(CSM2-RA-R2-TI): Cyber Security Maturity Model for Risk Assessment Using Risk Register for Threat Intelligence

Lakshmi Prasanna B¹,³, M SaidiReddy²

¹ Research Scholar, ²Associate Professor
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India.
³Assistant Professor, Department of Computer Science, RBVRR Women’s College, Hyderabad, Telangana, India.
Corresponding Author Email ID: mureddy33@klh.edu.in

Abstract. Because of the growing frequency sophistication, and severity of cyber security attacks, all businesses should ensure that cyber security risk is properly addressed in their enterprise risk management (ERM) programs. Risk Management, agreeing with the NIST Guide 8286 is the arrangement of "composed exercises to direct and control an association concerning risk". NISTIR 8286 characterizes a system and framework for hazard the executives. In any case, executing this norm without an in-depth plan can turn into a risk on associations. This paper provides a capability maturity model for risk assessment for threat intelligence using a risk register. This model helps the organization as reference and set clear path to survey risk assessments in accordance with latest threats.

Keywords: Risk Management, Risk Register, Threat Intelligence, Maturity model, NISTIR 8286

1. Introduction
Cyber-attacks are growing in scale, intensity, and ingenuity, as defense, enforcement, and risk management practitioners know. When someone in the industry tells us how important it is for our companies to pay attention to cyber security risk, most of us nod our heads in agreement. Nonetheless, several management teams and boards of directors continue to be perplexed by the magnitude of the problem.

NIST recently published a paper titled "Integrating Cyber security and Enterprise Risk Management" [1] to assist security practitioners in communicating the importance of preventative security to their management teams (NISTIR 8286). The use of a risk registry summarized as a "repository of risk information" – to effectively incorporate cyber security risk management is the focus of this guidance.

Threat Modeling is a systematic and organized protection methodology for identifying an application's security priorities, risks, and vulnerabilities, as well as determining where to focus efforts in designing, creating, and deploying safe applications. Threat modeling [2] has the components like Threat knowledge, Asset Identification, Mitigation capabilities, Risk evaluation, and Threat planning.

The impact of uncertainty on the achievement of goals is known as risk. As a result, all
organization’s face threats and uncertainty, and they want to control risk in an organized manner are becoming increasingly apparent. Risk management (RM) is described as [3] “a set of organized activities designed to guide and monitor an organization's risk exposure”. Various risk control practices are often used by organizations, and they do so in a variety of ways.

The risk assessment method is not always easy to execute, and certain companies give up before obtaining the expected results. This may be due to their inability to consistently and predictably carry out the risk assessment process over time. Maturity models are instruments that depict a journey toward a more streamlined and comprehensive way of doing business, which often involves a number of steps.

The goal of this paper is to feature the Risk Management (RM) frame of understanding via way of means of growing an artifact through the use of a well-mounted methodology. To outline a maturity version for RM, the version is primarily based totally on NISTIR 8286, which prescribes an RM shape and architecture.

We focus our attention in this paper on answering two research questions (RQ):

RQ1 - According to NISTIR 8286, what are the main tasks in a risk management process?

RQ2 – How will an RM maturity model be constructed to cope with the issues confronted with the aid of using diverse companies and industries?

To cope with those take a look at problems, this work is prepared into six sections. The most important terminology and meanings are defined in Section II, and its related work is given. Section III provides an overview of risk management and the risk register procedure. Section IV discusses hazard intelligence danger control. The RM Maturity Model is classified in Section V in phrases of the mapping among the RM Maturity Model Levels and the NISTIR 8286. Finally, in Section VI, the belief is discussed.

2. Background

After doing a literature review, the goal of this study is to evaluate cyber security maturity levels and make guidelines for improvement on the way to lower cyber dangers and vulnerabilities and grow cyber protection competencies. After evaluating many maturity models, the Cyber security Capability Maturity Model (C2M2) becomes selected to evaluate cyber protection competencies on the way to estimate an enterprise's risk.

To maintain a shared interpretation, this section defines the core terms and principles used in this article. Most organizations do not analyze or evaluate cyber security threats with the same rigor or reliable methods as other forms of risks within the organization, according to NIST's new risk paper, "Integrating Cyber security and Enterprise Risk Management. "As for the draft [2] of NIST, the key terms are defined as

Risk - Normally, it is calculated as a characteristic of the chance of a certain occasion happening and the possible effects of that event. Uncertainty is described as a condition of insufficient information for comprehending and knowing a specific occurrence, its consequences, or possibility.

Risk Register - "risk information repository" that includes an overview of a specific risk, the probability of it occurring, the possible cost effects, how it rates overall in importance relative to all other threats, the answer, and who owns the risk.

Risk Management – It is defined as "organized activities that lead and manage an organization's risk."

Risk tolerance - The willingness of the organization or related parties to accept residual risks in order to achieve their goals after responding to or evaluating risk. It is the acceptable degree of performance variation relative to the attainment of goals."
Watts Humphrey, the SEI group, and Mitre Corporation were hired to develop a tool to measure the capacities of the software firms with which the US Department of Defense collaborated in 1986 [4]. The first model of the CMM maturity model of capabilities was published in 1991. This model has had a lot of success and has developed into CMMI, which stands for Capability Maturity Model Integration.

This model [5] is very popular and is constantly updated and developed over time. It is today called the integrated version of the capability maturity model, hierarchical and continuous views can be used to connect to the maturity model of the system. There are maturity stages of step-by-step representations that correlate to the degree of process change over a series of predefined processes. Capacity thresholds are used in continuous representations to reflect the accomplishment of process change in particular process areas.

2.1. Examining and deciding on a cyber-security maturity model

The maturity models listed below were discovered in the literature offer a baseline against which an organization's present degree of maturity in its practices, processes, and procedures can be measured:

Researchers are currently working on a security maturity model. Several authors [6, 7] have examined the advantages and limitations of the current security maturity model. From 2012 to 2017, the comprehensive maturity model of information security [8] was strictly reviewed, and the current security maturity level [9, 10] was investigated in depth. Several of the most popular security models were selected for this study.

2.2 Identification of the model

The maximum important protection trendy, in step with Howe [11], is NIST 800-53.[12] It is a part of the National Institute of Standards and Technology (NIST) Cyber Security Framework, which has grown and been up to date on a everyday foundation over the preceding ten years. This framework defines protection measures [13] for Organizations like Federal Information Systems.

The Community Cyber Security Maturity Model (CCSMM), [14] which makes a specialty of a particular place of an organization, offers help on reacting to cyber threats on the network level.

The ISO/IEC 27000-series [15], a trendy for records control protection systems, presents pointers for growing one. ISA99/IEC 62443[16] is an association with present day computerization and manages frameworks. ISO/IEC 15408 suggests the concepts for a PC protection certificates. The Systems Security Engineering Capability Maturity Model (SSE-CMM), in any other case known as ISO/IEC 21827, is a protection designing improvement assessment that isn't always focused on on-line protection.

The Energy and Oil and Natural Gas Subsector cyber protection Capability Maturity Model (ES-C2M2)[17] and the Oil and Natural Gas Subsector cyber protection Capability Maturity Model (ONG-C2M2)[18] are each appropriate for the strength and oil and flammable fuel online areas.

The National Initiative for cyber protection Education Capability Maturity Model (NICE)[19] is a body of workers improvement, technique adulthood, and operational resilience version that doesn't encompass precise cyber protection pleasant practises. COBIT (Control Objectives for Information and Related Technology) is an IT management and manage layout that makes a specialty of statistics protection above cyber protection [20].

C2M2 is a cyber-protection Capability Maturity Model that makes a specialty of cyber protection and is meant for use in aggregate with the NIST framework; it's miles incredibly primary and is provided as a questionnaire.
One of the earliest adulthood models [21] used for records protection changed into Citigroup's Information Security Evaluation Maturity Model (ISEM). It makes a specialty of protection recognition and assessment, and it's been used as a version for growing opportunity cyber protection adulthood models, even though it isn't always presently applied with inside the industry.

The IBM Information Security Framework (IBMISF) [22] is a protection framework that makes a specialty of protection whole evaluation and assists agencies in figuring out their current protection posture. The (ISM3) [23] stands for Information Security Management Maturity Model is a commercial enterprise trendy that makes a specialty of statistics protection, hazard assessment, and technique integration.

3. Analysis of risk management with risk register process

Several authors and organization’s studying RM have offered several frameworks to handle the topic, although they primarily apply to big businesses and not all industries; manufacturing and financial industries are favored [24, 25] RM is created in major companies and particular industries, with its own definition and principles. RM is created in major companies and particular industries, with its own definition and principles. The level of hazards, according to prior studies, is dependent on the industrial sector [26, 27]. Other studies show that risk management is impacted by experience, risk understanding, and the firm's ownership structure, but not by industry type or ownership structure.

The "NIST" [28, 29] contains essential RM principles and ideas, just as, more as of late, "risk-based thinking" as a necessary part of by and large quality administration in a wide range of organizations. At the point when applied in a firm, the plan and execution of RM should think about the association's specific evolving requests.

Dangers ought to be reported in a risk register with appropriate data and design. To help better network safety the board, digital protection hazards should be reported and followed in digital protection hazard registers. A threat register is described as "a store of threat information, comprising facts amassed over the years on hazards."

A threat register often entails a portrayal of the danger, the consequences if the threat happens, alleviation arrangements, hazard proprietors, and positioning to distinguish higher need chances”. Cyber security risk registers are an important part of a company's cyber security risk management strategy. As further risk actions take undertaken, each register evolves and develops.

- The Risk Assessment process using the Risk Register is as follows.
  - **Determine the context**- Context refers back to the surroundings wherein the enterprise operates, that's impacted via way of means of the dangers it faces.
  - **Determine the dangers**- This involves spotting the entire variety of advantageous and bad dangers—that is, comparing which occurrences may assist or preclude objectives, which include the dangers related to passing up an opportunity.
  - **Examine the dangers**- This involves calculating the opportunity of every indicated threat occasion occurring, in addition to the feasible impact of the consequences mentioned.
  - **Rank the hazards**- In order of importance, every threat's publicity is evaluated primarily based totally on its chance and feasible impact, and dangers are then ranked in keeping with their publicity.
  - **Prepare and put into effect threat Reduction** -An initiative for every threat, the right response is identified, with threat recommend from management guiding the technique.
• **Keep an eye fixed on things, assessment them, and make adjustments as needed**-

As cyber protection dangers vary, non-stop tracking guarantees that organization threat occasions continue to be inside the set threat urge for risk thresholds.

![FlowChart of Risk Management using Risk Register Process](image)

**Figure1.** FlowChart of Risk Management using Risk Register Process.

'Figure1' represents the flowchart of RiskManagement using Risk Register Process. The context evaluation section is when the RM manner goals are first established, in step with the company's strategic goals, and then the resources.

The following are the important thing stages:[29,30] the detection of danger (relate the feasible risks), the risk assessment section (decide the probability and result of the recognized chance occurring), the risk remedy section (become aware of the way to lessen the incidence or effects of perfect risks, the way to lessen the effect of non-perfect risks, and pick the best responses to them), and the screen and evaluation section (have a look at the chance prevalence and if the remedy is powerful or not).

The conversation and interplay with stakeholders concerning the manner and the chance publicity is the procedure's very last action. Various methods and strategies for identifying, evaluating, and treating risks are used depending on the situation. These instruments might be qualitative, quantitative, objective, or subjective in nature.

4. **Risk management for threat intelligence**

The risk analysis process should enable an organization to assess its risk in terms of threats and vulnerabilities. The auditor will be able to classify the risk's severity and hence assign an overall relevance to each risk at this stage. It should be possible to develop a risk management strategy using this data [31, 32].

This should include the following:

• Preparing a dangerous treatment plan utilizing an assortment of control strategies.
• Analyzing singular dangers dependent on the effect of the dangers and weaknesses that have been distinguished from the dangers.
• Rate the individual dangers from most elevated to least significant.
• Create a dangerous treatment plan that classifies every one of the dangers and weaknesses arranged by its need to the association, along with certain potential controls.

**Table 1.** Notational Cyber security Risk Register Template.
‘Table 1’ shows an example National Cyber Risk Register template, which includes risk priority, description, risk category and kind, who the owner is and what their current status is, as well as the cost and impact of the risk.

Quantitative and qualitative [33, 34] approaches can be used to assess the possible risk. The formulas may be used to calculate the Risk function.

\[
\text{Risk} = \text{Threat} \times \text{vulnerability} \\
\text{Risk} = \text{Threat} \times \text{vulnerability} \times \text{impact}
\]  

4.1. Cyber Threat Intelligence (CTI)

A threat is an undefined occasion that has the capacity to disrupt an organization's operational and practical operations. Threat intelligence is available in quite a few forms, which include strategic, operational, tactical, and technical danger intelligence.

4.2. Integration of CTI (Cyber Threat Intelligence) with Risk Management

‘Figure 2’ depicts how risk management can be embedded in cyber threat intelligence in an enterprise/organization, where threat details can be collected from a risk register to identify external or internal threats and different preventive and deterrent control mechanisms can be used to mitigate the risk.

5. Maturity Model Design In Accordance With NIST Framework

The National Institute of Standards and Technology's (NIST) Cyber safety Framework [10, 13] is a hazard-primarily based totally framework that gives guidance for addressing cyber safety risks. Although the version outlines the implementation process, it gives little help to detect, analyze, and prioritizes gaps; set up a modern profile; carry out a hazard evaluation; set up a goal profile; and identify, analyze, and prioritize gaps.

The Risk Maturity Model (RMM) explains the primary metrics and activities that make up an enterprise risk management (ERM) software this is sustainable, repeatable, and mature. Organizations might also additionally use the hazard maturity self-evaluation to look at how properly their risk strategy control techniques align with the RMM indicators.

The RM Maturity Model's principal cause is to grow the effect of hazard control on an organization's business value. As visible in Figure, that have an impact will increase as you develop from a decrease to an extra adulthood level [10, 24]. Furthermore, the shortage of tactics and policies on the decrease tiers results in bad hazard control, which would possibly place the enterprise in threat without even knowing it.
Table 2. Levels in CMMI and RM-CMMI

| SNO | CMMI (Capability Maturity Model Integration) | Purpose | RM-CMMI (Risk Management- Capability Maturity Model Integration) | Purpose |
|-----|---------------------------------------------|---------|---------------------------------------------------------------|---------|
| 1   | -                                           | Level 0 – No RM                                 | -       |
| 2   | Level-1-Initial                             | Unpredictable, poorly conceived, and reactive process. | Level 1 – Initial RM | Risk Management is informal and Adhoc |
| 3   | Level-2-Managed                             | Projects and reactive processes are characterized by this process. | Level 2 – Managed RM | Basic Risk Management |
| 4   | Level-3-Defined                             | The process is characterized by its organization and proactive nature. | Level 3 – Defined RM | Standardized Risk Management Process |
| 5   | Level-4-Quantitatively Managed              | Control and measurement of the process.        | Level 4: Quantitatively Managed Risk Management; | Quantitative Risk Management Process |
| 6   | Level-5-Optimizing                         | Maintain a constant focus on process improvement. | Level 5: Risk Management Optimization | Continuous Risk Management Process |

‘Table 2’ represents the proposed RM-CMMI (Risk Management- Capability Maturity Model Integration) comparison with CMMI (Capability Maturity Model Integration) at all stages.

As policies and procedures are adopted, specified, recorded, and assessed at greater maturity levels, this risk is reduced. Risk management is completely incorporated into the organizational structure at the greatest maturity level (level 5) and is used to give a competitive advantage.

We added level 0 to the previously described maturity levels 1–5, which signifies the company is not doing any RM processes or tasks at all. As a result, level 0 is not referenced directly in the RM maturity model.

5.1. Maturity stages emerge

We added level-0 to the formerly defined maturity tiers 1–5, which indicates the enterprise isn't always doing any RM tactics or obligations at all. As a result, level 0 isn't always referenced at once with inside the RM maturity model.

To develop from level zero to level 1, the enterprise has to understand that an RM system is needed as a crucial function. Additionally, essential danger control responsibilities are finished with the purpose of making sure that danger is treated at some point in the enterprise.

As a result, the enterprise has a view of the requirement for a danger control system at maturity level 1 (Initial). Some risk management actions are utilized by the enterprise; however, they're usually haphazard and disorganized. This kind of activity is extra reactive than proactive. The company lacks strong surroundings wherein to create a risk control approach.

The consequences of danger control are sudden and hard to repeat, and that they depend extra on the competencies of the human beings with inside the enterprise than on using a longtime procedure.

At maturity level 2 (Managed), the enterprise makes an attempt to plan and perform danger control system sports according to with the risk control coverage that the company has created with stakeholders.
Despite those efforts, danger control is suffering from the replication of preceding a hit acts in preference to a dependent procedure. Risk management tasks are delegated to persons with the skills, defined roles, and sufficient resources to generate results that are repeatable to some extent. The organization's uniformity is lacking at this level. Risk management might vary greatly amongst departments within a business.

The danger the executives cycle is described, perceived, and indicated in standard cycles, apparatuses, and techniques at maturity level 3 (Defined). The system is used to give consistency all through the organization, and there is a concentrated way to deal with hazard the executives.

The association utilizes quantitative and measurable techniques to screen, survey, and assess the danger the board cycle at maturity level 4 (Quantitatively Managed).

At long last, at maturity level 5 (Optimizing), the danger the board interaction is persistently upgraded dependent on the data acquired at before levels. Everybody is committed, and hazard the executives is seen as an essential arrangement.

To advance from level X to even out X+1, the association should meet the entirety of the prerequisites from level X, coming about in a "stages" approach in this development model. Because corporations at this maturity level are continuously inventing and improving the threat control process, they make contributions scientifically to the increase of threat control as a domain [5].

Table 3. NIST Risk Management Framework

| Identify The Context | SP 800-30-Rev.1 | SP 800-30-Rev.1 | SP 800-39 |
|----------------------|-----------------|-----------------|-----------|
| Risk assessment (risk identification, risk analysis, risk level calculation) | 3.2. Task 2-1: Identify and describe possible threat sources. Task 2-2. Identify possible dangerous situations and threat sources Task 2-3: Identify vulnerabilities and conditions | 3.5.prepareTask P-14 , evaluate the Risk Assessment-System, Risk Assessment Report(PAR) Assess | 3.2. Assessing Risk |
| Risk Assessment | 3.2. Task 2-4: Calculate the negative consequences of threat occurrences. Task 2-5: Calculate the probability. Task 2-6: Assess the organization's risk. Report on Risk Assessment | | 3.3. Risk Report |
| Risk Treatment | 3.3. Task 3-1: Exchange of risk assessment results Task 3-2: Exchange of information on risk | | 3.4. Implementation, approval (3.6), POA, and M residual risks. |
| Monitoring and Review | 3.4. Task 4-1: Maintain on going risk factor monitoring Task 4-2: Update the risk assessment | | 3.4 Monitoring Risk |

‘Table 3’ shows the NIST risk management framework: SP 80030, 501 revision 1, risk assessment guide; SP 80037, revision 2, risk 502; and SP 80039
| Maturity level Assessment | Activity Point                                                                 | Assessment criterion                                                                                                                                 |
|--------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Level 0 – No RM          | -                                                                              | No Criteria                                                                                                                                              |
| Level 1 – Initial RM     | Collecting Risk Data, Setting risk expectations and priorities                | 1.1. Ask the project manager for information.  
1.2. Analyze the risk register  
1.3. Continue to monitor the Risk Register for data                                           |
| Level 2 – Managed RM     | Explains risk appetite to define risk tolerance statements.                  | 2.1. Define the RM's scope and limits.  
2.2. Establish RM policies.  
2.3. Define the technique for threat evaluation.  
2.4. Perform threat evaluation  
2.5. Conduct a threat evaluation and evaluation  
2.6. Define remedy options for people who are at threat.  
2.7. Establish threat remedies and manipulate targets and procedures.  
2.8. Obtain permission from control for any ultimate risks.  
2.9. Obtain control approval to undertake and execute the Risk Management Plan.  
2.10. At the organizational level, risk tolerance statements (and measurements) are used to apply risk appetite direction. Direction on how to use RM (for example, centralized services, compliance / auditing techniques, and inherited and applied shared controls at the system level). |
| Level 3 – Defined RM     | Risk tolerance statement is applied to reach the system level.               | 3.1. Create a risk management strategy  
3.2. Put the risk treatment plan into action.  
3.3. Put controls in place to achieve control goals  
3.4. Define the technique for figuring out the efficacy of the required controls.  
3.5. Implement schooling and consciousness campaigns  
3.6. Oversee the RM's operations  
3.7. Manage the RM's resources  
3.8. Implement risk detection and response processes and controls |
| Level 4: Quantitatively Managed Risk Management; Assessing and Reporting system level risk responses | 4.1. Monitor and assess procedures as well as other controls.  
4.2. Conduct frequent assessments of the risk type's efficacy.  
4.3. Evaluate the efficacy of controls  
4.4. Conduct a risk assessment review  
4.5. Examine any remaining hazards  
4.6. The review determined that the risk levels were acceptable.  
4.7. Carry out internal risk assessments |
| Level 5: Risk Management Optimization | Aggregating and integrate Business level Risk Management in enterprise |
|-------------------------------------|-------------------------------------------------|
| 5.1 - Implement the RM enhancements that have been discovered. | |
| 5.2 - Take the necessary corrective and preventative measures | |
| 5.3 - Inform all interested parties about activities and improvements. | |
| 5.4 - Ascertain that improvements meet their goals. | |
| 5.5. An integrated Enterprise Risk Register with aggregated and normalized Enterprise Risk findings that are aligned with those of other risk categories. | |

‘Table 4’ represents Proposed RM-CMMI Mapping with Maturity Model, in which we compare risk parameters based on NIST Framework by considering latest Threats and vulnerabilities.

A maturity model is a tool that assists individuals in assessing a person's or group's present efficacy and determining what capabilities they need to learn next in order to enhance their performance while taking risk into consideration, as the number of potential cyber assaults grows every day.

Risk management maturity models are a great method for companies to assess where they are now, compare where they are now to where they want and need to go to get the most benefit, and talk about the value and cost of investing more in risk management. More precise defect detection in process development processes reduce software development or administration cost.

### 6. Conclusion

The creation of a maturity model for the RM system is the intention of this article. The latter can be used by the RM feature to observe and verify the present strengths and shortcomings of the RM system as a governance tool. The version, on the alternative hand, is not only for analytical purposes. It can also be applied to create a roadmap for the RM feature's evolutionary development in phrases of capabilities, effectiveness, and efficiency. The first phase of the item describes the RM activities that had been used as a baseline to peer if current models are able to read an RM system comprehensively.

(RQ1)-The findings suggest that current maturity models do now no longer appropriately cover the complete reference baseline because they most effectively manage the activities selectively. As an end result, no current maturity version can cope with the said issue. Finally, according to the studies plan, we determined to create a brand new maturity version.

(RQ2)-To the solution, the second one studies question, “How should a maturity Model precise to RM be designed that objectives the demanding situations of various organization’s and industries?” we portrayed the development of an improvement version for RM, which includes the real version simply as its evaluation with inside the second piece of the paper.

The version that has been constructed is primarily based totally on contemporary maturity model systems and consists of ideas and procedures from the NIST Risk parameters
according to contemporary threats. Throughout the improvement system, we took an awesome attempt to make sure that usable observed end results become produced. The implemented methodology, of course, has its very own set of restrictions. In order to increase the scope of the maturity model's observation, we suggest that the RM maturity model be evaluated and subtle inside distinctive business sectors, ensuing in an extra popular RM maturity model that may be benchmarked throughout industries.

References

[1] Stine K, Quinn S, Witte G, Gardner RK “Integrating Cyber security and Enterprise Risk Management (ERM)” 2020.

[2] “National Institute of Standards and Technology” (Online), Available at https://www.nist.gov/cyberframework/informative-references 2020.

[3] ISO 31000:2009, “Risk Management – Principles and Guidelines,” 2013.

[4] D. Ahern, A. Clouse, R. Turner, “CMMI Destilled: A Practical Introduction to Integrated Process Improvement, Third Edition,” Addson Wesley Professional, 2008.

[5] CMMI Product Team, “CMMI for Development, Version 1.3,” Carnegie Mellon Univ., no. November, p. 482, 2010.

[6] Le, Ngoc T. and D. Hoang. “Can maturity models support cyber security?” 2016 IEEE 35thInternational Performance Computing and Communications Conference (IPCCC) (2016): pp1-7.

[7] Lessing, M. “Best practices show the way to information security maturity”, 2008.

[8] Karokola, Geoffrey & Kowalski, Stewart & Yngström, Louise,” Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models” P.1 – 9, Information security for South Africa, Johannesburg, 15–17 August 2011.

[9] Rea-Guaman AM, San Feliu T, Calvo-Manzano JA, et al. “Comparative study of cyber security capability maturity models” International Conference on Software Process Improvement and Capability Determination, pp.100–113, Springer, 4 October 2017.

[10] Rea-Guaman A, Sanchez-Garcia I, Feliu TS, et al. “Maturity models in cyber security: a systematic review” 12th Iberian conference on information systems and technologies (CISTI), Lisbon, Portugal, 14–17 June 2017.

[11] Howe N.” Cyber security in railway signaling systems”, Institution of Railway Signal Engineers News. 2017, p.1–4.

[12] Force JT and Initiative T,” Security and privacy controls for federal information systems and organizations”, NIST Spec Publ 2013; 800: 8–13.

[13] Barrett MP,” Framework for improving critical infrastructure cyber security version 1.1”, NIST cyber security framework, www.nist.gov/publications/frameworkimproving-critical-infrastructure-cybersecurity-version-11.
[14] White GB, “The community cyber security maturity model”, IEEE international conference on technologies for homeland security (HST), Waltham, MA, USA, 15–17 November 2011.

[15] Disterer G, “ISO/IEC 27000, 27001 and 27002 for information security management”, Journal of Information Security, 2013; volume-4:92–100.

[16] ISA-62443-2-1: 2009, “Security for industrial automation and control systems: establishing an industrial automation and control systems security program”, 2010.

[17] ES-C2M2, “Electricity subsector cyber security capability maturity model (ES-C2M2)”, www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cyber-security.

[18] ONG-C2M, “Oil and natural gas subsector cyber security capability maturity model (ONG-C2M2)”, www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-oil.

[19] Newhouse W, Keith S, Scribner B, et al, “National initiative for cyber security education (NICE) cyber security workforce framework”, NIST Special Publication, vol.800. USA: NIST, 2017, p.181.

[20] ISACA. Cobit 5. USA: ISACA. “COBIT 5 for Risk “2013, Published by ISACA, COBIT 5, Risk IT ISBN: 9781604204582.

[21] Masinsin RQ, “Secretary of defense corporate fellows program: final report”, New York, NY: Time. 2008.

[22] Buecker A, Borrett M, Lorenz C, et al, ”Introducing the IBM security framework and IBM security blueprint to realize business-driven security”, IBM Red paper 2010;4528: 1–96.

[23] Aceituno V, "ISM3-information security management maturity model", Version 2.1. San Francisco, CA, USA: ISM3 Consortium, the Open Group, 2007.

[24] Anass Bayaga, "Information and Communication Technology (ICT) Risk Models and Performance of Small and Medium Enterprises (SMEs)", the Anthropologist, 15:2, 177–183, DOI: 10.1080/09720073.2013.11891304, 2013.

[25] Teyssier, C, “Risk Management: Lever for SME Development and Stakeholder Value Creation”, United Kingdom: Wiley, 2017.

[26] S. Papastergiou, and N. Polemi, “MITIGATE: A dynamic supply chain cyber risk assessment methodology,” In Smart Trends in Systems, Security and Sustainability, pp.19, Springer, Singapore, 2018.

[27] J. Meszaros, and A. Buchalcevova, “Introducing OSSF: A framework for online service cyber security risk management,” Computers & Security, vol.65, pp.300–31, 2017.

[28] Steven Cockcroft, What is the NIST Framework? ITNOW, Volume 62, Issue 4, winter 2020, Pages 48–49, https://doi.org/10.1093/itnow/bwaa116
[29] National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[30] D. Proenca, J. Estevens, R. Vieira, and J. Borbinha, “Risk Management: A Maturity Model Based on ISO 31000,” 2017 IEEE 19th Conference on Business Informatics (CBI), 2017.

[31] Albakri, A., Boiten, E., De Lemos, R” Risks of sharing cyber incident information”, Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018, pp. 1–10 (2018).

[32] Aksu, M.U., et al.: “A quantitative CVSS-based cyber security risk assessment methodology for IT system”, Proceedings - International Carnahan Conference on Security Technology (2017).

[33] J.W. Candra, O.C. Briliyant, and S.R. Tamba, “ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute),” 2017 11th International Conference on Telecommunication Systems Services and Application (TSSA).IEEE, 2017.

[34] A. Yeboah-Ofori, and S. Islam, “Cyber Security Threat Modeling for Supply Chain Organizational Environments,” Future Internet, vol.11, no.3, pp.1-25, 2019.