A SURVEY AND ANALYSIS OF CYBER SECURITY MATURITY MODELS

A thesis

submitted in partial fulfilment of the requirement for the Degree of

Master Of Computer Application(MCA)

of

Jadavpur University

by

Subhrajit Saha

ROLL NO. 002010503015

Under the supervision of

Prof. Chandan Mazumdar

Department of Computer Science and Engineering

Jadavpur University, Kolkata-700032

FACULTY OF ENGINEERING AND TECHNOLOGY

JADAVPUR UNIVERSITY

Certificate of Recommendation

This is to certify that the dissertation entitled "**A SURVEY AND ANALYSIS OF CYBER SECURITY MATURITY MODELS**" has been carried out by Subhrajit Saha (University Registration No. **154223** of **2020-2021**:, Examination Roll No. **MCA2360035**:) under my guidance and supervision and be accepted in partial fulfilment of the requirement for the Degree of Master of Computer Application . The research results presented in the thesis have not been included in any other paper submitted for the award of any degree in any other University or Institute.

……

Prof. Chandan Mazumdar (Thesis Supervisor)

Department of Computer Science and Engineering

Jadavpur University, Kolkata-32

Countersigned

…….

Prof. Nandini Mukhopadhyay

Head, Department of Computer Science and Engineering,

Jadavpur University, Kolkata-32.

…….

Prof. Ardhendu Ghoshal

Dean, Faculty of Engineering and Technology,

Jadavpur University, Kolkata-32

FACULTY OF ENGINEERING AND TECHNOLOGY

JADAVPUR UNIVERSITY

Certificate of Approval

This is to certify that the thesis entitled "A SURVEY AND ANALYSIS OF CYBER SECURITY MATURITY MODELS" is a bonafide record of work carried out by Subhrajit Saha in partial fulfilment of the requirements for the award of the Degree of Master in Computer Application in the Department of Computer Science and Engineering, Jadavpur University during the period of January 2023 to June 2023. It is understood that by this approval, the undersigned does not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn there in but approves the thesis only for the purpose

……..

Signature of Examiner 1

Date:

……..

Signature of Examiner 2

Date:

FACULTY OF ENGINEERING AND TECHNOLOGY

JADAVPUR UNIVERSITY

Declaration of Originality and Compliance of Academic Ethics

I hereby declare that this thesis entitled "A SURVEY AND ANALYSIS OF CYBER SECURITY MATURITY MODELS " contains a literature survey and original research work by the undersigned candidate as part of my Degree of Master of Computer Application.

All information has been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

Name: Subhrajit Saha

Registration No: **154223** of **2020-2021**

Exam Roll No.: **MCA2360035**

Thesis Title: “A SURVEY AND ANALYSIS OF CYBER SECURITY MATURITY MODELS”

…..……..

Signature with Date

Acknowledgement

I would like to thank the holy trinity for helping me deploy all the right resources and shaping me into a better human being. I would like to express my deepest gratitude to my advisor, Prof.Chandan Mazumdar, Department of Computer Science and Engineering, Jadavpur University, for his admirable guidance, care, patience and for providing me with an excellent atmosphere for doing research. Our numerous scientific discussions and his many constructive comments have greatly improved this work. Without his enthusiasm, encouragement, support and endless optimism, this thesis would hardly have been continued. Most importantly, none of this would have been possible without the love and support of my family. I thank my parents , whose forbearance and whole-hearted support helped this endeavour succeed. This thesis would not have been completed without the inspiration and support of several wonderful individuals. I appreciate all of them for being part of this journey and making this thesis possible.

……..

Subhrajit Saha

Registration No: **154223** of **2020-2021**

Exam Roll No.: **MCA2360035**

Department of Computer Science & Engineering, Jadavpur University

Abstract:

In an increasingly networked and digital world, companies face increasing threats to their information systems and data. The Cyber-security Maturity Model has proven to be a valuable tool for assessing and improving an organization's information security. This thesis makes a comprehensive comparative analysis of different cyber security models**,** with the aim of revealing their strengths, limitations and applicability in different organizational contexts.

The research uses a systematic research methodology to analyse a set of cyber-security maturity models established in academia and industry. The selected models include **Integrated Capability Maturity Model (CMMI)**, the **National Institute of Standards and Technology (NIST) Cyber-security Framework,** the **ISO/IEC 27001.2013 standard,** and the **Cyber-security Model (C2M2).**

The study focuses on key dimensions such as risk assessment, vulnerability management, incident response, and governance and employee awareness. It examines the structures, methods**,** and metrics of the frameworks to assess their effectiveness in guiding organizations toward improving cyber-security resilience. In addition**,** the ease of implementation, resource requirements and scalability of each model are explored**.**

By comparing and contrasting the strengths and weaknesses of these cyber-security maturity models, the study aims to provide insight into choosing the most appropriate framework for organizations of different sizes, industries and risk profiles. In addition, options for integrating and synchronizing multiple models will be explored to create a customized and comprehensive cyber-security framework that meets the needs of the organization.

The results of this cast light upon on the current landscape of cyber security maturity models and highlight their contributions and limitations. Benchmarking enables organizations to make informed decisions about the selection, implementation and adaptation of cyber-security frameworks to improve their overall security**.**

Finally**,** this thesis contributes to the development of cyber-security practices by providing a comprehensive assessment of different maturity models that facilitate the development of robust and adaptive strategies to secure organizational assets in an evolving threat landscape.

Contents:

CHAPTER 1: Introduction

In today's highly connected digital environment, organizations are exposed to ever-growing cyber threats that can compromise sensitive data, disrupt operations, and damage reputations. Therefore, establishing and maintaining robust cyber security measures is of at most importance. The cyber security maturity model has proven to be a valuable framework to help organizations assess and improve their cyber security posture.

The Cyber security Maturity Model provides organizations with a structured approach to assessing their current security capabilities, identifying gaps and vulnerabilities, and achieving higher levels of cybersecurity maturity. These models address key areas such as risk assessment, incident response, governance, and employee awareness, and provide organizations with a roadmap for systematically improving their cyber security practices. As cyber security maturity models become more prevalent, it becomes important to understand their similarities, differences, and applicability in different organizational contexts.

A comparative analysis of these models can help organizations choose the most appropriate framework to meet their specific needs, resources and risk profile. In addition, such comparisons facilitate the identification of best practices and areas for improvement within each model, facilitating further development and refinement of the cyber security framework as a whole. The purpose of this work is to conduct a comprehensive comparative analysis of prominent cyber security maturity models to gain insight into their effectiveness, strengths, limitations, and suitability for various organizational environments.

By researching and evaluating key aspects and components of these models, organizations can make informed decisions about model selection, adoption, and customization. Studies include, but are not limited to, the Capability Maturity Model Integration (CMMI), the National Institute of Standards and Technology (NIST) Cyber security Framework, the ISO/IEC 27001:2013 standard, and the Cyber security Capability Maturity Model. focus on the cyber security maturity model. (C2M2). These models represent different perspectives and are widely adopted in both academia and industry. A comparative analysis explores the structures, techniques, and metrics used by each model, revealing their strengths and weaknesses.

In addition, the study evaluates the practicality and feasibility of adopting these frameworks in organizations considering factors such as ease of implementation, resource requirements, and scalability. By conducting this comparative analysis, this study contributes to the existing body of knowledge on cyber security maturity models to help organizations make informed decisions when selecting and implementing an appropriate framework is intended for .The findings of this study will provide valuable insights for organizations looking to improve their cyber security

resilience and facilitate the development of robust and adaptive strategies to protect against evolving cyber threats.

Overall, this research contributes to the advancement of cybersecurity practices by facilitating the assessment and understanding of various cyber-security maturity models, ultimately leading to stronger and more effective cyber-security practices in organizations across sectors and industries. It is intended to lead to cyber security measures**.**

CHAPTER 2: RELATED WORK

From [1] we know what the metrics to compare software process improvement framework are and from [2] we get the method or roadmap how to compare the cybersecurity maturity models. Here few ideas from SPI Framework has been borrowed which overlapped with the cyber-security field.

In [1] we get to know about the about the different SPI framework which are developed over a period of time covering variety of aspects which made it difficult for a head on comparison .So ,a taxonomy covering 25 points is developed to compare the SPI Frameworks.

In [2] we got a demonstration of the taxonomy used in [1] to conclude a comparative study between various Cyber-security Maturity Models. Mainly they are distinguished based on threat detection, Organization, Application sector, responsibilities level of documentation and results conclude as general or specific or yes/no.

But this thesis enhances the related work by considering several different evaluation criteria. We just cannot compare the cyber security models direct comparisons as they are intended for different aspects some are general some are related to specific fields (C2M2 (Energy fields)).

In [2], the study was conducted without including certain criteria. Those are:

1) Maturity Progression whether the model suggest reach greater level of maturity.
2) If the model is prescriptive and descriptive?
3) Domains of different maturity models.
4) Evaluation criteria.
5) Evaluation process.
6) Maturity levels.
7) What are the objectives in different fields which help to gain the same results across the models?
8) The assets used and its alignment with the process to achieve the goals.
9) Adaptability and scalability and improvement
10) Threats detection and mitigation (anticipating future risk)

This work considers the above criteria. Moreover, several key themes that are relevant to cybersecurity maturity models have been considered in this research. These include cybersecurity frameworks, maturity assessment methodologies and implementation challenges. The work analyses different models in the light of the above and compares and contrasts them using a common terminology.

The rest of the thesis is organized as follows. Chapter 3 explains the various cyber-security maturity models studied in this thesis (C2M2, NIST Framework, and PRISMA).Taxonomy (the grounds on which the comparison is drawn) is detailed in

Chapter 4.The process for conducting a comparative study is covered in Chapter 5.Chapter 6 includes a comparison and analysis of cybersecurity maturity models with a table. Conclusion and future work are covered in Chapter 7.

CHAPTER 3:

In this chapter, the widely accepted Security Maturity Models are described.

3.1 Cybersecurity Capability Maturity Model(C2M2):

C2M2 stands for Cybersecurity Capability Maturity Model, a framework developed by the U.S. Department of Energy (DOE) to assess and improve the cybersecurity posture of organizations in the energy sector. It provides organizations with a structured approach to assessing and improving their cybersecurity capabilities, with a focus on protecting critical infrastructure.

Cyber-security practices in the model enable organizations to protect and sustain assets in a manner that aligns with their importance in supporting IT service delivery and organization missions.

This supports the model's intent of providing descriptive rather than prescriptive guidance.

This is a tool for organization to evaluate their cyber security capabilities and optimize the security investments .This focuses on IT (Information Technology tools) and OT (Operation Technology Tools).

To measure the maturity of the here we have three levels MIL [0-3]. At each levels there are set of attributes which and by achieving it the organization has achieved the level and capability.

The model is implemented in the following steps as follows:

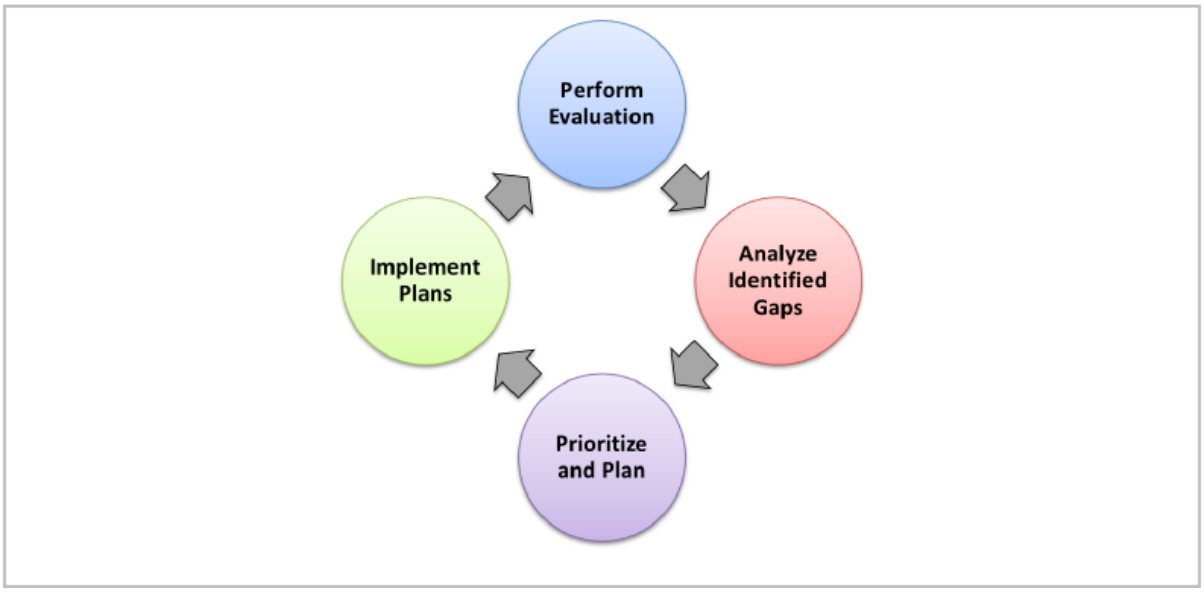
- Evaluation.
- Find Gaps.
- Prioritize the plans.
- Implement Plans.

Self-Evaluation: Select the appropriate personnel to evaluate the function in scope against the model practices.

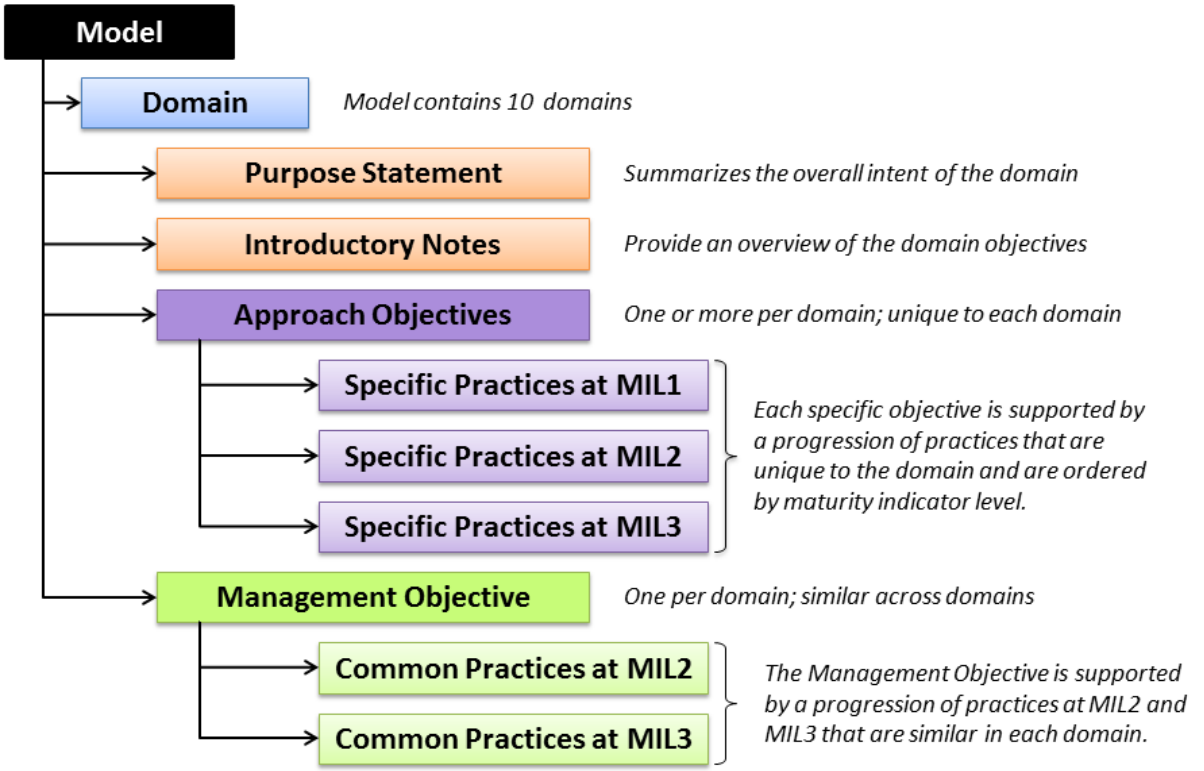
Analyze Identified Gaps: The results of self-evaluation are analyzed and gap between the expected results and the current results to determine whether these gaps are meaningful and important for the organization to address.

Prioritize and Plan: After the gap analysis is complete, the organization should prioritize the actions needed to fully implement the practices that enable achievement of the desired capability in specific domains.

Implementation of Plan: Plans developed in the previous step should be implemented to address the identified gaps.



This model represent spiral model where there is always a scope for improvement.



Maturity indicator level:

The model defines four maturity indicator levels, MIL0 through MIL3, which apply independently to each domain in the model. MIL defines two maturity progressions.

Four aspects of MIL are critical to understanding and applying the model.

1. Maturity metrics apply independently to each domain. As a result, organizations using this model will be able to work in different domains with different MIL ratings. For example, an organization can operate in one domain at MIL1, another domain at MIL2, and a third domain at MIL3.

2. MIL is cumulative within each domain. To obtain the MIL in a particular area, an organization must perform all practices at that level and previous levels. For example, to achieve her MIL2 within her domain, the organization must perform all of her MIL1 and MIL2 domain practices. Similarly, an organization must implement all MIL1, MIL2, and MIL3 practices to achieve MIL3.

3. Setting target MILs by domain is an effective strategy for using models to guide cybersecurity program improvement. Organizations should familiarize themselves with model practices before setting a target MIL. Gap analysis and improvement activities should focus on achieving these targets.

4. Practice performance and the MIL success must be aligned with the organization's business objectives and cybersecurity strategy. Aiming for the best MIL in all areas may not be optimal. Organizations must weigh the potential benefits against the costs of achieving a particular her MIL. However, the model is designed to enable all organizations, regardless of size, to achieve her MIL1 in all domains.

Maturity Indicator Level (MIL)	Level description
MIL 0	The model contains no practices for MIL0. Performance at MIL0 simply means that MIL1 in a given domain has not been achieved
MIL 1	In each domain, MIL1 contains a set of initial practices. To achieve MIL1, these initial activities may be performed in an ad hoc manner, but they must be performed
MIL 2	The organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time
MIL3	At MIL3, the practices in a domain are further stabilized and are guided by high-level organizational directives, such as policy

There are 10 Domains:

1.Risk Management:

Establish, operate and maintain an enterprise cybersecurity risk management program to identify, analyse and mitigate cybersecurity risks to the enterprise and its mission, including business units, subsidiaries, associated infrastructure and stakeholders.

This area actually analyses and prioritizes cybersecurity risks and tolerances. A cybersecurity risk management strategy includes a risk assessment methodology, a risk monitoring strategy, and a cybersecurity governance program.

Cybersecurity risk management include defining, identifying and assessing, responding (accepting, preventing, mitigating, communicating) and monitoring risks in a manner that meets the needs of the organization.

Objectives:

1. The Risk Management (RM) domain comprises three objectives:

1. Establish Cyber security Risk Management Strategy.

2. Manage Cyber security Risk.

3. Institutionalization Activities.

2. Asset, Change, and Configuration Management:

This domain's attribute set identifies the logical or physical assets that make up the company's assets.

Stores information about assets such as software version, asset owner, and physical location.

Depending on the company's risk and its mission, configure the facility in the same way using the same tasks.

Allows legal changes to assets, but prevents illegal changes.

Manage changes to assets, analyze requirements to avoid undesired events that cause unacceptable vulnerabilities in the production environment, ensure all changes are in accordance with change control processes, and identify unauthorized changes to do.

The Asset, Change, and Configuration Management (ACM) domain comprises four objectives:

1. Manage Asset Inventory
2. Manage Asset Configuration
3. Manage Changes to Assets
4. Institutionalization Activities

3 Identity and Access Management:

Establishing and maintaining identity begins with the provisioning and deprovisioning of an entity's identity. Entities include individuals (internal or external), devices, systems, or processes that require access to assets.

Access control involves defining access requirements, granting access to assets based on those requirements, and revoking access when it is no longer needed. Access requests are associated with assets and provide guidance on what types of entities are allowed to access the asset, what access restrictions are allowed, and what authentication parameters apply to do.

The Identity and Access Management (IAM) domain comprises three objectives:

1. Establish and Maintain Identities
2. Control Access
3. Institutionalization Activities.

4 Threat and Vulnerability Management:

Identify threats to assets that align with your company's mission.

A cybersecurity threat is the potential to adversely affect an organization's operations (including its mission, functions, image, and reputation), resources, or other organization through technology and communications infrastructure through unauthorized access, destruction, or disclosure. Defined as a situation or event. Modifications to affect information or denial of IT services.

A cyber vulnerability is a vulnerability or flaw in a technology, communication system or device, procedure, or internal control that can be exploited by a threat.

1. Identify and respond to threats
2. Mitigate cyber vulnerabilities
3. Institutional activities

5 Situational Awareness:

Developing situational awareness entails gaining near-real-time knowledge of a dynamic working environment. Activities and technologies to collect, analyze, alert and alert, display and use operational and cybersecurity information, including status and summary information from other model areas, to create a Common State of Operations (COP) establish and maintain

The Situational Awareness (SA) area has four goals.

- Run logging
- Conduct monitoring
- Create and maintain a common corporate image
- Institutional activities

6 Information Sharing and Communications:

The goal of information sharing is to help organizations, companies, or to strengthen the cybersecurity of the industry. Maintained by the government.

In this domain the organizations share the threats and vulnerability information produced in the process with the organization in the same industry.

1. Share cybersecurity information.
2. Institutional activities.

7 Event and Incident Response, Continuity of Operations:

This domain caters the followings:

- Cyber attacks should be identified and reported.
- Detect escalating cybersecurity events and report incidents (risk-based criteria, threat assessments).
- Responding to cyber events and incidents (limiting the impact of cyber security events).
- Continuity plans include activities necessary to maintain an organization's critical operations in the event of a disruption, such as a major cybersecurity incident or disaster.

The Event and Incident Response, Business Continuity (IR) area has five objectives.

1. Detect cybersecurity events

2. Escalate cybersecurity events and report incidents

3. Response to Incidents and Escalated Cybersecurity Events

4. Plan for continuity

5. Institutional activities

8 Supply Chain and External Dependencies Management:

Suppliers or customers are external dependencies. A vendor dependency is an external party (such as an operating partner) on which the enterprise IT service delivery depends.

Customer dependencies are external parties (including operating partners) that depend on the company to provide IT services.

The cybersecurity characteristics of products and services vary widely. Without proper risk management, serious threats such as software of unknown origin and counterfeit (possibly malicious) hardware arise. The supply chain and external dependency management (EDM) area has three goals:

1. Identify dependencies

2. Manage dependency risks

3. Institutional activities

9 Workforce Management:

Organization or enterprise leverage cutting-edge technology and people with deep knowledge of cyber technology and risk. Assign titles, roles, and responsibilities to personnel and train them accordingly to develop knowledge of threats and vulnerabilities.

The Workforce Management (WM) area consists of her five goals:

1. Assign cybersecurity responsibilities

2. Manage the employee lifecycle

3. Development of cyber security human resources

4. Raise cybersecurity awareness

5. Institutionalization Activities.

10 Cyber security Program Management:

A cybersecurity program is an integrated set of activities designed and managed to achieve the cybersecurity objectives of an organization's or enterprise's IT services. Either way, you can implement a cybersecurity program.

This is done at the organizational level, but from a higher level implementation and business perspective, it can benefit the organization by consolidating activities and leveraging enterprise-wide resource investments.

The cybersecurity program management (CPM) area includes five goals:

1. Establish a cybersecurity program strategy

2. Cyber Security Program Sponsor

3. Establish and maintain cybersecurity architecture

4. Practice secure software development

5. Institutional activities

There is a phase called institutionalize which means to what degree the essential practices are in ingrained or followed by the organization. This phase is common to all domains.

(3.2) NIST (National Institute of Standards and Technology)

NIST composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cyber security activities.

- **Framework Core:**
  a. **Identify.** -> Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities.
  Examples of outcome Categories within this Function include: Asset Management. Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
  b. **Protect**. -> Develop and implement appropriate safeguards to ensure delivery of critical services. Identity Management and Access Control; Awareness and Training; Data Security, Information Protection Processes and Procedures; Maintenance; and Protective Technology.
  c. **Detect.** -> Develop and implement appropriate activities to identify the occurrence of a cyber-security event. Anomalies and Events; Security Continuous Monitoring and Detection Processes.
  d. **Response**. -> Develop and implement appropriate activities to take action regarding and detected cyber security incident.
  e. **Recover.** -> Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security incident.
  This model is prescriptive rather than descriptive. This model also follows spiral model.

- **Tiers:**
  Tier1: **Partial**
  - Risks are not know.
  - No industrial Practice.
  - Cybersecurity risk is very dimly understood at the organisational level.
  - No Communication with other organizations.

  Tier2: **Risk Informed**
  - Organizational knowledge of cybersecurity risk exists, but no organization-wide approach to manage cybersecurity risk has been devised.
  - Management approves risk management procedures, although they may not be made organizational policy.
  - Although there are occasional assessments of organizational and external assets for cyber risk, these are rarely repeatable or recurring.
  - Cyber risk assessment of organizational and external assets happens, but it is rarely repeatable or recurring.

- No Information flow outside the organization only information produced inside organization and shared inside organization.

Tier3: **Repeatable**

- Risk management procedures used by the organization are explicitly approved and stated in policy.
- Risks are documented.
- To address cybersecurity risk, an organization-wide strategy has been implemented. Policies, procedures, and processes that include risks are established, carried out as planned, and evaluated.
- Communications done both ways it regularly interacts with and receives information from other entities that supplements information generated internally, and it exchanges information with other entities.

Tier4: **Adaptive**

- Previous Experience is counted .Based on prior and present cybersecurity efforts, including lessons learned and prediction indicators; the organization modifies its cybersecurity practices.
- Risk Management Strategy corresponds organizational objectives,
- Cybersecurity risk management is part of organizational culture and evolves from earlier activity awareness and continual awareness of actions on their systems and networks.
- Prioritize the risks based on the information received. As the threat and technology landscapes vary, it receives, generates, and reviews prioritized information that supports ongoing risk analysis.

Profiles:

Profiles assist in conveying risk within and between organizations and meet business/mission needs. This Framework does not dictate Profile templates, allowing for implementation flexibility.

A comparison of Profiles (for example, the Current Profile and the Target Profile) may show gaps that must be filled in order to satisfy cybersecurity risk management objectives. A plan of action to fill these gaps in a specific Category or Subcategory can contribute to the roadmap indicated above. The organization's business needs and risk management processes dictate the prioritization of gap mitigation.

This risk-based strategy enables an organization to assess the resources required (e.g., staffing, financing) to meet cybersecurity objectives in a cost-effective and prioritized manner.

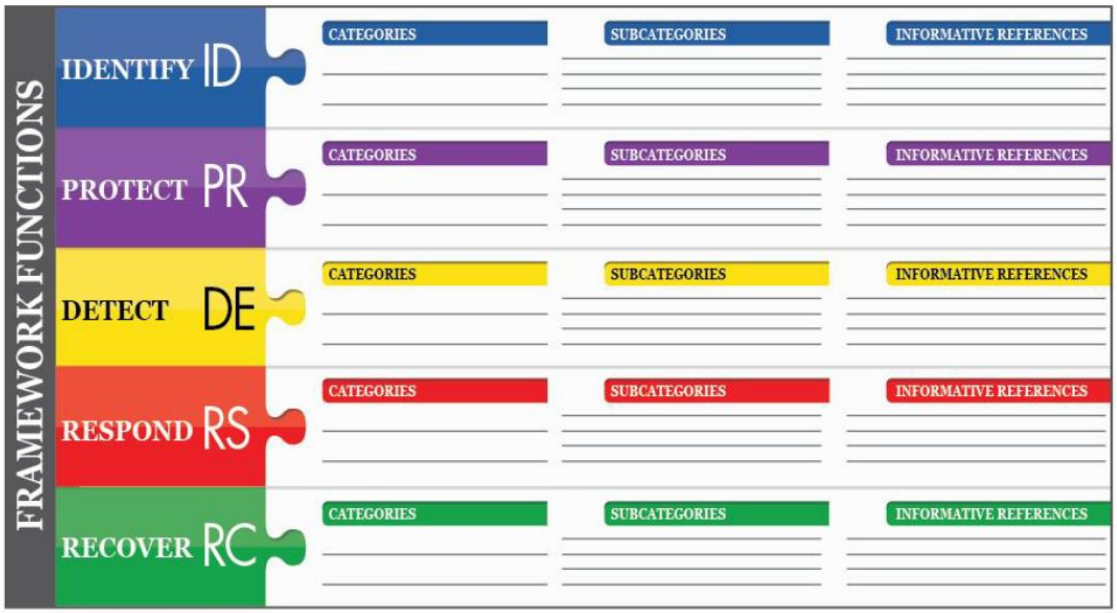


Figure 1: Framework Core Structure

(3.3)PRISMA(Program Review for Information Security Assistance)

PRISMA standards for Program Review for Information Security Assistance. It is a NIST Computer Security Resource Centre's (CSRC) project that incorporates guidelines from NIST SP 800-53.

The PRISMA methodology is a means of employing a standardized approach to review and measure the information security posture of an information security program.

A PRISMA review focuses on nine primary reviews with five level of maturity: policies, procedures, implementation, test, and integration.

a. **IT Security Maturity Level 1**: Policies

   Organizations should have formal documentation containing "will" or "shall" statements that are available to employees.

b. **IT Security Maturity Level 2:** Procedures

   Policies necessitate operational processes in order to apply security controls. Procedures define how, where, when, who, and what an organization's security controls should be implemented. These documents also explain the concept behind the control implementation and who is in charge of what.

c. **IT Security Maturity Level 3:** Implementation

   Organizations implement policies and procedures for a set target audience. This target audience includes stakeholders, top management, contractors, and vendors.

d. **IT Security Maturity Level 4:** Test

   Threat environments continuously evolve, and hence, organizations cannot have static security practices. This maturity level requires that organizations should conduct regular tests to check the effectiveness of their implementations.

e. **IT Security Maturity Level 5:** Integration:

   The highest PRISMA maturity level reviews the program or agency for "integration" of the previous four maturity levels, i.e., information security (1) policies, (2) procedures, (3) implementation, and (4) testing. A program or agency may only attain a higher maturity level after the previous maturity level is attained.

   - Evaluate threats and upgrade existing security controls to evolve and adapt

- Periodical review of policies, procedures, implementation, and tests
- Threats are continually re-evaluated, and controls adapted to changing information security environment.

A PRISMA review focuses on part or all of the strategic and technical aspects of an information security program. The review identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in the following nine (9) Topic Areas (TA):

1. Information Security Management and Culture,

2. Information Security Planning,

3. Security Awareness, Training, and Education,

4. Budget and Resources,

5. Life Cycle Management,

6. Certification and Accreditation,

7. Critical Infrastructure Protection,

8. Incident and Emergency Response, and

9. Security Controls.

The first eight (8) TAs focus on the strategic aspects of information security program management. The review identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in eight areas. The last TA reviews the technical aspects of the overall information security program.

TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30		
2	Information Security Planning	0.20	0.20			
3	Security Awareness, Training, and Education		0.65	0.37	0.31	
	STA **Title**					
	3.1 Security Awareness, Training, and Education					
	Criteria:					
	3.1 1. Have employees and contractors received adequate training to fulfill their security responsibilities prior to access of the system?	Policy maturity question	Procedures maturity question	Implementation maturity question	Test maturity question	Integration maturity question
	3.1 2. Is information security training and professional development for personnel documented and monitored?	Policy maturity question	Procedures maturity question	Implementation maturity question	Test maturity question	Integration maturity question
	3.1 Etc.	⋮	⋮	⋮	⋮	⋮
4	Budget and Resources		0.40	0.20		
5	Life Cycle Management					
6	Certification and Accreditation	0.80	0.30			
7	Critical Infrastructure Protection		0.60	0.30		
8	Incident and Emergency Response	0.80	0.50			
9	Security Controls	0.80	0.60	0.60		

Section 2, *PRISMA Approach Overview*, will provide more detail on the PRISMA maturity levels and scoring.

CHAPTER 4:

The Taxonomy:

When comparing cyber-security maturity models, it may be helpful to create a taxonomy outlining key evaluation criteria. The recommended taxonomy for comparing cybersecurity maturity models is:

1. Frame structure:

- **Categorization of cyber security domains:**

How does this model define and organize various aspects of cyber-security such as risk management, incident response and governance?

- **Maturity level**:

Does the model include a hierarchical maturity scale to measure and track the organization's cybersecurity progress?

- **Dependencies and connections**:

Does this model consider dependencies and interrelationships between various cyber security domains or components?

2. Evaluation method:

- **Evaluation criteria:**

What specific criteria or metrics does the model use to assess an organization's cyber-security maturity level in each domain?

- **Evaluation method:**

How does the model assign points or maturity levels based on scoring criteria?

- **Data collection and analysis:**

What methods or tools are recommended for collecting and analysing data to assess cyber security maturity?

3. Implementation notes:

- **Roadmap or action plan:**

Does this model provide a structured roadmap or action plan for organizations to improve their cyber-security maturity? How detailed and actionable are the instructions?

- **Resource requirements:**

What resources, including people, budget, and technology, are needed to effectively implement the model?

- **Scalability and Adaptability:**

How scalable is this model for organizations of different sizes, industries, or maturity levels? Can it be adapted to specific organizational circumstances?

4. Conformity with standards and regulations.

- Integration with industry standards:

Do your models comply with widely accepted cybersecurity standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework?

- **Regulatory Compliance:**

Does this model address regulatory requirements and help organizations achieve compliance in a particular industry or jurisdiction?

5. Stakeholder involvement:

- Organizational efforts:

How does this model facilitate participation and collaboration among diverse stakeholders, such as management, IT teams, and employees?

- **Communication and reporting:**

Does this model provide guidelines for communicating cyber security maturity levels to internal and external stakeholders? How is reporting and accountability supported?

6. Flexibility and continuous improvement:

- Adaptability to new threats:

To what extent does this model consider emerging cybersecurity threats and technologies?

- Feedback loops and iterative improvements:

Does this model encourage a continuous improvement process that allows the organization to improve its cybersecurity maturity over time based on lessons learned and changing circumstances? Using this taxonomy, organizations consider important aspects such as framework structure, evaluation methodology, implementation guidance, alignment with standards and regulations, stakeholder

involvement, and flexibility for continuous improvement. Systematically evaluate and compare different cyber security maturity models. Such comparisons enable organizations to make informed decisions and select the cyber security maturity model that best suits their particular needs and goals.

CHAPTER 5:

Methodology Used for Performing the Comparative Study:

The most relevant cyber-security models were identified, namely: C2M2, NIST Framework, and PRISMA.
The method to be able to carry out **a** comparative study of the mentioned models based on the classification of software improvement environments is proposed by Halvorsen and Conradi**.**

In Halvorsen and Conradi the comparisons done on five points:
General: qualities that characterise the broad characteristics of the improvement environment fall under this category.
Process: This group of characteristics comprises those that specify how the environment is used.
Organisation: This category covers characteristics that explain how features are related to an organization's properties and the context in which they are employed.
Quality: The elements under this category pertain to the quality dimension and include things like how to assess quality, how to view quality, and what quality implies in terms of quality indicators.
Result: characteristics in this category define the outcomes of using the environment, the expenses associated with reaching the outcomes, and the procedures used to validate the outcomes.

This research enhances the above methodology and considers the following aspects for the comparative analysis of cybersecurity maturity models.

Framework Structure: It says the architecture of the domains, levels of maturity, the areas where these models can be implemented.

Assessment Methodology: It says the data collection methodology after which evaluation is done based on the evaluation criteria.

Implementation Guidance: The roadmap is made which is to be followed and the resources are identified (technical or financial) and the adaptability and scalability with the size of the company or the context of the organization.

Alignment with Standards and Regulations: The model align with the industrial standards (NIST Informative Reference).
Is the model designed to take into account regulatory requirements and assist organisations in achieving compliance in specific industries or jurisdictions?

Stakeholder Involvement: Encourage participation and collaboration among many stakeholders, like as executives, IT teams, and employees.
Is there guidance in the model for communicating cybersecurity maturity to internal and external stakeholders?

Flexibility and Continuous Improvement: How it responds new cybersecurity threats and technologies? Does the model encourage on-going improvement?

6 Analysis and Comparative Study:

1.Framework Structure: Categorization of cybersecurity domains, Levels of maturity, Dependencies and interrelationships are covered.

C2M2 has 10 domains (**Management of Assets, Change, and Configuration (ASSET), Management of Threats and Vulnerabilities (THREAT), (RISK) Risk Management, Access Control and Identity Management, Response to events and incidents, continuity of operations, and situational awareness, Risk Management for Third Parties (Third Parties),Management of the workforce (WORKFORCE),The architecture of cybersecurity,Programme Management for Cybersecurity**) and in each domain has [0-3] levels of maturity.

NIST has 5 DOMAINS **identity, protect, detect, respond, and recover** and there are [0-4] levels of maturity levels for each domain.

PRISMA has 9 Domains (Information Security Management and Culture, Information Security Planning, Security Awareness, Training, and Education, Budget and Resources, Life Cycle Management, Certification and Accreditation, Critical Infrastructure Protection, Incident and Emergency Response, and Security Controls.). There are 5 levels of maturity

Maturity Level 1: Policies,

Maturity Level 2: Procedures,

Maturity Level 3: Implementation,

Maturity Level 4: Testing,

Maturity Level 5: Integration

The idea of interdependence is one of the fundamental ideas in C2M2. A dependency is a connection between two or more assets, like a database and software programme. If one asset is insecure, it could affect the other assets on which it depends. To lower the danger of a cybersecurity event, C2M2 emphasises the value of controlling dependencies. Organisations should make a list of all their dependencies, evaluate the risk involved with each dependency, and put controls in place to lessen that risk.

The NIST Cybersecurity Framework (CSF) domains are interdependent and form a continuous cycle of cybersecurity activities. Each domain builds on the results of the previous domain. For example, in the Identify domain, understanding the assets, risks, and needs of the organization lays the groundwork for developing security measures in the Protect domain. Similarly, response domains build on detection domains in which an organization detects and responds to cybersecurity incidents.

PRISMA domains are also interconnected and interdependent. They cover different aspects of information security management and there are potential interactions and dependencies between domains. For example, the effectiveness of risk management practices in risk management can influence the design and implementation of appropriate access controls in access control management.

2.Assessment Methodology: This includes Evaluation criteria, Scoring methodology, Data collection and analysis.

C2M2:

The evaluation is done on following points:-

- Governance,
- Risk Management,
- Security Controls,
- External Dependencies,
- Situational Awareness,
- Training and Awareness,
- Performance Measurement.

The Cybersecurity Capability Maturity Model (C2M2) scoring system is a four-level scale that assesses an organization's application of cybersecurity practises. The four tiers are as follows:

- Not implemented: The organisation has no cybersecurity practises in place to achieve this goal.
- The organisation has certain cybersecurity practises in place for this goal, but they are not fully applied or effective.
- The organisation has most of the cybersecurity practises in place for this goal, and they are generally effective.
- Fully implemented: The organisation has fully implemented all of the cybersecurity practises necessary to achieve this goal.

NIST Framework:

The evaluation is done on following points:-

- Information Security Governance,
- Risk Management,
- Security Architecture and Engineering,
- Asset Management,
- Access Control,
- Security Operations,
- Security Incident Management,
- Business Continuity and Disaster Recovery,

- Compliance.

It provides guidance on risk management, security management, and cybersecurity best practices. Organizations can use these guidelines to assess their cybersecurity posture and compare it to recommended practices. Assessments typically involve assessing an organization's compliance with specific control requirements, conducting risk assessments, and verifying compliance with relevant standards and regulations. Assessment results help organizations identify gaps and prioritize cybersecurity improvements.

PRISMA:

The following five major aspects form the basis of the PRISMA evaluation criteria:

- The organization's overall information security strategy, including its guiding principles, operating guidelines, and supervision methods.
- The agency's procedures for locating, evaluating, and reducing threats to its information assets are known as risk management.
- Asset management refers to the agency's procedures for locating, categorising, and safeguarding its data assets.
- How well the agency's security controls are implemented and working.
- The agency's initiatives to increase information security knowledge among its staff members and contractors.

The PRISMA rating system is based on a maturity scale with five levels:

- Regulation: The agency has regulations in place that deal with the particular criterion.
- processes: The agency has put in place processes to carry out the policies.
- The agency has put the rules and procedures into place.
- Testing: To ensure that the controls and procedures are effective, the agency has put them to the test.

Procedures and controls have been incorporated by the agency into its overall information security programme.

Only when a prior maturity level has been reached can a higher maturity level be acquired. Therefore, none of the maturity levels can be reached for a particular criterion if a policy is not documented for it.

Each of the review criteria is given a weight by the PRISMA team. The weights are determined by how significant each criterion is to the program's overall information security. The factors that are given the most weight are those that are most important for safeguarding the agency's information assets.

During the PRISMA data collecting phase, details on the agency's information security programme, including its policies, processes, and security controls, are

gathered. Interviews, questionnaires, and document reviews can all be used to collect this data.

3.Implementation Guidance:

C2M2 (Cybersecurity Capability Maturity Model):

This model has following steps evaluate organization’s current state, identify priorities, create an action plan, implement improvements, progress monitoring.

The resources may contain people, software resources and hardware resources expertise, assessment tools, stakeholder engagement, time and effort.

C2M2 is designed to adapt to different organizations and industries. Domains and maturity levels within C2M2 can be customized to fit an organization's individual cybersecurity objectives, infrastructure, and risk posture.

The Cybersecurity Capability Maturity Model (C2M2) is a scalable framework that organisations of all sizes and types can employ. The approach is based on five stages of maturity, ranging from Initial to Advanced, and gives recommendations for how to increase cybersecurity capabilities at each level.

NIST Framework:

This model has following steps Understand NIST Frameworks, Assess Current State, Identify Gaps, Develop Remediation Plan, Implement Remediation, and Maintain Compliance.

The resources required are NIST Publications, Compliance Resources, Technology Tools, and Personnel.

NIST Cybersecurity Framework, provide customizable policies applicable to different industries and disciplines. They provide organizations with a flexible structure to assess and improve their cybersecurity posture. Organizations can customize their implementation of NIST guidelines based on their specific needs, risk profile, and regulatory requirements.

The NIST framework is scalable because it can support organizations of varying size and complexity. Organizations can scale up their implementation efforts by phasing in additional controls, conducting more comprehensive risk assessments, and aligning with higher levels of cybersecurity maturity.

PRISMA:

The roadmap is broken down into four sections:

Planning: During this stage, businesses should evaluate their ISM procedures as they currently stand and pinpoint areas for development. They ought to create a strategy for putting the improvements into practise.

Implementation: During this stage, businesses should put the planning-phase improvements into action. This can entail putting in place new security measures, educating staff about security best practises, or creating fresh security regulations.

Assessment: During this phase, organisations should evaluate the success of the changes they made. They must also pinpoint any new regions that require development.

Continuous improvement: During this phase, businesses should keep enhancing their ISM procedures. This could entail keeping an eye on security threats, performing security audits, and putting new security controls in place.

The amount of resources needed for PRISMA depends on the organization's size and complexity. As range of materials are offered by the PRISMA programme to assist organisations in strengthening their information security posture. Some reosurces are like Tools, Funding,Staff,Time,

PRISMA is a fantastic tool for businesses of all sizes and in all sectors due to its adaptability and scalability. PRISMA can be used by large corporations to undertake in-depth analyses of their information security programmes or by small firms to evaluate their basic information security requirements. Organisations in regulated areas, such healthcare and financial services, can utilise PRISMA to show compliance with legislation unique to those sectors.

4. Alignment with Standards and Regulations :

C2M2 (Cybersecurity Capability Maturity Model):

C2M2 was created to be compatible with a variety of industry standards, laws, and frameworks. It offers a thorough framework that can be in line with other cyber-securities norms like COBIT, ISO 27001, and NIST Cybersecurity Framework.

The regulations are more likely to be followed by organisations that reach a higher C2M2 maturity level. This is so because the model stresses how crucial it is to have a thorough cyber-securities programme that covers all facets of risk management, incident response, and compliance.

NIST Framework:

The NIST recommendations frequently supplement existing cybersecurity norms and laws. Organisations can align their cybersecurity practises with acknowledged standards and best practises in the industry using the NIST frameworks as a base.

Regulatory requirements are frequently aligned with NIST frameworks, such as the NIST Cybersecurity Framework and related Special Publications. Organisations frequently use NIST recommendations to comply with various regulatory requirements, particularly those relating to cybersecurity.

PRISMA:

A flexible technique called PRISMA can be combined with industry standards to give a thorough evaluation of an organization's information security programme. PRISMA can be used to evaluate if a company complies with particular industry requirements, like:

The ISO/IEC 27001 standard is a widely accepted framework for information security management. It was developed by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

The Payment Card Industry Data Security Standard (PCI DSS), a collection of security guidelines created to safeguard cardholder data, is referred to as PCI DSS.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA is a federal statute that governs the security and privacy of medical data.

PRISMA can also be used to assess compliance with industry-specific regulations, such as those governing the financial services, healthcare, and energy industries.s

Some advantages of utilising PRISMA to evaluate regulatory compliance include the following:

PRISMA may assist organisations in identifying and addressing security issues, enhancing their information security policies and practises, and putting in place technological and operational controls to safeguard their information assets.

Increased regulatory compliance: PRISMA can assist organisations in demonstrating compliance with rules unique to their industry, like HIPAA and PCI DSS.

Reduced risk of data breaches: By locating and fixing security flaws, PRISMA can assist organisations in lowering the risk of data breaches.

Enhancing staff productivity, boosting consumer confidence, and lowering the cost of security incidents are all ways that PRISMA may help businesses operate better.

5. Stakeholder Involvement:

In all three frameworks, stakeholder involvement is essential for successful adoption, implementation, and continuous improvement of cybersecurity practices.
Stakeholder engagement provides a more comprehensive understanding of an organization's or sector's specific needs, challenges and risk profile.

The C2M2, NIST, and PRISMA frameworks all stress the value of reporting and communication. The cybersecurity reporting and communication standards from C2M2 and NIST place a strong emphasis on transparency in reporting capabilities, risks, and incidents. The PRISMA team will communicate with the agency throughout the review process, providing regular updates on the progress of the review and soliciting input from the agency on the findings and recommendations. The PRISMA team will also produce a final report that summarizes the findings of the review and provides recommendations for improvement.

6. Flexibility and Continuous Improvement:

Both the C2M2 and NIST frameworks demonstrate adaptability to new threats by providing organizations with flexible frameworks that can be updated and adapted to meet evolving cybersecurity risks. Emphasis on continuous improvement and alignment with the latest best practices. A hybrid framework called PRISMA incorporates components from C2M2 and NIST. As a result, it offers a good compromise between the two frameworks. PRISMA is more equipped to adapt to new threats than C2M2 because it is more recent but is based on NIST's expertise.

The C2M2,NIST and PRISMA frameworks emphasise an approach to cybersecurity improvement that is feedback-driven and iterative, with organisations routinely assessing, planning, implementing, and monitoring their cybersecurity practises and incorporating input to make iterative improvements.

Table 1 presents a summary of the comparative analysis of Cybersecurity Maturity Models.

Table 1: Comparative Analysis of Cybersecurity Maturity Models:

Feature	C2M2	NIST	PRISMA
Domain classification for cybersecurity	10 Domains	5 DOMAINS	9 Domains
Levels of maturity	[0-3] levels of maturity	4 tiers	5 levels
Dependencies and interdependence	C2M2 emphasizes the importance of managing dependencies in order to reduce the risk of a cybersecurity incident.	The NIST Cybersecurity Framework (CSF) domains are interdependent and form a continuous cycle of cybersecurity activities. Each domain builds on the results of the previous domain	Yes, domains are also interconnected and dependent on each other. Risk management practices can influence proper access control design and implementation in access control management
Evaluation standards	Security Controls, Governance, Risk Management	Risk Assessment, Security Controls, Security Awareness and Training	The PRISMA evaluation criteria are based on the following five key areas- Asset management, risk management, and governance security measures, security education and awareness.
Scoring procedures	Maturity levels for scoring.	Maturity levels for scoring.	Maturity levels for scoring.
Gathering and analysing data	Interviews, surveys, and document reviews from previous tests and results threats and vulnerability test in compliance with risk management strategy are used in C2M2 to evaluate cybersecurity	Through a variety of techniques, such as vulnerability scans and audits, NIST focuses on data collection for risk assessments and security control evaluations.	During the PRISMA data collecting phase, details on the agency's information security programme, including its policies, processes, and security controls, are gathered. Interviews, questionnaires, and document reviews can all be used to collect this data.

	skills.		
A road map or an action plan	Analyse the situation now, Establish Priorities, Create an action plan, Adopt Improvements, Track Progress	Analyse the situation now, Establish Priorities, Create an action plan, Adopt Improvements, Track Progress	The roadmap is broken down into four sections: Planning Implementation Assessment Continuous improvement
Resources required	Stakeholder Engagement, Time and Effort, Expertise, Assessment Tools	NIST Publications, Compliance Resources, Technology Tools, and Human Resources	The resource requirements for PRISMA vary depending on the size and complexity of the organization Funding Technical assistance Training and education Access to a community of security professionals
Adaptability and scalability	Yes, scalable as well as adaptable.	Yes, scalable as well as adaptable.	Yes, scalable as well as adaptable.
Compatibility with industry standards	Yes, compatible with industry benchmarks.	Yes, compatible with industry benchmarks	Yes, compatible with industry benchmarks.
Observance of regulations	The regulations are more likely to be followed by organisations that reach a higher C2M2 maturity level. This is so because the model stresses how crucial it is to have a thorough cyber-securities programme that covers all facets of risk management, incident response, and compliance.	On the other hand, NIST frameworks are frequently in line with legal standards and can help businesses comply with various legal requirements.	PRISMA can also be used to assess compliance with industry-specific regulations, such as those governing the financial services, healthcare, and energy industries

Engagement in the workplace	By promoting a culture of cybersecurity knowledge and accountability, C2M2 can have a beneficial effect on workplace engagement.	The NIST Framework for Cybersecurity, for example, offers advice to organisations on how to develop a proactive and risk-based approach to cybersecurity.	The PRISMA framework emphasizes the importance of stakeholder involvement in all stages of the innovation process. Stakeholders can include people, organizations, or groups who are affected by or have an interest in the innovation
Reporting and communication	Throughout the cybersecurity evaluation and improvement process, C2M2 emphasises the necessity of clear and effective reporting and communication.	The necessity of communication and reporting in cybersecurity management is emphasised in NIST frameworks, particularly the NIST Cybersecurity Framework and accompanying Special Publications	The PRISMA team will communicate with the agency throughout the review process, providing regular updates on the progress of the review and soliciting input from the agency on the findings and recommendations. The PRISMA team will also produce a final report that summarizes the findings of the review and provides recommendations for improvement.
Adaptability to new threats	The C2M2 frameworks demonstrate adaptability to emerging threats by offering organisations a flexible framework that can be updated and altered to suit evolving cybersecurity issues.	The NIST frameworks demonstrate adaptability to emerging threats by offering organisations a flexible framework that can be updated and altered to suit evolving cybersecurity issues.	The Programme Review for Information Security Management Assistance for new threat adaptability is a thorough examination of the current status of information security management and the issues that organisations confront in adapting to new threats.
Loops of feedback and iterative improvement	C2M2 promotes an iterative and feedback-driven approach to cybersecurity enhancement.	NIST frameworks, such as the NIST Cybersecurity Framework, advocate for a feedback-driven, iterative approach to cybersecurity management.	Feedback loops and iterative improvement are two important concepts in the Program Review for Information Security Management Assistance (PRISMA) process. Feedback loops allow for the continuous

			improvement of the program by providing information on how well it is meeting its objectives. Iterative improvement allows for the program to be refined and improved over time based on this feedback.
Maturity Progression whether the model suggest reach greater level of maturity	Not always encourage to level up to higher level of maturity. Only if the objective demands.	Always encourage to level up to next higher level of maturity	It can customize the requirements at each maturity level as per the objectives.
If the model is prescriptive and descriptive	Descriptive as all the requirements are specified clearly and well documented.	Prescriptive requirements are at higher level and in depth as methods are vaguely mentioned. Implementations the organization can define.	Descriptive as all the requirements are specified clearly and well documented

Chapter 7:

Conclusion and future work:

This thesis includes a comparative examination and analysis of several cybersecurity maturity models, including C2M2, NIST Framework, and PRISMA. Each model is tailored to certain areas of usage, such as C2M2 for energy and PRISMA for healthcare, whereas NIST is just a collection of practices to be followed with no specific domain in mind. Again, with C2M2 and PRISMA, the practices in each maturity level to be attained can be customised, but the NIST Framework always recommends the highest level of maturity in each scenario. All are meant to establish an immune system for cyber-attacks in order to defend various assets and will get adapted to varied threats over time.

In the future, the goal is to create a framework that contains best practices and assessment tools so that we may deploy such models across many domains, as opposed to domain-specific C2M2 or PRISMA models.

Chapter 8:

Bibliography:

1. A Taxonomy to Compare SPI Frameworks (Christian Printzell Halvorsen1, Reidar Conradi2)

2. Comparative Study of Cybersecurity Capability Maturity Models.

3. Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0.

4. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

5.Program Review for Information Security Management Assistance (PRISMA) (Pauline Bowen, Richard Kissel).

6. INFORMATION SECURITY MATURITY MODEL FOR NIST CYBER SECURITY FRAMEWORK (Sultan Almuhammadi and Majeed Alsaleh).

7. The Community Cyber Security Maturity Model**.**

8.https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2**.**

9.https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework

10.https://csrc.nist.gov/Projects/program-review-for-information-security-assistance**.**