A Concept & Compliance Study of Security Maturity Models with ISO 21827

Rabii Anass[1], Assoul Saliha[2] and Roudiès Ounsa[1]
[1]*Mohammed V University in Rabat, EMI, Siweb Team, Morocco*
[2]*Mohammed V University in Rabat, ENSMR, Siweb Team, Morocco*

Keywords: Information Security, Cyber Security, Information Systems, Maturity Model, ISO 21827, SSECMM, CCSMM, MMISS-SME.

Abstract: Ever since the success of maturity models in software engineering, the creation of security maturity models began enlarging the choice pool for organizations. Yet their implementation rate has been low and their impact difficult to perceive. This security maturity model choice grew even larger in the last decade regardless of the existence of the standard security maturity model ISO 21827. Amongst governmental approaches, CCSMM is the US national security maturity model supported by a presidential policy for national preparedness. MMISS-SME is one of the only validated security maturity model created by academia between 2007 and 2018. Our research aims to study the added value and compliance of CCSMM and MMISS-SME with the ISO 21827 standard and their shared core concepts. We presented each security maturity model's main lines and modeled their core concepts. Our study shows that the standard encompasses all security engineering concepts yet leaving room for characterization and customization to the organizations. However, CCSMM and MMISS-SME provide nuances in both functions and concepts seeing that they were created for specific contexts such as SMEs or the US local government and their vital organisms.

1 INTRODUCTION

The term "maturity" describes the capacity to progressively improve a specific ability until it reaches a desired goal or a normally occurring culmination (Mettler, 2011). Maturity manifests in all aspects capable of change and improvement. Maturity models serve as a means to evaluate how organizations manage that specific aspect and how they could improve their current state. In our context, we address security maturity models (SMM). The main functions of a security maturity model usually are to assess the state of security and to provide a road-map for improvement (Le and Hoang, 2016). Therefore, a maturity model defines multiple milestones an organization must reach to be at a certain "Maturity Level" by meeting a set of requirements. SMMs rose to prominence after the success of the Capability Maturity (CMM) Model used in software engineering (Humphrey, 1988). They stood out from the already used security standards ISO 27001/27002 (ISO, 2019b) or NIST framework (Barrett, 2020) for their progressive improvement aspect. They provide better insight for organizations in terms of security priorities and targeted sets of actions (Mckinsey, 2017). Security maturity models have become more abundant with the creation of 20 newer SMM between 2007 and 2018 (Kassou and Kjiri, 2012) (Rigon et al., 2014) (Barclay, 2014). Governments have also acknowledged their utility by adopting existing security maturity models or creating their own (ANSSI, 2009). Each of these security maturity models evaluates maturity differently by using different metrics and therefore having different prerequisites to reach a maturity level. The ISO initiative culminates with the release of the ISO 21827 (ISO, 2019a) standard produced in 2002 and recently confirmed in 2014. This diversity joined to the domain dynamicity leads to indecisiveness amongst organizations as well as the academic community (ReaGuaman, 2017) (Le and Hoang, 2016). Therefore, we think there is a need to conduct an in-depth analysis of emerging SMMs in relation to ISO 21827.

Our study focuses on 2 representative security maturity models: The Community Cyber Security Maturity Model (CCSMM) and the Maturity Model for Information System Security in Small and Medium Enterprises (MMISS-SME). We chose CCSMM for our study because it is one of the most prominent available governmental security maturity models in

Anass, R., Saliha, A. and Ounsa, R.
A Concept Compliance Study of Security Maturity Models with ISO 21827.
DOI: 10.5220/0009569703850392
In *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020) - Volume 2*, pages 385-392
ISBN: 978-989-758-423-7

use (White, 2007). In fact, in 2011, it was chosen as the USA's governmental security maturity model through the Presidential Policy Directive PPD-8: National Preparedness (Department of Homeland Security, 2018). On the other hand, according to recent systematic literature review, most studies presenting a security maturity model produced by academia between 2007 and 2018 haven't evaluated the impact of their models on the implementing organization (Rabii A., 2020). This is presumably due to the difficulty of implementing a security maturity model or the sensitivity of this task. We have chosen MMISS-SME amongst SMMs made by academia for having been tested in 11 organizations providing an automated tool for its implementation and guidance (Sánchez, 2007) (Sanchez et al., 2008). Our study seeks to answer the following research questions:

- Given the existence of the ISO 21827 standard, what is CCSMM's and MMISS-SME's specific added value?
- What is the common core of concepts for these security maturity models?
- Are CCSMM and MMISS-SME compliant with ISO 21827?

To that end, we first describe each SMM's genesis highlighting their objective. Then we present their architecture by the means of our package diagrams highlighting their different facets. Then, we detail their core concepts. Afterwards, we verify concept similarities and differences with ISO 21827 and what they entail for the model's main functions. We finally discuss their compliance with the standard.

2 OVERVIEW OF ISO 21827, CCSMM AND MMISS-SME

In this section we present ISO 21827, CCSMM and MMISS-SME. We will discuss the context of their genesis,outline their main functions through their architectural model. Finally we analyze the concepts they set forth.

2.1 ISO 21827

2.1.1 Genesis

ISO 21827 or SSECMM was created by the "Information security, cyber security and privacy protection" committee (ISO/IEC JTC 1/SC 27) to support organizations in improving their security engineering practices for all security systems. Similarly to any ISO standard, it went through many verification phases and finally approved by the Common Criteria and the Alternative Assurance Working Groups. It was first published in 2002, revisited in 2008, validated in 2014 and is currently under review.

2.1.2 Main Lines & Architecture

ISO 21827 is used by organizations as a tool to evaluate their security engineering actions and provide an improvement plan. As is shown in the domain model in Fig 1, it is structured into 2 dimensions: Capability dimension and Domain dimension. The capability dimension contains the 6 maturity levels: Not Performed, Performed Informally, Planned & Tracked, Well Defined, Qualitatively Controlled, and Continuously Improving. Each maturity level is described by a set of "Common Features" that encompass institutionalization of processes reflecting how security is managed within the organization. For example, "Defining a standard process", "Performing the standard process" and "Coordinate practices" are the "Common Features" for level 3. Each common feature is described by a set of "Generic Practices" (GP).

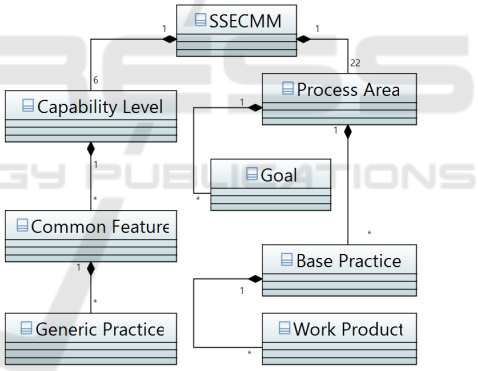

Figure 1: ISO 21827 Domain Model.

In the domain dimension, ISO 21827 defines 11 security engineering "Process Areas" (PA) and 11 project and organization PAs covering all aspects of security engineering. Each process area has a set of goals that represent the expected state of an organization that is successfully performing the process area. Each PA includes all "Base Practices" (BP) that are required to meet its goals. The security maturity evaluation grid is constituted of the pairing of all the "Base Practices" of a PA with the GPs of all common features.

2.1.3 Core Concepts

The concepts SSECMM details in its BPs and GPs aim to thoroughly encompass all aspects of security

engineering as the SMM defines it. We propose the package diagram in Fig 2 modeling these different aspects and which concepts they interact through.

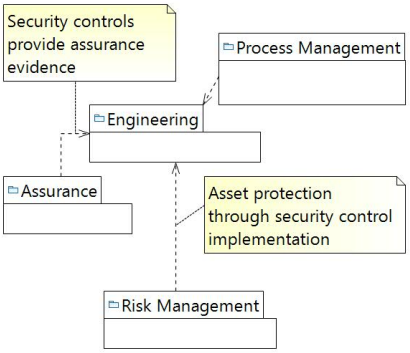

Figure 2: ISO 21827 Domain Class Diagram.

First, the "Risk Management" aspect includes the concepts involved in risk reduction. In fact, all *Assets* have *Vulnerabilities* and thus are under *Threats*. This package also contains, the ensuing *Risks*, their calculated *Impact*, the responsible *Threat agent* and the probable *Incident*.

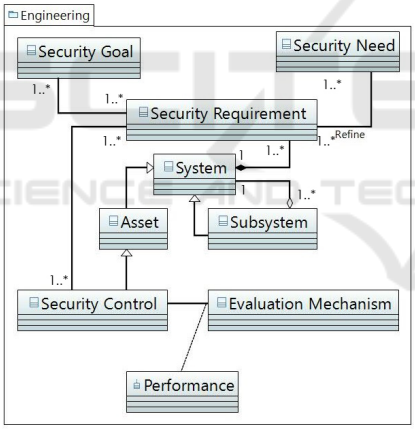

Figure 3: ISO 21827 Engineering Class Diagram.

In the "Engineering" package shown in Fig 3 ,we modeled the *Security Requirements* that the *System* has. Every requirement is either derived from internally expressed *Security Goals* or externally enforced *Security Needs*. The organization then implements a *Security Control* to fulfill these requirements. A control is defined as any asset designed to reduce the level of an unaccepted risks by addressing one or multiple security requirement. Finally, these controls are periodically evaluated to see if they fulfill their task or are in need of change, improvement or decommissioning.

The "Assurance" Package models the assurance the system procures through each control's *Assurance Evidence*. The evidences ensure that every *Assurance Objective* is met providing a guarantee that all *Security Needs* and *Security Goals* are met.

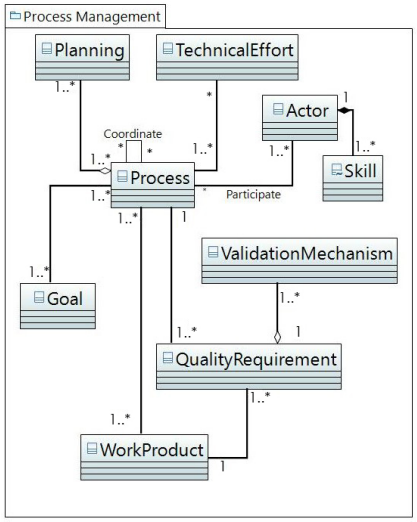

Figure 4: ISO 21827 Process Management Class Diagram.

Lastly, the "Process Management" package modeled in Fig 4 contains a set of *Processes* designed to reach specific *Goals* while meeting a set of *Quality Requirements*. Each process has *Actors* with different *Skills* involved, follows a *Planning* and produces *Work products*. Processes can also coordinate with one another if needed.

2.2 CCSMM

2.2.1 Genesis

In 2006, The Center of Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio conducted multiple security exercises for the local community determining that vital organisms required better security policies. The CCSMM was then created to improve cyber readiness as a scaling model aiming to reach nationwide use. It emphasizes the importance of collaboration between entities, spreading relevant and useful information for a better security posture. The CCSMM distinguishes between different scales of entities: organization, community, state, and nation. The model remains unchanged from its 2006 version.

2.2.2 Main Lines & Architecture

The CCSMM offers a framework for security maturity evaluation and model-based improvement, yet does not precise the means. It urges for the implementation of the most adequate standards or approaches

depending on the organization's context such as the recommended NIST's "Framework for Improving Critical Infrastructure Cyber Security". This lets organizations choose which approach to implement depending on internal context, changes in the field or policies.

The CCSMM aims to evaluate 4 areas of security called "Dimensions": Awareness, Information Sharing, Policies and Planning. The human aspect being the most important and the weakest link in security, it is important to make sure that communities within or outside the organization understand the importance of cyber-threats, their own actions and their preparedness. Information sharing sheds light on the importance of collaboration in order to improve the current state of security or defend against an escalating breach. Policies include all day to day activities detailing the recommended course of action. Finally, Planning deals with recovery and continuity plans.

Each of these dimensions has its own capability level: Initial, Established, Self-Assessed, Integrated and Vanguard. The capability level evaluation is done through a set of predefined exercises designed for each dimension, capability level and scale. In order to reach a certain maturity level, an organization must work on:

- Metrics to watch for in assessments and how to conduct them,
- Technologies that should be implemented,
- Training to achieve the necessary skill set for stakeholders to have,
- Documented processes to follow.

2.2.3 Core Concepts

Since the CCSMM does not specify security requirements, the concepts it uses are either related to "Risk Management" or "Capability Evaluation".

The "Capability Evaluation" package in Fig 5 models the evaluation of the *Entity*'s components using *Exercises*. An entity contains, a set of *Actors*, *Activities* and *Technologies*. Every actor possesses *Skills* and has had or must undergo *Training*. The entities also have *Communication Mechanisms* for cooperation. The CCSMM dictates that actors, technologies, activities and communication mechanisms have to be evaluated using specific *Evaluation Metrics* and *Evaluation Mechanisms*.

On the other hand, the "Risk Management" package contains the base concepts such as *Threat*, the targeted *Entity*, the exploited *Vulnerability*. However, the CCSMM provides a typology of threats depending on *Resources* allocated and the *Threat Agent's*

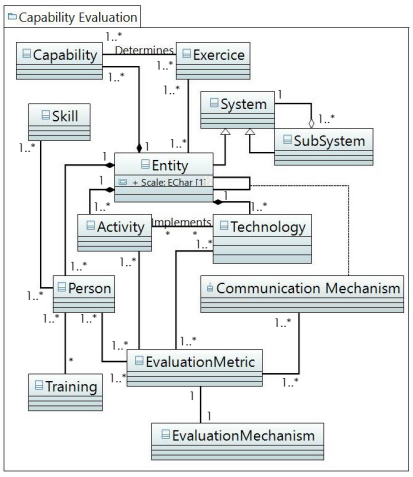

Figure 5: CCSMM Capability Evaluation.

Skill and *Motives*: *Unstructured Threats*, *Structured Threats* and *Highly Structured Threats*.

2.3 MMISS-SME

2.3.1 Genesis

MMISS-SME was created through the joint efforts of SICAMAN Nuevas Tecnologías and the ALARCOS Research Group as a security maturity model specifically oriented towards Small and Medium Enterprises (SME). This SMM was created to support SMEs in creating their Information Security Management System at a low implementation and maintenance cost. Through their research, they sought to adapt an existing security maturity model to the SME context choosing ISO 27002 as the appropriate approach. This SMM was later validated through test cases in 11 different organizations from different sectors. Further plans were made aiming to facilitate the creation of the improvement plan and keep updating the tool to keep up with changes.

2.3.2 Main Lines & Architecture

MMISS-SME's main contribution is helping SMEs build a simple, cheap, rapid, automated, progressive and maintainable security management system. The model has only 3 maturity levels and reaching each level provides the organization with a certificate materializing their progress. First, it sets to determine which maturity level the organization should strive for depending on several weighted factors such as number of employees, annual turnover and dependency on the information system. Once the desired maturity level is known, a security audit is conducted in order to determine the current maturity level using the

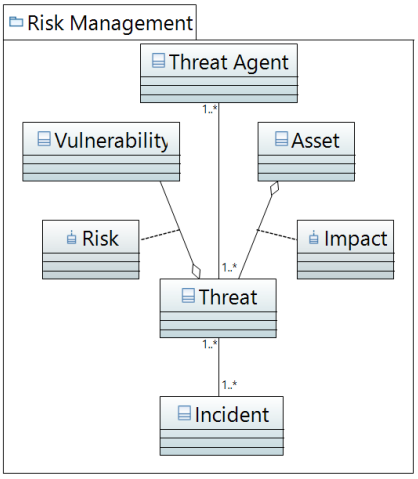

Figure 6: MMISS-SME Risk Management Class Diagram.

controls from a detailed checklist. This checklist consists of 735 sub-controls organized in dominions and distributed over the maturity levels. To reach the following level, the SME must fulfill at least 75% of the previous level's controls; this accounts for normally occurring time degradation. Next, in the risk analysis phase, MMISS-SME uses association matrices to minimize this phase's cost and yield the best results with minimum effort. Finally, the automated tool provides adequate course of actions for improvement highlighting which controls should be implemented and defining a priority order for efficiency.

2.3.3 Core Concepts

The MMISS-SME is centered around 2 packages: the "Risk Management" package and the "Information Security Management System" (ISMS) package.

The MMISS-SME is centered on the "Risk Management" facet as it uses several matrices in order to generate a risk model. The ISO 27002 standard is used to supplement controls and common risks to the association matrices. The matrices incorporate and associate emphVulnerability, *Threat*, and *Asset* as well as *Security Controls* subjected to an unaccepted *Risk*. The level of fulfillment of these controls influences the ISMS generation algorithm. Fig 6 models the concepts intervening in this phase of this risk analysis phase.

In the third and final "ISMS Generation Phase", the "ISMS" package incorporates all the results from the previous phase to determine what *Procedures*, *Technical Instructions*, *Registers*, etc must activate for the organization. In this pha se, the tool relies on association matrices to define which objects of the ISMS library to implement. These matrices use the relationship between existing *Regulations*, *Documentation*, and the *Security Controls* recommended by ISO 27002. The output of this phase is a set of regulations and procedures that must be satisfied in order to improve the organization's security level. The tool also provides priority levels for each requirement as well as *Metrics* to measure security progression.

3 RESULTS

- Research Question 1: Given the existence of the ISO 21827 standard, what is CCSMM's and MMISS-SME's specific added value?

First of all, CCSMM and MMISS-SME share generally the same main function as ISO 21827: security maturity evaluation. However, each of them was designed for a different scope and purpose therefore yielding different realizations. ISO 21827 is a standard designed to be used by all organizations of all types and sizes. It encompasses the entire engineering life cycle, the whole organization as well as interactions with other facets and other organizations. MMISS-SME on the other hand acknowledges the challenge small and medium organizations face and therefore its added value is providing a model less complex, less demanding and also providing an automated tool for its usage. Upon reaching a maturity level, MMISS-SME also provides a certification further rewarding SMEs with tangible advantages. CCSMM on the other hand was made to bring together different US entities and assist them to scale towards a cyber-ready nation. The CCSMM also provides more flexibility so that organizations implement more suitable approaches to their contexts. CCSMM also provides a framework evaluating the maturity and efficiency of the implemented approaches.

- Research Question 2: What is the common core of concepts for these security maturity models?

Secondly, we created the Venn Diagram in Fig 7 to showcase the common core of concepts as well as the differences. Evidently, we find the evaluated organization and the capability or maturity model it seeks to ascertain. We see that the risk management aspect uses the same concepts in all 3 security maturity models such as risk, vulnerability, threat and impact. We also see that all 3 models are aimed towards complex systems as we see systems composed of different objects such as processes or technology as well as actors and their skills for CCSMM and ISO 21827. These components are called assets in MMISS-SME and ISO 21827. Since the evaluation mechanism is automated in MMISS-SME, we only explicitly see it in CCSMM and ISO 21827.

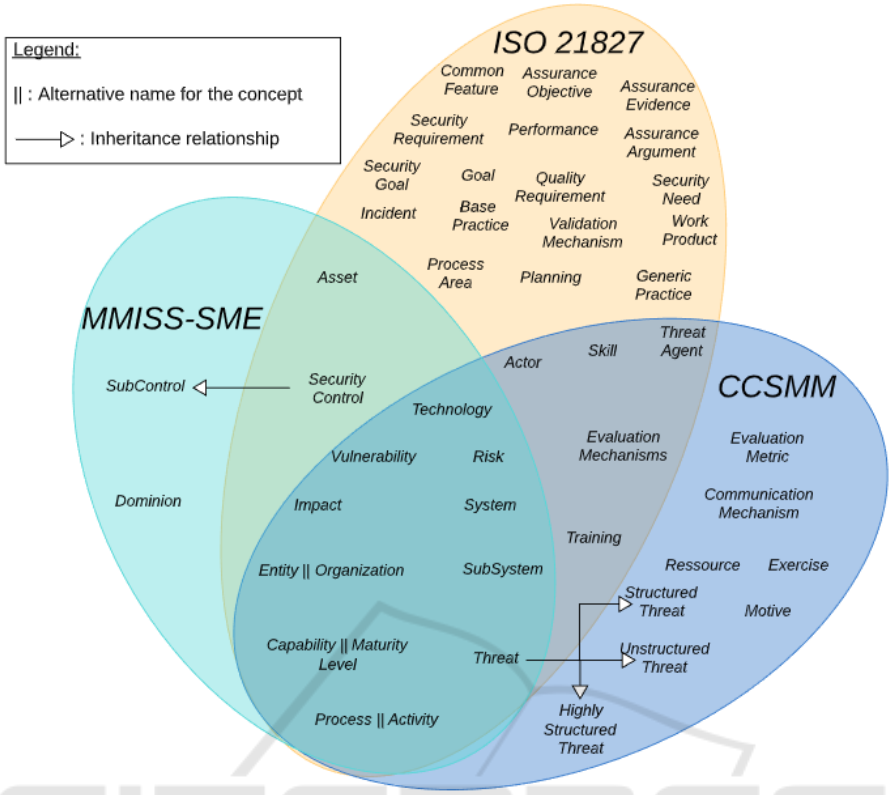

Figure 7: Security Maturity Model Concept Venn Diagram.

As for the differences, The CCSMM includes the resources available to the threat agent as well as their motive. This separation results in a typology of the scale of the threat in order to treat them differently. Unstructured threats are the most common and are dealt with on the daily. structured and highly structured threats are a higher level of priority as their have bigger impacts and might need the involvement of multiple entities. Since each model is structured differently, each introduces completely distinct concepts such as base practices, common features or process area for ISO 21827 or dominion for MMISS-SME, CCSMM even measures maturity through exercises. Finally, the major difference between MMISS-SME, CCSMM and ISO 21827 is handling the process management and assurance aspects. We find the concept of a process and its goal, planning, quality requirement and performance. ISO 21827 also requires an assurance argument containing evidence that all assurance objectives are met.

- Research Question 3: Are CCSMM and MMISS-SME compliant with ISO 21827?

Lastly, In terms of compliance of MMISS-SME and CCSMM with the standard ISO 21827, we will discuss their requirements and the concepts they involve. First off, the CCSMM does not specify which processes to implement or what their characteristics might be. This makes the CCSMM compatible with most existent approaches including ISO 21827. We also see a major compatibility in concepts as the differences are mostly due to the structure and organization of each security maturity model. We have the assurance and process management that can be incorporated in the CCSMM through concepts such as evaluation metric and mechanisms. The rest of the differences are the different natures of threats. We can deduce that CCSMM is compliant with ISO 21827. As for MMISS-SME, it was created to be a customized security maturity model with less requirements for SMEs. It also provides fewer maturity levels based on controls extracted from ISO 27002. These controls were created to supplement the ISO 27001 standard that provides requirements for the creation and maintenance of an ISMS. The requirements of the ISO 21827 and 27001 differ in their purpose as the former provides a progressive scale of improvement while the latter a baseline of requirements for ISMS management. A study evaluating MMISS-SME and ISO 21827's requirements and mapping their levels could evaluate their compliance.

4 DISCUSSION

Each of the models that we studied has a different context thus having different purposes. CCSMM was made for a segregated context explaining why it focuses on collaboration and flexibility. It understands the changing nature of security where approaches, frameworks and methods are constantly changing pinning the responsibility of choosing the adequate approach on the entities themselves. MMISS-SME has a different added value as it aims to be easy to implement and maintain for SMEs. The ISO 21827 standard on the other hand is meant to be an all-inclusive approach that handles all aspects of security engineering. It also has the most rigorous update mechanism while CCSMM does not require one and MMISS-SME has to keep up with the changes to, inter alia, ISO 2700.

This difference in intent and context echoes through the common core of concepts as well. We see that, ISO 21827 provides more concepts covering the assurance and process management aspects that are not addressed in MMISS-SME and CCSMM. We also see that the concepts that make up the risk management aspect are almost identical. We can also see that the missing concepts can be derived from the existing ones in ISO 21827. We can use this large base of concepts to model the requirements of any security maturity model. Regardless from the differences in structure, both MMISS-SME and ISO 21827 use the concept security control while CCSMM does not provide any at all allowing the adoption of external ones.

Lastly, we saw that CCSMM supports the implementation of any approach the entity deems adequate for their context, thus organizations can implement the ISO 21827 practices. However, since they have different evaluation methods and different thresholds for their maturity levels, they will yield different levels. On the other hand, MMISS-SME consists of requirements that are within the reach of SMEs while also providing an implementation tool. Further studies are required to prove the correspondence between each security maturity model's levels.

5 CONCLUSION

In this study, we set out to study 2 security maturity models from different contexts and compare their concepts as well as study their added value and compliance with the ISO 21827 standard. The ISO 21827 or SSECMM standard provides a thorough model encompassing all aspects of security engineering. It thoroughly encompasses all security engineering aspects and is compatible with other disciplines. We have chosen to study the CCSMM a security maturity model adopted by the U.S. government aiding communities in their quest to be cyber-ready through collaboration. MMISS-SME, a vetted approach, designed to assist small and medium enterprises to reach higher maturity level through the use of a tool while also providing a certification per level. We found that ISO 21827 provides most of the core concepts needed to model the other 2 security maturity models.The standards' concepts could be also extended to fit specific contexts or customization through specialization. That is the case with both CCSMM and MMISS-SME, their additional concepts are used to support the nuance in main functions or scope.We saw that both CCSMM and MMISS-SME were made for the USA governmental and vital organism structure and SMEs respectively. Finally, while CCSMM is compliant with the standard, the correspondence between MMISS-SME and ISO 21827.

6 FUTURE WORK

Future studies could focus on different security maturity models studying how their requirements can be expressed and modeled. These studies can rely on the base concepts provided by ISO 21827 and study if specialised concepts are needed depending on the context. This can enable compliance or validation studies of novel security maturity models with the existing standard. Modeling security maturity models' requirements can also help create generic SMM implementation tools. Finally, seeing that security constantly evolves, studies can also concern the security engineering ontology.

REFERENCES

ANSSI (2009). Publication : Guide relatif à la maturité ssi.

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (cm2). *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards?*

Barrett, M. P. (2020). Framework for improving critical infrastructure cybersecurity version 1.1.

Department of Homeland Security (2018). Presidential policy directive 8: National preparedness.

Humphrey, W. (1988). Characterizing the software process: a maturity framework. *IEEE Software*, 5(2):73–79.

ISO (2019a). Iso 21827 : Systems security engineering — capability maturity model.

ISO (2019b). Iso/iec 27001 information security management.

Kassou, M. and Kjiri, L. (2012). Soasmm: A novel service oriented architecture security maturity model. *2012 International Conference on Multimedia Computing and Systems*.

Le, N. T. and Hoang, D. B. (2016). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*.

Mckinsey (2017). Deployment models: How mature are your operational practices?

Mettler, T. (2011). Maturity assessment models: a design science research approach. *International Journal of Society Systems Science*, 3(1/2):81.

Rabii A., Assoul S., R. O. (2020). Information & cyber security maturity models: A systematic literature review.

ReaGuaman, San Feliu, C.-M. S.-G. (2017). Comparative study of cybersecurity capability maturity models. *Communications In Computer And Information Science*, pages 100–113.

Rigon, E. A., Westphall, C. M., Santos, D. R. D., and Westphall, C. B. (2014). A cyclical evaluation model of information security maturity. *Information Management & Computer Security*, 22(3):265–278.

Sanchez, L. E., Piattini, M., and Medina, E. F. (2008). Practical application of a security management maturity model for smes based on predefined schemas. *Proceedings of the International Conference on Security and Cryptography*.

Sánchez, Piattini, M. (2007). Mmiss-sme practical development: Maturity model for information systems security management in smes. *Proceedings of the 5th International Workshop on Security in Information Systems*.

White, G. (2007). The community cyber security maturity model. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS07)*.