IoT Security Maturity Model: NIST Cybersecurity Framework 1.1 Mappings

An Industry IoT Consortium Whitepaper

2024-03-27

Authors

Pierre Kobes (Kobes Consulting), Frederick Hirsch (Upham Security), Ron Zahavi (Auron Technologies).

CONTENTS

FIGURES

TABLES

This document is intended for organizations who wish to improve the security maturity of their organization and wish to use and relate the NIST Cybersecurity Framework 1.1[1] guidance with the Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM). The NIST Cybersecurity Framework 2.0 is also relevant and anticipated[2].

The NIST Cybersecurity Framework (CSF) offers a "taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts". This taxonomy is organized in terms of outcomes such as Identify, Protect, Detect, Respond and Recover in CSF 1.1 (and adding Govern in 2.0). The IoT Security Maturity Model (SMM) offers a set of practices that include outcomes related to governance (including strategy and governance, threat and risk assessment, and supply chain dependencies), hardening (including identity and access management, asset protection, data protection) and enablement (including vulnerability and patch management, situation awareness, and event and incident response and continuity of operations). Both include processes for working with these outcomes. These two approaches can both be used to improve organizational communication, understanding and security, can be used top down and/or bottom up and can be used together. These mappings can help practitioners related and use both approaches.

The SMM set of documents consisting of the Practitioners Guide, profile documents and mapping guidance, provides a detailed model and approach for achieving a good fit of security governance, technology, and operations maturity to meet business needs. The "IoT Security Maturity Model: Practitioners Guide"[3] defines the SMM and includes detailed general guidance, providing a foundation from which communities can consider their specific needs and concerns. This general guidance can be extended with mappings that relate industry requirements, best practices and controls to the maturity guidance as well as profiles that can be used to consider industry and device specific concerns in more detail.

Currently there are mappings available to relate International Society of Automation (ISA) and its ISA99 committee 62443 guidance to the SMM[4].

Guidance is also available on how to create SMM profiles[5]. So far, profiles have been created for Digital Twins[6], Mining Extraction[7], and Retail Point of Sale Devices[8].

[1] [NIST-CSF11]

[2] [NIST-CSF20]

[3] [IIC-SMMP2020]

[4] [IIC-SMM-62443M-2023]

[5] [IIC-SMM-PG2024]

[6] [IIC-SMM-DTP2022]

[7] [IIC-SMM-MEP2023]

[8] [IIC-SMM-RP2022]

The Iot Security Maturity Model can be used in conjunction with other detailed guidance, such as the IIC Industrial Internet Reference Architecture[9], the IIC Industrial Internet of Things Connectivity Framework[10], IC Industrial Internet of Things Security Framework[11], and the IIC Industrial Internet of Things Trustworthiness Framework Foundations document[12].

The NIST Cybersecurity Framework is intended to help organizations start or improve their cybersecurity programs. This guidance can be used in conjunction with the SMM to improve security maturity and address security concerns relevant to organizations in an appropriate manner. This document relates the two approaches, exposing both commonality and areas where each contributes further to the other.

There is no simple generic solution that can address security needs for every system. Organizations have differing needs, and different systems need various strengths of protection mechanisms. The same technology can be applied in other ways and to different degrees, depending on needs. The SMM helps organizations determine priorities to drive their security enhancements. The security maturity reflects the proper of fit of their choices to their needs.

The security maturity model fosters effective and productive collaboration among business and technical stakeholders. Business decision makers, business risk managers and owners of IoT systems, concerned about proper strategy for implementing security practices with the appropriate maturity, can collaborate with analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation. They can also consider the viewpoints of regulators and other parties such as insurance providers. It is up to system architects, designers, testers and installers to verify the correct requirements are chosen for the application, and the implementation correctly embodies these requirements.

To drive proper investment, the IoT Security Maturity Model includes both organizational and technological components. Organizations use the model to set their maturity target, understand their current maturity and determine what they need to do to move to a higher maturity state.

The IoT SMM and associated mappings may be used to improve communication, understanding and investments in security of new systems as well as refining existing systems. This can be done with *Security maturity target refinement*. Assume we have the established security maturity target for the system under consideration. Using the mapping tables defined below, it is possible to set up more concrete requirements on the practice implementation (what needs to be done) and concrete indicators of achievement. To do so, the indicators of achievement for the SMM target comprehensiveness and lower levels should be compared side-by-side with the requirements mapped to these levels.

[9] [IIC-IIRA-2022]

[10] [IIC-CF-2022]

[11] [IIC-IISF2-2023]

[12] [IIC-TFF-2021]

A NIST Cybersecurity Framework analysis can be used as input to an SMM maturity assessment, accelerating the process of understanding SMM targets and performing assessments. Similarly, the understanding from SMM target setting, assessments and gap analysis can be used to contributed to a NIST cybersecurity framework analysis.

This document provides mappings for the NIST Cybersecurity Framework Version 1.1[13] and anticipates mapping changes for Version 2.0[14].

1 KEY CONCEPTS

1.1 SMM Security Maturity

Security maturity is about effectiveness, not the use of security mechanisms to achieve arbitrary security levels.

Not all systems require the same strength of security mechanisms and procedures to meet their security maturity targets. The organization's leadership determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementations of security mechanisms and processes are considered *mature* if they are expected to be effective in addressing those goals. It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity. The SMM defines *security maturity* as the degree of confidence that the current security state meets all organizational security needs and all organizational security-related requirements. Security maturity is a measure of the understanding of the overall current security approach including its necessity, benefits and cost to support. This security approach needs to include people, processes and technology, a holistic approach that goes beyond technical controls alone. Contributing factors include the specific threats to an organization's industry vertical, safety, regulatory, ethical and compliance requirements, the organization's threat profile and the unique risks present in an environment.

1.1.1. SECURITY MATURITY VS. SECURITY LEVEL

Security level, such as the one used in the 62443 standard[15], is a measure of the strength of a security measure (e.g. stronger cryptography) while security maturity is about the level of understanding of the need and confidence in appropriate corresponding implementation. Increasing security levels relate to increasing security threats and corresponding risk-reduction ability. The SMM does not say what the appropriate security level should be. Rather, it provides

[13] [NIST-CSF11]

[14] [NIST-CSF20]

[15] According to: *https://webstore.iec.ch/publication/7033*

guidance and structure for organizations to select the maturity appropriate for their industry and system. The notion of security level must not be confused with security maturity. However, achieving an appropriate security level can contribute to achieving the needed system maturity.

Organizations are interested in finding out if their IoT solutions are secure, and how to protect them to meet their needs. A maturity model helps organizations understand how to match their security investment with their goals and needs, while a security requirement framework identifies what mechanisms are available and can be applied to reach certain levels of security.

This document presents a high-level introduction to the IoT Security Maturity Model, the NIST Cybersecurity Framework, and a mapping between the IoT SMM practices and levels and the NIST Cybersecurity Framework guidance.

1.2 SMM Approach toward Organizing Security Understanding

The SMM provides a means to set maturity targets and perform assessments to manage security efforts better.

1.1.2. SMM Domains, Subdomains & Practices

The domains of governance, enablement and hardening determine the priorities of security maturity enhancements at the strategic level.

Governance is the "establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization."[16] *Governance* influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation. The culture of the organization is reflected in the governance and the degree of importance placed on security.

Enablement is the implementation of security mechanisms and procedures needed to create a system meeting the policy and operational requirements. Enablement uses architectural design to address business risks and specific practices to enable operations.

Hardening is the use of security practices during system operation. This includes identifying ongoing risks through situational awareness, monitoring system operation and managing change of the system (e.g. patching).

When planning, different priorities can be placed on the different domains and subdomains based on risk analysis and other factors. Business stakeholder conversations and decisions can focus at this level without going into the details of the practices. Subsequent implementation will use the practices based on these priorities. The domains and subdomains also serve to organize the practices logically, making clear where different alternatives may be used to address

[16] *https://transitionpointba.com/governance/*

requirements of a given domain or subdomain. **Error! Reference source not found.** displays the h ierarchy of domains and associated subdomains and practices.

The model has been designed to be extensible and provides the ability to add new domains, subdomains, and practices in the future.

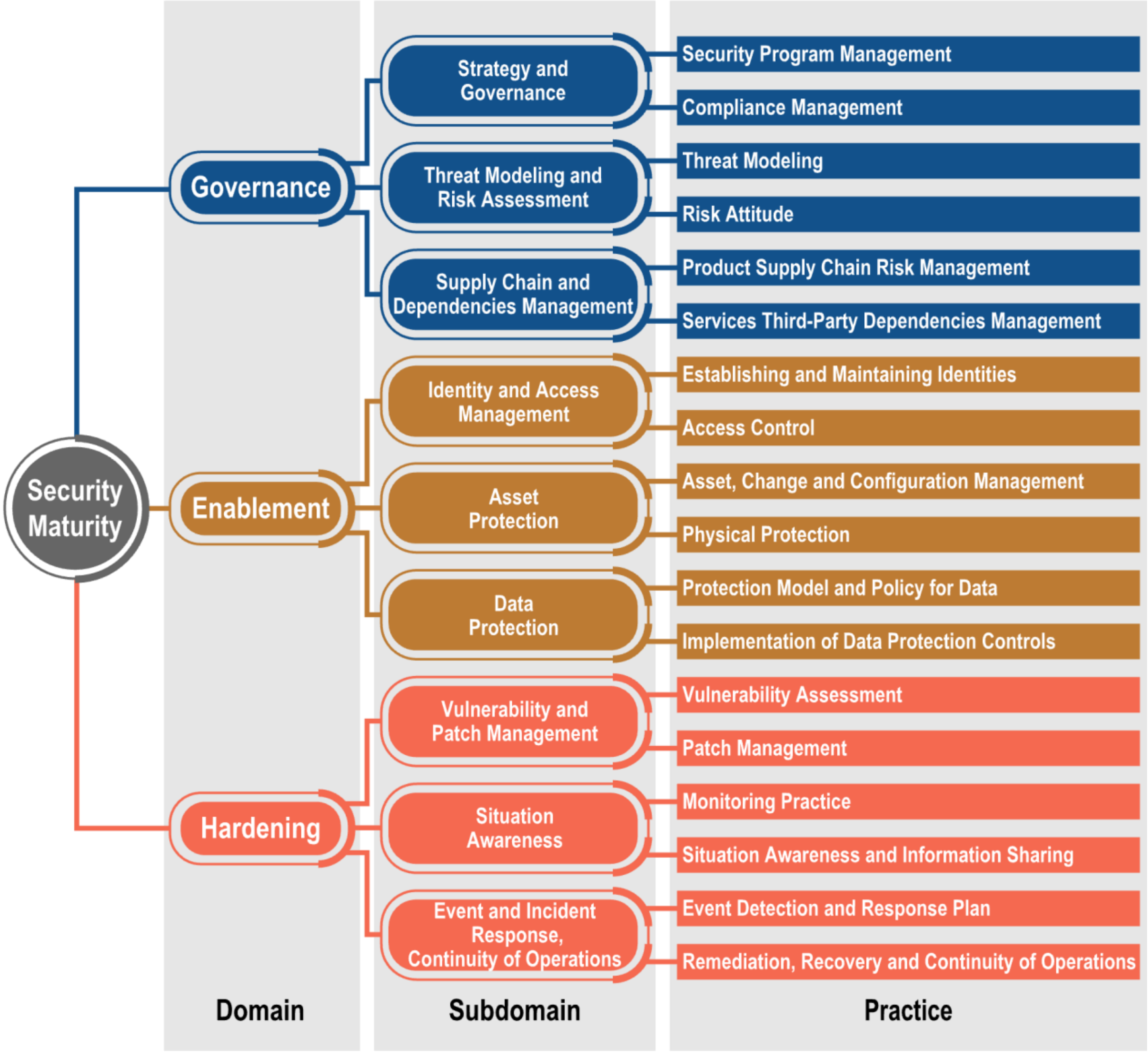

Security Maturity
Governance
Enablement
Hardening
Strategy and Governance
Threat Modeling and Risk Assessment
Supply Chain and Dependencies Management
Identity and Access Management
Asset Protection
Data Protection
Vulnerability and Patch Management
Situation Awareness
Event and Incident Response, Continuity of Operations
Security Program Management
Compliance Management
Threat Modeling
Risk Attitude
Product Supply Chain Risk Management
Services Third-Party Dependencies Management
Establishing and Maintaining Identities
Access Control
Asset, Change and Configuration Management
Physical Protection
Protection Model and Policy for Data
Implementation of Data Protection Controls
Vulnerability Assessment
Patch Management
Monitoring Practice
Situation Awareness and Information Sharing
Event Detection and Response Plan
Remediation, Recovery and Continuity of Operations
Domain
Subdomain
Practice

Figure 1-1: IoT Security Maturity Model Hierarchy.

There are two orthogonal dimensions to the evaluation of the security maturity: comprehensiveness and scope. *Comprehensiveness* captures the degree of depth, consistency and assurance of security practices. Use of comprehensiveness in this model reduces complexity by considering different aspects together such as organizational security awareness, degree of implementation of practices, and assurance of the practices (and their evolution). For example, a higher level of comprehensiveness of threat modeling implies a more automated, systematic, and extensive approach.

Scope reflects the degree of fit to the industry or system needs. This captures the degree of customization of the security measures that support security maturity domains, sub domains or practices. Such customizations are typically required to address industry- or system-specific constraints of the IoT system.

Comprehensiveness and scope help manage and prioritize security maturity practices. Certain systems may not require certain practices at all, yet this can still reflect a high level of security maturity when that decision is appropriate. Avoiding unnecessary mechanisms reduces costs and lowers complexity, which will reduce risks. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

The SMM aligns the comprehensiveness (degree of depth, consistency, and assurance of security measures) and scope (degree of fit to the industry or system needs) of security needs with the investment in appropriate practices.

1.2.1 SMM Comprehensiveness Levels

There are five SMM comprehensiveness levels for every security domain, subdomain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones. The overall maturity of an organization's approach to IoT security is based on how well the assessed comprehensiveness levels of the SMM practices match the SMM comprehensiveness level targets for those practices. An organization is not more mature with higher comprehensiveness levels since higher levels may not be appropriate to the need, but rather for the fit.

Level 0, None: There is no common understanding of how the security practice is applied and no related requirements are implemented (as this level has no assurance or practices applied, we do not discuss it further).

Level 1, Minimum: The minimum requirements of the security practice are implemented. There are no assurance activities for the security practice implementation.

Level 2, Ad hoc: The requirements for the practice cover main use cases and well-known security incidents in similar environments. The requirements increase accuracy and level of granularity for the environment under consideration. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks. For this assurance, one may apply measures learned through successful references.

Level 3, Consistent: The requirements consider best practices, standards, regulations, classifications, software, and other tools. The tools establish a consistent approach to practice deployment. The assurance of the implementation validates the implementation against security patterns, design with security in mind from the beginning and known protection approaches and mechanisms. This includes creating a system with the security design considered in the architecture and design as well as definition defaults.

Level 4, Formalized: A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance of the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. This assurance uses semi-formal to formal methods.

1.2.2 Scope Levels

There are three levels of scope for every security domain, subdomain and practice, from Level 1 to Level 3, with higher numbers indicating a narrower and more specific scope.

Level 1, General: This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

Level 2, Industry specific: The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sector-specific issues, particularly those regarding components and processes that are prone to certain types of attacks and known vulnerabilities and incidents that have taken place.

Level 3, System specific: This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios.

As we mentioned previously, mappings enable aligning SMM practices with other frameworks and guidance for detailed understanding on addressing gaps discovered when performing an SMM assessment against an SMM target.

1.3 The NIST Cybersecurity Framework

“The NIST Cybersecurity Framework (Framework or CSF) 1.1 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them.”[17].

The NIST Cybersecurity Framework is structured around five core functions intended to organize cybersecurity outcomes at a high level: *identify*, *protect*, *detect*, *respond*, and *recover*.

[17] [NIST_CSF11]

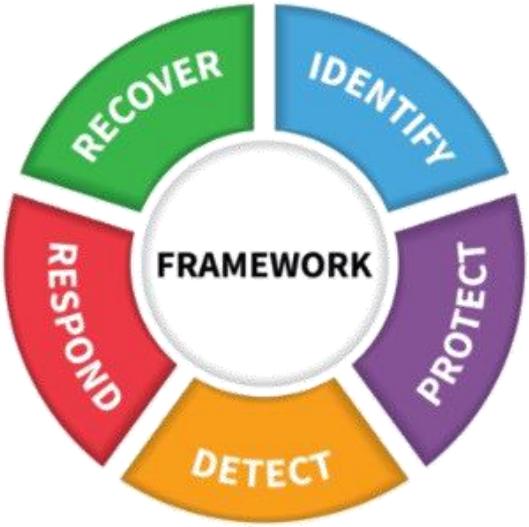


Figure 1-2: NIST Cybersecurity Framework 1.1 Functions

These functions are summarized as follows in the NIST Cybersecurity Framework 1.1 document:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

The NIST Cybersecurity Framework defines both current state and target state as follows:

A *Current Profile* covers the Core's outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.

A *Target Profile* covers the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives. A Target Profile takes into account anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and cybersecurity threat intelligence trends.

These NIST CSF profiles are similar to the SMM current assessment and target goals and should not be confused with SMM profiles since the word 'profile' is used to mean different things in these two approaches.

The framework can be used to determine the current profile, set a target profile, and prioritize and implement changes to move to the target profile.

Framework tiers are defined to enable organizations to determine the target levels they wish to achieve, similar in concept to the SMM comprehensiveness levels, though the SMM levels take more into account:

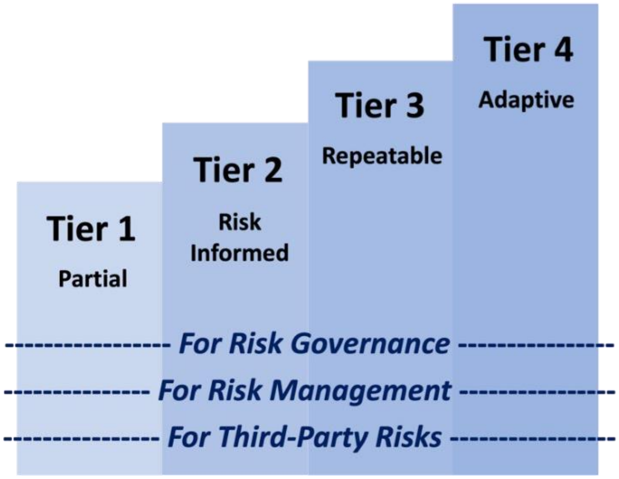
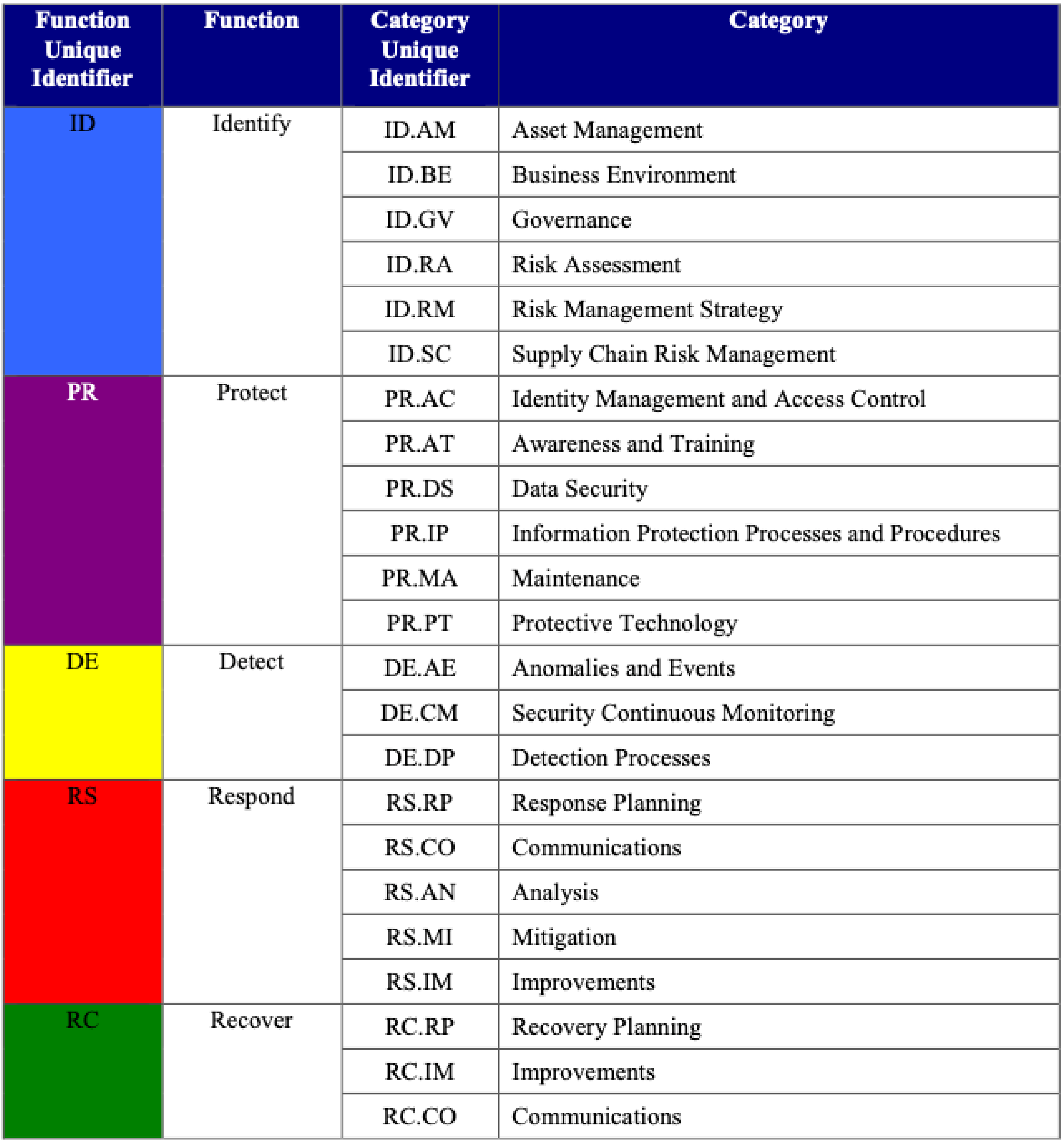


Figure 1-3: NIST Cybersecurity Framework Tiers (from 2.0 draft)

The framework core is organized as follows:

Figure 1-4: NIST Cybersecurity Framework Core



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The identifiers are used in the SMM mapping tables. For example, "**ID.AM-01**: Inventories of hardware managed by the organization are maintained" is mapped to SMM Table 9, Asset, Change and Configuration Management at Comprehensiveness level 2.

2 General Mapping Considerations

2.1 Trustworthiness

The SMM is focused on security and does not directly address other aspects of trustworthiness such as safety, reliability, resilience, and privacy; the mapping of trustworthiness related NIST requirements in this document is limited to how they relate to security. Despite this, a system assessment should consider trustworthiness characteristics and include verification and validation (V&V) considerations and general availability concerns (beyond the security denial-of-service concept).

2.2 Example of How to Use the Mappings

One approach to using these mappings is to first determine the target comprehensiveness level required for an SMM practice. This is done as discussed in the SMM practitioner's guide[18]. Once this SMM target is determined, then the corresponding mapping tables in this document can be used to understand NIST Cybersecurity requirements that may be used to achieve that level.

For example, assume the SMM target for physical security is determined to be comprehensiveness level 3. To achieve this target all the SMM comprehensiveness levels up to that level need to be achieved, so levels 1 (minimum), 2 (ad hoc) and 3 (consistent) should all be achieved, based on the guidance in the SMM practitioner's guide. This NIST mapping can assist with achieving that by referencing NIST Cybersecurity Framework guidance specific to the practice and comprehensiveness levels that can be used to achieve the SMM comprehensiveness level (for example, by referencing the references in the NIST CSF for those sub-categories to obtain detailed requirements and guidance).

This mapping document shows that to achieve level 3 maturity for physical protection the following NIST CSF functions and categories are relevant:

- SMM Level 3: DE.CM-2
  - Function: Defend (DE)
  - Category: Security Continuous Monitoring (CM)
  - Subcategory: The physical environment is monitored to detect potential cybersecurity events
- SMM Level 2: PR.PT-4
  - Function: Protect (PR)
  - Category: Protective Technology (PT)
  - Subcategory: Communications and control networks are protected
- SMM Level 1: PR.AC-2

[18] [IIC-SMMP2020]

    - Function: Protect (PR)
    - Category: Identity Management, Authentication and Access Control (AC)
    - Subcategory: Physical access to assets is managed and protected
- SMM Level 1: PR.IP-5
    - Function: Protect (PR)
    - Category: Information Protection Processes and Procedures (IP)
    - Subcategory: Policy and regulations regarding the physical operating environment for organizational assets are met

To give a little more detail for just one of these, PR.IP-5 provides the following informative references which can be used to help taking action to achieve the SMM maturity:

- **COBIT 5** DSS01.04, DSS05.05
  ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
- **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
- **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE- 14, PE-15, PE-18

3 NIST Cybersecurity Mapping Considerations

The 2.0 version of the Cybersecurity Framework has been published and adds *govern* to the list of functions as well as revising the definitions of the other functions. The draft definition of the new function is given in the CSF 2.0 as follows:

- ***Govern** (GV) - The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

The *Govern* function is viewed as central to the other functions in the CSF 2.0, as follows:

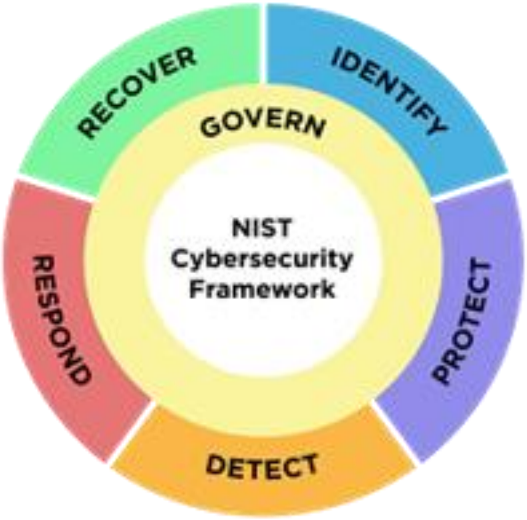


Figure 3-1: NIST Cybersecurity Framework 2.0 Functions

The *Govern* function will have a number of categories:

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC

This mapping document does not map the *Govern* function but it should be clear that the SMM tables related to governance are appropriate. A future revision of this mapping will address NIST CSF 2.0 in detail.

4 SMM Mappings to NIST Cybersecurity Framework

The mapping tables provide reference to specific guidance in the NIST Cybersecurity Framework that is relevant to the maturity levels noted in the tables. In some cases, there will be no mapping since there is no NIST Cybersecurity Framework guidance directly appropriate to that maturity level for that table. This will be noted as "*No mappings.*" This does not mean that no action is required to achieve that maturity level, but rather that there is no additional mapping guidance provided in this document. The reader is still responsible for understanding the general guidance offered in the Security Maturity Model Practitioner's guide and implementing it appropriately possibly using other SMM profile or mapping documents in addition to this mapping document.

4.1 Security Program Management (SMM Practice 1)

Security Program Management			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
ID.AM-6 ID.BE-3 ID.GV-2 DE.DP-1 RC.CO-1	ID.BE-2 ID.GV-1 PR.AT-4 PR.AT-5 PR.IP-2 PR.IP-11 RS.CO-1	ID.BE-1 ID.GV-3 ID.GV-4 ID.RM-2 ID.RM-3 PR.AT-3 PR.IP-8	PR.AT-1 PR.AT-2

Table 4-1: Security Program Management Mappings.

4.2 Compliance Management (SMM Practice 2)

Compliance Management			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	ID.GV-3	*No mappings*

Table 4-2: Compliance Management Mappings.

4.3 Threat Modeling (SMM Practice 3)

Threat Modeling			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
ID.RA-2 ID.RA-3 PR.DS-4	*No mappings*	ID.RA-4	*No mappings*

Table 4-3: Threat Modeling Mappings.

4.4 Risk Attitude (SMM Practice 4)

Risk Attitude			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
ID.GV-4	ID.RA-5 ID.RA-6 ID.RM-1 ID.SC-1 ID.SC-2	ID.BE-1 ID.RM-2	ID.RM-3

Table 4-4: Risk Attitude Mappings.

4.5 Product Supply Chain Risk Management (SMM Practice 5)

Product Supply Chain Risk Management			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
ID.SC-1 PR.AT-3	ID.BE-1 ID.BE-4 ID.SC-2 ID.SC-3	*No mappings*	ID.BE-5 ID.SC-4 DE.CM-6

Table 4-5: Product Supply Chain Risk Management Mappings.

4.6 Services Third-Party Dependencies Management (SMM Practice 6)

Services Third-Party Dependencies Management			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
No mappings	ID.SC-3	*No mappings*	ID.SC-4

Table 4-6: Services Third-Party Dependencies Management Mappings.

4.7 Establishing And Maintaining Identities (SMM Practice 7)

Establishing And Maintaining Identities			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
No mappings	PR.AC-1	PR.AC-7	PR.AC-6

Table 4-7: Establishing and Maintaining Identities Mappings.

4.8 Access Control (SMM Practice 8)

Access Control

Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
PR.AC-3	PR.AT-2 PR.MA-2	PR.AC-4 PR.PT-3 PR.PT-4	*No mappings*

Table 4-8: Access Control Mappings.

4.9 Asset, Change And Configuration Management (SMM Practice 9)

Asset, Change and Configuration Management			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
PR.DS-7	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5 PR.IP-1 PR.IP-3	PR.IP-2 PR.MA-1 PR.PT-3	PR.DS-3 PR.DS-4 PR.IP-6

Table 4-9: Asset, Change and Configuration Management Mappings.

4.10 Physical Protection (SMM Practice 10)

Physical Protection			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
PR.AC-2 PR.IP-5	PR.PT-4	DE.CM-2	*No mappings*

Table 4-10: Physical Protection Mappings.

4.11 Protection Model And Policy For Data (SMM Practice 11)

Protection Model and Policy for Data

Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	ID.AM-5 PR.DS-5 PR.IP-6 PR.PT-2	ID.AM-3 DE.AE-1	PR.IP-7

Table 4-11: Protection Model and Policy for Data Mappings.

4.12 Implementation Of Data Protection Controls (SMM Practice 12)

Implementation of Data Protection Controls			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
PR.DS-1 PR.DS-2	PR.AC-5 PR.DS-5 PR.PT-2 PR.PT-4 DE.AE-1	PR.DS-6	PR.IP-6

Table 4-12: Implementation of Data Protection Controls Mappings

4.13 Vulnerability Assessment (SMM Practice 13)

Vulnerability Assessment			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**

ID.RA-1 DE.DP-1	PR.IP-12 RS.AN-5 RS.MI-3	DE.CM-8	*No mappings*

Table 4-13: Vulnerability Assessment Mappings.

4.14 Patch Management (SMM Practice 14)

Patch Management			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
RS.AN-5 *No mappings*	PR.IP-12 RS.MI-3	PR.MA-1	*No mappings*

Table 4-14: Patch Management Mappings.

4.15 Monitoring Practice (SMM Practice 15)

Monitoring Practice			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
PR.PT-1 DE.DP-1	DE.AE-1 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2	DE.AE-2 DE.AE-3 DE.CM-7	DE.DP-3 DE.DP-5

	DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.DP-2 RS.AN-1		

Table 4-15: Monitoring Practice Mappings.

4.16 Situation Awareness And Information Sharing (SMM Practice 16)

Situation Awareness and Information Sharing			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
ID.RA-2 RS.CO-5	RS.CO-2 RS.CO-3 RS.AN-5 RC.CO-1	PR.IP-8 DE.DP-4 RC.CO-2	*No mappings*

Table 4-16: Situation Awareness and Information Sharing Mappings

4.17 Event Detection And Response Plan (SMM Practice 17)

Event Detection and Response Plan			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
DE.AE-4	PR.IP-9 DE.CM-3	PR.IP-10 DE.DP-3	ID.SC-5

DE.AE-5 RS.RP-1 RS.CO-2 RS.AN-1	DE.CM-4 DE.CM-5 DE.CM-6 DE.DP-1 DE.DP-2 RS.CO-1 RS.CO-4 RS.AN-2 RS.AN-3 RS.AN-4	DE.DP-4 RS.IM-1 RS.IM-2 RC.CO-1	DE.DP-5 RS.CO-5 RC.CO-3

Table 4-17: Event Detection and Response Plan Mappings.

4.18 Remediation, Recovery And Continuity Of Operations (SMM Practice 18)

Remediation, Recovery and Continuity of Operations			
Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
No mappings	PR.IP-4 RS.MI-1 RS.MI-2 RC.RP-1 RC.IM-2	PR.DS-4 PR.PT-5	ID.SC-5 PR.IP-10 RS.CO-2 RC.IM-1 RC.CO-1 RC.CO-2

Table 4-18: Remediation, Recovery and Continuity of Operations Mappings

.

5 NIST Cybersecurity Framework mappings to SMM Practices

These mappings relate NIST CSF 1.1 functions to corresponding SMM practice and comprehensiveness levels.

5.1 Identify

ID	The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device.	
ID.AM	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
ID.AM-1	Physical devices and systems within the organization are inventoried	SMM 9 C2
ID.AM-2	Software platforms and applications within the organization are inventoried	SMM 9 C2
ID.AM-3	Organizational communication and data flows are mapped	SMM 11 C3
ID.AM-4	External information systems are catalogued	SMM 9 C2
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	SMM 9 C2
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	SMM 11 C2
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	SMM 1 C1

ID.BE	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	▨
ID.BE-1	The organization's role in the supply chain is identified and communicated	SMM 1 C3
ID.BE-1	The organization's role in the supply chain is identified and communicated	SMM 4 C3
ID.BE-1	The organization's role in the supply chain is identified and communicated	SMM 5 C2
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	SMM 1 C2
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	SMM 1 C1
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	SMM 5 C2
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	SMM 5 C4
ID.GV	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	▨
ID.GV-1	Organizational cybersecurity policy is established and communicated	SMM 1 C2

ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	SMM 1 C1
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	SMM 1 C3
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	SMM 2 C3
ID.GV-4	Governance and risk management processes address cybersecurity risks	SMM 1 C3
ID.GV-4	Governance and risk management processes address cybersecurity risks	SMM 4 C1
ID.RA	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	▨
ID.RA-1	Asset vulnerabilities are identified and documented	SMM 13 C1
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	SMM 3 C1
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	SMM 16 C1
ID.RA-3	Threats, both internal and external, are identified and documented	SMM 3 C1
ID.RA-4	Potential business impacts and likelihoods are identified	SMM 3 C3
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	SMM 4 C2
ID.RA-6	Risk responses are identified and prioritized	SMM 4 C2

ID.RM	The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	SMM 4 C2
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SMM 1 C3
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SMM 4 C3
ID.RM-3	The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SMM 1 C3
ID.RM-3	The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SMM 4 C4
ID.SC	The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SMM 4 C2
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SMM 5 C1

ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	SMM 4 C2
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	SMM 5 C2
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	SMM 5 C2
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	SMM 6 C2
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	SMM 5 C4
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	SMM 6 C4
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	SMM 17 C4
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	SMM 18 C4

5.2 Protect

PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	▨
PR.AC	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	SMM 7 C2
PR.AC-2	Physical access to assets is managed and protected	SMM 10 C1
PR.AC-3	Remote access is managed	SMM 8 C1
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	SMM 8 C3
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	SMM 12 C2
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	SMM 7 C4
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)	SMM 7 C3
PR.AT	The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	

PR.AT-1	All users are informed and trained	SMM 1 C4
PR.AT-2	Privileged users understand their roles and responsibilities	SMM 1 C4
PR.AT-2	Privileged users understand their roles and responsibilities	SMM 8 C2
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	SMM 1 C3
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	SMM 5 C1
PR.AT-4	Senior executives understand their roles and responsibilities	SMM 1 C2
PR.AT-5	Physical and cybersecurity personnel understand their roles and responsibilities	SMM 1 C2
PR.DS	Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	
PR.DS-1	Data-at-rest is protected	SMM 12 C1
PR.DS-2	Data-in-transit is protected	SMM 12 C1
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	SMM 9 C4
PR.DS-4	Adequate capacity to ensure availability is maintained	SMM 3 C1
PR.DS-4	Adequate capacity to ensure availability is maintained	SMM 9 C4

PR.DS-4	Adequate capacity to ensure availability is maintained	SMM 18 C3
PR.DS-5	Protections against data leaks are implemented	SMM 11 C2
PR.DS-5	Protections against data leaks are implemented	SMM 12 C2
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	SMM 12 C3
PR.DS-7	The development and testing environment(s) are separate from the production environment	SMM 9 C1
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity	*No mapping*
PR.IP	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	SMM 9 C2
PR.IP-2	A System Development Life Cycle to manage systems is implemented	SMM 1 C2
PR.IP-2	A System Development Life Cycle to manage systems is implemented	SMM 9 C3
PR.IP-3	Configuration change control processes are in place	SMM 9 C2

PR.IP-4	Backups of information are conducted, maintained, and tested	SMM 18 C2
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	SMM 10 C1
PR.IP-6	Data is destroyed according to policy	SMM 9 C4
PR.IP-6	Data is destroyed according to policy	SMM 11 C2
PR.IP-6	Data is destroyed according to policy	SMM 12 C4
PR.IP-7	Protection processes are improved	SMM 11 C4
PR.IP-8	Effectiveness of protection technologies is shared	SMM 1 C3
PR.IP-8	Effectiveness of protection technologies is shared	SMM 16 C3
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	SMM 17 C2
PR.IP-10	Response and recovery plans are tested	SMM 17 C3
PR.IP-10	Response and recovery plans are tested	SMM 18 C4
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	SMM 1 C2
PR.IP-12	A vulnerability management plan is developed and implemented	SMM 13 C2

PR.IP-12	A vulnerability management plan is developed and implemented	SMM 14 C2
PR.MA	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	▨
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	SMM 9 C3
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	SMM 14 C3
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	SMM 8 C2
PR.PT	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	▨
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	SMM 15 C1
PR.PT-2	Removable media is protected and its use restricted according to policy	SMM 11 C2
PR.PT-2	Removable media is protected and its use restricted according to policy	SMM 12 C2
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	SMM 8 C3
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	SMM 9 C3
PR.PT-4	Communications and control networks are protected	SMM 8 C3
PR.PT-4	Communications and control networks are protected	SMM 10 C2

PR.PT-4	Communications and control networks are protected	SMM 12 C2
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	SMM 18 C3

5.3 Detect

DE	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	▨
DE.AE	Anomalous activity is detected and the potential impact of events is understood.	
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	SMM 11 C3
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	SMM 12 C2
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	SMM 15 C2
DE.AE-2	Detected events are analyzed to understand attack targets and methods	SMM 15 C3
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	SMM 15 C3
DE.AE-4	Impact of events is determined	SMM 15 C2
DE.AE-4	Impact of events is determined	SMM 17 C1
DE.AE-5	Incident alert thresholds are established	SMM 15 C2
DE.AE-5	Incident alert thresholds are established	SMM 17 C1

DE.CM	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
DE.CM-1	The network is monitored to detect potential cybersecurity events	SMM 15 C2
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	SMM 10 C3
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	SMM 15 C2
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	SMM 15 C2
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	SMM 17 C2
DE.CM-4	Malicious code is detected	SMM 15 C2
DE.CM-4	Malicious code is detected	SMM 17 C2
DE.CM-5	Unauthorized mobile code is detected	SMM 15 C2
DE.CM-5	Unauthorized mobile code is detected	SMM 17 C2
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	SMM 5 C4
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	SMM 15 C2
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	SMM 17 C2
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	SMM 15 C3
DE.CM-8	Vulnerability scans are performed	SMM 13 C3

DE.DP	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	▨
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	SMM 1 C1
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	SMM 13 C1
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	SMM 15 C1
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	SMM 17 C2
DE.DP-2	Detection activities comply with all applicable requirements	SMM 15 C2
DE.DP-2	Detection activities comply with all applicable requirements	SMM 17 C2
DE.DP-3	Detection processes are tested	SMM 15 C4
DE.DP-3	Detection processes are tested	SMM 17 C3
DE.DP-4	Event detection information is communicated	SMM 16 C3
DE.DP-4	Event detection information is communicated	SMM 17 C3
DE.DP-5	Detection processes are continuously improved	SMM 15 C4
DE.DP-5	Detection processes are continuously improved	SMM 17 C4

5.4 Respond

RS	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	

RS.RP	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	▨
RS.RP-1	Response plan is executed during or after an incident	SMM 17 C1
RS.CO	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	▨
RS.CO-1	Personnel know their roles and order of operations when a response is needed	SMM 1 C2
RS.CO-1	Personnel know their roles and order of operations when a response is needed	SMM 17 C2
RS.CO-2	Incidents are reported consistent with established criteria	SMM 16 C2
RS.CO-2	Incidents are reported consistent with established criteria	SMM 17 C1
RS.CO-2	Incidents are reported consistent with established criteria	SMM 18 C4
RS.CO-3	Information is shared consistent with response plans	SMM 16 C2
RS.CO-4	Coordination with stakeholders occurs consistent with response plans	SMM 17 C2
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SMM 16 C1
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SMM 17 C4

RS.AN	Analysis is conducted to ensure effective response and support recovery activities.	▨
RS.AN-1	Notifications from detection systems are investigated	SMM 15 C2
RS.AN-1	Notifications from detection systems are investigated	SMM 17 C1
RS.AN-2	The impact of the incident is understood	SMM 17 C2
RS.AN-3	Forensics are performed	SMM 17 C2
RS.AN-4	Incidents are categorized consistent with response plans	SMM 17 C2
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SMM 13 C2
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SMM 14 C1
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SMM 16 C2
RS.MI	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
RS.MI-1	Incidents are contained	SMM 18 C2

RS.MI-2	Incidents are mitigated	SMM 18 C2
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	SMM 13 C2
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	SMM 14 C2
RS.IM	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	▨
RS.IM-1	Response plans incorporate lessons learned	SMM 17 C3
RS.IM-2	Response strategies are updated	SMM 17 C3

5.5 Recover

RC	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	
RC.RP	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	▨
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident	SMM 18 C2
RC.IM	Recovery planning and processes are improved by incorporating lessons learned into future activities.	▨
RC.IM-1	Recovery plans incorporate lessons learned	SMM 18 C4

RC.IM-2	Recovery strategies are updated	SMM 18 C2
RC.CO	Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	
RC.CO-1	Public relations are managed	SMM 1 C1
RC.CO-1	Public relations are managed	SMM 16 C2
RC.CO-1	Public relations are managed	SMM 17 C3
RC.CO-1	Public relations are managed	SMM 18 C4
RC.CO-2	Reputation is repaired after an incident	SMM 16 C3
RC.CO-2	Reputation is repaired after an incident	SMM 18 C4
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	SMM 17 C4

Annex A GLOSSARY

The terms and their definitions in this section are specific to this document and may not be applicable to other IIC documents including the Industry IoT Vocabulary Technical Report.

Comprehensiveness is a measure of the completeness, consistency and assurance of the implementation of measures supporting the security maturity domain, subdomain or practice.

The maturity *current state* represents the maturity as captured by an assessment of the organization.

Domains are the strategic priorities for security maturity. In the SMM, there are three domains: governance, enablement, and hardening.

Enablement is the implementation of security controls and practices needed to create an operational system meeting the policy and operational requirements.

Governance is the “establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization.”[19]

Hardening is the use of security practices during system operation.

Industrial Internet of Things (IIoT) describes systems that connect and integrate industrial control systems with enterprise systems, business processes, and analytics.

A *Practice* comprises the typical activities performed for a given subdomain; they provide the deeper detail necessary for planning. Each sub domain has a set of practices.

Scope is a measure of the applicability to a specific vertical or system.

Security maturity is a measure of an understanding of the current security level, its necessity, benefits, and cost of its support. Maturity is captured by two dimensions, comprehensiveness and scope.

The *security maturity profile* is a typical security maturity target for a specific type of device, organization or system. Using security maturity target profiles simplifies the process of establishing the target for common use cases. Establishing a library of security maturity target profiles for common IoT scenarios is a subject for further development.

A *Subdomain* is the basic means to address a domain at the planning level. Each domain currently defines three subdomains.

Target state is the desired “end state” security maturity for an organization or system. The security maturity target can apply to a new system under development or an existing brownfield system. The security maturity target is determined based upon the business objectives of the organization or group.

[19] *https://transitionpointba.com/governance/*

Annex B REFERENCES

Note: For additional information on 62443, please refer to: *https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards*

[IIC-CF-2022] Rajive Joshi (Lead, R. T. I., Paul Didier (Cisco), Christer Holmberg (Ericsson), Jaime Jimenez (Ericsson), Timothy Carey (Nokia). The Industrial Internet of Things Connectivity Framework. 2022. https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/06/IIoT-Connectivity-Framework-2022-06-08.pdf

[IIC-IIRA-2022] Shi-Wan Lin (Thingswise/Intel, A. C.-e., Eric Simmon (NIST, also co-editor), Daniel Young (Toshiba), Bradford Miller (GE), Jacques Durand (Fujitsu), Graham Bleakley (IBM), Amine Chigani (GE), Robert Martin (MITRE), Brett Murphy (RTI) and Mark Crawford (SAP). The Industrial Internet Reference Architecture, Version 1.10. 2022. *https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf*

[IIC-IISF2-2023] Keao Caindec (Farallon Technology Group), M. B. W.-S., Bassam Zarkout (IGnPower), Sven Schrecker (Amazon Web Services), Frederick Hirsch (Upham Security), Isaac Dungana (Red Alert Labs), Robert Martin (MITRE), Mitch Tseng (Tseng Info). Industry Internet of Things Security Framework (IISF), Version 2.0. 2023. https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/06/IISF-Version-2.pdf

[IIC-SMM-62443M-2023] Eric Cosman (OIT Concepts), J. G. D., Frederick Hirsch (Upham Security), Pierre Kobes (Kobes Consulting), Ekaterina Rudina (Kaspersky), & Ron Zahavi (Microsoft). IoT Security Maturity Model: 62443 Mappings for Asset Owners, Product Suppliers and Service Providers (updated). 2023. https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/08/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf

[IIC-SMM-DTP2022] Jon Geater (Jitsuin), F. H. U. S., Detlev Richter (TÜV SÜD), Michael Robkin (Six By Six), Ron Zahavi (Microsoft). IoT Security Maturity Model Digital Twin Profile. 2022. https://www.digitaltwinconsortium.org/wp-content/uploads/sites/3/2022/06/SMM-Digital-Twin-Profile-2022-06-20.pdf

[IIC-SMM-MEP2023] Lehlogonolo Ledwaba (Mandela Mining Precinct), Carel Kruger (Mandela Mining Precinct), & Frederick Hirsch (Upham Security), R. Z. A. T. IoT Security Maturity Model Mining Extraction Profile. 2024. https://www.iiconsortium.org/wp-content/uploads/sites/2/2024/02/SMM_Mining_Extraction_Profile_02072024.pdf

[IIC-SMM-PG2024] Frederick Hirsch (Upham Security), R. Z. A. T., Lehlogonolo Ledwaba (Mandela Mining Precinct). Guidance for Creating IoT Security Maturity Model Profiles. 2024. https://www.iiconsortium.org/wp-content/uploads/sites/2/2024/03/Guidance_for_Creating_IoT_Security_Maturity_Model_Profiles_02292024.pdf

[IIC-SMM-RP2022] Frederick Hirsch (Upham Security), A. M. L., Bart McGlothin (Cisco), Leonid Rubhakin (Aptos), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft). IoT SMM: Retail Profile for Point-of-Sale Devices. 2020. https://www.iiconsortium.org/pdf/SMM-Retail-Profile.pdf

[IIC-TFF-2021] Buchheit, M., Hirsch, F., Martin, R. A., Bemmel, D. V., Espinosa, A. J., Zarkout, B., . . . Tseng, M. The Industrial Internet of Things Trustworthiness Framework Foundations. 2021. https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

[IIC-SMMP2020] Frederick Hirsch (Fujitsu), S. C. E. D.,Matt Eble (Praetorian), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft). IoT SMM Practitioner’s Guide Version 1.2. 2020. https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

[NIST-CSF11] National, I. O., & Technology, S. A. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[NIST-CSF20] National, I. O., & (2024), S. A. T. The NIST Cybersecurity Framework (CSF) 2.0. 2024. https://doi.org/10.6028/NIST.CSWP.29

AUTHORS AND LEGAL NOTICE

This document is a work product of the Industry IoT Consortium (IIC) ISA Contributing Group, chaired by Jim Gilsinn *(*Dragos), Frederick Hirsch (Upham Security), Ron Zahavi (Microsoft) in conjunction with the IIC/DTC Security and Trustworthiness Working Group, chaired by Keao Caindec (Farallon Technology Group).

Authors: The following persons contributed substantial written content to this document:

Pierre Kobes (Kobes Consulting), Frederick Hirsch (Upham Security), Ron Zahavi (Microsoft).

Technical Editor: Chuck Byers (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.