CMMI® Institute

Cybermaturity Platform Model Development

Approach for Building Resilience ..... March 17, 2019

Prepared for CMMI by:
G2 Incorporated

302 Sentinel Drive, Suite 300
Annapolis Junction, MD 20701

Table of Contents

Table of Figures

Table of Tables

1 Cybersecurity Resilience

CMMI's Cybermaturity Platform (CMMI-CP) is a risk-based, capability driven, approach to building a resilient cybersecurity program. A key factor in CMMI's approach for building cybersecurity resilience is the management of enterprise security risks, as seen below in Figure 1. Managing these risks involves operationalizing security, understanding the maturity of enterprise capabilities, and ensuring the workforce is prepared to handle a security incident. These core components allow organizations to evaluate and build resilient cybersecurity programs.

Figure 1 Cybersecurity Resilience

To assist organizations in building an effective and resilient cybersecurity program, the Cybermaturity Platform self-assessment focuses on identifying enterprise risk, setting standardized maturity targets, aligning risk to those maturity targets within Capabilities Areas, and prioritizing a roadmap to building organizational resilience.

Leveraging decades of experience within CMMI, the Cybermaturity Platform helps organizations identify, measure, and achieve a capability maturity level that is right for them based on the organization's security risk tolerances. An organization's workforce is another critical component of a cybersecurity program. The Cybermaturity Platform Practices also help organizations understand how to assign, train, and maintain a workforce that operates at the appropriate security maturity level for the organization.

The SecOps approach integrated within the Cybermaturity Platform ensures the organization's operating processes and technology support the business objectives in managing risk. As technology, security threats, and operating requirements change within an organization the cybersecurity program must adapt. The Cybermaturity Platform leverages these diverse aspects of an organization to provide risk informed activities, or Practices, that will assist them in mitigating security risks within their environment. By providing these risk-informed Practices to organizations, they are better prepared to perform daily activities in a manner that incorporates the organization's security expectations.

Operating in a secure state allows organizations to more easily maintain compliance, achieve regulatory goals, and reduce security risks simply by performing their routine activities. This concept of secure operations or SecOps makes organizations more secure by integrating security into business operations.

1.1 Transitioning to Risk Based Capability Driven Resilience

Many organizations focus on compliance-based risk reduction before evaluating actual risks in the operational environment. Performing compliance-based risk reduction before the evaluation of actual risks can be misleading and lead to inefficient use of resources. The approach of the CMMI Cybermaturity Platform is to drive resilience through the reduction of enterprise risks, with compliance as a resulting outcome rather than the primary goal. The Platform helps an organization determine the level of maturity that enables the organization to achieve its security goals, including conformance with legal or contractual requirements, in a cost-effective manner. While achieving organizational compliance goals is not, itself the focus of the self-assessment tool, that achievement may be an added benefit to organizations that are committed to building enterprise cyber resilience. To support this goal, the Cybermaturity Platform identifies enterprise risks and capability priorities before aligning to regulations and requirements. This ensures that when regulatory requirements are reviewed, organizations have already implemented their highest priority capabilities to drive down risk.

The Cybermaturity Platform is not intended to take the place of implementation tools such as vulnerability scanners, intrusion detection systems, or asset management tools. The Platform works to support tools like these by confirming that organizations have implemented both automated tools and underlying processes. Example Practices include validation that cybersecurity products have been implemented (e.g., "Automated vulnerability scanning tools review all applicable systems on the network) but also that they've been implemented in accordance with good practices (e.g., A validated vulnerability scanner is used that looks for both code-based vulnerabilities and configuration-based vulnerabilities) and are effective (e.g., Network scanning tools are evaluated to ensure that appropriate tools are being utilized by the organization.)

2 Risk Based Approach

Many organizations begin implementing cybersecurity controls out of fear of an incident or as a reaction to an incident. This often results in controls being implemented to address the effect of an incident without considering the cause. Due to organizations having varying threats and vulnerabilities, calculating enterprise risk can become a complex task. The Cybermaturity Platform was influenced by

standard industry risk approaches including NIST SP 800-30[1], OCTAVE[2], and FAIR[3] to create a simplified Risk Profile providing a characterization of an organization's risk.

The Cybermaturity Platform begins each assessment by evaluating the enterprise risks that could lead to an incident by asking organizations to consider the likelihood and impact of Potential Vulnerabilities and Potential Events to their organization. By calculating enterprise risk through Risk Scenarios informed by the Potential Vulnerabilities and Potential Events, the Cybermaturity Platform is able to identify and provide a characterization of an organization's highest risks.

Security risk assessments are a critical phase of defining an appropriate security program. However, many organizations are unable to complete a full risk assessment due to the lack of qualitative information, lack of time, or lack of experience in completing a risk assessment. The Cybermaturity Platform assists organizations by taking the key concepts from standard, and widely accepted, risk assessment processes. These key concepts are then integrated and summarized to develop a simplified Risk Profile within the Cybermaturity Platform. This simplified Risk Profile allows organizations to better understand the risk to their business as well as identify risk thresholds that can be used to set goals to inform objectives for their security program.

2.1 Risk Scenarios

The Cybermaturity Platform Risk Profile is informed by 15 Potential Vulnerabilities and 13 Potential Events resulting in 111 unique Risk Scenarios. While there could be thousands of Potential Vulnerabilities alone, the Cybermaturity Platform takes the approach of characterizing vulnerabilities and risks to create a manageable Risk Profile with a balanced approach for identifying risk.

The Risk Profile is developed based upon the intersection of a Potential Vulnerabilities and a Potential Event resulting in a Risk Scenario which describes an actual incident that could compromise the security of an organization. The Potential Vulnerabilities selected for the Cybermaturity Platform, characterize specific weaknesses within an organization that could be exploited by a threat actor to realize a Potential Event. The selected Potential Events, are specific types of cybersecurity events that pose a direct threat to business operations and critical assets. Potential Events define what could happen to resources (e.g. assets, data, people, etc.) if a Potential Vulnerability is exploited.

To provide organizations with confidence that they are adequately representing their most common attack types in the Risk Profile, they are provided the option of selecting a common Incident Pattern. Incident Patterns are categories of potential security events summarized based on a shared set of Potential Vulnerabilities. By selecting a common Incident Pattern as well a likelihood and impact value, the organization's Risk Profile will be pre-filled to reflect the organization's largest threats.

2.2 Risk Levels

The Cybermaturity Platform Risk Profile is completed by answering a series of 124 questions. 111 questions are focused on determining the likelihood of each Potential Vulnerability leading to applicable

[1] NIST SP 800-30 r1: Guide for Conducting Risk Assessments, September 2012
[2] Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Software Engineering Institute, May 2007
[3] Factor Analysis of Information Risk (FAIR), The FAIR Institute

Potential Events. The remaining 13 questions determine the impact the Potential Events would have on an organization if a Potential Vulnerability is realized.

The likelihood and impact of each Risk Scenario is characterized on a four-point scale (Very Low, Low, High, Very High). While many risk models include either a three or five level scale, the Cybermaturity Platform intentionally deviates from this norm by choosing a four-point scale. The middle level on many three and five-point scales is 'moderate' which allows organization to stick to the middle resulting in all risks being at the same level. For the purposes identifying relative risk, the Cybermaturity Platform does not allow a moderate option which forces organizations to choose from Very Low, Low, High, or Very High risk. Appendix C includes a glossary of key terms used within the Cybermaturity Platform including the definitions for the likelihood and impact levels.

After completing the 124 questions by assigning likelihood and impacts to the Risk Scenarios, each scenario's Risk Level is calculated. Using the organization selected likelihood and impact values, the Cybermaturity Platform determines the security risk to the organization in the case that the Risk Scenario is realized. Once the Risk Profile has been completed, Risk Scenarios can be ranked based on Risk Levels to allow organizations to identify the highest risk scenarios and understand which Potential Vulnerabilities and Potential Events pose the largest risk to their organization.

2.3 Unique Risk Targets

Due to the 496 possible inputs in the Risk Profile, each organization that completes the Risk Profile will be able to create a profile that is unique to their business. By taking the output of this unique Risk Profile, the ranked Risk Scenarios can be prioritized within the Cybermaturity Platform to enable organizations to understand their highest risks and to make risk-informed decision regarding their security program. By providing this customized Risk Profile, organizations are able to prioritize their actions based on their highest risk areas.

Each of the 111 Risk Scenarios are mapped to individual Practices at specific Maturity Levels ranging from one to five. Using these mappings, the Cybermaturity Platform is able to calculate a target organizational Maturity Level based upon the Risk Profile.

3 Capability Maturity

As organizations implement cybersecurity capabilities, it is important that there is a clear understanding of what functionality is being implemented as well as how the functionality is being executed by staff and integrated into the organization. Through the measurement of cybersecurity capabilities, organizations gain an understanding of the robustness of their security capabilities allowing them to evaluate whether their current cybersecurity maturity is appropriate for their business and the risks in their environment. Having a clear understanding of this relationship highlights unmitigated risk and enables organizations to make informed decision regarding the resources needed to mitigate risk and build cybersecurity resilience.

3.1 The CMMI Standard

For nearly three decades, CMMI has partnered with companies to measure organizational processes and improve capabilities. As described below in Table 1, CMMI's maturity scale ranges from Level 1 (Initial) to Level 5 (Optimized). The Cybermaturity Platform expands upon CMMI's expertise in measuring maturity to build cybersecurity resilience through capability maturity measurement.

Table 1 CMMI Maturity Level Definitions

	CMMI Definitions
Level 5 (Optimized)	Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.
Level 4 (Quantitatively Managed)	Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.
Level 3 (Defined)	Organization-wide standards provide guidance across projects, programs, and portfolios.
Level 2 (Managed)	Projects are planned, performed, measured, and controlled.
Level 1 (Initial)	Work gets completed but is often delayed and over budget.

3.2 Comprehensive Goal Setting

To effectively build cybersecurity resilience, organizations must focus on the people that work for and interact with the company, the policies and procedures in place to direct employees and partners, as well as the technical solutions used to keep their businesses running. The Cybermaturity Platform leverages CMMI's existing five level maturity scale and redefines each level for cybersecurity capabilities. The Maturity Levels defined by CMMI and adopted within the Cybermaturity Platform establish expected outcomes at each of the five maturity levels: Performed, Managed, Defined, Quantitatively Managed, and Optimized. To ensure organizations focus on the three cybersecurity factors discussed above, the Cybermaturity Platform deconstructs each of CMMI's existing five level maturity scale to reflect people, process, and technology as defined in Table 2.

Table 2 CMMI Cybermaturity Platform Maturity Level Definitions

	General	*People*	*Process*	*Technology*
Level 1 *(Initial)*	Represents a minimum standard of care. Basic functions may be performed. These functions are performed informally and may not be prioritized commensurate with risk.	General personnel capabilities may be performed by an individual, but are not well defined	General process capabilities may be performed by an individual, but are not well defined	General technical mechanisms are in place and may be used by an individual
Level 2 *(Managed)*	Basic functions are achieved with relative consistency. Subset of the organization has developed plan, but formal organization strategy or documented plan has not been developed.	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Adequate procedures documented within a subset of the organization	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place
Level 3 *(Defined)*	Formal plans and strategies define the consistent achievement of functions across the organization. Lagging indicators provide understanding of the work performed.	Roles and responsibilities are identified, assigned, and trained across the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization
Level 4 *(Quantitatively Managed)*	Achievement of outcomes is measured and reported. Leading indicators contribute to proactive risk management and continual improvement	Achievement and performance of personnel practices are predicted, measured, and evaluated	Policy compliance is measured and enforced. Procedures are monitored for effectiveness.	Effectiveness of technical mechanisms are predicted, measured, and evaluated
Level 5 *(Optimized)*	Mechanisms for outcome achievement are integrated into organizational activities	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

4 Capability Driven Practices

Practices are single outcome statements that build the security capabilities defined within the Cybermaturity Platform. Many requirements and regulations are in place across industries, but very few align to enterprise risk and measure capability maturity. Each individual Practice in the Cybermaturity Platform is aligned and tagged to relevant security standards, Risk Scenarios, Maturity Levels, and capabilities to ensure that organizations get a comprehensive understanding of the capabilities their organization should be targeting.

4.1 Cybermaturity Platform Architecture

Similar to other CMMI maturity models, the architecture of the Cybermaturity Platform is composed of a hierarchy of Functional Areas, Capability Areas, Practice Areas, and Practices. The comprehensive architecture addresses key cybersecurity topics currently described across a large set of technical controls and best practice documents. By aligning with leading frameworks and standards documents, the Cybermaturity Platform model can be viewed as a comprehensive model describing the required practices for building cybersecurity resilience.

In this model, each Practice aligns to a Practice Area defining a specific cybersecurity resilience topic. Each Practice Area aligns to a Capability Area describing a collection of Practice Areas aimed at achieving the same cybersecurity objective. The highest level in the architecture is the Functional Area which is composed of a collection of Capability Areas. Each Functional Areas describes a high-level capability required for an effective cybersecurity program. This hierarchy can be seen below in Figure 2. The figure depicts one of the seven Functional Areas in the Cybermaturity Platform, *Identify and Manage Risk*.

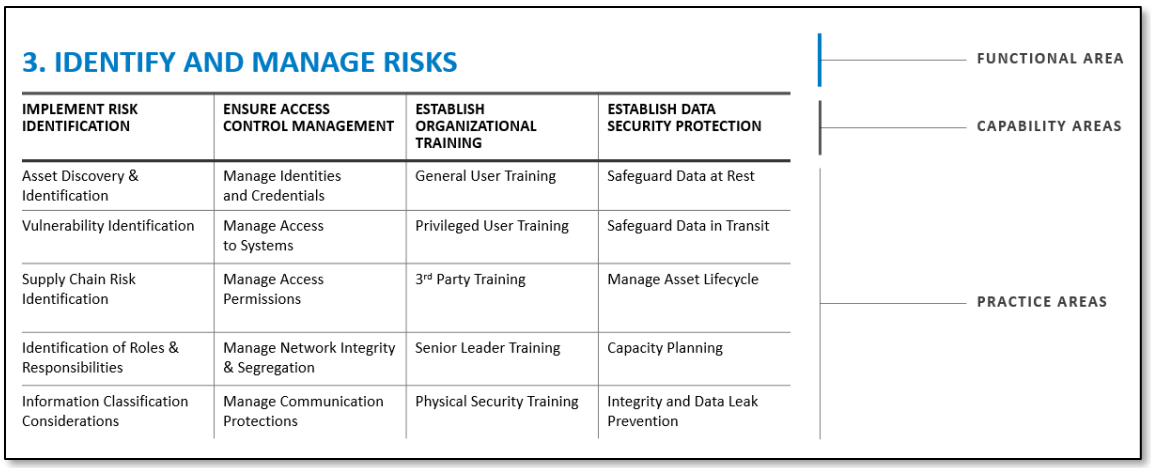

Figure 2 CMMI Cybermaturity Platform Hierarchy

The Cybermaturity Platform model currently includes over 3,000 Practice outcomes that are divided among 80 Practice Areas, aligned to 21 Capability Areas, under seven 7 Functional Areas. Five of the seven Functional Areas reflect a lifecycle approach to cybersecurity by achieving the following functions: Identify and Mange Risks, Ensure Risk Mitigation, Ensure Risk Detection, Ensure Risk Response, and Ensure Resilience. The two remaining Functional Areas, Ensure Governance Framework and Apply Risk Management are strategic functions necessary for building resilience. The outcomes of the Ensure Governance Framework and Apply Risk Management Function Areas inform the other Functional Areas to enable an effective cybersecurity program.

A comprehensive view of the model illustrating the relationships between all Functional Areas, Capability Areas, and Practice Areas can be found in Appendix A: CMMI Cybermaturity Platform Placemat.

4.2 Attributes of a Practice

The core of the Cybermaturity Platform Self-Assessment is the Practices that make up the security capabilities. Practices are discrete statements describing an action that is taken by an organization. Practices are selected by organizations during the self-assessment to indicate completion and identify the current state of a security program. The tool then uses the output from the risk profile and the unselected Practices to create a prioritized Roadmap of action items for organizations to use to build cybersecurity resilience.

Practices are statements understandable by IT professionals with little to no computer security experience. They are written as discrete, single outcome statements that an individual must be able to answer as either 'true' or 'false' when considering if an organization has the Practice in place. A collection of Practices within a given Practice Area comprehensively describe how to effectively implement that Practice Area. An organization's Maturity Level for each Practice Area is defined by evaluating the highest Maturity Level at which all Practices are marked as implemented.

Each Practice is aligned to selected industry standards, organizational security risk, maturity levels, and the Threat Kill Cycle. Creating this relationship between industry standards and the CMMI maturity levels allows the Cybermaturity Platform to not only inform an organization of the types of controls that need to be in place, but how advanced and well implemented these controls should be in order to mitigate the risks to their environment.

Due to the continually changing threat landscape, the Cybermaturity Platform will be reviewed and updated biannually to ensure that Practices are kept up to date as threats and best practices evolve.

4.3 Practice Alignments

The industry standards selected for alignment to Practices in the first version of the Cybermaturity Platform include the NIST Framework for Improving Critical Infrastructure Cybersecurity (The Cybersecurity Framework or CSF), ISO/IEC 27001: Information technology- Security techniques- Information security management systems- Requirements, and ISO/IEC 27002: Information technology- Security techniques- Code of practice for information security controls.

Industry standards also reviewed during development of the Cybermaturity Platform include NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations the CIS Top 20 Critical Security Controls, and the COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.

In addition to these industry standards, all Practices have been given a tag to indicate whether the Practice supports a People, Process, or Technology aspect within the cybersecurity program. Providing this tag highlights the importance of focusing on all three when building cybersecurity resilience.

Practices are also tagged to the proprietary CMMI Risk Profile aligning Potential Events with Potential Vulnerabilities to create Risk Scenarios. Each tagged Risk Scenario is assigned a Risk Level of Very Low, Low, High, or Very High based on the level required to mitigate Potential Vulnerabilities and Potential Events.

The final alignment selected for the first version of the Cybermaturity Platform is to the CMMI Threat Kill Cycle (TKC). The CMMI TKC was developed by leveraging industry standards as well as previous experience monitoring how threat actors progress their attacks. Table 3 CMMI Threat Kill Cycle Practices

within the Cybermaturity Platform model are mapped to the appropriate stages in the CMMI defined TKC, defined in Table 3.

Table 3 CMMI Threat Kill Cycle

Cycle Step	*Description*
Reconnaissance Prep (RE)	*Practices that assist in identifying sensitive information and ensuring it is protected from public access. Sensitive information may include benign information that when paired with other benign information provides sensitive details regarding the organization (e.g., company size, company affiliations, etc.)*
Delivery (DE)	*Practices that prevent the delivery and implementation of malware. (Execution on initial victim)*
Exploitation (EX)	*Practices that prevent the execution of malicious or otherwise unauthorized software. (Execution beyond initial victim)*
Command and Control (C2)	*Practices that identify communication channels and system process that provide command and control access to the attacker.*
Internal reconnaissance (IR)	*Practices that include the identification and prevention of unauthorized data connections, transfers, or modification.*
Lateral Movement (LM)	*Practices that provides parathion within operating environments and detect unauthorized communications within the network.*
Persistence (PE)	*Practices that detect and protect unauthorized services and process from executing.*
Action (A)	*Practices that assist in the detection and protections of malicious activities including data exfiltration, data manipulation, and installation of additional malware (e.g. backdoors)*

Tagging these reference points strengthens the model by providing organizations the ability to report alignment to multiple standards through one evaluation.

5 Roadmap

Using the Risk-based Maturity Targets identified through the completion of the Risk Profile and the Practice to Maturity Level alignments, the Cybermaturity Platform identifies a Roadmap of all Practices necessary to achieve an organization's target maturity. By gathering input on organizational risks, capabilities, and maturity, the Cybermaturity Platform provides a risk-informed prioritized list tailored directly from the organization's risk profile. This tailored, prioritized Roadmap empowers organizations to build cybersecurity resilience within their organization based on the missing activities required to meet their specific identified enterprise risk.

5.1 Prioritized Actions

With the information provided by organizations in the Risk Profile, the Cybermaturity Platform is able to identify Target Maturity Levels for each Practice Area as well as the relative riskiness of each Practice Area. The Roadmap produced by the Cybermaturity Platform is able to use this information to provide organizations with a prioritized list of all Practices needed to reach their risk-based Maturity Targets.

By understanding which Practice Areas pose the greatest risk to organizations, individuals can make informed decisions regarding capability development and resource utilization.

5.2 Align to Industry Standards

In addition to the Roadmap, the Cybermaturity Platform offers alternative views for measuring cybersecurity capabilities. As discussed in Section 4.3, all Practices are tagged to relevant industry standards documents. As a result of these alignments, the Cybermaturity Platform currently provides three industry standard views including the NIST Framework for Improving Critical Infrastructure Cybersecurity (The Cybersecurity Framework or CSF), ISO/IEC 27001 & 27002: Information technology-Security techniques as well as CMMI's Threat Kill Cycle.

Each of these views provides a lens through which an organization can see the alignment of the Cybermaturity Platform Practices to the industry standards. These views provide a simple way to view both the Practices that the organization has completed as well as the Practices that the organization needs to implement in order to reach their Risk-based Maturity Targets as they align to industry standards.

By providing these reference points, organizations have the ability to report alignment to multiple standards through one evaluation.

6 Building Organizational Resilience

Building resilience within an organization requires a thorough understanding of the capabilities that are critical for operating a business as well as a clear understanding of the risks to the enterprise. The Cybermaturity Platform Self-Assessment enables organizations to align enterprise risk to their key capabilities to create standardized Maturity Targets that will empower them to build resilience within their organization.

Identifying the threats and vulnerabilities that are most likely to impact operations helps organizations prioritize their cybersecurity program. The Cybermaturity Platform leverages the organizations business expertise to define risk tolerances for the business. By aligning these risks to Practices within the Cybermaturity Platform, the platform can provide organizations with the risk informed activities required to mitigate risk to an acceptable level.

Focusing on actual risks to the organization before compliance-based risk provides organizations with a realistic view of the missing capabilities that pose the greatest risk to their business. The Cybermaturity Platform aids organizations in identifying these capabilities with the greatest risk and then aligns them to industry standards as a byproduct, ensuring that the requirements dictated by industry are implemented in a way that meets the needs of the individual organization.

Appendix A: CMMI Cybermaturity Platform Placemat

1. ENSURE GOVERNANCE FRAMEWORK

ESTABLISH GOVERNANCE	GOVERN CYBERSECURITY RESOURCES	ESTABLISH STAKEHOLDER REPORTING
Apply Information Security Management Policy Process	Evaluate Resource Management Needs	Apply Stakeholder Reporting Requirements
Apply Governance System	Direct Resource Management Needs	Direct Stakeholder Communication and Reporting
Direct Governance System	Monitor Resource Management Needs	Monitor Stakeholder Communication
Monitor Governance System		

2. ESTABLISH RISK MANAGEMENT

ESTABLISH RISK STRATEGY	ESTABLISH BUSINESS RISK CONTEXT	IMPLEMENT RISK MANAGEMENT
Apply Risk Management Strategy	Determine Mission Dependencies	Apply Organization Risk Mgmt. Process
Apply Risk Management	Determine Legal / Regulatory Requirements	Integrate Risk Mgmt. Program
Define Organizational Risk Tolerance	Determine Strategic Risk Objectives	Manage External Participation
Determine Critical Infrastructure Requirements		

3. IDENTIFY AND MANAGE RISKS

IMPLEMENT RISK IDENTIFICATION	ENSURE ACCESS CONTROL MANAGEMENT	ESTABLISH ORGANIZATIONAL TRAINING	ESTABLISH DATA SECURITY PROTECTION
Asset Discovery & Identification	Information Classification Considerations	General User Training	Safeguard Data at Rest
Vulnerability Identification	Manage Identities and Credentials	Role-based User Training	Safeguard Data in Transit
Supply Chain Risk Identification	Manage Access to Systems	Third Party Training	Manage Asset Lifecycle
Identification of Roles & Responsibilities	Manage Access Permissions		Capacity Planning
	Manage Network Integrity & Segregation		Integrity and Data Leak Prevention
	Manage Communication Protections		

4. ENSURE RISK MITIGATION

ESTABLISH SECURE APPLICATION	ESTABLISH INFORMATION PROTETCION PROVISIONS	ESTABLISH PROTECTION PLANNING	ESTABLISH PROTECTIVE TECHNOLOGY PROVISIONS
Secure Application Development	Apply Configuration Baselines	Apply Information Sharing	Apply Logging and Audit Processes
Secure Development Testing	Apply Change Control	Develop and Maintain Response Plans	Apply Media Protections
Manage System Engineering Process	Apply Backup Processes	Develop and Maintain Recovery Plans	Safeguard Operational Environment
Safeguard Development Environment	Apply Maintenance Processes	Apply Personnel Security	
Manage Software Update/Release Processes	Apply Mobile Device Management	Apply Vulnerability Mgmt. (Patch) Process	
		Apply Retention and Destruction Measures	

5. ENSURE RISK DETECTION

ESTABLISH CYBERSECURITY INCIDENT DETECTION	ESTABLISH CONTINUOUS MONITORING	ESTABLISH DETECTION
Apply Network Baselines	Monitor Networks	Test Detection Processes
Aggregate / Correlate Data	Monitor Physical	Detect Malicious Code
Determine Impacts	Monitor Personnel	Detect Mobile Code and Browser Protection
Alert Thresholds	Monitor Third Parties	Apply Security Assessment

6. ENSURE RISK RESPONSE

ESTABLISH INCIDENT RESPONSE	ESTABLISH INCIDENT ANALYSIS	MITIGATE DETECTED INCIDENTS
Execute Response Plan	Implement Incident Investigation Processes	Ensure Incident Containment
Response Roles & Responsibilities	Implement Forensics Capability	Ensure Incident Mitigation
Incident Reporting	Apply Response Categorization	
Ensure Information Sharing		

7. ENSURE RESILIENCE

ESTABLISH INCIDENT RECOVERY
Execute Recovery Plan
Recovery Communications

Appendix B: Glossary

Capability Area	Discrete cybersecurity activities that comprise a Functional Area. A Capability Area is a collection of Practice Areas aimed at achieving the same cybersecurity activity. The Capability Area is used for industry benchmarking and internal reporting of Measured Maturity vs Target Maturity.
Cybersecurity Resilience	An organizations ability to detect, assess, respond and mitigate cybersecurity threats
Functional Area	Describes a high-level capability required for an effective cybersecurity program. The Functional Area is the top level within the CMMI Cybermaturity Platform architecture.
Impact	Effect of exploiting a Potential Event through a Potential Vulnerability.
Incident Pattern	Categories of Potential (security) Events summarized based on a shared set of Potential Vulnerabilities.
Likelihood	Probability of a Potential Event exploiting a Potential Vulnerability.
Maturity Levels	A benchmark of an organization's capability across a given set of Practices, Capability Areas, and Functional Areas.
Measured Maturity	The Maturity Level identified based upon Practices that an organization currently has in place.
Potential Event	A specific type of cybersecurity event relevant to an organization that poses a direct threat to business operations and critical assets
Potential Vulnerability	A weakness within an organization that a threat actor could use to realize a potential event.
Practice Area	A logical grouping of Practices that define a specific cybersecurity resilience topic. A group of Practice Areas comprise a Capability Area.
Practices	Discrete statements describing an action that is taken by an organization. Practices are outcomes that are aligned to specific Maturity and Risk Levels.
Risk Level	Each Risk (Scenario) Level is calculated using the organization selected likelihood and impact values to determine the security risk to the organization in the case that the Risk Scenario is realized.
Risk Profile	Ranking of the Risk Scenarios based upon data gathered from assigning likelihood and impact values to Potential Events and Potential Vulnerabilities.
Risk Scenario	Incident that compromises the security of an organization. The likelihood and impact of each Risk Scenario is measured to determine the security risk to the organization if the Risk Scenario is realized.
Risk-based Maturity Target	The target Maturity Level necessary to address the risks identified by the Risk Profile.
Risk Threshold	Amount of risk an organization is willing to accept. Realized risk beyond the threshold will provide a significant negative affect to the organization.
Roadmap	List of prioritized capabilities broken down into discrete outcome statements that are necessary for meeting a Risk-based Maturity Target.
Threat Actor	An internal or external actor that intends to or has caused a negative incident or event to occur.
Views	A representation of the data within the Cybermaturity Platform model. Views are used to align the Cybermaturity Platform Roadmap with industry standards (e.g. ISO 27001/ISO27002, NIST Cybersecurity Framework, CMMI Threat Kill Cycle, etc.).

Potential Event Impact Level Definitions

Very High (Impact)	A catastrophic adverse effect refers to terminal or nearly terminal loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; irrecoverable damage to organizational assets; or result in catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
High (Impact)	A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Low (Impact)	A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very-Low (Impact)	Insignificant

Potential Vulnerability Likelihood Level Definitions

Very High (Likelihood)	Risk Scenario is almost certain to occur; or occurs more than 100 times a year.
High (Likelihood)	Risk Scenario is likely to occur; or occurs between 10-100 times a year.
Low (Likelihood)	Risk Scenario is rarely likely to occur; or occurs more than once every 10 years.
Very Low (Likelihood)	Risk Scenario is unlikely to occur; or occurs less than once every 10 years.

Risk (Scenario) Level Definitions

Very High	Very high risk means that a threat event could be expected to have catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	High risk means that a threat event could be expected to have a severe adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	Low risk means that a threat event could be expected to have an adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.