpose	Assessment of cybersecurity capabilities for any organization comprises of a maturity model evaluating a tool	Tailored to energy subsector	Tailored to three areas: process and analytics, integrated governance, skilled practitioners	Tailored to as assessment tools to identify organizational risk and determine their cybersecurity maturity	Tailored to ensuring citizens and government and business are protected African member states
Organization Size	large	large	large	large	All
Organization Environment	whole	whole	Specific	Specific	Specific
Depth of Assessment	Specific	Specific	General	Specific	General
Field Applicable	Organization	Electricity	Workforce	Financial	African states
Assessment	Organization maturity	Electricity grid protection	Organization maturity	Organization maturity	Data protection
Validation	Surveys and case studies	Surveys and case studies	Surveys and case studies	Surveys and case studies	Nil
Implementation Cost	Nil	Nil	Nil	Nil	Nil

Note: Nil means yet to be determined

Table 9 shows the comparisons of the identified models, these models have quite many similarities. These similarities include cybersecurity orientation, maturity models, and organizational size this indicated shows objective one of the research is identified. Based on table 9, it indicated cybersecurity capability maturity model are applied in many organizations, but mostly organization with critical assets uses the model for cyber threat protection, this analysis shows that objective two is achieved. However, there are some areas to which they differ, these areas include the depth of assessment and the field of application. The results further show in the investigation of the models includes the following

- Most models are more specific than generic.
- The adoption of a model appears to be impossible as most models are designed on a particular purpose.
- Implementation cost is not identified, as there is a lack of valid assessment on the implementation.

6. Conclusion

Cybersecurity capability maturity models are widely used in many organizations for protecting their assets against any threats, however, there is still limited research on the area as is considered to be new. This indicated a need to know the current models and their mode of assessment. The models identified are fully based on cybersecurity but adopting can be impossible. These comparisons tables give a clear view of all the models and how to choose an appropriate model for an organization based on the features used. Lastly. All models found

after the SR lacks cost implementation, therefore, to know how much to spend for implementing any model depends highly on the size of the organization and the number of critical assets to be protected.

7. Research direction

This paper clarified the C2M2 properties and shows their similarities and applications domain, based on the reviews of all the available models, no any author explain the implementation cost. Therefore, future research can focus on how cybersecurity capability maturity models cost of implementation is in an organization as no model explains the financial standpoint of the implementation.

Acknowledgment

This journal would not have been possible without the exceptional support of the institution. We would also like to thank all the reviewers that gave their comments to make this paper suitable to the public.

References

[1] Kitchenham. Guidelines for performing Systematic Literature Reviews in Software Engineering [Internet]. Durham Durham, UK; 2007. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471&rep=rep1&type=pdf
[2] Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J, Linkman S. Systematic literature reviews in software engineering - A systematic literature review. Inf Softw Technol [Internet]. 2009;51(1):7–15. Available from: https://doi.org/10.1016/j.infsof.2008.09.009.
[3] Webster J, Watson RT. Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Q. 2002;26(2):xiii–xxiii.
[4] MAREW T, KIM J, BAE DH. Systematic Mapping Studies in Software. Int J Softw Eng Knowl Eng. 2007;17(1):33–55. https://doi.org/10.1142/S0218194007003112.
[5] Kitchenham BA, Budgen D, Pearl Brereton O. Using mapping studies as the basis for further research - A participant-observer case study. Inf Softw Technol [Internet]. 2011;53(6):638–51. Available from: https://doi.org/10.1016/j.infsof.2010.12.011.
[6] Paulk MC. A History of the Capability Maturity Model for Software. Softw Qual Profile. 2009;1(1):5–19.
[7] Goksen Y, Cevik E, Avunduk H. A Case Analysis on the Focus on the Maturity Models and Information Technologies. Procedia Econ Financ [Internet]. 2015;19(15):208–16. Available from: https://doi.org/10.1016/S2212-5671(15)00022-2.
[8] Weber C V, Garcia SM, Bush M. Key Practices of the Capability Maturity Model. 1993.
[9] Adler RM. A dynamic capability maturity model for improving cyber security. 2013 IEEE Int Conf Technol Homel Secur HST 2013. 2013;230–5. https://doi.org/10.1109/THS.2013.6699005.
[10] Budgen D, Turner M, Brereton P, Kitchenham B. Using Mapping Studies in Software Engineering. Ppig [Internet]. 2008;2:195–204. Available from: http://www.ppig.org/papers/20th-budgen.pdf.
[11] White GB. The Community Cyber Security Maturity Model The Center for Infrastructure Assurance and Security. Proc 40th Hawaii Int Conf Syst Sci. 2007;(June):1–8. https://doi.org/10.1109/HICSS.2007.522.
[12] Curtis PD. Evaluating and Improving Cybersecurity Capabilities of the Energy Critical Infrastructure. 2015 IEEE Int Symp Technol Homel Secur. 2015;1–6. https://doi.org/10.1109/THS.2015.7225323.
[13] Johnson L. Cybersecurity framework. Secur Control Eval Testing, Assess Handb. 2020;(February 2014):537–48. https://doi.org/10.1016/B978-0-12-818427-1.00012-4.
[14] Miron W, Muita K. Technology Innovation Management Review Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. Technol Innov Manag Rev [Internet]. 2014;4(October):33–9. Available from: www.timreview.ca. https://doi.org/10.22215/timreview/837.
[15] Sorini A, Staroswiecki E. 8. Cybersecurity for the Smart Grid [Internet]. The Power Grid. Elsevier Ltd; 2017. 233–252 p. Available from: https://doi.org/10.1016/B978-0-12-805321-8.00008-2.
[16] Angel Marcelo Rea-Guaman, Tomás San Feliu JAC-M and IDS-G. Comparative Study of Cybersecurity Capability Maturity Models Angel. Comput Stand Interfaces Softw Process Improv Capab Determ Conf 2017. 2018;60:1–2.
[17] Von Solms SHB. A maturity model for part of the African Union Convention on Cyber Security. Proc 2015 Sci Inf Conf SAI 2015. 2015;1316–20. https://doi.org/10.1109/SAI.2015.7237313.