Evaluations of Information Security Maturity Models

Measuring the NIST Cybersecurity Framework Implementation Status

Alsaleh, Majeed
King Fahd University of Petroleum and Minerals.(KFUPM), Dhahran, Saudi Arabia
e-mail: g198925300@kfupm.edu.sa

Niazi, Mahmood
King Fahd University of Petroleum and Minerals.(KFUPM)., Dhahran, Saudi Arabia
e-mail: mkniazi@kfupm.edu.sa

***Abstract*—Many organizations with critical infrastructure sectors and other businesses have started to adopt the National Institute of Standards and Technology (NIST) cybersecurity framework. As cybersecurity is a long-term investment, organizations adopting the framework need to sustain their cybersecurity capabilities and ensure growth toward the maturity level needed to deliver the desired outcome. Therefore, the maturity capability of the cybersecurity program needs to be assessed regularly. Several capability maturity models can be used to measure the progress of implementing the cybersecurity program. However, attempts are still being made to define a capability maturity model to be used specifically for measuring the cybersecurity programs that adopt the NIST cybersecurity framework. With the aim of identifying and applying evaluation criteria, this paper reviews multiple existing maturity models and compares their scale levels definitions and the used assessment methodology. The researchers determined the criteria based on subject matter experts' feedback. A survey was conducted to define the values of the criteria that organizations are looking for in order to select the best-fit capability maturity models to use in measuring the progress of NIST CSF implementation.**

Keywords-cyber security; information security; maturity model; measurement metrics.

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) issued the Cyber Security Framework (CSF) in 2014 [1] as a response to the Executive Order signed by President Obama on February 12, 2013 [2]. This framework was quickly adopted by many organizations around the world. In a study by Gartner [3], the framework was expected to grow in usage from 30% in 2015 to 50% by 2020. However, after the Executive Order signed by President Trump on May 11, 2017 [4], the framework is expected to be adopted by more organizations worldwide. The executive order clearly places the accountability for managing the cybersecurity risk on the heads of executive departments operating critical infrastructure and heads of federal agencies; thus making the compliance to the framework requirements involuntarily. The growth of the framework implementation has been fast outside the United States of America too. For example, many Oil and Natural Gas (ONG) companies around the world have adopted the framework [5].

The NIST issued an update to the framework, with new features added and more clarifications for some of the terms used to measure cybersecurity such as, the term compliance [6]. The update also addressed the supply chain as one new cybersecurity category was added to the previous 22 categories. Moreover, the link between the framework and the Internet of Things (IoT) was established as a possible area of risks associated with operational technology and cyber-physical system environments [7]. Table I below summarizes the structure of the core components of the framework along with the key changes and updates in the new version of the framework.

TABLE I: FRAMEWORK VERSIONS COMPARISON

Version	Functions	Categories	Sub-categories	Informative References
V1.0 [1]	5	22	98	5
V1.1 [6]	5	23	108	5

One of the key changes in the new version of the framework emphasizes the role of cybersecurity risk management measurement (cost vs. benefit) in a newly added section called "Self-Assessing Cybersecurity Risk". Moreover, the NIST officially recognized the importance of measuring cybersecurity by including it as an item on the Roadmap for Improving Critical Infrastructure Cybersecurity. Using the framework components will enable organizations to measure their risk along with the cost and benefits of mitigating it while deciding which level of risk (risk tier out of the four risk tiers) is acceptable to the organization. This is determined by considering many factors including legal regulatory requirements, the threat environment, and an organization's current risk management practices. The framework suggests leveraging external guidance such as, existing Capability Maturity Models (CMMs) to allow organizations to measure the status of their NIST CSF implementation progress [8].

However, there are varieties of CMMs that may or may not be associated with specific best practices standards or frameworks. For example, industry best practices standards, such as, Control Objectives for Information and Related Technologies (COBIT) and the Information Security Forum (ISF) Standard of Good Practice (SoGP) for Information Security have their own Maturity Models (MMs) that can be utilized to measure the NIST CSF implementation progress [9] [10]. On the other hand, the Systems Security Engineering Capability Maturity Model (SSE CMM) [11], Capability Maturity Model Integration (CMMI) [12], ONG subsector Cybersecurity Capability Maturity Model (ONG C2M2) [13], Information Security Management Maturity Model (ISM3) [14], and Community Cybersecurity Maturity Model (CCSMM) [15] are examples of MMs that can be used to measure the implementation of any given framework. Worth noting is that the wide range of NIST CSFs adopted not only spans many organizations but also covers more areas such as, building cybersecurity [17] and cyber cloud security [18].

Therefore, due to the varieties of available CMMs, organizations may lose some benefits of using a unified CMM or compatible ones that allow smooth mapping to the NIST CSF framework. For example, an organization may not get an accurate progress update if it does not use the same CMM for identifying the baseline (where it stands currently) and the desired higher levels of cybersecurity maturity over time. This is due to various difficulty levels of mapping each CMM to the NIST CSF framework and vice versa [19]. Benchmarking is another benefit that might not be possible if organizations not using a unified CMM or compatible ones that allow smooth mapping to the NIST CSF framework.

This paper's main objective is to identify and apply evaluation criteria through reviewing multiple existing MMs and comparing their scale levels definitions and their used assessment methodologies. The researchers sought the feedback of Subject Matter Experts (SME) through a survey to define the criteria for selecting the best-fit CMMs that can be used in measuring the NIST CSF implementation progress.

This paper consists of seven sections: The first section is the Introduction, and the second section provides an overview of the NIST CSF framework and its components, Section III reviews seven CMMs, Section IV reviews and compares the levels of the CMMs, Section V discusses the survey, Section VI analyzes the survey results, and Section VII is the Conclusion.

II. The NIST Framework Components

The NIST CSF has three components: 1) the profile, 2) the risk tiers, and 3) the core functions [6]. The three components can be utilized by organizations in a variety of ways, considering the current situation of the organization, that is, whether they are at the very initial stages of implementing a cybersecurity program or are already adopting existing best practices and standard frameworks. The framework is not meant to be a substitute for any existing cybersecurity program of the organization, but to complement and allow for more improvement opportunities to strengthen the cybersecurity program.

A. The Profile Component

This component of the framework is considered the tool for capturing the organization's current cybersecurity status. It is utilized to document the current and the planned risk tiers and determine which of the cybersecurity activities should be selected for implementation in improving the current situation and to track progress to achieve the desired security status.

B. The Risk Tiers Component

The risk approach followed by an organization for managing the cybersecurity risk and the processes in place influence the organization's placement in one of the four risk tiers defined by this component. Yet the risk tiers do not indicate the maturity of the cybersecurity program of the organization [6] [8] [20].

C. The Core Functions Component

The core functions component is the part of the framework where all controls are listed as "subcategories". The latest version of the framework [6] has 108 subcategories as against the 98 subcategories of the previous version [1]. The subcategories account for 23 categories that can be looked at as processes of cybersecurity activities or objectives to be achieved by implementing some or all subcategories.

While the previous version of the framework has 22 categories, the new version has added one more to address the supply chain. The categories then make the core five functions: Identify, Protect, Detect, Respond, and Recover. The five functions shape the high-level and strategic view of the organization's efforts in managing its cybersecurity risk and the implemented cybersecurity program. Table II provides examples of the subcategories of the framework.

TABLE II. EXAMPLES OF SUBCATEGORIES OF THE NIST CSF FRAMEWORK

Function	Category	Sub-Categories
Protect	(PR.DS) Data Security	PR.DS-1: Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

ISBN: 978-1-61208-893-8

III. Capability Maturity Models

This section will review the selected CMMs and analyze their levels, domains, and assessment methods.

A. *Community Cyber Security Maturity Model (CCSMM)*

This model was originally designed to measure the capability maturity of cybersecurity practices run by communities [15]. It is not meant to assess individual organizations, though it was also extended later to cover organizations and states. The model is structured to address the improvement of four areas on a scale of five levels [16]. The improvement areas are called dimensions, namely planning, policies, awareness, and information-sharing. The maturity of these dimensions is measured in five levels starting with "Initial" as the lowest level, through "Established", "Self-Assessed", and "Integrated" till "Vanguard", which is the highest maturity level. The model uses assessment criteria that help check the level of the community with respect to the four dimensions, which range from minimal or little at the initial level to mandatory, fully integrated, full-scale, or "vanguard", which is the fifth level. The scale levels and the dimensions are measured as per the satisfaction of the criteria used to verify the status of cybersecurity implementation. Table III illustrates the criteria of the CCSMM.

B. *Information Security Management Maturity Model (ISM3)*

This model was originally designed as an extension of quality management, that is, ISO 9001 for Information Security Management (ISM) systems, to focus on the common cybersecurity processes of organizations and not on controls. As an extension of the quality assurance standard, the ISM3 is used to build a quality assurance process framework [14]. The five ISM system configuration levels are like maturity levels that measure organizations' progress in implementing cybersecurity programs.

The five maturity levels of the model are 1) undefined, 2) defined, 3) managed, 4) controlled, and 5) optimized. The domains of the models are grouped into the following four categories, each of which includes the required processes for achieving every maturity level:

1. General (3 processes)
2. Strategic management (6 processes)
3. Tactical management (11 processes)
4. Operational management (25 processes)

This model provides optional certifications related to ISO 9001 at each maturity level and ISO 27001 at Levels 4 and 5. Table IV illustrates the processes used in the ISM3.

TABLE III. CCSMM Criteria For Verifying Cybersecurity Maturity

5. Vanguard	Awareness is mandatory by the business	Fully integrated	Full-scale combined exercises and assessment of complete fusion capability	Continue to integrate cyber in Continuity of Operations Plans (CO-OP)
4. Integrated	Leaders and organizations promote awareness	Formal information-sharing internal and external to the community	Self-directed cyber exercises with assessment	Integrate cyber in CO-OP
3. Self-Assessed	Leaders promote awareness	Formal local information sharing	Self-directed tabletop cyber exercises with assessment	Include cyber in COOP; formal cyber incident response/recovery
2. Established	Leadership is aware of cyber threats	Informal information-sharing	No assessment but aware of requirements	Aware of the need to integrate
1. Initial	Minimal cyber awareness	Minimal information-sharing capabilities	Minimal cyber assessments and policy evaluations	Little inclusion of cyber in the community's COOP
Levels\ Diminutions	Awareness	Information Sharing	Policies	Plans

TABLE IV. ISM3 CRITERIA FOR VERIFYING THE PROCESS CAPABILITY MATURITY

<table>
<tr><td>5. Optimized</td><td colspan="22">for a <b>high investment</b> in ISM processes that are managed to result in a <b>highest</b> risk reduction with <b>compulsory use of process metrics</b></td></tr>
<tr><td>4. Controlled</td><td colspan="22">for a <b>high investment</b> in ISM processes that are managed to result in a <b>highest</b> risk reduction</td></tr>
<tr><td>3. Managed</td><td colspan="22">for a <b>significant investment</b> in ISM processes that are managed to result in a <b>highest</b> risk reduction</td></tr>
<tr><td>2. Defined</td><td colspan="22">for a <b>moderate investment</b> in ISM processes that are managed to result in a further risk reduction</td></tr>
<tr><td>1. Undefined</td><td colspan="22">for a <b>minimum investment</b> in <b>essential</b> ISM processes that are managed to result in a significant risk reduction</td></tr>
<tr><td rowspan="2"><b>Levels\</b>
<b>Categories</b></td><td>GP1</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>SSP1</td><td>.</td><td>.</td><td>.</td><td>SSP6</td><td>TSP1</td><td>.</td><td>.</td><td>.</td><td>TSP11</td><td>OSP1</td><td>.</td><td>.</td><td>.</td><td>.</td><td>OSP2</td></tr>
<tr><td colspan="6">General</td><td colspan="5">Strategic Management</td><td colspan="5">Tactical Management</td><td colspan="6">Operational Management</td></tr>
</table>

C. Process Assessment Model (PAM) for the COBIT Framework

PAM is a process capability base assessment model for assessing information technology enterprises' implementation of COBIT 5 [9] [21]. The model is structured to address the improvement of 37 processes on a scale of six levels [14]. The 37 processes are defined and classified into five categories (domains). Each process is assessed against nine pre-defined attributes distributed among the maturity levels.

A standard rating scale of four status levels is used to further evaluate and score each attribute as defined in the ISO/IEC 15504 standard [14]. The rating scale measures and scores the percentage of achievement; it considers a process in achievement range from 0 to 15% as "not achieved", a process in achievement range between 15% and 50% as "partially achieved", a process in achievement range between 50% and 85% as "largely achieved", and process in achievement range between 85% and 100% as "largely achieved". The levels commence with Level 0 that indicates "Incomplete Process" and then Levels 1 to 5 to indicate the statuses of "Performed Process", "Managed Process", "Established Process", "Predictable Process", and "Optimizing Process", respectively.

The 37 processes have been classified under the five categories as follows:

1. Evaluate, Direct, and Monitor (5 processes)
2. Align, Plan, and Organize (13 processes)
3. Build, Acquire, and Implement (10 processes)
4. Deliver, Service, and Support (6 processes)
5. Monitor, Evaluate, and Assess (3 processes)

Table V illustrates the attributes used in the PAM.

D. Information Security Forum (ISF) Standard of Good Practice (SoGP) for Information Security

The ISF MM assesses, in combination, the activities performed and the supporting processes' capabilities [10]. The maturity level is an indication of how comprehensive the implementation of high-level activities is along with the capabilities of the processes supporting the activities that maintain and sustain the performance consistency and effectiveness. The model is structured to assess the processes' capabilities by evaluating the 21 domains in which each domain covers one information security discipline. The 21 domains are grouped into the following five strategies:

1. People (2 domains)
2. Strategic (6 domains)
3. Technical (6 domains)
4. Connections (2 domains)
5. Crisis (5 domains)

The model uses a scale of six levels that starts with Level 0, which indicates that the process is "Incomplete". Levels 1 to 5 represent the following process statuses: "Performed", "Planned", "Managed", "Measured", and "Tailored". The maturity level is defined by the number of requirements to be met in each activity. A standard rating scale of three status levels is used to further evaluate and score each activity. The rating scale measures and scores the percentage of requirements met; it considers the implementation of 0 to 15% requirements as "Not Met", implementation between 15%

TABLE V. PAM CRITERIA FOR VERIFYING THE PROCESS CAPABILITY MATURITY

5. Optimizing	Process: 1) Innovation 2) Optimization				
4. Predictable	Process: 1) Measurement 2) Control				
3. Established	Process: 1) Definition 2) Deployment				
2. Managed	1) Performance management 2) Work product management				
1. Performed	1) Process performance				
0. Incomplete	No attributes				
Levels\ Categories	Evaluate, Direct and Monitor	Align, Plan and Organize	Build, Acquire, and Implement	Deliver, Service, and Support	Monitor, Evaluate, and Assess

and 85% of requirements as "Partially Met", and implementation of more than 85% of requirements as "Met".

Table VI illustrates the assessment criteria of the ISF MM.

E. Systems Security Engineering Capability Maturity Model (SSE CMM)

The SSE MM was developed to address the absence of a comprehensive framework for evaluating security engineering practices in order to measure and improve the performance of security engineering principles [11]. The model's scope is the security engineering secure system lifecycle, from designing to commissioning and decommissioning. Thus, this model can be applied to organizations that provide security engineering services.

The model was designed to be a fixable tool that can measure process improvement, process capability, or the trustworthiness of the process outcome.

The model has been structured to assess process capabilities by evaluating all the practices (called best practices)

TABLE VI. ISF MM CRITERIA FOR VERIFYING PROCESS CAPABILITY MATURITY

5. Tailored	The activity is performed, planned, managed, measured, and subject to **continuous improvement. It is tailored** to specific areas.																	
4. Measured	The activity is performed, planned, managed, and is **monitored.**																	
3. Managed	The activity is performed and planned, and there are sufficient organizational resources to support and **manage** it.																	
2. Planned	The activity is performed and supported by **planning** (which includes the engagement of stakeholders and relevant standards and guidelines)																	
1. Performed	The activity is **performed.**																	
0. Incomplete	The activity is **not** performed.																	
Levels\ Categories	D1	D2	.	.	D6	D7	.	.	D12	D13	D14	D15	.	.	.	D19	D20	D21
	Strategic					**Technical**				**Connections**		**Crisis**					**People**	

under each process. The model uses a scale of six levels that begins with Level 0, which indicates that the process is “Not Performed”. Levels 1 to 5 represent the following process statuses: “Performed Informally”, “Planned and Tracked”, “Well Defined”, “Qualitatively Controlled”, and “Continuously Improving”, respectively. The model assesses about 60 security practices that are classified under 11 process domains that address the major areas of security engineering.

Moreover, the model has been expanded to assess over 60 practices performed under 11 process domains in the project and organizational areas. The model uses general assessment criteria that check the capability of the process based on the applied practices. Table VII illustrates the assessment criteria for SSE CMM.

TABLE VII. SEE CMM CRITERIA FOR VERIFYING PROCESS CAPABILITY MATURITY

<table>
<tr><td>5. Continuously Improving</td><td colspan="7">Improving Organizational Capability</td></tr>
<tr><td>4. Qualitatively Controlled</td><td colspan="7">Establishing Measurable Quality Goals
Objectively Managing Performance</td></tr>
<tr><td>3. Well Defined</td><td colspan="7">Defining a Standard Process
Performing the Defined Process
Coordinating the Process</td></tr>
<tr><td>2. Planned and Tracked</td><td colspan="7">Planning Performance
Disciplined Performance
Verifying Performance
Tracking Performance</td></tr>
<tr><td>1. Performed Informally</td><td colspan="7">Base Practices are Performed</td></tr>
<tr><td>0. Not Performed</td><td colspan="7">No process is performed</td></tr>
<tr><td rowspan="2"><b>Levels\ Categories</b></td><td>PA1</td><td>.</td><td>.</td><td></td><td>PA11</td><td>.</td><td>PA22</td></tr>
<tr><td colspan="4">Security Engineering Process Areas</td><td colspan="3">Project and Organizational Process Areas</td></tr>
</table>

F. Capability Maturity Model Integration (CMMI)

The new version of the CMMI was announced by the CMMI institute in early 2018 [12]. After expanding the model to include services and supplier management later in the same year, the model now consists of 22 process areas grouped into four categories: project management, process management, engineering, and support [12]. The model’s objective is to build organizational capability for improving performance for their selected activities, which may include cybersecurity.

The model is structured to assess the process categories by evaluating all 22 practices under each process area. The model uses a scale of five levels, which includes Level 1 “Initial” that indicates that no process area has been performed. Levels 2 to 5 represent the process statuses of “Managed”, “Defined”, “Quantitatively Managed”, and “Optimizing”.

The model assesses the 22 process areas that are performed and distributed over the four maturity levels (Levels 2 to 5). The distribution of the process areas is as follows: 7 in maturity level 2, 11 in maturity level 3, 2 in maturity level 4, and 2 in maturity level 5. Each process area consists of best practices, guidance, or activities to be performed. Table VIII illustrates the assessment criteria for CMMI.

G. Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG C2M2)

This model was originally designed as a derivative of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to serve the ONG subsector [13]. The model has been structured to address the implementation of a set of cybersecurity practices, grouped into 10 domains, on a scale of four levels.

Each domain consists of a number of practices that are categorized into the following groups of objectives:

1. Risk Management (three objectives)
2. Asset, Change, and Configuration Management (four objectives)
3. Identity and Access Management (three objectives)
4. Threat and Vulnerability Management (three objectives)
5. Situational Awareness (three objectives)
6. Information Sharing and Communications (two objectives)
7. Event and Incident Response, Continuity of Operations (five objectives)
8. Supply Chain and External Dependencies Management (three objectives)
9. Workforce Management (five objectives)
10. Cybersecurity Program Management (five objectives)

Each domain is assessed independently and scored cumulatively where all the practices in a given level and its predecessor levels are implemented. Unlike other MMs, ONG C2M2 defines a different set of evaluation criteria for each objective to verify the implementation of practices. Table IX provides examples of the evaluation criteria for one objective.

TABLE VIII. CMMI CRITERIA FOR VERIFYING PROCESS CAPABILITY MATURITY

5. Optimizing	1. Causal Analysis and Resolution 2. Organizational Performance Management			
4. Quantitatively Managed	1. Organizational Process Performance 2. Quantitative Project Management			
3. Defined	1. Decision Analysis and Resolution 2. Integrated Project Management 3. Organizational Process Definition 4. Organizational Process Focus 5. Organizational Training		6. Product Integration 7. Requirements Development 8. Risk Management 9. Technical Solution 10. Validation 11. Verification	
2. Managed	1. Configuration Management 2. Measurement and Analysis 3. Process and Product Quality Assurance 4. Project Monitoring and Control 5. Project Planning 6. Requirements Management 7. Supplier Agreement Management			
1. Initial	No process area has been addressed			
Levels\ Categories	PA1	. . . PA11	. . . .	. . . . . PA22
	Process Management	Project Management	Engineering	Support

TABLE IX. EXAMPLES OF EVALUATION CRITERIA FOR ONG C2M2 OBJECTIVES

	Manage Asset Configuration
MIL1	a. Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly.
	b. Configuration baselines are used to configure assets at deployment.
MIL2	c. The design of configuration baselines includes cybersecurity objectives.
MIL3	d. Configuration of assets are monitored for consistency with baselines throughout the assets' life cycles.
	e. Configuration baselines are reviewed and updated at an organizationally defined frequency.

The model maturity scales, called Maturity Indicator Levels (MILs), include MIL 0, which indicates that no practice has been performed, and MILs 1 to 3, which indicate the statuses of "performed but Ad-hoc", "Defined and Resourced", and "Governed and Effectively Resourced", respectively.

IV. SCALE LEVELS OF CAPABILITY MATURITY MODELS

Table X compares the seven CMMs and gives an insight into the similarity of the descriptions and the meanings of the levels.

A. *Level 1: Practice Existence*

All CMMs define the first level as the mere existence of the assessed practice in the organization. However, each CMM leverages a slightly different language to convey the same meaning. SSE focuses on the "base practices" that are categorized by the statement "you have to do it before you can manage it." Whereas, both ISF and ONG focus on the concept of "performed practices" to emphasize their existence. Finally, PAM requires processes to be "implemented"

TABLE X. A COMPARISON OF THE LEVELS OF CMMS

Levels/ CMM	Level 1	Level 2	Level 3	Level 4	Level 5
SSE CMM [11]	Performed Informally	Planned and Tracked	Well Defined	Quantitatively Controlled	Continuously Improving
PAM [21]	Performed Process	Managed Process	Established Process	Predictable Process	Optimizing Process
ISF [10]	Performed	Planned	Managed	Measured	Tailored
CMMI [12]	Initial	Managed	Defined	Quantitatively	Optimizing Managed
CCSMM [15]	Initial	Established	Self-Assessed	Integrated	Vanguard
ISM3 [14]	Undefined	Defined	Managed	Controlled	Optimized
ONG [13]	Performed but Ad-hoc	Defined and Resourced	Governed and Effectively Resourced	N/A	N/A

due to its process-oriented nature. It is worth noting that such processes are not required to be documented at this level by the PAM. This is also true for the ONG model, as practices are explicitly stated to be "ad-hoc". This formality aspect is less clear in the other models, though it can be implicitly inferred by contrasting this particular level with the next levels. Cybersecurity can be assessed against this level for the presence of its core best practices. Therefore, a cybersecurity CM would consider this level as the first level.

B. Level 2: Practice Formalization

Apart from SSE, all CMMs define this level around formalizing practices by involved stakeholders through documenting and endorsing process/procedure requirements such as, inputs/outputs, clear roles and responsibilities, and planning of resources. Cybersecurity can be assessed against this level for the formalization of its core best practices into organization-wide processes/procedures. Therefore, a cybersecurity CM would consider this level as its second level. SEE, on the other hand, defers this level to the third level and requires an intermediate level before practice formalization, which is focused on project-level formalization. Projects are regarded by the SSE as learning opportunities for the organization, from which formal processes/procedures are later established. Common lessons learned are the basis for the later formalized processes/procedures. Projects can be formalized similar to processes/procedures, though only at the project level.

Other CMMs implicitly consider this intermediate level as part of Level 1. Such projects can be seen as more than ad-hoc practices but also less than formalized processes/procedures. Projects tend to have a shorter lifespan and are more focused on the group of practices. Whereas, processes/procedures tend to have a much longer lifespan and apply to the whole organization. Therefore, it is safe to include this SSE level under Level 1 by expanding the definition of existent practices to ad-hoc and formalized projects.

C. Level 3: Practice Governance

Again, except SSE, all CMMs define this level as establishing governance over formalized practices by defining and enforcing organizational structures with proper authority/accountability, policies/standards/guidelines, and job specifications in terms of required knowledge/skills. This level is as far as ONG goes; hence, it lacks the subsequent levels. PAM, however, extends the definition of this level by requiring a certain degree of the Planning, Doing, Checking, and Adjusting (PDCA) lifecycle for a more flexible and agile style of governance. Cybersecurity can be assessed against this level for the governance of formalized organization-wide processes/procedures. Therefore, a cybersecurity CM would consider this level as its third level.

D. Level 4: Practice Monitoring

All CMMs, excluding the ONG one, define this level around the quantification of outcomes by governed processes/procedures against organizational goals using metrics for measuring performance and enabling informed optimizations based on facts. Stockholders set the operational limits of these metrics and are kept informed on the metrics on an agreed-upon regular basis. Cybersecurity can be assessed against this level for the monitoring of governed processes/procedures. Therefore, a cybersecurity CM would consider this level as its fourth level.

E. Level 5: Practice Optimization

All CMMs, excluding the ONG one, define this level as the requirement of regular/continuous improvement cycles of monitored processes/procedures. This level is associated with operational excellence programs in first-class worldwide companies, which satisfy their specific/unique needs. Improvements are based on data from monitoring desired operational limits. It is important to note that improvement must be sustainable over a considerable number of years to claim this level. Cybersecurity can be assessed against this level for the optimization of monitored processes/procedures. Therefore, a cybersecurity CM would consider this level as its fifth level.

V. EVALUATION CRITERIA

To identify the best fit CMM for measuring the maturity of organizations that are adopting or planning to adopt NIST CSF, we sought the opinions of SMEs. Interviews were conducted with four SMEs in the field of cybersecurity, information security management, information systems audits, and internal control management. The feedback of the interviews was analyzed, and the common areas of focus were combined to draft the survey questions. The drafted survey focused on four aspects related to the CMM: the scale, domains, assessment criteria, and administration.

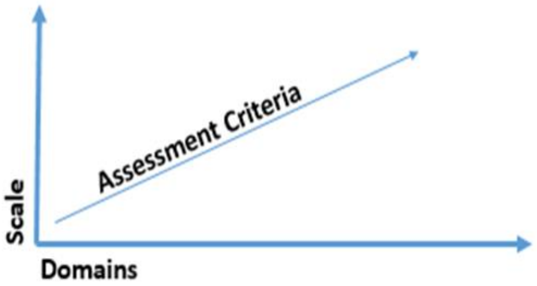

Figure I Common Areas of Focus for SMEs for Evaluating CMMs

Scale: Capability Maturity Models represent the organization’s capability through various numbered levels. However, the majority are five-level scales. The descriptions of those levels vary.

Domains: Each CMM assesses the capability maturity of the activities that build, cumulatively or by stages, the maturity level based on requirements defined as domains. The NIST CSF provides informative resources for mapping the number of framework domains to functions/categories/subcategories. Additionally, some frameworks map their domains with the NIST CSF functions/categories/subcategories.

Assessment Criteria: There are two types of assessment criteria: one that assesses each domain activities with the same generic question/s for each level over the different domains and the other uses specific questions about each level or even about each domain for verification.

Administration: Some of the CMMs were originally designed to be used with specific frameworks, while many are generic and not linked to any specific framework. Some are freely available, and others are licensed. Training and assessment guides could be provided in various formats, including in-class and hands-on practices. Some are associated with industry certificates, while others are not.

VI. SURVEY DESIGN AND ANALYSIS

To address the common areas of focus, we designed a survey consisting of 16 questions and shared the draft with the interviewed SMEs. The final sets of survey questions were communicated to many organizations in the oil and gas industry. Given the short survey period, twelve cybersecurity professionals responded to the survey. Of the participants, 58% were Governance, Risk, and Compliance (GRC) specialists (that is, 25% compliance specialists, 17% governance, and 17% as risk specialists). Another 25% of the participants were senior information system auditors. Furthermore, 8% of the participants were compliance officers, and 8% were process performance assessors. The key selection criteria of the participants were their roles, profession, and involvement in cybersecurity capability implementations and maturity assessments.

The feedback received on the survey was analyzed, and top organizational preferences were considered for constructing the evaluation criteria for comparing the reviewed CMMs. Table XI illustrates the selected criteria and compares them with each CMM.

Q1: Does your organization adopt the NIST CSF or is it planning to?

Of the responses, 75% were that their organizations are currently adopting the NIST CSF, and 25% are that their organizations were planning to adopt the framework.

Q2: Is there any governance requirement that mandates the adoption of the NIST CSF?

More than 66% of organizations are adopting or planning to adopt the framework due to governance requirements. The remaining are voluntarily adopting the framework.

Q3: How many times have you assessed your organization’s maturity?

While all organizations assessed their cybersecurity maturity at least once, more than 58% did the assessment more than three times.

Q4: Did you use the same CMM in all the assessments?

Out of all the organizations that did the assessments more than once, 75% used the same CMM for the assessment and 25% used different CMMs.

Q5: Did you use or do you plan to use the result for benchmarking?

It was found that 90% of the organizations either have used the result of the assessment or are planning to use it for benchmarking with other organizations in their field of operation.

Q6: Did you use or do you plan to use CMMs to certify your organization?

Including the certification as part of the assessment goals was the intent of 50% of the organizations.

Q7: What is your preference related to training?

More than 90% of the organizations prefer that the selected MM provide training in various formats, including in-class.

Q8: Did you use or do you prefer using a CMM linked to a framework?

It was found that 75% of the organizations prefer that the selected MM be linked to a framework.

Q9: Did you use or do you prefer using a CMM that is mapped to the NIST CSF functions/categories/subcategories?

It was found that 75% out of the organizations preferred to use a CMM linked to a framework or preferred to have the linked CMM mapped to the NIST CSF functions/categories/subcategories in general.

Q10: Would you prefer that the mapping was done by the NIST or the CMM owner?

More than 66% of the organizations want the mapping to be done by the NIST, specifically as part of the informative references.

Q11: What is the preferred level of mapping?

More than 66% of the organizations prefer “one-to-one” mapping, while 25% prefer “close to one-to-one” mapping, and the remaining have no preferences.

Q12: What are the scale levels you have used or prefer using?

More than 83% of the organizations prefer using a five-level scale CMM.

Q13: Do you prefer using the descriptions of the scale levels as they are or do you modify them?

More than 66% of the organizations prefer using the description of the scale levels as they are, while the remaining preferred to modify it.

Q14: Did you use or do you prefer using generic criteria or specific criteria for assessing each domain in each level?

In terms of the assessment methods, more than 83% of the organizations prefer using generic criteria for assessing each domain of each level. The remaining prefer using specific criteria for assessing each domain of each level.

Q15: Did you use or do you prefer using assessment criteria that allow different weights for the assessed process/activity?

More than 66% of the organizations have used or are planning to use assessment criteria that allow different weights for the assessed process/activity. About 16% do not prefer using criteria that allow different weights. Moreover, the same percentage of organizations have no preferences regarding the weights specified.

Q16: What is the scoring preference?

Finally, 50% of the organizations preferred the use of a cumulative scoring method, 25% of the organizations preferred using a non-cumulative, and 25% of the organizations preferred using a combined scoring method (non-cumulative for compliance and cumulative for performance).

As shown in Table XI, none of the reviewed CMMs has a one-to-one mapping to the NIST CSF framework. ISM3 gets first place for satisfying all other evaluation criteria (8 out of 10), followed by PAM, which satisfied 7 out of 10.

VII. CONCLUSION

There exist several CMMs that can be used to measure the progress of implementing a cybersecurity program. However, with the evolving risk of cybersecurity threats, specifically for organizations with critical infrastructure, the adoption of the NIST CSF has been widely popular. Yet no specific CMM has made a clear-cut model to be used specifically for measuring the cybersecurity programs that adopt the NIST cybersecurity framework. Many factors need to be considered by an organization in choosing one CMM versus another; additionally, one CMM should be used over time to accurately measure the progress of implementing the NIST CSF and to maintain and sustain the desired maturity level. Moreover, benchmarking with other organizations has been deemed necessary for sharing the lessons learned and best practices for maintaining and sustaining the high cybersecurity maturity level efficiently and effectively. This is another reason for organizations to use a unified CMM or compatible ones that allow smooth mapping to the NIST CSF framework.

This paper has come up with evaluation criteria based on SMEs’ feedback and a survey of the most common requirements that organizations have regarding choosing a CMM for measuring the progress of their implementation of NIST CSF. The criteria considered four aspects for selecting the CMM. These aspects are the scale, domains, assessment criteria, and administration. This article also reviewed seven CMMs: CCSMM, ISM3, PAM for the COBIT framework, ISF SoGP for Information Security, CMMI, SSE CMM, CMMI, and ONG C2M2. The reviews of these CMMs considered the models’ scales, domains, and assessment methods. Further, the paper compared the models based on the above aspects as well, as determined the evaluation criteria.

The result showed that all models did not meet the “one-to-one” mapping criterion and did not allow the use of weighted values for each control. ISM3 meets the remaining criteria followed by PAM for COBIT. However, no evidence indicates that these two CMMs are as wildly used as the NIST CSF. Future studies could aim to identify which CMM is in the top quadrant in practical life.

TABLE XI. THE EVALUATION CRITERIA AND THEIR VALUE VERSUS EACH CMM

CMM/Evaluation Criteria	SSE	PAM	ISF	CMMI	CCSMM	ISM3	ONG
Certification	✗	✗	✗	✓	✗	✓	✗
Training in various formats, including in-class	✓	✓	✓	✓	✓	✓	✓
Linked to a framework	✗	✓	✓	✗	✗	✓	✗
Mapped to NIST CSF functions/categories/subcategories	✓	✓	✓	✗	✗	✓	✗
Mapping done by the NIST	✗	✓	✗	✗	✗	✓	✗
“One-to-one” mapping	✗	✗	✗	✗	✗	✗	✗
Five-level scale	✓	✓	✓	✓	✓	✓	✗
Generic criteria for assessing each domain of each level	✓	✓	✓	✗	✗	✓	✗
Weighted value for each control	✗	✗	✗	✗	✗	✗	✗
Cumulative scoring methodology	✓	✓	✗	✓	✓	✓	✓

Additionally, in the future, case studies on organizations that have implemented the NIST CSF should be reviewed. Furthermore, the possibility of one-to-one mapping of NIST CSF to other frameworks or domains of CMMs needs to be assessed.

REFERENCES

[1] National Institute of Standards and Technology. NIST: “Framework for Improving Critical Infrastructure Cyber Security,” [Online]. Available from: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, 2014. [retrieved: 2021.04.25]

[2] B. Obama, “Executive Order 13636, Improving Critical Infrastructure Cybersecurity,” [Online]. Available from: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf, February 12, 2013. [retrieved: 2021.04.25]

[3] Gartner: “Gartner Webinar, Framework for Improving Critical Infrastructure Cybersecurity,” [Online]. Available from: https://www.gartner.com/user/registration/webinar?resId=3163821, 2015. [retrieved: 2021.04.25]

[4] D. Trump, “Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” [Online]. Available from: https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf, May 11, 2017. [retrieved: 2021.04.25]

[5] M. Nygaard and S. Mukhopadyay, “Dragonstone Strategy Kickoff Report (No. LLNL-TR-805864),” Lawrence Livermore National Lab (LLNL), Livermore, CA (United States), 2020.

[6] NIST: “Framework for Improving Critical Infrastructure Cyber Security,” [Online]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 2018. [retrieved: 2021.04.25]

[7] I. Lee, “Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management,” Future Internet, 12(9), p. 157, 2020.

[8] S. Almuhammadi and M. Alsaleh, “Information Security Maturity Model for NIST Cyber Security Framework,” [Online]. Available from: https://airccj.org/CSCP/vol7/csit76505.pdf, 2017, 2018. [retrieved: 2021.04.25]

[9] Information Systems Audit and Control Association. ISACA: “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,” 2012.

[10] Information Security Forum. ISF: “Time to Grow Using Maturity Models to Create And Protect Value,” in Information Security Forum (ISF), 2014.

[11] Carnegie Mellon University. CMU: “Systems Security Engineering Capability Maturity Model (SSE-CMM) Model Description Document Version 3.0,” 1999.

[12]Capability Maturity Model Integration Institute. CMMI: “The CMMI Institute Announces CMMI Development V2.0,” 2018.

[13] Department of Energy. DoE: “Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2 v1.1),” Department of Energy, Washington, DC: US, 2014

[14] V. Aceituno, “Information Security Management Maturity Model (ism3) v2. 10, Stansfeld,” ISM3 Consortium, 2007

[15] G. White, “The community Cyber Security Maturity Model in Technologies for Homeland Security (HST), 2011 IEEE International Conference on IEEE, pp. 173–178, 2011.

[16] N. Sjelin and G. White, “The Community Cyber Security Maturity Model,” Cyber-Physical Security. Springer, Cham, pp. 161–183, 2017.

[17] M. Mylrea, S. Gourisetti, and A. Nicholls, “An Introduction to Buildings Cyber Security Framework,” Computational Intelligence (SSCI), 2017 IEEE Symposium Series on IEEE, pp. 1–7, 2017.

[18] N. Le and D. Hoang, “Capability Maturity Model and Metrics Framework for Cyber Cloud Security,” Scalable Computing: Practice and Experience, vol. 18, no. 4, pp. 277–290, 2017.

[19] D. Proença and J. Borbinha, “Information Security Management Systems: a Maturity Model Based on ISO/IEC 27001”, International Conference on Business Information Systems, Springer, Cham, 2018.

[20] A. Dedeke, “Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles,” IEEE Security & Privacy, no. 5, pp. 47–54, 2017.

[21] ISACA: COBIT Process Assessment Model (PAM): Using COBIT 5, ISACA, 2013.