MODULE 4: CYBERSEC INCIDENT MANAGEMENT MATURITY MODEL

The **SEI's Incident Management Maturity Model** is a practical framework that helps organizations assess and improve their capabilities for responding to security incidents. It is based on two existing models: the **Security Incident Management Maturity Model (SIM3)** and the **ENISA CSIRT (Computer Security Incident Response Team)** maturity approach. The SIM3 model was developed by the CSIRT community and has been applied by teams all over the world since 2009. It defines 44 indicators of maturity across four domains: organization, human, tools and processes. The ENISA CSIRT maturity approach was proposed by the European Union Agency for Cybersecurity (ENISA) and provides a three-tier classification of CSIRTs based on their services, cooperation, and quality management.

The SEI's Incident Management Maturity Model combines these two models and aligns them with the requirements of relevant EU policies, such as the NIS Directive. The model can be used by organizations to measure their current level of maturity, identify gaps and areas for improvement, and plan their development roadmap. The model also supports benchmarking and comparison among different organizations or sectors.

4.1 OVERVIEW

SEI'S INCIDENT MANAGEMENT MATURITY MODEL.

The **Software Engineering Institute** (SEI) has been at the forefront of American efforts to counter cyber threats for several decades. To this end, it has produced (in conjunction with others a maturity model that allows organisations to proactively evaluate and improve their ability to manage cyber security incidents.

It is intended for process improvement, it does not measure how well a given incident management activity is performed, only that it is performed. The rationale behind this approach is to allow individual organisations to devise their own implementation, having been given sufficient guidance to do so.

These incident management capabilities have evolved over many years. They are based on a set of metrics developed by the *US Defense Information Systems Agency* (DISA) and *National Security Agency* (NSA) in 2000-2002. The *Department of Homeland Security* (DHS) and *United States Computer Emergency Readiness Team* (US-CERT) funded the initial work to adapt the *U.S. Department of Defense* (DoD) version for Federal use in 2003–2005.

There are multiple aspects to successfully managing computer security incidents. Usually, the primary focus is on the response actions to remedy the incident. As a result, the organization fails to adequately consider that there is more to incident management than reacting when a threatening event occurs. Being proactive is arguably more important than reactive alone; it is the combination of the two that works best.

The capabilities listed here provide a baseline of incident management practices. The incident management capabilities—each including a series of indicators—define the benchmark.

You can use these guidelines to assess how your current incident management functions are defined, managed, and measured. It provides the basis for improvements to the incident management function.

WHAT ARE THESE CAPABILITIES?

The capabilities are used to evaluate an incident management function. In any sizeable organization, one or more groups will be involved in incident management. Each group has a set of its own goals, tasks, and activities (their mission) that must be completed to support the overall strategic mission of the organization. The capabilities in this report explore different aspects of incident management activities for protecting, detecting, and responding to unauthorized activity in an organization's information systems and computer networks, as well as for establishing and sustaining the ability to provide those services.

Each capability includes a set of indicators, which are used by an assessment team to determine whether a capability has successfully been achieved or met. The results from an assessment can help an organization determine the comprehensiveness of its incident management function.

WHAT WE MEAN BY INCIDENT MANAGEMENT FUNCTION (IMF)

An incident management function is a set of capabilities (the people, processes, technology, etc. that provide an ability or capacity to perform some task) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the incident management function (refer to Alberts and colleagues for more information [Alberts 2004]). These capabilities can be provided internally by security or network operators; be outsourced to managed security service providers (MSSPs); or be provided and managed by a computer security incident response team (CSIRT), security operations centre (SOC), or security team. We recognize that CSIRTs might not always be providing these capabilities.

For the sake of simplicity, the term incident management personnel are generally used in this report to refer to the groups (or individuals) performing incident management capabilities. The term incident management function includes everyone who is involved in the performance of incident management activities or the incident management process. The term constituency is used to refer to those who receive the services provided by whoever is performing incident management activities. The term organization is used to refer to the entire group that is composed of the incident management personnel as well as their constituency. Occasionally we use the term CSIRT, which refers to a designated function or group of people to perform a portion of the incident management functions.

Incident management capabilities are grouped into the five categories described in **Table 1— Prepare, Protect, Detect, Respond, and Sustain**. Each category contains a range of subcategories with a set of one or more capabilities. Each capability includes a set of indicators that describe the essential activities leading to adequate performance of that capability.

Within the five major categories and many subcategories, each capability is assigned a priority. These priorities can be useful when making decisions about where to focus improvement efforts.

- **Priority I** capabilities are critical services that an incident management function must provide.
- **Priority II** capabilities are the important services that should ideally be provided.
- **Priority III** constitutes the remaining capabilities. They represent additional best practices that enhance operational effectiveness and quality.

PREPARE	PROTECT	DETECT	RESPOND	SUSTAIN
• Establish IM Function • Core Processes and Tools	• Risk Assessment • Prevention • Operational Exercises for Incident Management • Training and Guidance • Vulnerability Management	• Network and Systems Security Monitoring • Threat and Situational Awareness	• Incident Reporting • Analysis • Incident Response	• MOUs and Contracts • Project/Program Management • IM Technology Development, Evaluation, and Implementation • Personnel • Security Administration • IM Information Systems

Categories and Subcategories

OVERVIEW OF THE MAJOR CATEGORIES (CHS 1 & 2)

The next few paragraphs provide an overview of the major categories: Prepare, Protect, Detect, Respond, and Sustain.

PREPARE

Prepare focuses on establishing an effective, high-quality incident management function. This includes formally recognizing an incident management function, defining roles and responsibilities, and establishing interfaces between the various groups and individuals performing or affected by incident management functions. High-level processes must be defined, and essential tools, such as an incident tracking system, need to be acquired and embedded.

Trusted relationships, both internal and external, are established for the purpose of sharing relevant and necessary information.

PROTECT

Protect relates to the actions taken to prevent attacks and to mitigate the impact of those that do occur.

Preventative actions secure and fortify systems and networks, which helps to decrease the potential for successful attacks against the organization’s infrastructure. In this model, Protect is focused on what changes can be made to the infrastructure as part of the response to contain or eradicate the malicious activity. It also includes taking proactive steps to look for weaknesses and vulnerabilities in the organization while understanding new threats and risks. Such steps can include:

- Performing security audits, vulnerability assessments, and other infrastructure evaluations to address weaknesses before they can be successfully exploited.
- Collecting information on new threats and evaluating their impact

Mitigation involves making changes in the constituent infrastructure to contain, eradicate, or fix actual or potential malicious activity. Such actions might include.

- Making changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure.
- Updating intrusion-detection system (IDS) or anti-virus (AV) signatures to contain new threats.
- Installing patches for vulnerable software

Changes to the infrastructure may also be made, based on the process improvement changes and lessons learned that result from a post-mortem review done after an incident is handled. These types of changes are made to ensure that incidents do not happen again or that similar incidents do not occur.

DETECT

In Detect, information about current events, potential incidents, vulnerabilities, or other security or incident management information is gathered proactively and reactively. With reactive detection, information is received from internal or external sources in the form of reports or notifications. Proactive detection calls for action by the designated staff to identify suspicious activity through monitoring and analysis of a variety of logging results, situational awareness, and evaluation of warnings about situations that can adversely affect the organization’s successful operation.

RESPOND

Respond includes the steps taken to analyse, resolve, or mitigate an event or incident. Such actions are targeted at understanding what has happened and what needs to be done to enable the organization to resume operation as soon as possible or to continue to operate while dealing with threats, attacks, and vulnerabilities. Respond steps can include:

- Analysis of incident impact, scope, and trends.
- Collection of computer forensics evidence, following chain-of-custody practices.
- Additional technical analysis related to malicious code or computer forensics analysis.
- Notification to constituents, stakeholders, and other involved parties of incident status and corresponding response steps.
- Development and release of alerts, advisories, bulletins, or other technical documents.
- Coordination of response actions across the organization and with other involved internal and external parties.
- Verification and follow-up to ensure that response actions were correctly implemented, and that the incident has been appropriately handled or contained.

SUSTAIN

Sustain focuses on maintaining and improving the CSIRT or incident management function itself. It involves ensuring that:

- The incident management function is appropriately funded.
- Incident management personnel are appropriately trained.
- Infrastructure and equipment are adequate to support the incident management services and mission.
- Appropriate controls, guidelines, and regulatory requirements are followed to securely maintain, update, and monitor the infrastructure.
- Information and lessons learned from the Protect, Detect, and Respond processes are identified and analysed to help determine improvements for the incident management operational processes.

EXPLANATION OF THE CAPABILITY STRUCTURE

The capabilities are formatted in a workbook structure that can be used during an assessment to both conduct the assessment and capture information. The structure for each incident management capability provides two basic sets of information:

- the capability itself, presented as a primary capability statement, and a more detailed set of indicators that can be used by the assessor to assess the performance of the capability.
- explanatory information and scoring guidance—additional information explaining the significance of the capability and how to assess the performance of that capability.

Each capability also includes a set of cross-references to selected regulations or guidance: the *Federal Information Security Management Act* (FISMA), *National Institute of Standards and Technology* (NIST) publications, and relevant best practices.

Each capability includes indicators to assess the performance of that capability. Within these indicators, when the word personnel are used, it refers to whomever is performing the activities associated with the capability. If other roles or more specific types of roles are being referenced, the indicator will specify which type of personnel.

These indicators are grouped into three areas: Required, Recommended Best Practice, and Institutional and Quality Improvement. All the indicators in the Required area must be met for an organization to successfully meet this capability. The indicators in the Recommended Best Practice area represent additional aspects that are recommended for a more complete or robust capability. The indicators in the Institutional and Quality Improvement area are those needed to ensure this capability can be sustained, that is, those things that would ensure the continuity or resilience of the capability even in the face of personnel changes. In addition, there are four types of indicators, specified by the italicized word occurring before the indicator statement:

- Prerequisites must be met before this capability can be performed or be performed adequately.
- Controls are available or exist that direct the proper execution of the activities.
- Activities are performed as part of this capability (and could be observed by an assessor).
- Quality indicators measure effectiveness, completeness, usefulness, institutionalization, and other quality aspects of the activities.

To help the assessor use the tables, the following list explains how the information for each capability is organized. Reading the table from left to right, the fields are

- Capability subcategory and number (e.g., 2.1 Risk Assessment)
- Capability reference number and statement—represents major category number, subcategory number, and specific capability number and statement (e.g., 2.1.1 Security risk assessments (RAs) are performed on the organization.)

- Priority—I through III (where priority I is the most important)
- Clarification—additional information explaining the purpose and description of the capability team guidance—information to help an assessment team score this capability
- References—standards, guidelines, or regulations relating to this capability, including a placeholder for organization-specific references
- Organization response—optional field if early information was collected from an organization indicating how they would respond to the capability
- Examples of evidence—list of possible evidence the team should look for during interviews, documentation reviews, or observations
- Scoring criteria—the indicators (preceded by a unique indicator number), scoring choices (Yes/No), and room to list evidence (i.e., the specific criteria the assessors can see or examine during the assessment to help them determine whether the capability is being performed)
- Final score— "Met" if all required indicators are met; "Not Met" if any required indicator is not met, Not Applicable—used when capability is excluded from scoring, Not Observed—used when capability was not observed during the assessment
- Evidence collected place to identify what documents were reviewed, interviews conducted, or activities observed
- Notes—additional notes made by the assessment team either in preparation for the assessment or during the assessment
- Suggestions for improvement—additional ideas for an organization to consider if it works to improve this capability beyond implementing the concepts in each indicator

4.2 PERFORMING ASSESSMENTS

A C2M2 capability assessment is a process of evaluating the maturity of an organization's cybersecurity practices based on a standardized model. The C2M2 stands for *Cybersecurity Capability Maturity Model,* and it consists of the 10 domains (described earlier), such as Risk Management, Asset Management, Identity and Access Management, etc.

Each domain has a set of objectives and practices that describe different levels of capability, from 0 (Incomplete) to 3 (Optimized). To perform a C2M2 capability assessment, an organization follows these steps:

1. **Select a facilitator and a team** of participants who are familiar with the organization's cybersecurity activities and processes.
2. **Choose one or more domains to assess**, depending on the scope and purpose of the assessment.
3. **Review the C2M2 model and its components**, such as the objectives, practices, indicators, and target states.
4. **Conduct a self-assessment** using the C2M2 toolkit, which provides a questionnaire and a scoring tool for each domain.
5. **Analyse the results and identify the strengths and gaps** in the organization's cybersecurity capabilities.
6. **Develop an action plan** to address the gaps and improve the capabilities based on the priorities and resources of the organization.
7. **Implement the action plan and monitor the progress** and outcomes of the improvement efforts.
8. **Repeat the assessment periodically** to measure the changes and track the maturity level over time.

A C2M2 capability assessment can help an organization to benchmark its cybersecurity performance, identify areas for improvement, and align its practices with best practices and standards.

USING THESE CAPABILITIES TO ASSESS THE INCIDENT MANAGEMENT FUNCTION OF AN ORGANIZATION

This section provides an overview of how the capabilities can be used to assess and improve an organization's incident management function. This section and the next provide an overview of the assessment methodology and considerations for scoring the capabilities. To generalize, this assessment method centres around using interviews, artefact reviews, and activity observations to determine how completely the incident management activities represented in the capabilities are performed.

It is possible to use these capabilities for a broad range of assessments. For example, the entire set of capabilities can be used to assess an organization's entire incident management function. A subset can be used to focus on only the specific responsibilities of an actual SOC, CSIRT, or security service provider. The extent or scope of an assessment is determined early in the process, based on the goals of the organization or the specific focus of the assessment sponsor. The assumption for this section is that the entire incident management function is being assessed. An assessment with a narrower scope would simply use fewer capabilities and assess fewer groups.

Incident management, as a complete function, includes activities that may be performed within a SOC, by a CSIRT, or by other groups across an organization. There may be several groups, each with some distinct or overlapping responsibilities that support management of cybersecurity events and incidents. In the latter case, applying these capabilities against only a designated centralized incident management function or CSIRT may result in an inaccurate or very limited view of the organization's total ability to effectively manage cybersecurity incidents. An assessment should consider all groups performing incident management activities to produce accurate results.

An assessment using these capabilities generally requires:

- **Assessment planning**: establishing points of contact, assessment scope, schedule, and resources and assembling the assessment team and supporting equipment and supplies
- **Pre-assessment**: preparing for on-site assessment activities; gathering information as needed before going onsite; analysing available documents and other artifacts; identifying groups and individuals (e.g., groups involved in Prepare, Protect, Detect, Respond, and Sustain activities) to interview onsite; allocating capabilities to those groups; and finalizing the onsite schedule
- **Onsite**: conducting interviews, observing activities, reviewing additional artefacts, documenting evidence collected, determining preliminary scores according to evidence rules, and gathering additional information, if possible, to fill any gaps
- **Post-assessment**: performing final analysis and scoring and, optionally, identifying recommendations for improvement, producing a report for stakeholders, and conducting required reviews
- **Close-out**: properly disposing or archiving of gathered information and conducting a "lessons learned" review

Some specific guidance for selecting assessment activities follows.

IDENTIFY THE GROUPS INVOLVED IN INCIDENT MANAGEMENT AND ALLOCATE THE CAPABILITIES

There are many techniques for identifying the groups involved in incident management. One technique uses a process model benchmark for incident management, such as that described by Alberts and colleagues. By comparing the organization to this process model of incident management activities, all groups performing such activities can be identified. An alternative is to use some form of work process modelling to map all groups and interfaces associated with incident management activities. Once the groups and activities are identified, capabilities can then be allocated to each group (e.g., allocate Detect capabilities to the groups performing network monitoring).

Bear in mind that there may not be clearly defined roles that align with the categories, and you may need to ask more than one group about the same set of capabilities to achieve complete coverage. While you can adjust your schedule of interviews and observations when onsite, it is best to keep schedule adjustments to a minimum.

ASSESS EACH GROUP

The simplest means of assessing each group against its capabilities is to conduct interviews or group discussions, observe the activity being performed or a demonstration of the activity, and ask the assembled individuals about each capability that is applicable to their group. Artefacts related to the capabilities can be requested and reviewed and, when necessary, additional activities can be observed. The assessment team should use the general scoring guidance in Section 4 of the model and the specific guidance provided with each capability to guide its assessment. (See Section 2 of the model, "Explanation of the Capability Structure," for a description of the sections and indicators provided for each capability.)

When more than one group shares the responsibilities to perform a certain capability, the assessment team should conduct interviews (or group discussions, observations, or process demonstrations, as applicable) with at least two of the involved groups, and then compare and assess the collective results from the different sources. (See Section 3.3 for further guidance about groups that cannot be assessed.) When the results for capabilities or individual indicators differ between groups, the lowest score generally prevails (i.e., if one individual or group indicates "Yes" to an indicator but another individual or group says "No," the combined score for the organization for that indicator will generally be "No").

All indicators are scored as either Yes or No, and Capabilities are scored at the end as "Met," "Not Met," "Not Observed," or "Not Applicable."

- "**Met**"—At a minimum, all the required indicators have been met.
- "**Not Met**"—One or more of the required indicators has not been met.
- "**Not Observed**"—A capability cannot be assessed because the assessment team does not have access to the individuals who can provide the correct answer or cannot observe that the activity or capability was performed.
- "**Not Applicable**"—The activity is not included in the assessment, which may mean that it is deliberately not performed by the organization as part of the incident management processes. Capabilities that are not applicable should be identified during assessment scoping.

DETERMINE WHAT TO DO ABOUT GROUPS THAT CANNOT BE ASSESSED

Given the complexities and political realities of some organizations, it may not be possible to meet with some groups or obtain access to certain types of information. At the very least, the interface to that group or the way in which those groups interact should be assessed. The organization can then decide if those groups should be assessed later.

Alternatively, those groups could assess themselves using applicable information from these capabilities and then provide the results (or feedback) to appropriate individuals. Another option is to use an external or third-party organization to perform the assessment on relevant groups. If part of the incident management function is outsourced and the organization being assessed can provide sufficient evidence to prove that the outsourced contractor or group is performing the capability, the outsourced contractor or group may not need to be assessed. If specific information cannot be reviewed, the assessment team and assessment sponsor will need to decide if the remaining evidence is sufficient to indicate an actual score or if "Not Observed" needs to be used.

USE THE RESULTS TO DECIDE WHAT TO IMPROVE

The organization, using the assessment results, has a clear idea of how it is meeting these capabilities with respect to incident management. It knows what its strengths and weaknesses are. To improve the processes, the organization can look at the resulting scores and begin to create a strategy for improvement building on its strengths. For example, the candidates for improvement could be sorted by priority order, so that unmet Priority I capabilities come first, and so on.

Existing strengths can be used to improve weaker areas. For example, if some capabilities have exceptionally good procedures and policies, use those as a basis for developing policies and procedures for capabilities that are not as robust or are missing. If there is a strong training program for some types of personnel, expand that program to include additional types of training for capabilities that are lacking.

A further review of results may be needed when considering improvements in Priority II through Priority III capabilities. For example, improving a Priority III capability from "Not Met" to "Met" might be less critical than improving a Priority II capability from "Not Met" to "Met." Each organization makes its own determination concerning the order in which to improve scores on any Priority II-III capabilities based on a review of the entire set and by considering the changes that are needed, the required resources, the mission, the goals, and the objectives.

Finally, a common type of improvement for all the capabilities can be found by looking at the non-required indicators: Recommended Best Practices and Institutional and Quality Improvement indicators. These types of improvements go beyond meeting the basic requirements and consider additional aspects that can build an exceptional incident management function. Even those capabilities for which required indicators were successfully met can be improved by implementing the non-required indicators.

Each capability should be examined to consider the relative consequences of “doing” or “not doing” the capability or required indicators therein. This examination can provide elemental insight into whether improvement might yield an unexpected result. Look to the suggested improvements for ideas on enhancing performance or identifying ways to improve. When applying the capabilities to identify improvements, use judgment and common sense, respect the budgetary process, and stay abreast of changing regulations and standards in this ever-evolving environment.

Ultimately, the end goal for these capabilities (or other types of assessments) is to strive for continuous improvement of the processes, so it is also a recommended best practice to periodically re-assess to see what new “current” state has been achieved. This re-assessment could be done annually or as conditions change (e.g., as new technologies are deployed, the infrastructure changes, or new partnerships or supply chains are adopted).

These capabilities should be considered a starting place for identifying improvements. They are not a precisely defined path for every organization to build the perfect incident management function, but they can be used as a guideline for what to include in an incident management function, based on the organization’s mission and the incident management function’s services.

4.3 SCORING THE CAPABILITIES

GENERAL GUIDANCE FOR SCORING CAPABILITIES

This section discusses scoring issues that the assessment team needs to remember as it is conducting an assessment. Each capability can have a score of "Met" or "Not Met." To determine the score for a capability, the assessment team applies the rules of evidence against all the information gathered from interviews, demonstrations, observations, and document or artefact reviews. Interviews are question-and-answer sessions with one or more people with peer relationships where the assessment team uses the capabilities as the basis for asking questions. In observations, the assessment team watches one or more people conduct their actual IM activities; the team observes only and does not question or ask for additional actions. In demonstrations, the assessment team interacts with the people performing real or hypothetical IM activities, asking questions, getting demonstrations of what could occur, or how tools might be used in hypothetical situations. Observations and interviews are similar. Document or artefact reviews are conducted by assessment team members to understand relevant parts of IM-related documents.

For each capability, all Required indicators must have an answer of "Yes" to obtain a successful or passing score for that capability (i.e., the capability is met). If one or more of the Required indicators has an answer of "No," the score for the capability is "Not Met." The Recommended Best Practice indicators and the Institutional and Quality Improvement indicators include those that are not necessarily required to achieve success for the capability but are recommended. These indicators are not included in the final determination of a capability being met or not met. They are currently provided for improvement purposes. See Section 4.3 for alternative scoring ideas.

EVIDENCE COLLECTION REQUIREMENTS

Sufficient evidence for establishing a passing score requires more than one document, interview, observation, or demonstration. The indicators listed with each capability are used to assist in the collection of evidence. The Evidence column to the right of each indicator is used to record the type of evidence (e.g., interview, observation, demonstration, or document review) or a description of the evidence that was used to score that indicator.

If a capability is to be scored "Met," all Required indicators for that capability have been determined to be covered (checked "Yes"). The coverage rules for sufficiency of evidence to determine if an indicator can be checked "Yes" are provided in Table 2 below. In summary, it takes at least two different types of sources to confirm an indicator. Note that in the rules for sufficiency, an interview and a demonstration are considered equivalent. An observation, then, needs the confirmation of an interview or demonstration, or a document review. A document review needs the confirmation from either an observation or a demonstration/interview. Also note that it takes at least one document, but in general, more than one document is preferred.

Evidence Rules

	Interview/ Demonstration	**Observation**	**Document/Artifact**
Interview/ Demonstration	Not Sufficient	√	√
Observation	√	Not Sufficient	√
Document/Artifact	√	√	Not Sufficient

CHECK COMPLETENESS AND QUALITY OF DOCUMENTED POLICIES AND PROCEDURES

When deciding if documented policies and procedures referenced in the indicators are adequate, assessment teams should consider the following:

- Does the policy or procedure adequately address the process, technology, requirements, expected behaviours, or another topic it is supposed to address?
- Do the procedures reflect what is done by personnel?
- Are the policies and procedures easily available to personnel?
- Are the policies or procedures being kept up to date? There should be a review and/or revision date or some indication that policies and procedures are reviewed and changed as needed. Also look for
  - a defined process and periodicity for reviewing and revising
  - established criteria for when to review (e.g., change in organization structure, major technology installation)
  - defined roles and responsibilities for review and update
  - a defined process for communicating changes and revisions throughout relevant parts of the organization
  - a change log history
  - indications the date was simply changed to make it look up to date5

It may also be useful to ask for any documents that are currently being revised to help evaluate their process for keeping documents up to date or to at least demonstrate that they are in the process of improving a current gap. Such findings will be useful when the organization decides what to improve. In most cases, policies (and processes) are included in the Required indicators, and documented, formal procedures are included in the Institutional and Quality Improvement indicators.

DETERMINE PERSONNEL KNOWLEDGE OF PROCEDURES AND SUCCESSFUL TRAINING

The assessment team should be able to determine from discussions with the personnel whether they understand the process (e.g., they are able to describe it intelligently and consistently). More importantly, the personnel should be able to easily show how they perform that work (e.g., show the forms that they fill in, describe the process they use to take information from an incident report that is displayed and extract information to feed into summary or other organizational or regulatory reports, or demonstrate how they perform analysis on a set of logs). A process can be consistently known and followed even without a formal, documented procedure. If a documented procedure does exist, the assessment team needs to determine if the procedure is followed.

Training can range from formal training that has complete packages with materials and dedicated instructors to informal, on-the-job mentoring by more senior, experienced personnel. The assessment team seeks to determine whether training is provided, that the training is sufficient to meet the needs of the organization, and, as shown in the Institutional and Quality Improvement indicators, that the personnel are knowledgeable and perform the procedures consistently.

During demonstrations, the assessment team can ask personnel to discuss the process they are following to show a level of understanding that supports knowledge of their capabilities about the activities being conducted. The observation of personnel performing tasks can also provide an indication of the maturity of their operations and training. For example, observation can show that personnel know the following:

- how to use the tools that support the capabilities
- where reports or data are archived
- what types of information are contained in reports or alerts or other documents and products
- where procedures, policy, or guidance documents are kept and how to access them if needed

SCORING VARIATIONS

It is possible for the assessment team and assessment sponsors to determine a different scoring algorithm (e.g., all the Required and Recommended Best Practice for a “Met” score). The only caution would be to use a consistent scoring algorithm over time to allow for accurate determination of improvement from one assessment to the next or for accurate comparison between assessed groups.

In addition to the “Met,” “Not Met,” “Not Observed,” or “Not Applicable” scores for a capability, some assessors have used a “Partial” score. “Partial” in this case would mean that some of the Required indicators have been met, but not all. “Partial” scores can be difficult to use as it becomes more subjective as to what percentage or number of Required indicators is needed to reach a “Partial” as opposed to a “Not Met” score. Some assessment teams have also found it useful to use “Not Observed,” or “Not Applicable” for the indicators as well as the capability. In that case, on the worksheet, the indicator can be scored as either a “No,” and the evidence column used to state the rationale for it being not observed, or scored as a “Yes,” with the rationale for it not being applicable in the evidence column.

4.4 THE CAPABILITIES

THE INCIDENT MANAGEMENT CAPABILITIES

The remainder of this document contains Version 3.0 of the capabilities, split into five sections:

- **Prepare**: Section 1 of the capabilities
- **Protect**: Section 2 of the capabilities
- **Detect**: Section 3 of the capabilities
- **Respond**: Section 4 of the capabilities
- **Sustain**: Section 5 of the capabilities

These capabilities are a living document. Periodic changes may be made to these capabilities, and new versions may be released.

PREPARE: SECTION 1 OF INCIDENT MANAGEMENT CAPABILITIES

Prepare is getting the incident management function up and operational. This includes getting the incident management function established, creating and implementing the necessary plans, defining the key work processes that will be essential to the smooth functioning of an incident management function, and establishing the necessary working relationships with both internal and external experts and groups who will provide needed assistance and expertise.

Getting formal recognition and designation as an incident management function, regardless of whether it is a formal CSIRT, is essential to ensuring that the other parts of the organization understand and agree to accept the services provided and provide the required information to the incident management function. If that does not happen, the IM function may not be able to perform effectively. Defining roles, responsibilities, and interfaces among groups of people performing incident management capabilities is needed to ensure everyone knows what their job is and how to work efficiently with other groups to detect, analyse, and respond to incidents.

The plans that are developed will establish and sustain the incident management function in terms of how it will function, communicate, and deal with incidents when they occur. The core processes are needed to define how the various key activities will be carried out, and the essential tools needed by the incident management function must be acquired. Chief among these tools is the incident repository where all the information relevant to incidents will be retained. This repository allows not only the immediate analysis of current incidents but also later analysis for trends and patterns, forensic analysis, and so forth.

Finally, no incident management function can be effective if it operates in isolation. IM personnel must establish trusted relationships with other experts to be aware of events and other types of attacks going on outside the organization and to reach back for additional expertise and help when faced with a new or unprecedented form of incident or the need for new tools. It takes time to get these relationships established and maintain them. This needs to be done as part of preparing.

Within the Prepare category, the subcategories and their capabilities include the following:

ESTABLISH IM FUNCTION

1.1 Establish IM Function—Establishing the IM function requires formal recognition and acceptance of its existence and its mission, who the people are who perform the activities and what they do and defining how it works with other groups.

1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).

1.1.2 An incident management plan has been developed and implemented for the organization.

1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.

1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.

1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.

CORE PROCESSES AND TOOLS

1.2 Core Processes and Tools—An incident management function needs to establish the core practices and the basic tools that will be required for effective performance of incident management activities. That includes understanding how work will be managed, incident information will be retained, and how the potential for insider threat can be controlled.

1.2.1 A communication plan for incident management activities has been established and disseminated.

1.2.2 An IM information management plan is established and followed.

1.2.3 An inventory exists of mission-critical systems and data.

1.2.4 Workflow management processes and/or systems are implemented.

1.2.5 A central repository exists for recording and tracking security events and incidents.

1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.

1.2.7 An insider threat program exists within the organization

Refer to Incident Management Capability Assessment Workbook. December 2018 TECHNICAL REPORT CMU/SEI-2018-TR-007

4.5 INCIDENT MANAGEMENT CAPABILITIES

LIST OF INCIDENT MANAGEMENT CAPABILITIES

A simple list of all the capability statements contained in the ***SEI-CMU's Cybersecurity Maturity Model***.

Capabilities	Priority
Prepare	
Establish IM Function	
1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).	II
1.1.2 An incident management plan has been developed and implemented for the organization.	I
1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.	I
1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.	I
1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.	III
Core Processes and Tools	
1.2.1 A communication plan for incident management activities has been established and disseminated.	II
1.2.2 An IM information management plan is established and followed.	II
1.2.3 An inventory exists of mission-critical systems and data.	I
1.2.4 Workflow management processes and/or systems are implemented.	III
1.2.5 A central repository exists for recording and tracking security events and incidents.	I
1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.	II
1.2.7 An insider threat program exists within the organization.	I
Protect	
Risk Assessment	

2.1.1 Security risk assessments (RAs) are performed on the constituents' organization.	I
2.1.2 The constituents get help correcting problems identified through security risk assessment (RA) activities.	II
Prevention	
2.2.1 The organization has an institutionalized malware prevention program.	I
Operational Exercises for Incident Management	
2.3.1 Operational exercises are conducted to assess the IM function of the organization.	II
Training and Guidance	
2.4.1 Guidance is provided to constituents on best practices for protecting their systems and networks.	II
2.4.2 Constituents are provided with security education, training, and awareness (ETA).	I
Vulnerability Management	
2.5.1 A patch management and alert program exists.	I
2.5.2 Proactive vulnerability assessment is performed on constituent networks and systems.	I
2.5.3 Constituents receive help to correct problems identified by vulnerability assessment activities.	II
Detect	
Network and Systems Security Monitoring	
3.1.1 Security monitoring is continuously performed on all constituent networks and systems.	I
External Sources of Incident Information	
3.2.1 Events and incidents are reported from outside the organization.	I
Threat and Situational Awareness	
3.3.1 Public monitoring of external security websites and other trusted sources of information is conducted.	I
3.3.2 Trend analysis is supported and conducted.	II

3.3.3 Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment, and constituents are notified of the updates.	I
3.3.4 Penetration testing is conducted on organizational networks and systems.	I
Respond	
Incident Reporting	
4.1.1 Events and incidents are reported from the constituency.	I
4.1.2 Incidents are reported to appropriate management in accordance with organizational guidelines.	I
4.1.3 Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines.	I
4.1.4 Incident management is supported for restricted information, networks, and systems.	I
Analysis	
4.2.1 Incident management personnel conduct triage of events and incidents.	I
4.2.2 Incident analysis is performed on declared incidents.	I
4.2.3 Incident correlation is performed to identify similar activity.	II
4.2.4 Impact of an incident is determined.	II
4.2.5 Incident root cause analysis is conducted.	II
4.2.6 Fusion analysis is performed to identify concerted attacks and shared vulnerabilities.	III
4.2.7 Retrospective analysis is conducted.	III
4.2.8 Media analysis is performed on constituent networks and systems.	II
4.2.9 Artifact or malware analysis is conducted.	II
Incident Response	
4.3.1 General incident response guidance and procedures are distributed to constituents.	II
4.3.2 Incidents are resolved.	I

4.3.3 Incident management personnel coordinate incident response across stakeholders.	I
4.3.4 Incident management personnel create alerts and warnings and distribute them as needed.	I
4.3.5 Incident management personnel verify that a response is implemented, as appropriate, and that the incident is closed, in accordance with organizational guidance.	I
4.3.6 Postmortem reviews of significant incidents are conducted, and lessons learned are identified and acted upon, as appropriate.	I
Sustain	
MOUs and Contracts	
5.1.1 A list of incident management services provided by the designated incident management function is documented.	II
5.1.2 The constituency provides advance notification of all changes or planned outages to their networks.	III
5.1.3 Formal agreements exist for managing IM activities with third parties across the supply chain.	I
Project/Program Management	
5.2.1 A financial plan exists for incident management activities.	III
5.2.2 A workforce plan exists for incident management personnel.	II
5.2.3 A personnel security plan exists for incident management personnel.	I
5.2.4 A quality assurance (QA) program exists to ensure the quality of provided products and services.	II
5.2.5 An established plan exists to ensure continuity of operations for incident management.	I
5.2.6 The effectiveness of the incident management function in meeting its mission is routinely evaluated and improved.	III
IM Technology Development, Evaluation, and Implementation	
5.3.1 The incident management function has the tools it needs to meet its mission.	I
5.3.2 Software tools are tested for use within the incident management environment.	II
5.3.3 The IT infrastructure for incident management is adequate to support incident management operations.	I
Personnel	

5.4.1 A training program exists for incident management personnel.	I
5.4.2 Support for professional development exists for incident management personnel.	III
Security Administration	
5.5.1 Physical protective measures are in place to protect incident management IT systems, facilities, and personnel.	I
5.5.2 An operations security (OPSEC) program exists.	I
IM Information Systems	
5.6.1 An inventory exists of mission-critical incident management systems, data, and information.	I
5.6.2 Defense-in-depth strategies and methodologies exist for hardening the incident management computer networks and systems.	I
5.6.3 Processes and technologies exist to support the confidentiality, integrity, and availability of incident management data and information.	I
5.6.4 Network security monitoring is performed on all incident-management-related networks and systems.	I
5.6.5 Security risk assessments (RAs) are performed on the incident management function.	I
5.6.6 Vulnerability assessments are performed on incident management systems and networks.	I
5.6.7 A patch management program is in place for the incident management systems.	I
5.6.8 More than one communications system or mechanism (other than email) exists for receiving and distributing notifications, information about new viruses, incidents, vulnerabilities, threats, and other kinds of warnings.	II

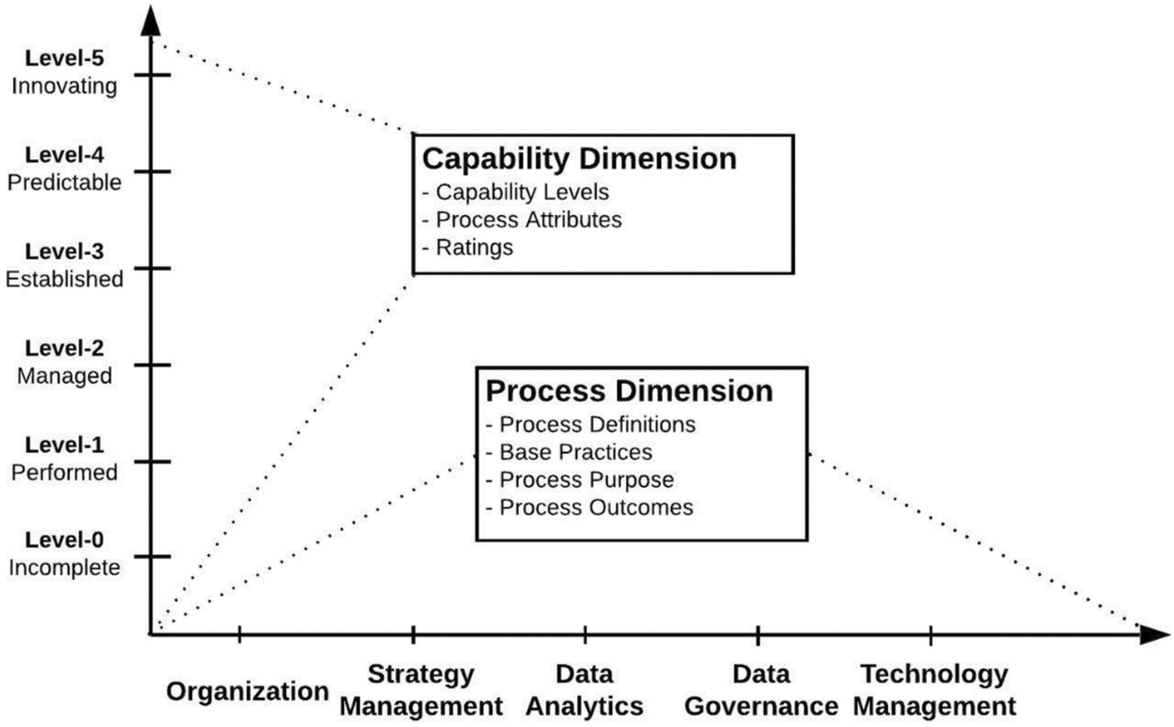
4.6 CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

The **Cybersecurity Capability Maturity Model (C2M2)** is a tool developed by the US Dept of Energy (DOE) to give organizations the means to consistently assess their cybersecurity capabilities. The assessment highlights way to *improve* an organisation's cybersecurity capability.

In this regard, the model helps organizations identify their current level of cybersecurity maturity and develop a roadmap for improving their cybersecurity posture over time.

The C2M2 is based on the SEI's *Capability Maturity Model Integration* (CMMI) framework, which is widely used in software engineering and other industries to assess and improve organizational processes.

The basic concept of the 'capability maturity models' has been applied across various industries and professions owing to its simple conceptual design and adaptability. They simply establish the comprehensive range of processes that must be performed for given discipline, then measures how well a particular process is being performed.



One of the advantages of the CMM (Capability Maturity Model) concept is that they are 'process model' that describes the process, but not how to execute the process, leaving that for the organisation to devise their own ways and means on the assumption that they know their business best. A 'one size fits all' model that prescribes the 'how' would not work in practice.

With this flexibility of application, but encompassing all required activities, a maturity model becomes an excellent process improvement tool. The concept was originally devised in the 1980's by Watts Humphrey at the Software Engineering Institute at Carnegie-Mellon University in Pittsburgh. There was a need to establish the means for the US Dept of Defense to evaluate the software development capabilities of suppliers of software intensive products to the DoD. And to provide those suppliers with the means to improve their capability.

The key rationale behind the design of CMMs (Capability Maturity Model) can be summarized as follows:

Assessing Current Capabilities - CMMs aim to provide a systematic and standardized way of evaluating an organization's current capabilities in a specific area. By assessing their capabilities against predefined maturity levels, organizations can gain insights into their strengths, weaknesses, and areas for improvement. This assessment helps organizations identify gaps and set realistic goals for enhancing their performance.

Establishing a Common Language - CMMs create a common language and shared understanding within an organization and across industries. They define key concepts, processes, and practices related to a specific domain, enabling organizations to communicate and collaborate effectively. This common language facilitates knowledge sharing, benchmarking, and comparison among different organizations.

Providing a Roadmap for Improvement - CMMs offer a structured roadmap for organizations to enhance their capabilities incrementally. By defining maturity levels and associated practices, CMMs provide organizations with a clear progression path. This roadmap allows organizations to prioritize and focus their efforts on areas that require improvement, ensuring a systematic and step-by-step approach to maturity enhancement.

Encouraging Continuous Improvement - CMMs emphasize the importance of continuous improvement and ongoing development. They recognize that maturity is not a static state but rather a journey of constant growth and evolution. CMMs encourage organizations to adopt a culture of learning, innovation, and adaptation, fostering a mindset of continuous improvement in their practices, processes, and performance.

Enabling Benchmarking and Best Practices - CMMs facilitate benchmarking against industry best practices and standards. They provide organizations with a reference point to compare their capabilities with peers and industry leaders. This benchmarking allows organizations to identify areas where they lag and learn from others' successes. It promotes knowledge sharing and collaboration, ultimately driving overall industry advancement.

Supporting Decision-Making and Resource Allocation - CMMs help organizations make informed decisions and allocate resources effectively. By providing a structured assessment of capabilities and areas for improvement, CMMs enable organizations to prioritize investments, allocate resources efficiently, and address critical gaps. This data-driven approach ensures that resources are allocated based on identified needs and strategic objectives.

In summary, the design of capability maturity models is grounded in the principles of assessment, improvement, common understanding, roadmap development, continuous learning, benchmarking, and resource allocation. CMMs serve as valuable tools for organizations to enhance their capabilities, establish industry best practices, and achieve higher levels of performance in a structured and systematic manner.

4.7 C2M2 MATURITY LEVELS

The C2M2 consists of five maturity levels, each with a set of capabilities that organizations must demonstrate to achieve that level. The five levels are:

INITIAL (LEVEL 1)

At this stage, cybersecurity practices are ad hoc and unorganized. The organization has limited awareness of cybersecurity risks and lacks a formal strategy. There may be a reactive approach to security incidents, and the focus is primarily on resolving immediate issues rather than implementing preventive measures.

The primary goal at this level is to establish a foundation for a structured cybersecurity program.

MANAGED (LEVEL 2)

At the managed level, the organization starts implementing *basic* cybersecurity controls and processes. There is a defined and documented cybersecurity policy and strategy. The organization has a better understanding of its critical assets and associated risks.

Incident response plans and procedures are established, and regular vulnerability assessments are conducted. The focus at this level is on establishing a management framework for cybersecurity.

DEFINED (LEVEL 3)

The defined level signifies a higher level of cybersecurity maturity. At this stage, the organization has a well-defined and documented set of cybersecurity processes and controls. Policies, procedures, and standards are in place and communicated throughout the organization.

Risk management processes are established, and cybersecurity responsibilities are clearly defined. Security awareness training programs are conducted for employees, and regular audits and assessments are performed to ensure compliance.

QUANTITATIVELY MANAGED (LEVEL 4)

At this level, the organization focuses on quantifying and measuring its cybersecurity capabilities. The organization collects and analyses security metrics to assess the effectiveness of its controls and processes.

Risk assessments are performed regularly, and security incidents are tracked and monitored using advanced tools and technologies.

Continuous improvement is a key aspect at this level, with the organization using data-driven insights to enhance its cybersecurity capabilities.

OPTIMIZED (LEVEL 5)

The optimized level represents the highest level of cybersecurity maturity. At this stage, the organization has a proactive and adaptive approach to cybersecurity. It continually monitors emerging threats and incorporates them into its security strategy.

The organization actively participates in information sharing and collaboration with industry peers and government entities. It leverages advanced technologies, such as artificial intelligence and machine learning, to detect and respond to cyber threats in real-time.

Regular testing, simulations, and exercises are conducted to ensure the effectiveness of cybersecurity controls and response plans.

4.8 PROGRESSING UP LEVELS

Once the organisation has implemented all the processes and controls associated with one level they can proceed to the next. And not before.

In this structured way, the *Cybersecurity Capability Maturity Model* lays out a definitive roadmap for organizations to identify their current maturity level, to set goals for improvement, and continuously improve their cybersecurity capabilities.

The assessment of an organization's maturity level is typically conducted through an assessment of its existing cybersecurity practices, policies, procedures, and technical controls. This assessment involves interviews, documentation reviews, and technical assessments. The results are then mapped against the maturity levels defined in the model to determine the organization's current level and identify areas for improvement. Evidence that processes are being performed is required when doing assessments.

This structured approach to building a robust cybersecurity program brings alignment with industry best practices and regulatory requirements. Customers may be interested to know a potential supplier’s maturity level and might prescribe a minimum level as a condition of doing business and integrating the organisation into a supply chain.

4.9 THE C2M2 DOMAINS

The C2M2 has comprehensive list of **10 domains** that must be addressed to achieve each maturity level:

1. Asset Management
2. Access Control
3. Awareness and Training
4. Data Security
5. Incident Response
6. Maintenance
7. Protective Technology
8. Risk Management
9. Situational Awareness
10. System and Communications Protection

Each domain is further divided into the maturity levels discussed above, which represent the degree to which the organization has implemented the associated cybersecurity practices.

Each of the domains listed above will have a maturity rating determined by the assessment. Typically, an organisation will have varied results across the domains, with some being performed more rigorously than others.

Again, the maturity levels in brief are:

1. **Initial**: The organization has not yet implemented any cybersecurity practices in this domain.
2. **Repeatable**: The organization has implemented some cybersecurity practices in this domain, but they are not consistently applied.
3. **Defined**: The organization has defined cybersecurity practices in this domain, and they are consistently applied.
4. **Managed**: The organization has established a process for managing cybersecurity in this domain.
5. **Optimized**: The organization has continuously improved its cybersecurity practices in this domain.

Organizations therefore use the C2M2 to consistently measure their cybersecurity capabilities over time, to identify target maturity levels based on risk, and to prioritize the actions and investments that allow them to meet their targets.

It is advisable to present the C2M2 as a useful tool for improvement, not as a kind of audit like the tax man might do to uncover wrongdoing. People become defensive if the wrong perception of this valuable tool for any organization that wants to improve its cybersecurity posture.

The C2M2 is aligned with internationally recognized cyber standards and best practices.

4.10 BENEFITS

In summary, the benefits of using the C2M2:

- Identify and prioritize cybersecurity risks.
- With a roadmap for improving cybersecurity capabilities.
- Measure their progress over time.
- Align cybersecurity with business objectives.
- Comply with cybersecurity regulations.

For more about the C2M2, you can visit the website: https://c2m2.doe.gov/ . The website provides a wealth of information about the model, including the model documentation, case studies, and resources for implementation.