IoT Security Maturity Model (SMM): Practitioner's Guide

An Industrial Internet Consortium Technical Report

Version 1.2 – 2020-05-05

Sandy Carielli (Entrust Datacard), Matt Eble (Praetorian), Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft)

CONTENTS

Part I: Model

Part II: The Core of The Security Maturity Model

Part III: Comprehensiveness Level Definition Guide

Part IV: Case Studies

Part V: Annexes

FIGURES

TABLES

1 Overview

In April 2018 the Industrial Internet Consortium (IIC) published the first of two documents relating to the IoT Security Maturity Model. The first document, IoT Security Maturity Model: Description and Intended Use[1], is for stakeholders to understand the purpose, need and intent of the model. This second document, the practitioner's guide, provides the model's details and describes how it is to be used.

The IoT Security Maturity Model (SMM) enables Internet of Things (IoT) providers to set security targets and invest appropriately in sensible security mechanisms that meet their requirements. Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.

The SMM provides a conceptual framework to help organizations select and implement the appropriate security controls from the myriad options. It helps an organization determine what their security maturity target state should be and assess their current state. Repeatedly comparing the target and current states identifies where further improvement can be made.

1.1 Relationship with Other IIC documents

We rely on the concepts discussed in the Industrial Internet Reference Architecture (IIRA)[2] and the Industrial Internet Security Framework (IISF)[3].

The IISF describes the need for trustworthy systems having assurance and focuses on security. It captures the information technology (IT) and operational technology (OT) dimensions of security for the industrial internet of things and describes security architectural considerations and requirements. It details key security building blocks, including endpoint protection, secure connectivity, security monitoring and analysis, configuration and management and others. This document offers an additional dimension to the concepts, security techniques and mechanisms described there by addressing the need for security maturity to guide the prioritization and investment in security controls, be they people, process or technology. The SMM addresses IT and OT systems and systems that reside at the endpoint, on the network or in the cloud, providing guidance on the maturity required to address specific IoT scenarios and the mechanisms to use to achieve that maturity.

The IIC Vocabulary[4] provides terminology and definitions for all IIC documents. Acronyms and additional terms relevant to this model are defined in the appendices.

[1] See [IIC-SMMD2020]

[2] See [IIC-IIRA2019]

[3] See [IIC-IISF2016]

[4] See [IIC-IIV2019]

We recommend that both business and technical stakeholders review the first document, IoT Security Maturity Model: Description and Intended Use[1] before tackling this document, the *IoT Security Maturity Model: Practitioner's Guide*.

[1] See [IIC-SMMD2020]

Part I: Model

2 THE SECURITY MATURITY MODEL

There is no silver bullet that can address security needs for every system. Organizations have differing needs, and different systems need different strengths of protection mechanisms. The same technology can be applied in different ways and to different degrees, depending on needs. The SMM helps organizations determine the priorities that drive their security enhancements and the maturity required to achieve them.

The 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 mature security practices, can collaborate with the analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation.

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

2.1 SECURITY MATURITY VS. SECURITY LEVEL

Maturity is about effectiveness, not the arbitrary use of mechanisms. 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.

Not all systems require the same strength of protection mechanisms or procedures to meet their security requirements. The organizational 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. Hence, *security maturity* is the degree of confidence that the current security state meets all organizational security needs and all organizational security-related requirements. That is to say, security maturity is a measure of the understanding of the overall current security level including people, processes and technology including its necessity, benefits and cost to support. 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.

Security level,[1] on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner. The SMM does

[1] According to [IEC-62443-33]

not say what the appropriate security level should be. Rather, it provides guidance and structure for organizations to select the maturity appropriate for their industry and system. Some users will apply the model to create industry- and system-specific profiles, which a broader audience can then use to assess maturity in a specific vertical or use case.

2.2 Requirements

When developing the SMM, the authors were guided by the following requirements.

Real-world applicability: The method for setting the security maturity target must consider functionality, safety, regulatory and legal requirements or guidelines, risk management, security and privacy policies, performance, costs and other business considerations. It must also consider known and emerging threats and affordable ways of countering them. The outcome of the process and the guidance for attaining the target should be directly applicable to the IoT infrastructure in question and therefore be actionable.

Consideration of different perspectives: The SMM facilitates a description of security maturity from different viewpoints including business and implementation views. It helps define security maturity goals from an organizational perspective and security maturity requirements from an implementation perspective. The model helps align these definitions and thus drive collaboration among all stakeholders who are working towards security maturity enhancement.

Appropriate security guidance: The SMM provides guidance for the assessment and further enhancement of security maturity that aligns security capabilities with a particular use case. Guidance should be practical and actionable.

Adaptable to changing threat environment: As infrastructure and threats evolve, the security target must be adaptable (e.g. firmware updates or patching) to remain relevant in the long run. It is insufficient to implement security measures only at the system design stage for systems with long operational lifespans.

Extensibility: IoT business models, products, guidelines, regulations, technologies and types of organizations will evolve. The SMM needs to be flexible enough to accommodate any changes.

2.3 Scope

The SMM explains how security practices may be aligned with existing security concerns in an effective way. It provides the classification and detailed description of security practices, criteria for their security maturity, relevant security concerns, techniques and capabilities, allowing for the assessment and planning of their implementation according to the established strategy. It also provides recommendations on the process for this assessment and implementation.

The focus of this practitioner's guide is on security. Security maturity can have an impact on the trustworthiness of systems. If the security maturity is low, reflecting poor understanding of requirements, this can open the possibility of security incidents that affect safety, privacy, reliability and resilience. This practitioner's guide does not detail maturity related to trustworthiness characteristics other than security but might be extended in the future to trustworthiness characteristics. The IIC Journal of Innovation includes an article outlining some possible approaches,[1] but detailed guidance remains for a future publication.

The details and recommendations are based on the strategic approach built during the collaborative work of security engineers and business risk owners. This approach is defined by the IoT Security Maturity Model: Description and Intended Use[2]. The practitioner's guide does not focus on the development of the strategy itself, relying on it as input into the process defined by this document.

2.4 Audience

The audience for this document includes:

Security practitioners responsible for their organization's systems. Practitioners translate business stakeholder objectives into the appropriate level of target security maturity.

Security assessment professionals, both internal to the organization, or independent third parties, who conduct current state assessments using the model and identify gaps between the current and target states.

Industry groups that will extend the model in industry- and system-specific ways.

Users of this SMM should be able to determine and clearly communicate the answers to these questions:

- Given the organizational requirements and threat landscape, what is my solution's target maturity state?
- What is my solution's current maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

2.5 Relationship to Other Models and Frameworks

This IoT Security Maturity Model is the first model of its kind to assess the maturity of organizations' IoT systems in a way that includes governance, technology and system management. Other models address part of what is addressed by the SMM: they may address a particular industry, IoT but not security, or security but not IoT. The SMM covers all these aspects and points to existing models to recognize existing work and avoid duplication.

Many related frameworks focus on security levels and security controls required to meet those levels. IIC will provide associated mappings between the SMM and the most popular frameworks. This will help practitioners identify which controls to implement as they plan to address gaps between current and target security maturity states.

[1] See [IIC-ESMM2018]

[2] See [IIC-SMMD2020]

The model fosters effective and productive collaboration among business and technical stakeholders. Business decision makers, business risk managers and operational users of IoT systems, concerned about proper strategy for implementing mature security practices, can collaborate with the analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation.

3 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.”[1] *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 seriousness placed on security.

Enablement is the implementation of security controls and practices needed to create an operational system meeting the policy and operational requirements. Enablement uses architectural design to address business risks and specific controls 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 requirements of a given domain or subdomain. Domains and subdomains make clear various perspectives. Figure 3-1 displays the hierarchy 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.

[1] *http://www.businessdictionary.com/definition/governance.html*

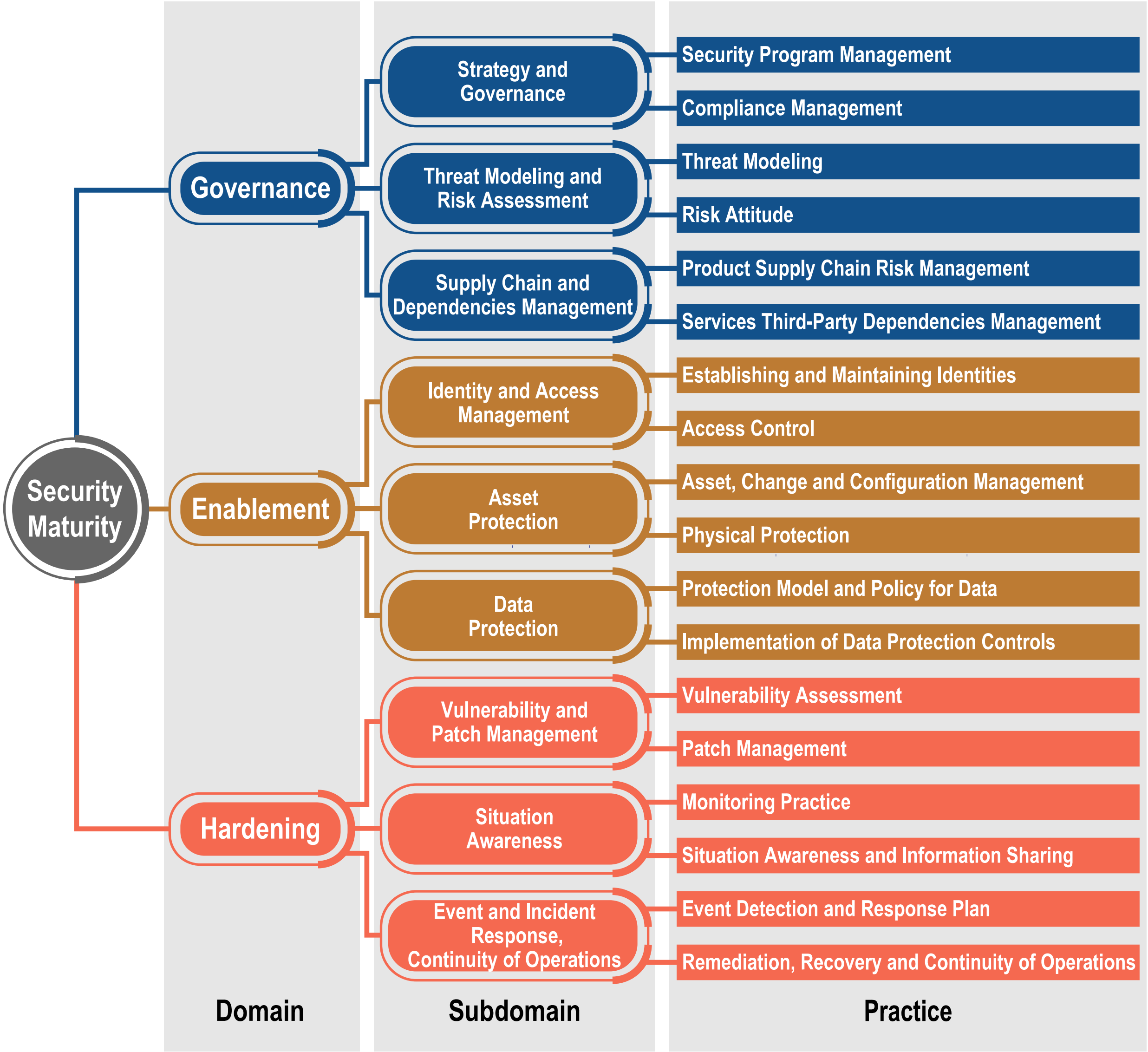

Security Maturity
Governance
Enablement
Hardening
Strategy and Governance
Threat Modeling and Risk Assessment
Supply Chain and Dependencies Management
Identity and Access Management
Asset Protection
Data Protection
Vulnerability and Patch Management
Situation Awareness
Event and Incident Response, Continuity 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 3-1: 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-specific or system-specific constraints of the IoT system.

Comprehensiveness and scope help score and prioritize security maturity practices. Certain systems may not require certain practices at all, which, if based on understanding of the requirements, can still reflect a high level of security maturity. Not having a highly sophisticated or narrowly scoped implementation of a security practice that could be over-engineered, given the particular system and the threats that it currently faces, is entirely appropriate. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

3.1 Comprehensiveness Levels

There are five comprehensiveness levels for every security domain, subdomain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree of comprehensiveness. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones.

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.

3.2 Scope Levels

There are three levels of scope for every security facet, 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.

4 TEMPLATE

Each SMM practice in this guide has a corresponding table describing the comprehensiveness at the *general* scope level. Table 4-1 shows a template for the practice table. For each comprehensiveness level, the table describes the objective and general considerations. General considerations include:

- a description of the level,
- what needs to be done to achieve that level and
- indicators of accomplishment to help assessors determine if the organization has met the requirements of the level.

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Objective Description	Objective Description	Objective Description	Objective Description
General considerations	Level Description	Level Description	Level Description	Level Description
	What needs to be done to achieve this level Considerations	**What needs to be done to achieve this level** Considerations	**What needs to be done to achieve this level** Considerations	**What needs to be done to achieve this level** Considerations
	Indicators of accomplishment Considerations	**Indicators of accomplishment** Considerations	**Indicators of accomplishment** Considerations	**Indicators of accomplishment** Considerations

Table 4-1: SMM Table Template

4.1 EXTENSIBILITY

The SMM can be extended in several ways. The scope of each practice can be extended by *industry*, *system*, or both. In addition, over time, the model may be extended with the addition of new subdomains and practices.

4.2 Extending the Practices

The SMM is designed to be extensible across a wide array of industries and systems. It addresses the general scope, which looks at common security maturity best practices in the industry. There is an opportunity to add industry-specific and system-specific scope to any or all of the practices.

The IIC will collaborate with a wide range of industry groups to encourage development of profiles—practice tables that go beyond general scope and include industry- and system-specific requirements for different comprehensiveness levels. For example, a retail group may create profiles of some or all practices that include best practices and regulatory requirements specific to the retail industry; they may also create system specific profiles for commonly used devices such as card readers or security cameras. A health care profile may include specific guidance related to *HIPAA*, while a system-specific profile could address considerations for, say, *FDA* pre- and post-market guidance for implanted medical devices.

Industry and system profiles need not be created for every practice in the model. An industry may decide that the general scope is sufficient for most of the governance-related practices but that a few of the enablement practices necessitate an industry-level point of view.

When extending for industry or system-specific considerations, the practice table as seen in Table 4-2, expands to include two additional rows.

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	<List of Level 1 industry specific considerations>	<List of Level 2 industry specific considerations>	<List of Level 3 industry specific considerations>	<List of Level 4 industry specific considerations>
System-specific considerations	<List of Level 1 system specific considerations>	<List of Level 2 system specific considerations>	<List of Level 3 system specific considerations>	<List of Level 4 system specific considerations>

Table 4-2: SMM Table Template with industry and system specific considerations

Industry-specific considerations include the sector-specific issues, particularly components and processes that are prone to certain types of attacks, known vulnerabilities, incidents that took place in similar systems and possible harm to this kind of operational technology as well as sector specific priorities including legal and regulatory guidance.

When there are considerations to note, cells for industry-specific considerations at a given level contain the following:

- industry-specific security needs (e.g. facilitating safety, keeping continuous execution),
- accepted and recommended approaches to the practice implementation,

- known constraints and
- what needs to be done to achieve the specific level and the indicators for accomplishment for that level.

While the general row in the table included headings for achieving the level and indicators of accomplishment, the industry row should include a general description of the industry-specific issues as noted above and for a comprehensiveness level with industry-specific considerations:

- what needs to be done to achieve that level and
- relevant industry guidelines for that level.

System-specific considerations include the specific security-relevant business needs and risks for the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios that combine the general and domain-specific objectives in a unique manner.

When there are considerations to note, cells for system-specific considerations at a given level contain the following:

- system description including context such as the relationship to other parts of the system and the connected industries,
- system-specific security needs (e.g. facilitating safety, keeping continuous execution),
- recommended approaches to the practice implementation,
- known constraints and
- what needs to be done to achieve the specific level and the indicators of accomplishments for that level.

Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture systems’ target security maturity and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

Table 4-3 is an example of a partially filled-in compliance practice using the above template for the industry and device scope.

Compliance Management				
This practice is necessary when strict requirements for compliance with evolving security standards is needed.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	*See main table.*			
General Considerations	*See main table.*			
Industry Scope Considerations		**What needs to be done to achieve this level** Ensure compliance with Internal privacy and data security requirements for the business. **Indicators of achievement** Internal privacy and data security compliance are integrated as part of overall compliance program.	**What needs to be done to achieve this level** Consider regulatory guidelines relevant to retailers including: Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS, 2010), and the PIN Transaction Security Devices (PTS, 2010). …	
Device Scope Considerations			Ensure compliance with PIN Transaction Security Devices (PTS, 2010) … **Indicators of achievement** Complete set of documents verifying and assuring compliance with security-related requirements. …	

Table 4-3: SMM Practice Table Example

Over time, the model may evolve via the addition of new subdomains and practices. This enables the model to maintain relevance as new security and IoT disciplines emerge. Such extensions may be added to future iterations of the model.

5 Process for Applying the Model

Figure 5-1 displays a typical SMM Process. We expect most organizations to first establish a maturity target. Business level stakeholders define the target using some form of a business objectives questionnaire. Technical level stakeholders take such objectives and translate them into more detailed security requirements based on their understanding of the system. Once a target has been created or a relevant industry profile identified, organizations would conduct an assessment to capture the current maturity state. The *security maturity* of the target state and current state can be compared to identify gaps and opportunities for improvement. Based on the gap analysis, business and technical stakeholders can establish a roadmap, take actions, and measure the progress. After implementing enhancements, organizations can perform another assessment. The cycle repeats to ensure that the appropriate security target is always maintained in an ever-changing threat landscape. This includes for example, a world where attacks that are initially difficult to mount and require high skill later can become easier be widely deployed because of the dissemination of toolkits and information.

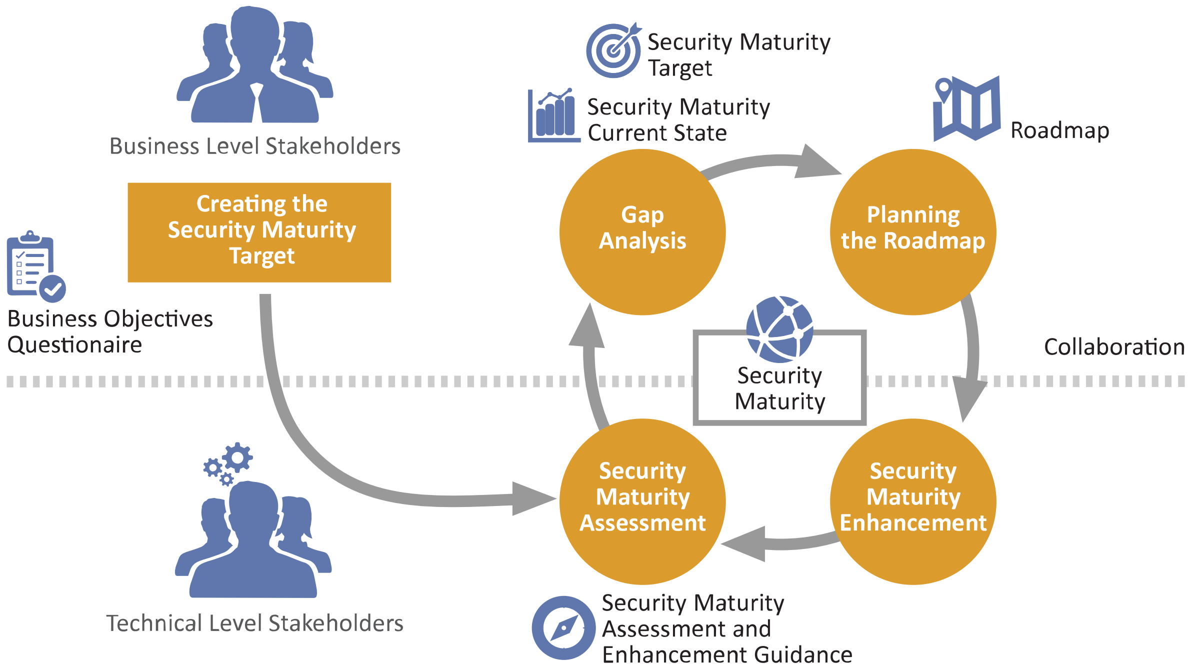

Business Level Stakeholders
Creating the Security Maturity Target
Business Objectives Questionaire
Technical Level Stakeholders
Security Maturity Target
Security Maturity Current State
Roadmap
Gap Analysis
Planning the Roadmap
Security Maturity
Collaboration
Security Maturity Assessment
Security Maturity Enhancement
Security Maturity Assessment and Enhancement Guidance

Figure 5-1: IoT Security Maturity Model Process

5.1 Establishing the Context

Before creating a maturity target or conducting a maturity assessment it is important to establish the context for the activity. First, there is a need to identify if the assessment addresses a complete end-to-end system, or a subsystem such as the cloud or edge, or a gateway device? Is the organization being assessed a solution provider, an end user or is it a vendor of a device or an IoT platform? Depending on the context it is possible that some of the practices may not be relevant and should be marked as *Not Applicable*.

5.2 Creating the Security Maturity Target

The security maturity target establishes the initial target security maturity state for a system. The target includes a consistent set of security practices, providing all stakeholders an understanding of the general security goals and the purpose of each security practice. The job of establishing the security maturity target falls to business stakeholders, and it should be carried out prior to any investment in enhancing security.

Once the security maturity target is available, it may be used in subsequent applications of the SMM, to create a target profile or evaluate a current maturity state assessment.

For a specific type of organization or system, it is useful to have a specific profile named a security maturity target profile. 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 scenarios is a subject for further development.

Most devices, networks and systems do not require the highest comprehensiveness and scope levels for every security domain, subdomain or practice. A system's security maturity target is defined as the set of all desirable values of comprehensiveness and scope for every security maturity domain, subdomain and practice.

The security maturity target is defined when referring to the comprehensiveness and scope for security maturity practices as seen in Table 4-3 (the SMM Table Practice Example, page 19). Each practice table has four columns, one for each comprehensiveness level. The objective in each level describes the general considerations that should be met. Guidance is provided in the form of general considerations.

How to create the security maturity target is described in the following three sections.

5.3 Determining the Comprehensiveness Levels

There are several steps to determine the comprehensiveness level as described below.

Establish the goal for each security domain—governance, enablement and hardening—according to the global vision of its role in the targeted maturity state. Define goals for each domain based on the overall goal. The goal chosen from this set determines the minimum comprehensiveness and scope levels for the whole domain. Security maturity sub-domains and practices considered within the domain will inherit these levels at this step. This first step provides a rough definition of the security maturity target.

The *Comprehensiveness Level Definition Guide*, Section 10, page 77 of this document lists comprehensiveness levels for domain goals.

It is possible to obtain the rough security maturity target by inheriting comprehensiveness and scope levels at the next tiers of the SMM hierarchy so that:

- the subdomains get the same comprehensiveness levels as the upper domains and
- the practices get the same comprehensiveness levels as the upper subdomains.

To get a detailed security maturity target, consider the established levels for domains as the base level for subdomains.

Then *consider the needs* covered by the security maturity subdomains in each domain. These include threats and continuous changes of threat landscape, compliance needs, and requirements from regulatory authorities. The prior step provided the initial comprehensiveness and scope levels for the domain. This step specifies whether there are specific security-related needs that require attention beyond the established baseline.

The *Comprehensiveness Level Definition Guide*, Section 10, page 77 of this document lists comprehensiveness levels for domain goals.

It is possible to stop here and obtain the security maturity target by inheriting practice comprehensiveness and scope levels from the subdomains.

To get the detailed security maturity target, consider the established levels for applying the initial levels of subdomains as the base level for their practices. If the practice level is changed to a higher or lower value this may impact the value of the subdomain level. A "+" value may be placed next to the subdomain level to indicate that further examination of the practice level values is warranted to understand the change. Please see Section 5.5, page 24, *Checking the consistency of the security maturity target* for further information.

Then *clarify the purpose* of every security practice within the subdomain. As subdomain prioritization emphasizes specific security needs, practice prioritization clarifies how the practices address these needs. Some practices may be entirely applicable and some only partially. Target comprehensiveness and scope levels for each practice reflect the level of assurance in covering subdomain needs.

This step considers the comprehensiveness and scope needed to implement security capabilities, thus providing a greater level of detail to the security maturity target. A detailed summary of typical practice purpose definitions corresponding to comprehensiveness levels is provided in the *Comprehensiveness Level Definition Guide* (Section 10, page 77).

5.4 DETERMINING THE SCOPE

To determine the scope for all practices, complete the following steps.

Check whether each security domain has specific requirements across the industry. If so, assign the industry-specific level to the domain and underlying subdomains and practices. Describe the industry-specific requirements for the domain, their source and how they apply.

Then check whether each security domain has specific requirements across several industries or only for the system. If so, assign the system-specific level to the domain and underlying subdomains and practices appropriately. Describe the system-specific requirements for the domain, their source and how they apply.

For each subdomain, if no changes were made for the parent domain, check whether the subdomain has specific requirements across the industry. If so, assign the industry-specific level to the subdomain and underlying practices. Describe the industry-specific requirements for the subdomain, their source and how they apply.

Otherwise, specify the industry-specific requirements for all subdomains, the source of these requirements and how they apply.

For each subdomain, if no changes were made for the parent domain, check whether the subdomain has the specific requirements across several industries or only for the system. If so, assign the system-specific level to the subdomain and underlying practices. Describe the system-specific requirements for the subdomain, their source and how they apply.

Otherwise, specify the system-specific requirements for all subdomains, the source of these requirements and how they apply. If the subdomains scope is changed to a higher or lower value this may impact the value of the domain scope. A "+" value may be placed next to the domain scope to indicate that further examination of the subdomain scope value is warranted to understand the change. Please see Section 5.5, page 24, *Checking the consistency of the security maturity target* for further information.

Then, for every practice, if no changes were made for the parent subdomain, check whether the practice has specific implementation across the industry. If so, assign the industry-specific level to the practice. Describe the industry-specific requirements for this practice implementation, their source and how they apply.

Otherwise, specify the industry-specific requirements for the practice implementation, the source of these requirements and how they apply.

Then for every practice, if no changes were made for the parent subdomain, check whether the practice implementation poses the specific requirements across several industries or only for the system. If so, assign the system-specific level to the practice. Describe the *system-specific* requirements for this practice implementation, their source and how they apply.

Otherwise, specify the system-specific requirements for the practice implementation, the source of these requirements and how they apply. If the practice scope is changed to a higher or lower value this may impact the value of the subdomain scope. A "+" value may be placed next to the subdomain scope to indicate that further examination of the practice scope value is warranted to understand the change. Please see Section 5.5, page 24, *Checking the consistency of the security maturity target* for further information.

5.5 Checking for Consistency of the Security Maturity Target

As the security maturity model defines a hierarchy for the security practices, facilitating the clear and logical representation of priorities for these practices, the security maturity target should be validated for its consistency against the model. If the target is inconsistent, enhancement will face challenges in prioritization and road-mapping.

Validation comprises the following checks:

Validate the subdomains and practices against the actual needs and purpose definitions. Perform this check in cases where the comprehensiveness and scope levels are assigned to subdomains and practices according to the levels of upper domains or subdomains. The stakeholders put the goals, needs and purpose definitions describing the organization's target security state and review them, applying changes where needed. For every change, consider whether the change corresponds to the same level, or whether to increase the level for this subdomain or practice. The level may be decreased along with the consistency checks outlined below.

Check for the consistency of target comprehensiveness definition. Any defined comprehensiveness level for the subdomain must be equal to or greater than the level set for the upper domain. Any defined comprehensiveness level for the practice must be equal to or greater than then level set for the upper subdomain. If the check is not passed, decrease the level of the upper domain or subdomain appropriately. The levels of underlying subdomains and practices keep their values.

Check for the consistency of target scope definition. Any defined scope for the subdomain must be equal to or more specific than the level set for the upper domain. Any defined scope for the practice must be equal to or more specific than level set for the upper subdomain. If the check is not passed, decrease the level of the upper domain or subdomain appropriately. The levels of underlying subdomains and practices keep their values.

If a subdomain comprehensiveness is determined to be at a higher level than its inherited value, then the domain has achieved the originally set base level "+". (The "+" indicates that a change has occurred from the original inherited value and is different than the domain base value.) The domain does not move to a higher level unless all its subdomains are marked at a higher level. If any element of the subdomain fails to meet the higher level, then it is deemed to be at the lower level and the domain itself is reduced and considered a lower level with the "+" identifier. If all the subdomains are at the same lower level, the domain must also be reduced to the lower level to maintain consistency.

If a subdomain scope is determined to be at a higher level than its inherited value, then the domain is considered to have achieved the originally set base level "+" (for example, Industry+ or System+). The domain only moves to a higher level when all its subdomains are marked at a higher level. If the subdomain is deemed to be at a lower level, the domain must be reduced and considered a lower level "+". If all the subdomains are at the same lower level, the domain must also be reduced to the lower level to maintain consistency.

If a practice comprehensiveness is determined to be at a higher level than its inherited value, then the subdomain is considered to have achieved the originally set base level marked with the indicator of “+” to alert to a change. The subdomain does not move to a higher level unless all its practices are marked at a higher level. If the practice is deemed to be at a lower level, the subdomain must be reduced and considered a lower level “+”. If all the practices are at the same lower level, the subdomain must also be reduced to the lower level to maintain consistency. In the example in Figure 5-2, the subdomain is initially set to a 2 and its practices inherit the 2. Upon analysis, it is determined that one practice is a 1 and another is a 3. The subdomain must then be reduced to match the lowest level 1 but can be described as a 1+.

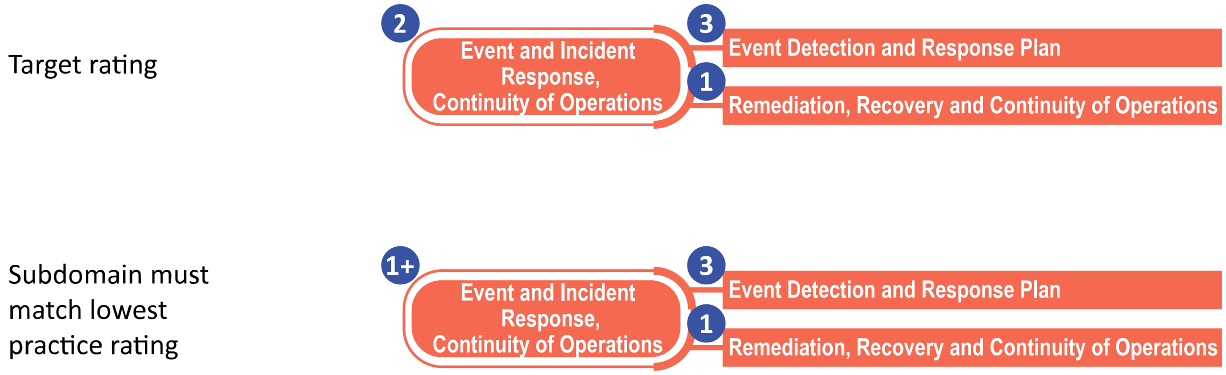

Target rating
2
Event and Incident Response, Continuity of Operations
3
Event Detection and Response Plan
1
Remediation, Recovery and Continuity of Operations
Subdomain must match lowest practice rating
1+
Event and Incident Response, Continuity of Operations
3
Event Detection and Response Plan
1
Remediation, Recovery and Continuity of Operations

Figure 5-2: Subdomain Consistency Check, reducing Subdomain value

If at some point all the practices match a higher level, as shown in Figure 5-3 then the subdomain value may be increased to match that of the practices.

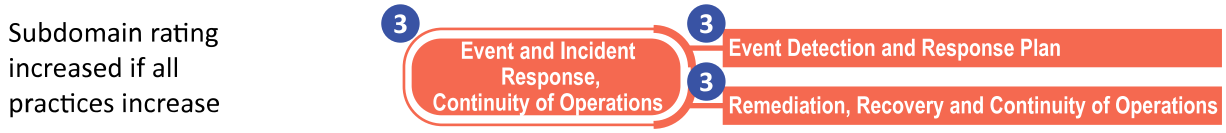

Subdomain rating increased if all practices increase
3
Event and Incident Response, Continuity of Operations
3
Event Detection and Response Plan
3
Remediation, Recovery and Continuity of Operations

Figure 5-3: Subdomain Consistency Check, increasing Subdomain value

If a practice scope is determined to be at a higher level than its inherited value, then the subdomain is considered to have achieved the originally set base level “+”. The subdomain moves to a higher level when all its practices are marked at a higher level. If the practice is deemed to be at a lower level, the subdomain must be reduced also and considered a lower level “+”. If all the practices are at the same lower level, the subdomain must also be reduced to the lower level to maintain consistency.

The consistency check must flow through the hierarchy to determine if changes at the subdomain level have affected the values of the domains above them. It is not valid, however, to average the levels at the higher level as such mathematical calculations are meaningless and do not provide sufficient insight as the meaning of the value. One must follow the “+” indicator and view the next level down in the hierarchy to determine what changed.

6 CONDUCTING A SECURITY MATURITY ASSESSMENT

A documented summary of fully or partially implemented security capabilities facilitates establishing a roadmap for maturity enhancements. The *current security maturity state* is the current maturity state of implemented security practices for the given system in a similar format to the security maturity target. Typically, a security assessment evaluates each security practice by auditing controls through evaluating controls' effectiveness through technical testing or penetration testing. We may then compare it against the target state so as to identify gaps and produce a roadmap to achieve target state.

To determine the current security state:

Determine the coverage of the assessment: Options include the entire organization, only selected parts of the organization, or only specific security practices. For each of the security practices that will be assessed, which stakeholders should be included, and which implemented controls should be evaluated? If a stakeholder cannot be included or a specific control cannot be evaluated in a reasonable time (for example, a supplier in another country), are there other avenues by which their security could be evaluated?

Determine assessment method: The next step is to determine a method for the assessment. Considerations include:

- Will the review be conducted by an in-house team or a third party?
- Will the testing method include policy reviews, interviews, audit, and penetration testing?
- What framework will be used to enumerate and evaluate possible controls?

Testing that focuses on evaluating the true effectiveness of controls provides a more accurate picture of security, but also tends to be more time consuming. The expertise required may also not exist in house.

Stakeholder preparation: Preparation increases the likelihood that the assessment can be completed in a reasonable time and that its final results are accurate. You should:

- identify stakeholders and points of contact and obtain business stakeholder buy-in,
- socialize the assessment and its goals with those stakeholders not involved in its planning,
- schedule interviews with the relevant stakeholders for the assessment team,
- gather relevant policies, documentation, contracts, previous assessment reports, etc. and
- prepare any accesses required for penetration testing, such as things like network access, and domain credentials.

Assessment: After preparation, the team should review the implemented security practices.

Reporting: The assessment team should document their findings in a formal report to business decision makers and other relevant stakeholders. It should interpret the team's findings through the lens of the organization's specific industry and business profile. It should address each security practice and its relevant controls and a low level of detail, so it is useful for reaching the target. It may include a system for scoring or measuring each control and practice, to provide the organization with metrics for relative prioritization, change over time, and other comparisons.

6.1 ACHIEVING A LEVEL

The organization meets a comprehensiveness level when it meets all the indicators of that level.

Transitioning between comprehensiveness levels is contingent upon clearly documenting the characteristics and requirements of the given level. Clarifying this information is necessary due to the variability in how the level is defined for different scenarios:

- For the minimal comprehensiveness level, define the practice implementation goals and the appropriate minimal measures.
- For the ad hoc comprehensiveness level, describe the use cases and baseline measures required for their support.
- For the consistent comprehensiveness level, document the recognized best practices, standards, regulations, and supporting tools where applicable.
- For the formalized comprehensiveness level, document the supporting process definition.

The transitions between the scope levels are determined by the sector specific issues and *system-specific* needs and risks identified during the security maturity target definition.

Therefore, before the security maturity assessment (and as a part of this assessment) the stakeholders must agree on the exact definitions of the comprehensiveness and scope levels, corresponding to the current guide, as shown on the Figure 6-1.

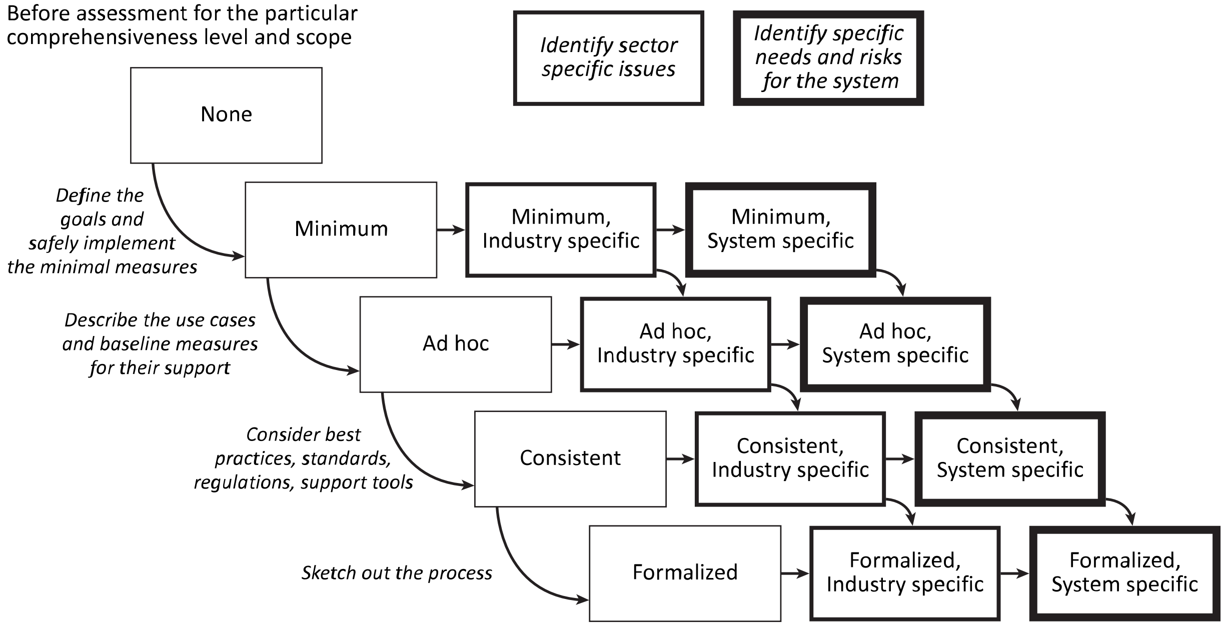

Before assessment for the particular comprehensiveness level and scope
Identify sector specific issues
Identify specific needs and risks for the system
None
Define the goals and safely implement the minimal measures
Minimum
Minimum, Industry specific
Minimum, System specific
Describe the use cases and baseline measures for their support
Ad hoc
Ad hoc, Industry specific
Ad hoc, System specific
Consider best practices, standards, regulations, support tools
Consistent
Consistent, Industry specific
Consistent, System specific
Sketch out the process
Formalized
Formalized, Industry specific
Formalized, System specific

Figure 6-1: States and transitions between the comprehensiveness and scope levels for security practices

Some organizations will need to demonstrate some, but not all, of the required items of a higher level. For example, if an organization has met all conditions for Level 2 but only some for Level 3, they can be considered a Level 2+; but they need to meet all the conditions of Level 3 before they can be considered a Level 3. Similarly, if an organization has met all items of a Level 1, 90% of Level 2 and some of Level 3, they would be recognized as a Level 1+.

At the practice level, it may be useful to describe how close an organization is to achieving the next level, and stakeholders will need to know the amount of investment to reach it. In such cases the assessment provider may use numbers such as "2.1" or "2.8" to describe the findings. Different mechanisms may be required as the context may be different in each case. A "2.8" may be meaningful in describing having reached 80% or most of the indicators of level 3, but not when there are 40% at level 3 and 10% at level 4, for example.

Unlike the target levels, which are set and can be inherited, the current-state assessment is performed bottom up by evaluating the practices in detail. A subdomain is identified by the lowest level of its practices. If the practices have different levels, the subdomain is identified as the lowest level "+" to indicate that the practices should be viewed to understand the context. The subdomain does not move to a higher level unless all its practices are marked at a higher level. In the case of comprehensiveness, this may be designated as Level 2+, if some practices are above Level 2, and in the case of scope, as "industry+", if some of the scopes are at the system scope level. It is not valid to average the practice levels at the subdomain level, nor is it clear unless the practices are explored if a subdomain level of a 2+ represents one practice of a 2 and another as a 3, a 2 and a 4, or a 3 and 2.

Once the values are set for the subdomains, a similar summary and check can be performed at the domain level. If the subdomains have different comprehensiveness levels, then the domain is identified as the lowest subdomain comprehensiveness level with a "+" added to indicate that the subdomains and practices should be viewed to understand the context. The domain does not move to a higher level unless all its subdomains are marked at a higher level. In the case of comprehensiveness, this may be designated as Level 2+ if some subdomains are above Level 2, and in the case of scope, as "Industry+", if some of the scopes are at the system scope level. Similarly to the practice values at the subdomain level, it is not valid to average the subdomains levels at the domain level, nor is it possible to understand the values unless the practices are explored.

6.2 Performing Gap Analysis

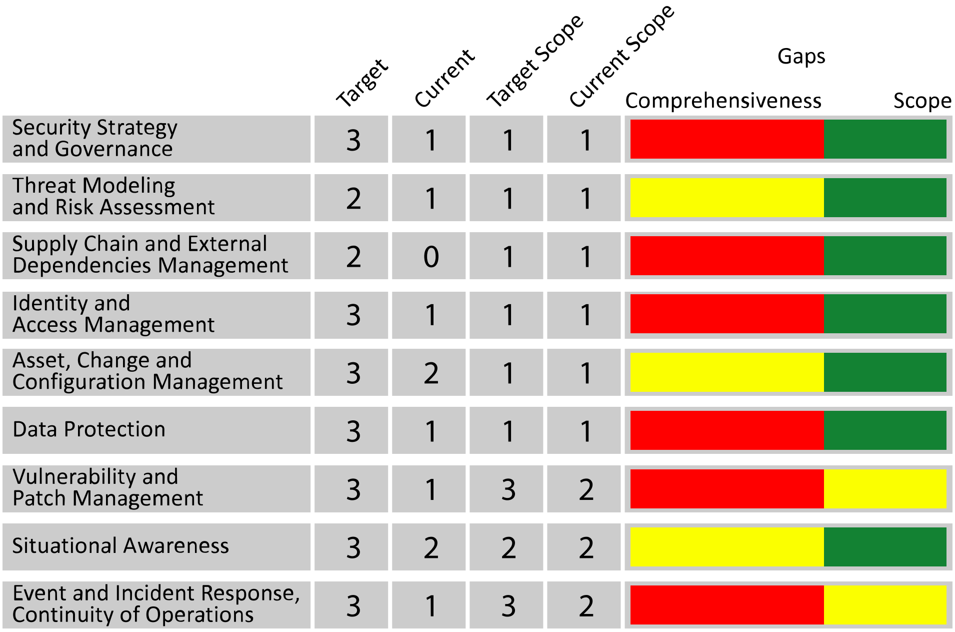
With the target state and current state in hand, the organization can perform a gap analysis to identify appropriate areas for security improvements and investment. For those controls where there is a difference between the two states, note the size of the gap to assist with prioritizing in the roadmap. Also note any situations in which a specific control may be short of the target state, but the potential ensuing risk is mitigated by another control. This process should yield a list of security controls that are short of target state, the gap between current and target state for those controls, and notes of any controls where the risk might be mitigated through other means.

Based on the comparison between target and current states, business and technical stakeholders can measure the progress and negotiate the steps for security maturity enhancement. Three possible visualizations for gap analysis are shown in Figure 6-2, Figure 6-3 and Figure 6-4. Figure 6-2 shows a heat map based on the levels of the target and current comprehensiveness and scope. The heat map displays the gaps for each, where red indicates a large gap, yellow a small gap and green as no gap.

Figure 6-3 uses a bar chart to compare comprehensiveness levels between the target and current state, with the differences between the bars showing the gap. Shading can be used to display and compare the scope (in this example, *general* scope is an empty bar, industry scope is a patterned bar, and system scope is a filled bar).

The third visualization in Figure 6-4 is a radar or spider chart showing the current and target comprehensiveness states, with the difference between the levels representing the gap. In this chart, the symbols are used to visualize the scope, with different symbols for the *general*, *industry* and *system* scopes. Where the symbols do not match between current and target, this indicates a gap in scope levels.

Gaps in the maturity are determined by gaps in the comprehensiveness and scope. If gaps exist for a particular practice, the maturity for that practice is lower than desired and needs to be improved. If no gaps exist (score is even, or current state is higher than the target) then the maturity of the organization is sufficient or ahead of the need.



	Target	Current	Target Scope	Current Scope	Gaps	
					Comprehensiveness	Scope
Security Strategy and Governance	3	1	1	1	🟥	🟩
Threat Modeling and Risk Assessment	2	1	1	1	🟨	🟩
Supply Chain and External Dependencies Management	2	0	1	1	🟥	🟩
Identity and Access Management	3	1	1	1	🟥	🟩
Asset, Change and Configuration Management	3	2	1	1	🟨	🟩
Data Protection	3	1	1	1	🟥	🟩
Vulnerability and Patch Management	3	1	3	2	🟥	🟨
Situational Awareness	3	2	2	2	🟨	🟩
Event and Incident Response, Continuity of Operations	3	1	3	2	🟥	🟨

Figure 6-2: Gap Analysis for Security Maturity Target

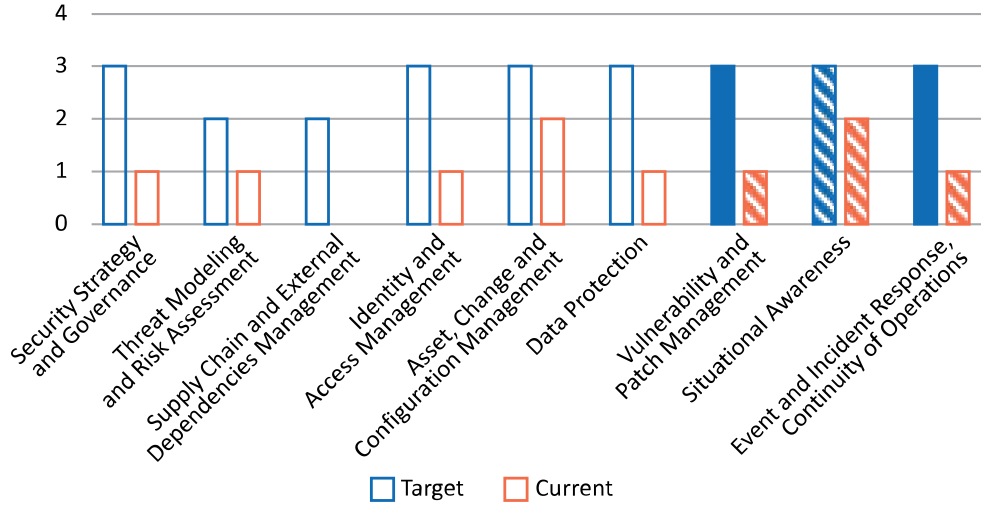


Figure 6-3: Gap Analysis for Security Maturity Target

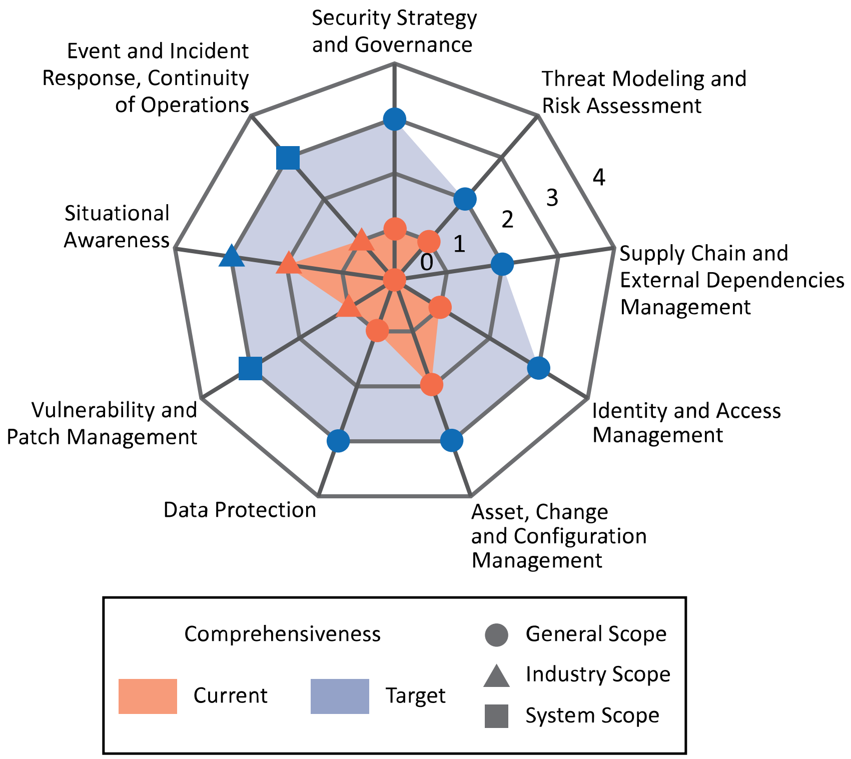


Figure 6-4: Gap Analysis for Security Maturity Target

As discussed in Section 6.1, page 28, in some instances it may be desirable to indicate how close an organization is to closing the gaps. In that case the values need to represent values between the levels and not just the levels themselves. For example, a "2.1" may be used to show a large gap from level 3, while a "2.8" may be used to indicate a small gap. As the size of the gap depends on the assessment and context, it is up to the assessment provider to determine how best to display the data.

6.3 Planning the Roadmap

Next, use the results of the gap analysis to build a roadmap for future security improvements. The roadmap prioritizes the activities according to the identified gaps, major business and security needs and concerns, available resources and expertise and accepted business practices.

Security maturity can be enhanced by improving the comprehensiveness and by shifting the scope. If one of these dimensions doesn't need to improve, the steps for improving the other one may be planned and executed. If both comprehensiveness and scope need to improve, the stakeholders should consider the comparative importance of comprehensiveness and scope for that practice, and the possibility of improving one before another (see Table 4-2, page 19).

Then for each practice where the *current state was short of target*:

- identify where the comprehensiveness should be improved immediately due to safety, regulatory, legal, ethical, or contractual obligations,
- identify where the scope should be improved immediately for similar reasons,
- identify which remediations would yield the target state. Use best practice guides to identify the most effective control improvements and
- prioritize the remediation according to safety, regulatory, legal, ethical, or contractual obligations.

For each *potential remediation*, identify its cost in money and organizational resources. Clarify the effect of the remediation and what resulting security improvements would occur.

Develop a roadmap for security improvement. The roadmap should prioritize remediations that would satisfy legal or regulatory requirements and those that would result in the most improvement at lowest cost. Other considerations when developing the roadmap include:

- possible dependencies between security controls. i.e., situations in which a change to Control A would not lead to an improvement until an improvement is made in Control B,
- improvements that may affect multiple controls,
- time and resources required to implement each remediation and
- time and resources required before an implemented change is fully effective.

Then *establish* ownership, milestones, and deadlines for each remediation item.

The gap analysis helps the organization develop a roadmap to improve its security posture and maturity. Understanding the gaps informs the organization as to the relative priority of different security requirements and controls. The model identifies the conditions needed to achieve a certain level of comprehensiveness and scope.

6.4 Making Security Enhancements

Organizations can leverage best practices, such as those being defined by the IIC, to apply specific controls and processes to help them move to a target maturity state. An example is the Data Protection Best Practices [IIC-DPBP2019] guidance.

The organization should execute the roadmap, enacting the identified remediations to drive the organization towards its target state. The improvement process is more effective with senior executive sponsorship, so consider implementing a stakeholder steering committee to meet regularly and track progress. This ensures accountability and can implement course corrections, in the event improvements do not go according to plan.

6.5 Continuous Improvements

Figure 5-1 showed the *IoT Security Maturity Model Process.* A persistent mature system security state is only achievable via continued security assessments and improvements, orchestrated over time. Consequently, we iterate over a Plan-Do-Check-Act cycle (Act, in this case, means accepting a new baseline if the check on the result of the improvement step is successful). The cycle begins by establishing the target for security maturity for a specific system. Then an iterative high-level process of security maturity improvement begins, as shown in Figure 6-5. The pace of change in security threats and approaches to mitigate them determine how frequently to execute the cycle.

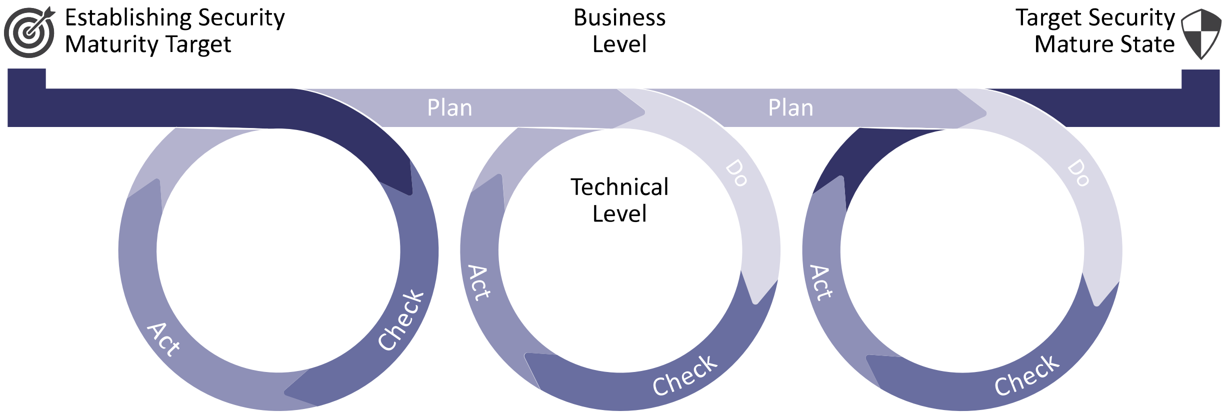

Establishing Security Maturity Target
Business Level
Target Security Mature State
Plan
Plan
Technical Level
Do
Do
Act
Check
Act
Check
Act
Check

Figure 6-5: SMM Improvement Cycle

6.6 Subsystems

The SMM can apply to an entire solution or to its components. In some cases, an organization manages the entire solution and can evaluate the solution using a single set of tables. In other cases, such as an organization that manages its infrastructure at the edge but uses a third-party communications network and a third-party cloud, the organization may wish to create a separate set of SMM tables for each subsystem. The cloud provider may employ highly mature processes for managing its infrastructure, including staff background checks, physical security, and patch management processes. In this case, the SMM may indicate that the current comprehensiveness for patch management is level 4. Conducting a separate assessment of devices at the edge, which may be unprotected in the field, may indicate the current comprehensiveness for patch management is level 2.

If targets are set differently for different subsystem, evaluate whether the differences introduce additional risks into the overall system. Depending on the scenario, a level 2 at the edge may indicate a deficiency that can pose additional risk into the cloud. However, for some scenarios, the difference may be acceptable.

Consider attacks from insiders or attackers using insider credentials in your strategy. Segmentation alone may not remove insider attack risks and can provide a false sense of security, so consider the impact of insider attacks on a system with multiple segments. One example is obtaining information from one segment (e.g., the cloud) and using that information to attack another segment (e.g., an enterprise system). Another is changing data in one segment to sabotage operations elsewhere. A third example is compromising a privileged user with accounts on multiple segments.

Part II: The Core of The Security Maturity Model

This part presents the core of the SMM in a set of practice tables grouped by domain (governance, enablement, and hardening) and subdomains. Each table corresponds to a SMM practice and describes the general scope considerations for each defined comprehensiveness level.

Following each table is an example, using various industry use cases, to demonstrate how an organization might use the table to pick a target state or to evaluate its current state.

7 Governance Domain

Governance policy and management of its implementation influences and informs all decisions related to security, including the prioritization of practices. This section outlines subdomains directly related to governance including strategy, threat modeling and risk assessment, and lastly supply chain and external dependencies management. All of these subdomains determine the security posture of the organization and the policies related to other parties and the external environment.

7.1 Strategy and Governance Subdomain

Security strategy and governance supports organizational strategy as well as providing security and compliance with regulations, laws and contractual obligations. It also supports reputation protection and running the core business.

7.1.1 Security Program Management Practice

Security Program Management				
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Describe general security provisions.	Create a security program aligned with organizational structure and systems.	Align the security program with appropriate widely recognized security standards.	Manage security program over time: Implement clear planning, timely provision and control of security activities with periodic assessments.
General considerations	This level represents a basic understanding of security concerns and the desire to document them.	This level represents acting based on the desired plan and creating the appropriate organization.	This level represents awareness of external standards and regulations and incorporates them	This level provides for continuous improvement and management over time.

Security Program Management *(cont. from page 35)*				
			into the management practices.	
	What needs to be done to achieve this level Document the internal and external issues relevant to security management. Identify security management structure, measures, responsibilities, and methods to communicate this information to personnel. Coordinate and align roles and responsibilities including expertise in devices, networks and IoT infrastructure with internal roles and external partners.	**What needs to be done to achieve this level** Identify and document systems, networks, and processes to be managed to address the security issues. Plan the resources for security management, communication, training and awareness. Create skill centers for the identified roles. Business stakeholders support security initiatives and understand their roles and responsibilities. OT stakeholders provide operational viewpoint.	**What needs to be done to achieve this level** Align the security program with appropriate standards to meet regulatory requirements or to achieve consistency across the organization, including subsidiaries. Incorporate understanding of standards into security management, communication, training and awareness programs. Integrate teams across skill centers. Perform critical infrastructure and sector-specific (IT and OT) risk analysis to inform the organization’s determination of risk tolerance. Ensure that third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	**What needs to be done to achieve this level** Achieve situational awareness by tracking threats, regulatory requirements and evolving technologies over time. Set the timeframes for periodic reviews and updates of measures, plan the efforts and resources. Conduct periodic training and awareness-building and testing activities. Scale integrated teams by creating an IoT center of excellence and adjust teams for proof of concept, pilot, system scaling, and production phases.
	Indicators of accomplishment Documents covering general goals, interested parties, priorities and scope of security management, awareness measures.	**Indicators of accomplishment** Accepted information security program and policy. Documents covering resources including systems, processes,	**Indicators of accomplishment** Established communications between the stakeholders and external authorities.	**Indicators of accomplishment** Documented plan and process for periodic review and assessment of the security management program.

Security Program Management *(cont. from page 35)*				
	A dedicated staff with defined responsibilities for security.	devices, and networks, required budget, and the division of responsibilities.	Assessment reports demonstrating conformance of security management practices to the relevant standards Integrated teams have been established.	Established and documented mechanisms for ongoing situational awareness related to threats. Established and maintained assurance program roadmap supported by all interested parties.

Table 7-1: Security Program Management

Example

A mid-size manufacturing plant determines that its security program needs to be aligned with the [IEC-62443-21] industry standard, so it sets a maturity target for security program management at comprehensiveness level 3: *consistent*. The current state assessment indicates that its security program structure does not follow the standard and relies on existing internal organizational structure. The current state comprehensiveness for security program management is level 2, *ad hoc*.

7.1.2 Compliance Management Practice

Compliance Management				
This practice is necessary when strict requirements for compliance with evolving security standards is needed.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Create organizational awareness of the need for compliance.	Analyze and understand compliance requirements for implementation.	Ensure implementation meets obligatory compliance requirements and audit leads to certification.	Manage compliance with systematic techniques including automation and well-established assessment process.
General considerations	At this level, the organization's adherence to compliance regimes is inconsistent.	At this level, the organization demonstrates an understanding of its compliance requirements and has the ability to perform assessments or choose to outsource them.	At this level, mandatory and regulatory requirements are incorporated.	At this level, a continuous process is established, and an automated solution is introduced.
	What needs to be done to achieve this level Identify and monitor the general security-related compliance drivers, including compliance with protocols, standards and consortia certification. Outsource all or most of the activities regarding keeping the system compliant to security standards.	**What needs to be done to achieve this level** Define a plan to meet external compliance requirements based on details research of relevant compliance regime. Check if the implemented practices accurately represent requirements and reconsider if they diverge. Perform the conformance and compliance assessment activities using an internal or outsourced team.	**What needs to be done to achieve this level** Perform the compliance audits and consider regulatory guidelines from the controlling authorities to align the systems, networks, edge node hardware, or processes with the appropriate requirements. Systematically, but independently, manage the compliance for IT, OT and IoT.	**What needs to be done to achieve this level** Proactively stay abreast of upcoming changes to compliance regimes and ensure adherence to those changes before they come into effect. Automate and conduct on a regular basis the collection, analysis, storing and retrieval of audit data. Keep the current and historic audit data per project centralized and allow access to approved individuals only. Establish a process for assessment for those requirements from the regulatory authorities

Compliance Management *(cont. from page 38)*				
				that do not allow automated checks by implementing the similar scheme of obtaining and storing the data. Consider IT, OT, and IoT holistically.
	Indicators of accomplishment Documented motivation and security-related compliance drivers. Informal compliance assessment results and identified gaps.	**Indicators of accomplishment** Approved requirements and allocated time and resources to ensure compliance. Detailed pass/fail results of these activities are delivered to project stakeholders for evaluation. A centralized program and plan containing a response statement for each requirement that captures the concept of what should be done to ensure the requirement is met or note why it does not apply.	**Indicators of accomplishment** Complete set of documents verifying and assuring compliance with security-related requirements. Valid certificates and other supporting evidence.	**Indicators of accomplishment** Policies and tools used to automate the processes surrounding the audit data lifecycle. The required data is accessible and not stove piped within separate parts of the organization. Established policy for the organization on contributing the input or comments into compliance regimes that effect it and may have personnel solely responsible for its compliance and risk programs.

Table 7-2: Compliance Management

Example

A large OEM in the automotive industry develops state-of-the-art components and technologies that must comply with safety and emerging security standards. The OEM needs to automate processes for compliance management and participate in the development of security recommendations for the new technologies. Therefore, it sets its maturity target for compliance at comprehensiveness level 4. Upon current state assessment the organization learns that while it is following the required procedures, they are being automated. The current state comprehensiveness for compliance management is level 3, *consistent*.

7.2 Threat Modeling and Risk Assessment Subdomain

The threat modeling and risk assessment subdomain identifies gaps in specific configurations, products, scenarios and technologies and prioritizes countermeasures accordingly.

7.2.1 Threat Modeling Practice

Threat Modeling				
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Consider general IT security issues as threats.	Perform vulnerability analysis to Identify threats. Address in an ad-hoc manner.	Describe and classify threats in an accurate (optionally formal) way.	Reveal and clearly describe IT, OT and IoT factors both known and specific that may put the system at risk.
General considerations	At this level, threats are only based on known typical IT security threats.	At this level, the organization performs vulnerability assessments to understand threats as they pertain to the organization. The organization can discern specific IT, OT and IoT threats.	At this level, accepted formal threat modeling methods are used, and automated tools are used for threat modeling.	At this level, threat modeling is built into business processes and driven by business goals and risk profile.
	What needs to be done to achieve this level Collect the available information about typical IT security vulnerabilities and incidents and recognize those which are relevant as threats.	**What needs to be done to achieve this level** Perform a vulnerability assessment for IT, OT, and IoT. (At this level, they are typically managed separately). Use the generally accepted vulnerability evaluation schemes (such as Common Vulnerability Scoring System or CVSS).	**What needs to be done to achieve this level** Describe the threats during the analysis using generally accepted classifications like CAPEC or OWASP Top10. Optionally use the tools to describe the architecture of the system to identify threats automatically and possible resolution. Address the IT, OT, and IoT-specific (for example, edge device	**What needs to be done to achieve this level** Validate the security threats against objectives set according to business needs. Base the threat model upon the set of clearly identified security assumptions about system environment (including physical security), trustworthiness constraints, and key actor’s behavior. IT, OT, and IoT threats are integrated.

Threat Modeling *(cont. from page 40)*				
			physical compromise) threats. Consider the results of threat modeling and risk assessments as a part of formal processes to address and prevent the identified concerns.	Organize the particular threats and attack vectors as a consistent hierarchical structure, including all identified security issues.
	Indicators of accomplishment Business-level documents mention general security threats, such as sensitive data disclosure, denial of service attacks, or infiltration with malware.	**Indicators of accomplishment** A vulnerability assessment report is available and identifies common and typical threats valid for the identified use cases.	**Indicators of accomplishment** Identified tools and documented methods for the threat assessment. An assessment report that consistently describes the classified threats, vulnerable technologies, exploitation method or attack pattern, level of risk and possible resolutions.	**Indicators of accomplishment** The accepted method for threat analysis and modeling comprising a part of the rhythm of the business, accounts for business goals and risk, and is performed consistently. The periodic assessment reports demonstrating threat analysis experience and lessons learned over time.

Table 7-3: Threat Modeling

Example

An automotive manufacturer considers possible threats for interfering with the operations of a vehicle key fob. They set their target maturity comprehensiveness level to 1 as they consider certain IT threats, such as a *DoS attack* that may prevent a key fob from operating and allowing the driver to open the door. Over time, new threats, such as an amplification of the vehicle proximity signal, emerge and the manufacturer needs to consider the possibility that a door can be opened when the key fob is far away. The manufacturer realizes they need to perform additional threat modeling and resets their target maturity comprehensiveness level from 1 to 2.

7.2.2 Risk Attitude Practice

Risk Attitude				
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Informally define risk notion at a high level.	Establish procedures for detailed risk assessment, differentiating the importance of risks.	Systematically measure and appropriately manage risks.	Integrate risk management with strategy.
General considerations	At this level, there is no formal approach to managing risk and it is only defined in general terms.	At this level, risk is better understood but managed in an ad-hoc manner.	At this level, risk is driven by business objectives and best practices and common methods are applied.	At this level, risk management is part of continuous processes and business cycles.
	What needs to be done to achieve this level Apply a general risk management approach for all types of information security risks, as well as other types of risks. Optionally, involve third parties to perform the risk analysis.	**What needs to be done to achieve this level** Apply a more detailed approach to risk analysis, assessment and concrete countermeasures. Multiple mitigations are applied to each threat. Countermeasures mitigate the consequences of a successful attack on any one vector. Consider external and internal issues that are relevant to the purpose of the system of interest and that affect its ability to achieve the intended outcomes. Consider risks related to outsourcing, third-party contractors or other partners in the supply chain. Consider devices at this level.	**What needs to be done to achieve this level** Systematically address IT, OT, and IoT. (At this level, they are typically managed separately). Identify, prioritize and analyze potential security threats, vulnerabilities, and consequences using accepted methods. Use methods that characterize risks quantitatively or qualitatively and structure as scenario based or asset based. Third parties are part of the process.	**What needs to be done to achieve this level** Establish a continuous process of risk management to include appropriate decisions based on identified risks. Establish the risk-management strategy and identify the harm and its likelihood of threats. Integrate IT, OT and IoT. Identify the alternative courses of action and responses, evaluate and determine if they are consistent with organizational risk tolerance.

Risk Attitude *(cont. from page 42)*				
		Enable procedures to address risks and ensure the system of interest can achieve its intended outcomes; prevent, or reduce, undesired effects; and achieve continual improvement. Consider IT, OT and IoT independently with a discrete coordination with third parties.		
	Indicators of accomplishment The definition of main risks that reflects their types, their priorities, how they connected to the various issues (business, regulatory compliance, security, safety, etc.) and how they may be connected to security threats. Consideration of common risks associated with traditional information (electronic or paper), classical IT systems and applications, business partners, joint ventures, outsourcing partners, and the like.	**Indicators of accomplishment** The approved, probably quantitative, scale for measuring risks. The description of case-based security-related risks associated with internal and external factors including their empirical quantitative rates according to the scale.	**Indicators of accomplishment** A risk assessment method applicable to IT-, OT- and IoT-related processes. Risk-handling strategy describing avoidance, mitigation, acceptance, and transference criteria with appropriate actions.	**Indicators of accomplishment** A roadmap for the periodic evaluation of risks, their types, their connections with both external and internal factors and their interconnections. The periodic reports to the business about newly identified risks and required changes to the risk handling strategy.

Table 7-4: Risk Attitude

Example

A restaurant supplier provides the technology for managing customer wait times using pagers provided at check in. The supplier does not consider the possible break in into such devices to be a high risk or a high impact event and sets their target maturity comprehensiveness level at 1. A third-party assessment confirms that the supplier solution and restaurant environment operate at this level.

7.3 Supply Chain and External Dependencies Management Subdomain

Supply chain and the external dependencies management subdomain aim at controlling and minimizing a system’s exposure to attacks from third parties that have privileged access and can conceal attacks.

7.3.1 Product Supply Chain Risk Management Practice

Product Supply Chain Risk Management				
This practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Establish integrity procedures for suppliers and their supplied components and monitor their accomplishment.	Implement analysis, contracts and methods for reviewing and protecting the supply chain.	Obtain certificates or other security assurance artifacts for essential components.	Codify the supply chain risk management policy and processes.
General considerations	At this level, basic direct measures for integrity control are applied.	At this level, analysis and methods are added to track measures and their effectiveness.	At this level, best practices are applied, and an assurance program enacted to track progress.	At this level, the approach is standardized across the supply chain.
	What needs to be done to achieve this level Implement common measures to reduce the risks posed by the supply chain agents and third parties. Such measures include at least tamper evidence protection during shipping and warehousing, physical access control of the personnel providing integration and maintenance, wiping	**What needs to be done to achieve this level** The analysis of certain supply chain threats is added and all-source intelligence analysis is used to tailor acquisition strategies, tools, and methods. Implement the methods for reviewing and protecting development plans, evidence, and documentation that are commensurate	**What needs to be done to achieve this level** Identify process-defined supply chains. Implement a set of methods to address supply-chain risk with respect to computer systems, networks and their components, and to educate the acquisition workforce on threats, risk and required security controls.	**What needs to be done to achieve this level** Implement a standardized process to address supply-chain risk with respect to information systems and system components, and to educate the acquisition workforce on supply-chain threats, risk, and required security controls. Use the acquisition and procurement processes early in the system

Product Supply Chain Risk Management *(cont. from page 44)*				
	memory and factory reset of the equipment before its disposal. Ensure the authenticity of supplier to validate that counterfeit or alternate components are not substituted en route. Consider the entire supply chain, beginning with measures at the chip manufacturer, and all the way to the cloud.	with the role of the appropriate system or component, its level of criticality and exposure to attacks. Apply the measures at each phase of the supply chain and contract separately. Identify the dependencies and critical functions for delivery of critical services. Consider provisioning solutions for independent components.	Consider an integrated end-to-end provisioning solution. Manage third-party vulnerabilities and risks by requiring them to be addressed by the third parties. Conduct random audits of suppliers to verify their compliance with contractual obligations.	development life cycle to provide an important vehicle to protect the supply chain. Ensure that a comprehensive verification process makes suppliers consistently adhere to security requirements. Anticipate third-party risks and create incident plans to handle potential situations and provide redundancy. Establish resilience requirements for third-party critical services for all operating states (e.g., normal operations, under attack, during recovery).
	Indicators of accomplishment Documents (separate or the part of security program) refer to the basic measures for integrity control of valuable components. Contracting for services and work covers the awareness and responsibilities for the basic integrity control measures.	**Indicators of accomplishment** Documents identifying the particular cases to be controlled at the contractual level. Contracts may specify the documentation protection requirements. Document templates for the identified typical cases (e.g., inspection checklists and return forms)	**Indicators of accomplishment** A document describing the supply chains relevant to the main business processes. Security-assurance requirements as certificates and other documents to be provided. Security assurance reports or certifications are available to demonstrate the appropriate measures taken for appropriate levels of supply-chain threats.	**Indicators of accomplishment** A roadmap for periodic evaluation of risks posed by the untrusted supply chain to rationalize the validity of assurance requirements and sponsor the appropriate certification incentives for suppliers (if needed).

Table 7-5: Product Supply Chain Risk Management

Example

A distributor of non-versatile wearable such as fitness bracelets determines that tamper-protection packaging is sufficient to ensure the device has not been compromised between the manufacturer and the point-of-sale. The distributor determines that comprehensiveness level 1 is sufficient as the target for this case.

7.3.2 Services Third-Party Dependencies Management Practice

Services Third-Party Dependencies Management				
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Monitor the reputation of contractors and establish basic contracts.	Provide quality of the services with service-level agreements and progress metrics in the contracts.	Obtain third-party evidence for the service quality.	Codify the trust management policy for contractors.
General considerations	At this level, basic agreements are established with third parties to ensure compliance with security requirements.	At this level, conformance to the agreements is tracked, and service-level agreements (SLAs), progress metrics (e.g. KPIs, etc.) are defined.	At this level, the SLAs, KPIs, etc. are tracked and reports provided.	At this level, an assessment is conducted to evaluate third parties against potential risks.
	What needs to be done to achieve this level Require all third-party agents including technology providers, partners, contractors and managed services to comply with the security requirements in accordance with established agreements.	**What needs to be done to achieve this level** Establish the contracts, business exchange agreements, and SLAs define KPIs and measurable outcomes and responses to noncompliance. The KPIS and SLAs for IT, OT, and IoT are separate. Requirements set by the regulating authorities are considered as obligatory.	**What needs to be done to achieve this level** Implement the defined agreements ranging from extensive control (contracts), to very limited control (acquire external services). Ensure the clear understanding of which level is acceptable for the system of interest and supporting this level by the organizational measures. Consider the chains of trust.	**What needs to be done to achieve this level** Require a security assessment to be conducted before the acquisition or outsourcing to ensure it does not pose significant risks. Consider the permeation of trust and document and monitor the basis for trust. Identify chains of trust and consider the trust of every involved party and its impact on the whole level of trust to the chain.

Services Third-Party Dependencies Management *(cont. from page 46)*				
	Note that these agreements can be made in a variety of ways, as requirements for the agreements are very basic and may not prevent abuses that exploit the weaknesses of complex agreements.	Provide the compliance with regulations such as GDPR and quality requirements such as Baldrige.	Note that risk management for use of external services is shared with third parties according to business and legal agreements. Track and report IT-, OT- and IoT-incidents with tools. (At this level, they are typically managed separately). Push the quality requirements and compliance of regulations into the third-party organizations.	Share the risk management relating to the use of third-party services with third parties according to business and legal agreements and regulatory needs. Codify the approach so that requirements and complete system view are well understood. Treat IT, OT, and IoT holistically.
	Indicators of accomplishment General documented agreements with third parties for required security requirements. General separation of security-related duties and responsibilities among parties.	**Indicators of accomplishment** SLAs, KPIs are defined per established contracts. Security policies covering timeframes, commitment for updates, patches, and maintenance of devices that may be in the field for years, and the responsibility for the incidents in case of violation.	**Indicators of accomplishment** Third-party assessment reports covering the SLAs, KPIs and associated QoS. Documented requirements for conducting the forensic activities in case of incident and the appropriate responsibility.	**Indicators of accomplishment** The roadmap for periodic evaluation of risks posed by the untrusted maintenance, identification of new external agents that may affect security, and update of contractual obligations accordingly. Clearly identified and documented connections with legislation and regulatory requirements.

Table 7-6: Services Third-Party Dependencies Management

Example

A manufacturer of vehicles for public transportation relies on many parts providers, software developers and integrators, resulting in a very complex integration effort. Security, safety and privacy of information are all important. The manufacturer must ensure that the requirements, trust and risk are all managed across the complete set of partners in the supply chain. Therefore, it sets the maturity target at

> comprehensiveness level 4, *formalized*. During a current state assessment, the organization discovers that it manages KPIs and SLAs, but that it still treats aspects of trustworthiness and IT and OT separately. It sets its comprehensiveness level at level 2, *ad hoc*.

8 Enablement Domain

The security enablement domain is used to implement security controls and practices necessary to create an operational system, based on governance decisions related to security policy and the need to address business risks using the best available means. Security policy and controls are subject to periodic review and assessment. The enablement domain includes identity and access management, asset protection, and data protection.

8.1 Identity and Access Management Subdomain

The identity and access management subdomain aims to protect the organization and control the use of resources by the identified agents to reduce the risk of information leakage, tampering, theft or destruction.

8.1.1 Establishing and Maintaining Identities Practice

Establishing and Maintaining Identities				
This practice helps to identify and constrain who may access the system and their privileges.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Basic people and device identity.	Dynamic device identity.	Device identity management is unified with people and system-identity management.	Maintain and control the use of identities of people, systems and things throughout their lifecycle.
General considerations	At this level, devices are managed and tracked with simple, static identifiers. People may be managed at organizational level.	At this level, critical devices are authenticated, and the role-based identities are introduced.	At this level, the organization comprehensively manages the identities of people, systems and things and implement root of trust in some areas.	At this level, the organization manages the full identity lifecycle and requires roots of trust for all identities.

Establishing and Maintaining Identities *(cont. from page 48)*				
	What needs to be done to achieve this level Ensure that valuable devices in the organization can be identified and managed. Ensure that those who need access can access the assets.	**What needs to be done to achieve this level** Identify equipment to be authorized and provide the appropriate scheme and technical means for its identification and authentication. Define the roles for the staff members involved into the key scenarios.	**What needs to be done to achieve this level** Implement inventory of equipment, systems and devices and human identity management automatically. Integrate authentication schemes, including multi-factor authentication where appropriate.	**What needs to be done to achieve this level** Implement automated unified identity management that addresses the entire identity lifecycle. Implement identity proofing in accordance with relevant regulations or system requirements. Use a system wide capability to identify people, systems, and things. Provide hardware key protection and hardware root of trust where required
	Indicators of accomplishment Valuable devices have a unique identifier. There is an organizational mechanism for the identification of staff members and visitors.	**Indicators of accomplishment** Each device has a unique persistent identity. Certificates are used for mutual authentication with other devices and the cloud. Human identities are associated with roles.	**Indicators of accomplishment** Identity management uses a known solution. Key management infrastructure may support identity management by providing trust anchors for authentication. Authentication requirements are commensurate with the risk of the transaction.	**Indicators of accomplishment** Unified identity management covers registration and identity issuance, usage, re-issuance, updating suspension, expiration and revocation (e.g. CA system). All people, systems and things go back to a hardware root of trust (e.g. a secure element). User identity proofing meets system requirements.

Table 8-1: Establishing and Maintaining Identities

Example

A financial institution accepts transactions from a variety of devices and smart industrial components. The institution must understand and manage the identities of all components from cradle to grave. Therefore, it sets the maturity target for establishing and maintaining identities to comprehensiveness level 4, *formalized*. During the assessment, the financial institution realizes that while it manages the full identity lifecycle for devices, it has not set up hardware roots of trust for many critical identity elements; hence its current comprehensiveness level for establishing and maintaining identities is level 2, *ad hoc*. The financial institution prioritizes hardware roots of trust in their roadmap, with a goal of moving to level 4 in the next assessment.

8.1.2 ACCESS CONTROL PRACTICE

Access Control				
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Constrain the ability of external agents to access devices and IT components.	Constrain the ability of both internal and external agents to access devices and IT components.	Manage access to devices and IT components in a unified, consistent manner.	Implement a consistent process for managing access over the lifecycle of both users and IT and OT systems, enforcing access control with high assurance, monitoring, testing, and revoking the rights in a way that meets business needs and constraints.
General considerations	At this level, basic access controls are applied to devices and to IT components in a siloed manner and focused mostly on external threats.	At this level, access controls consider both internal and external threats. IT and OT access are still managed separately. Third party systems may be implemented to manage user access rights.	At this level, access to IT and OT components is considered holistically, and organizations begin to automate access permission assignment.	At this level, access control expands to include governance and lifecycle.
	What needs to be done to achieve this level Implement generic access control based on common-purpose mechanisms	**What needs to be done to achieve this level** Describe the goals for access control for both external and internal agents with	**What needs to be done to achieve this level** Ensure that access control policy is appropriate for both	**What needs to be done to achieve this level** Define and implement access management and lifecycle practices that address access to

Access Control *(cont. from page 50)*				
	supported by application, service, operating system, network or device. Ensure that these common-purpose mechanisms provide proper segregation of external and internal agents and limit access to external agents.	the available use cases. Verify the access control policy against these goals. To minimize exposure and risk the Trusted Computing Base should be as small as possible.	IT and OT components. Define the reference points at which to monitor and control access and implement access control requirements. Subject highly privileged users to screening.	IT and OT systems, including de-provisioning once users no longer require access. Ensure the consistency of access control across the whole organization or system. Conduct access control periodic testing (penetration testing, red/blue team exercises).
	Indicators of accomplishment External perimeter is defined at the network level, with limited permissions for those accessing externally, including employees accessing remotely. Accounts are segregated at operating system or application level, and guest accounts are constrained.	**Indicators of accomplishment** Organization has implemented role-based access control for both IT and OT components, but implementations and policies are silo-ed. Roles, rights and management are documented. Privileged users understand their roles and responsibilities. For individual systems, services, and applications, access control is enforced at the proper level and appropriately described, for both internal and external actors. Compartmentalization should be used to prevent breaches from propagating between the hardware components or	**Indicators of accomplishment** Role-based access control is in place and addresses both IT and OT components in a unified manner. Access control rules follow principle of least privilege. Access control at the connected, enterprise level is supported by network, application and system level technologies. Access control practices are automated in at least some cases.	**Indicators of accomplishment** Access control governance and lifecycle policies are documented. Access control practices are mostly automated, including governance and lifecycle practices. Access-control practices are monitored and tested periodically.

Access Control *(cont. from page 50)*				
		software components within a device.		

Table 8-2: Access Control

Example

A retailer is implementing a state-of-the-art security system, with connected cameras and inventory sensors. The retailer realizes that camera information is sensitive, and that access must be controlled carefully. They determine that they need to look at access control holistically for both IT and OT components in their security system, and they set the target comprehensiveness for access control at level 3, *consistent*. During their first assessment, they realize that the previous Chief Information Security Office (CISO) developed an access-control policy focused only on protecting against external actors, so they are currently at comprehensiveness Level 1 (Minimum) (Minimum), minimal.

8.2 Asset Protection Subdomain

The asset management subdomain is put in place to protect physical and digital assets. This is an area of strong collaboration between IT and physical security teams.

8.2.1 Asset, Change and Configuration Management Practice

Asset, Change and Configuration Management				
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Manage configurations and changes of isolated assets.	Manage assets as a system of systems, with hierarchies and inherited policies.	Manage IT and OT assets in an integrated manner.	Manage the process for the asset lifecycle from provisioning to replacing, including emergency changes.
General considerations	At this level, organizations are aware of which assets are critical.	At this level, organizations begin to implement formal asset management, change management and inventory programs. A standard protocol for device updates and security renewal allows to proactively mitigate emerging threats and reinstate	At this level, asset and configuration management programs apply equally to IT (hardware and software) and OT assets.	At this level, the asset management policy addresses cradle-to-grave lifecycle of IT and OT assets.

Asset, Change and Configuration Management *(cont. from page 52)*				
		the security on devices that have been compromised.		
	What needs to be done to achieve this level Establish and document acceptable use for critical assets. Ensure that acceptable use rules are followed. These rules can address device and media handling, access restrictions, limiting asset distribution to a minimum required to support the functionality, etc.	**What needs to be done to achieve this level** Create an asset inventory and assign a designated owner for valuable assets. Classify and label the physical and information assets involved in the main use cases. Develop procedures for handling, processing, storing, and communicating assets consistent with their classification. Create baseline configurations for systems, change and configuration management procedures where appropriate.	**What needs to be done to achieve this level** Ensure that asset management, change management and configuration management policies cover IT and OT assets. Develop guidelines for protecting software assets, including boot-process integrity, software integrity (e.g., malware detection), memory protection and secure updates. Incorporate principle of least functionality by configuring systems to provide only essential capabilities.	**What needs to be done to achieve this level** Expand asset management policy to provide a lifecycle structure for managing IT and OT assets from procurement and enrollment to decommission and disposal. Ensure policy addresses both individual components and complete systems (e.g., plane engine and complete plane) at all stages of the lifecycle. Implement hardware secured boot processes and secure updates to ensure system integrity
	Indicators of accomplishment Critical assets have documented acceptable use policies. Development and testing environments are fully separated and segmented from production environments.	**Indicators of accomplishment** An inventory listing the assets such as equipment, information, hardware or software and considering both individual assets and hierarchical collections of assets. The description of the procedures with connections to use cases. The asset management policy is	**Indicators of accomplishment** Asset, change and configuration-management practices integrated across IT and OT. Asset, change and configuration-management practices may vary by region to address local requirements, such as GDPR. Change management procedures include assessments of the	**Indicators of accomplishment** Procedures are in place for hardware decommissioning and disposal, with consideration for the sensitivity of the data that was processed by the hardware. Configuration-management procedures establish a process for identifying items (devices, hardware, software, firmware and

Asset, Change and Configuration Management *(cont. from page 52)*				
		appropriate to the assets managed and the system complexity and provides the framework for asset management, including assignment of owners and roles and responsibilities. Change-management procedures include identifying and recording the significant changes to equipment, software and procedures. Configuration-management procedures address roles and responsibilities. Baseline configurations are maintained and updated.	potential security impact of changes. Assets are disposed of in accordance with regulatory and environmental guidelines.	documentation) throughout the system development life cycle and for managing the configuration of those items. As the system continues through its lifecycle, new items are identified, and some existing items may no longer need to be under configuration control. Asset planning considers capacity requirements and looks to ensure sufficient capacity to maintain resource availability.

Table 8-3: Asset, Change and Configuration Management

Example

A global health care network manages a large number of connected devices and related IT assets, along with sensitive patient data. Given the risk of misuse of those assets, the health care network sets a target of comprehensiveness level 4, *formalized*, for asset, change and configuration management. During their assessment, they determine that their formal asset management program applies more to their OT and device assets than to their IT assets. They are starting to look at how their practices need to differ based upon regional requirements. Their current state is comprehensiveness level 2, *ad hoc*.

8.2.2 Physical Protection Practice

Physical Protection				
This practice's policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Generally, constrain the access to physical assets.	Establish and manage physical security perimeters.	Automate finer grained physical access control, customizing constraints for factors such as time and manner of physical access.	Address all aspects of physical security and safety, prevent theft, and ensure ongoing safe operation.
General considerations	At this level, the organization limits physical access to devices on a one-off basis.	At this level, the organization deploys physical security controls for groups and spaces in accordance with defined policy or requirements.	At this level, the organization leverages its identity management and monitoring systems to manage access to physical assets.	At this level, physical protections are well defined and consistent across the organization, address both security and safety and are periodically reviewed and assessed.
	What needs to be done to achieve this level Adopt physical security policies to protect devices from accidental or intentional physical damage or operational disruption.	**What needs to be done to achieve this level** Define trust zones in IT system architecture and establish physical security perimeters in IT and OT deployments to separate and protect the systems within each zone. Tamper-evident housings are deployed outside the secure perimeter.	**What needs to be done to achieve this level** Automate identity management and alerting systems to manage and report on physical access to locations and assets. Enforce more granular access control rules, such as time of day. Tamper-resistant housings for systems and things that are deployed outside of secure perimeter.	**What needs to be done to achieve this level** Clearly define security perimeters, with their siting and strength dependent upon the assets contained within the perimeter and the results of a risk assessment.

Physical Protection *(cont. from page 55)*				
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Physical security policies in place for individual devices.	Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) correspond to established trust zones and protect areas that contain IT and OT systems. Access rules enforce perimeters to limit human access to critical IT and OT systems. Group policies are in place to manage collections of physical assets.	Existing IT access management and monitoring infrastructure is extended to manage access to OT and other physical assets. For physically isolated components, use of removable media and devices is appropriately restricted, preferably with physical locking of the relevant connectors and interfaces.	Physical barriers, where applicable, prevent unauthorized physical access and environmental contamination. Physical protection requirements are periodically reviewed and updated at different stages of the assets’ lifetimes. The monitoring and alarm systems, where applicable, establish the required level of resistance to physical break-ins. Assurance measures ensure that there are no gaps in the perimeter or areas where a break-in could easily occur.

Table 8-4: Physical Protection

Example

A garment manufacturing plant that produces casual apparel relies upon a handful of critical systems (both physical machines and the IT system monitoring their performance) to produce their output. Their goal is to protect workers and prevent assembly line disruptions by establishing perimeters around these critical assets. Therefore, the plant sets its maturity target for physical protection at comprehensiveness level 2, *ad hoc*. When assessing their current state, they note the physical barriers and proximity cards that control access to their critical systems and determine that their current state matches their target.

8.3 DATA PROTECTION SUBDOMAIN

The data protection subdomain prevents unauthorized data disclosure or manipulation of data, both for data at rest, in transit and in use. This is important for security, privacy, regulatory compliance, legal and intellectual property protection.

8.3.1 PROTECTION MODEL AND POLICY FOR DATA PRACTICE

Protection Model and Policy for Data				
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Declare that IT and OT data should be protected from unauthorized access.	Develop data classification systems within discrete environments.	Data protection policy is unified across IT and OT.	Categorize and consistently protect the data according to the requirements of stakeholders throughout the data lifecycle.
General considerations	At this level, basic IT and OT data protections are in place in accordance with relevant regulatory requirements.	At this level, data is classified according to its business and security impacts, but classification of IT and OT data is siloed.	At this level, data protection policy looks holistically at all types of data, and the organization begins to automate classification and policy.	At this level, data is considered throughout its entire lifecycle and in accordance with change and configuration management.
	What needs to be done to achieve this level Implement data protection policy based upon relevant laws and regulation. Address the security concerns for data in motion, data at rest and data in use.	**What needs to be done to achieve this level** Expand data protection policy to include data classification, tying the data to its business and security objectives within different IT and OT environments.	**What needs to be done to achieve this level** Create unified data policy to address data generated from and processed through IT and OT sources. Substantiate data protection rules by referring relevant standards, guidelines, and best practices.	**What needs to be done to achieve this level** Expand data protection policy to include the complete data lifecycle. Integrate the data protection policy with change and configuration management policy.

Protection Model and Policy for Data *(cont. from page 57)*				
		Determine specific measures for protecting different classes of data.		
	Indicators of accomplishment Policy that reflects applicable laws, directives, regulations, policies, standards and guidance. Data residency and regional requirements influence policy. Policy stipulates protection of Personally Identifiable Information (PII) according to generally recognized rules and regulatory requirements.	**Indicators of accomplishment** Policy defines types of data to be protected according to business and security requirements. Policy specifically addresses PII, confidential data and business critical data. Access control and other policies are aligned with protection requirements for different classes of data. The concrete data protection measures (encryption, access restrictions, media control, isolation or backup) may not be listed or may be referred to only generically. Policy, if necessary, sets constraints on external connections, Internet services, cloud storage, and other applications that may cause intentional or unintentional data leakage. Similarly, the policy may set constraints on removable media and BYOD to facilitate data confidentiality.	**Indicators of accomplishment** Data classification policy considers the business context of the data. For each class of data considered confidential, policy describes required protection measures (e.g., encryption, access control, data flow control) and their required implementation (e.g., encryption algorithms). Where encryption algorithms are recommended, policy allows for multiple options, where available, and recommends algorithm agility (the ability to update algorithms as needed with minimal impact on the rest of the system). The policy also describes data integrity measures and their required implementation.	**Indicators of accomplishment** The security policy defines the types of sensitive information, the security goals and the means used to get these goals for every information unit within the defined trust zones. For each data type, policy defines how it is routed into the system, how it is stored, and the retention period. If information is transferred between components within one trust zone, the policy may set the rules for this transfer and accountability or monitoring requirements. When information must be transferred between trust zones with different rules and requirements, the security policy provides guidance on designated policy enforcement points between interconnected systems. Such guidance may include prohibiting information transfer (i.e., allowing read only), enforcing one-way information flows

Protection Model and Policy for Data *(cont. from page 57)*				
		The policy, if necessary, sets backup and redundancy requirements to address data integrity. Policy specifies storage life and destruction policies for data.		and implementing trustworthy regrading mechanisms to reassign security attributes and security labels. The policy may consider mandating specific architectural solutions to help enforce specific security policies. The policy may mandate that teams develop solutions with algorithm agility in mind.

Table 8-5: Protection Model and Policy for Data

Example

A food manufacturing plant is concerned that their secret recipes might be stolen, through theft or reverse engineering of OT processes. They determine that their data protection policy needs to be unified across IT and OT, and they set their target comprehensiveness for protection model and policy for data to level 3, *consistent*. During the assessment, they note that they have fairly thorough data classification policies, but they are separate for different environments and not unified across IT and OT. Therefore, their current maturity is comprehensiveness level 2, *ad hoc*.

8.3.2 IMPLEMENTATION OF DATA PROTECTION PRACTICES PRACTICE

Implementation of Data Protection Practices				
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Take advantage of built-in protection controls (OS, network, services).	Apply additional mechanisms to protect data groups.	Implement systematic data protection measures across the entire system.	Ensure the required protection of each data element in transit, at rest and in use.
General considerations	At this level, data protection occurs at the system level, using system-level controls but few, if any, third-party products.	At this level, the organization considers whether built-in controls are sufficient to meet data protection requirements for different sub-systems and considers whether additional mechanisms or products are needed.	At this level, the organization protects data across the entire system, using multiple mechanisms at different layers. In many cases, data protection measures are automated	At this level, the organization implements mechanisms to protect data throughout the lifecycle, including at the destruction phase. Ensure immutability and source authentication of data.
	What needs to be done to achieve this level Use built in controls to meet the data protection policy requirements. Employ common-purpose measures such as encryption of data in motion by common-purpose mechanisms such as TLS.	**What needs to be done to achieve this level** Assess data protection strategy for broader sub-systems or for larger groups of data. Implement relevant network and application controls to constrain access to data such as network segmentation, filtering, virtual machines, gateways and other measures to manage data flow.	**What needs to be done to achieve this level** Implement data protection requirements systematically. Ensure that data protection controls are chosen to fit the data protection policy and rules, as recommended by the standards and best practices. In many cases, data protection measures are automated.	**What needs to be done to achieve this level** Ensure that key management is in place to protect access to encrypted data. Conduct periodic assessment of data flow control mechanisms. Introduce detection mechanisms supporting the work of data protection policies and controls. Mechanism to ensure immutability and source authentication of data has been implemented (e.g. Distributed Technology

Implementation of Data Protection Practices *(cont. from page 60)*				
				with signing using secure identity)
	Indicators of accomplishment Data protection measures address confidentiality, integrity and availability requirements. Data protection measures meet privacy and residency requirements from applicable laws and regulations.	**Indicators of accomplishment** Data protection measures focus on restricting data access, constraining data flow, and monitoring data access and use. Specific measures are implemented only if it is prescribed by the policy.	**Indicators of accomplishment** Data in-motion, in-use, and at-rest is protected against disclosure and uncontrolled changes by applying functions such as confidentiality controls, integrity controls, access control, isolation and replication. Software and firmware packages and versions are verified through appropriate integrity checking mechanisms. Data owners have a choice of mechanisms to protect data and opt to implement the most appropriate controls to address security requirements, operational requirements and business need. Data protection mechanisms can be easily replaced as they become outdated (for example, no algorithms are hard coded into the implementation). These mechanisms protect the data against disclosure and intentional or accidental corruption	**Indicators of accomplishment** Data encryption implementation is implemented with algorithm agility in mind and includes key management measures such as PKI and other trust schemes. Technical protections (such as DLP or service restrictions) prevent the accidental spilling or unauthorized sharing of data.

Implementation of Data Protection Practices *(cont. from page 60)*				
			according to the confidentiality, integrity, privacy and data retention policies, and enforce the control of the information flow within the system and between interconnected systems based on the defined information flow control policies. The level of protection, and assurance on its enforcement is commensurate with the impact of data loss or falsification.	

Table 8-6: Implementation of Data Protection Practices

Example

A manufacturer of an automotive over-the-air patching gateway must ensure that code and information is protected at all times. Data must be protected in transit, at rest and while in use. Their maturity target for implementation of data protection practices is comprehensiveness level 4, *formalized*. The assessment indicates good practices for integrity checking, key management and cryptographic agility; in addition, there are mechanisms in place to prevent data leakage. Their current state is determined to match their target: level 4, *formalized*.

9 Hardening Domain

The hardening domain relates to security practices used during the operation of the system, including vulnerability and patch management, situational awareness, and event and incident response for continuity of operations. The security hardening domain includes organizational and technical measures to assess, recognize and remediate ongoing risks to improve the trustworthiness of the system.

9.1 Vulnerability and Patch Management Subdomain

Vulnerability and the patch management subdomain policies and procedures are used to keep component systems up to date and less prone to attacks due to vulnerabilities in those component systems. Situational awareness is also necessary to keep abreast of changing vulnerabilities.

9.1.1 Vulnerability Assessment Practice

Vulnerability Assessment				
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Consider whether widely known vulnerabilities are present in organizational assets.	Verify whether business critical assets are adequately protected from known vulnerabilities.	Perform holistic vulnerability analysis of the system as a whole using automation and third-party evaluations.	Perform regular deep customized vulnerability assessments throughout lifecycle.
General considerations	This level meets the need for overall protection against widely deployed attacks and targeted attacks requiring low skills. Assessment is performed on a departmental basis without an overall organizational plan.	This level meets the need for improved protection of critical components against targeted attacks by attackers requiring medium skill-level and involves deeper review of vulnerabilities.	This level meets the need for the improved protection of critical components against attackers with medium skills and against insider attacks.	This level meets the need for the continuous monitoring of system vulnerabilities and exposures throughout the system lifecycle to withstand targeted attacks.
	What needs to be done to achieve this level Appoint a person for assessing well-known	**What needs to be done to achieve this level** Identify critical components.	**What needs to be done to achieve this level** Establish an assessment scheme involving regular	**What needs to be done to achieve this level** Implement periodic activities involving third parties to

Vulnerability Assessment *(cont. from page 63)*				
	vulnerabilities in any given component. Informally describe the types and examples information sources for the assessment.	Appoint personnel, detail and prioritize their responsibilities for the vulnerability assessment, and establish reporting procedures. Describe the obligatory and optional information sources for the assessment.	vulnerability scanning of all assets using automated tools and third-party evaluations. Incorporate threat intelligence received from information sharing forums and sources into vulnerability assessment program. Ensure the vulnerability program accounts for changes in the organization’s inventory in near real-time. Describe the supposed types of vulnerabilities, level of details in their description, format of the report. Establish program to improve quality of components during entire lifecycle, including design and development. Establish process for continuous improvement of vulnerability assessment process.	discover the vulnerabilities. Negotiate the methods, tools, and prioritize the activities according to the exposure of components to attacks and the associated risks. Review the results of third-party assessments and the vulnerability management program to identify strategic process improvements.
	Indicators of accomplishment The duties for the responsible person contain the duty to monitor the designated systems for well-known vulnerabilities. Information about vulnerabilities is	**Indicators of accomplishment** The vulnerability assessment process is implemented by the efforts of a specially formed team, internal or external to the organization. An oversight process ensures that	**Indicators of accomplishment** A routine vulnerability discovery and remediation process takes place. The results of the vulnerability management program are actively tracked by business	**Indicators of accomplishment** Comprehensive vulnerability assessment process is implemented periodically according to the established method. Results of third-party assessments and the

Vulnerability Assessment *(cont. from page 63)*				
	directly requested from the responsible personnel when required.	identified vulnerabilities are remediated within a time period appropriate to the severity of vulnerability. List of components most critical or known for being targets of attacks and their vulnerabilities are requested from the maintenance personnel when required, including operating systems, and general software and services.	stakeholders and the board. The results of the vulnerability assessment are available by request and contain enough details and score evaluation for every discovered vulnerability.	vulnerability management program are reviewed to identify strategic process improvements.

Table 9-1: Vulnerability Assessment

Example

A smart manufacturing company would like to ensure they manage their vulnerabilities holistically using tools and third part evaluators. They set their comprehensiveness level for the vulnerability assessment practice to level 3, *consistent*. Upon performing an internal assessment, they discover that they have team that does not use tools and only looks for known vulnerabilities. They set their current state comprehensiveness level for the practice to level 2, *ad hoc*.

9.1.2 Patch Management Practice

Patch Management				
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Follow security advisories issued by vendors and install the provided patches.	Prioritize patching based on risks and confirm that specific components are protected against the most probable attacks. Periodically review patch status.	Automate patching with centralized support for patch management.	Protect components with a long lifecycle and those that are not easily patched due to certification or operational requirements.
General considerations	This level implements a manual process for installing software security patches as provided by vendors.	This level defines a process for updating not only the software that is most exposed to attacks, but also the components whose compromise may lead to the direst consequences and implements a process for periodic updates of software based on the results of risk analysis and vulnerability assessment. A standard process for delivering OS and application updates ensures seamless and timely response to emerging security issues.	This level implements a centralized and automated process for patch updates for all resources, including cloud and edge.	This level provides for managing components and devices with long life cycles and those that are not easily patched by managing patching over the life cycle as well as using other techniques to address vulnerabilities addressed by patches.
	What needs to be done to achieve this level Establish the rules for installing software patches provided by vendors.	**What needs to be done to achieve this level** Prioritize the software update process according to the risk analysis and vulnerability assessment results.	**What needs to be done to achieve this level** Establish the rules for patching uniformly and consistently using automation and centralized management.	**What needs to be done to achieve this level** Establish and manage patch management process continuously over time with considerations for the

Patch Management *(cont. from page 66)*				
	Use the automated updates where possible.	Include the preliminary testing of the security patches and updates where required.	Initiate the process of replacing the appropriate software with another version or other similar software when it is not possible to install a security update that is necessary to decrease the risks to acceptable values.	lifecycle of both IT and OT components. Examine the software of critical systems to understand it deeply, including the vulnerabilities leading to patches.
	Indicators of accomplishment Policy for applying the vendor patches. The components connected to the Internet obtain security updates regularly, while other software and devices are updated in case of security incident, or upon obtaining the notification about serious or mass attack that may affect them.	**Indicators of accomplishment** The information about available patches is obtained either automatically or from the specific security advisories provided by vendors, security companies, and CERTs. There are responsible personnel that may provide the information about status of software updates by request. IT and OT are handled separately. Patching is reviewed periodically. Consequences of vulnerabilities associated with software components being exploited are understood and documented. Patch management is prioritized, and the organization maintains awareness of available patches.	**Indicators of accomplishment** A scalable and systematic risk-based approach to software patching or replacement is in place. Decision-making strategy for the cases where immediate patching is not applicable.	**Indicators of accomplishment** Continuous patch management is linked to a continuous risk management activity. Consideration and protection of long-lifespan system components where continuous patching is not feasible.

Table 9-2: Patch Management

Example

A supply chain company has sensors and devices installed in their depots as well as in vehicles and shipping containers and packages. They would like to be able to manage the security, firmware updates, and patches for their devices centrally and securely patch over the air. They set the target comprehensiveness to level 4, *formalized*. Upon internal inspection, they discover that they receive patch information automatically for their IT systems, but their IoT device management is performed separately and manually. They set their current level of comprehensiveness to level 2, *ad hoc*.

9.2 Situational Awareness Subdomain

The situational awareness subdomain comprises techniques and organizational and community activities used to achieve an understanding of the current security state enabling an organization to prioritize and manage threats more effectively.

9.2.1 Monitoring Practice

Monitoring Practice				
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	From time to time check individual diagnostic logs of components, devices, sensors and systems.	Obtain status events from devices and check for correct expected operation. Malware is detected.	Collect, consolidate, and analyze monitoring information holistically from a variety of sources with human expertise for analysis.	Use automation and continuous monitoring with analytics to identify concerns.
General considerations	This level implements the basic monitoring of security events using the built-in mechanisms of components, devices, sensors, operating systems, services, and software.	This level employs events generated by individual components, devices, sensors and systems to detect security issues. Malware is detected.	At this level, information from various monitoring sources are consolidated and managed holistically.	This level implements the continuous real-time monitoring of all relevant types of security events using the most appropriate means and automation for analysis.
	What needs to be done to achieve this level Follow existing general security guidance on basic security monitoring using existing	**What needs to be done to achieve this level** Consider events caused by both human actions (e.g., access to the sensitive resources, credentials	**What needs to be done to achieve this level** Consider different sources and various additional advanced monitoring systems	**What needs to be done to achieve this level** Automate most of the analysis of security events and conduct required manual

Monitoring Practice *(cont. from page 68)*				
	mechanisms without any specific concerns for the particulars of the specific system. Assign the responsibility for the analysis of security related events is to the system administrator or other person responsible for the software, system and network in daily use.	management) and existing processes (e.g., software updates, periodic on-demand malware scans). Failure reporting provides insight into device and application failures and visibility into emerging security threats. Focus on the events that may have most significant impact on the normal system functioning, so the recommendations for analysis refer the results of risk assessment. Communicate the information about events within the organization.	(intrusion detection systems, SIEMs, etc.). Involve skilled security personnel or third-party contractors that track security events and provide information about the current security state to the responsible stakeholders. Protect the monitoring information, for example with secure logging.	review where appropriate. Perform the monitoring at various system levels – hosts, network, specific equipment and may involve the skilled security personnel or third-party contractors (e.g., in a form of Security Operation Center). Implement the whole cycle of monitoring from establishing incident indicators tied to risks to the protection and backup of monitoring data. Test and continuously improve detection processes.
	Indicators of accomplishment Responsible personnel who are aware of the current security state. The analysis of security state is based on basic indicators such as the absence of anomalies in system logs.	**Indicators of accomplishment** Use of general monitoring mechanisms is related to potential consequences of high impact and documented. Malware detection procedures and techniques have been established.	**Indicators of accomplishment** Monitoring information is combined to create a consolidated view relevant to the main risks. Additional tools and techniques beyond generic tools are deployed and appropriate expertise is engaged.	**Indicators of accomplishment** Continuous monitoring, use of automation for analysis, use adaptive protection and AI techniques, protection of monitoring data and appropriate expertise is engaged. The description of revealed incident is given in terms of business security objectives.

Table 9-3: Monitoring

Example

An oil and gas company conducts a current state assessment of their operations and identifies that they are manually viewing device logs to identify any potential problems and alerts. They set their maturity to comprehensiveness level 1, *basic*.

> They would like to transition to an automated system that will monitor all their machines and devices and allow operators to view the results and act on them. They set their target Comprehensiveness Level to 3, *consistent* and begin planning to address the gap.

9.2.2 SITUATIONAL AWARENESS AND INFORMATION SHARING PRACTICE

Situational Awareness and Information Sharing				
This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Obtain information on external incidents as needed. Provide some information to external parties need-to-know and as needed.	Have a general awareness of external incidents and implement a policy sharing information to external parties on a need-to-know basis.	Learn information about external incidents in systematic manner. Information sharing policy supports responsible disclosure.	Set up a two-way sharing of zero-day threats and incidents across the industry.
General considerations	This level defines recommendations for sharing information about serious general incidents to external parties, but decisions are made ad hoc. Awareness of external incidents is based on the most publicized incidents.	This level defines a policy on incident information sharing, including when, how and to whom information is to be shared. It also includes general awareness of external information.	This level makes awareness of external incidents systematic.	This level supports sharing of zero-day vulnerabilities and is applicable if the security assessment and testing activities are implemented within the organization.
	What needs to be done to achieve this level Specify the incident and vulnerability disclosure policy according to the legislative and regulatory background and necessary expertise-exchange considerations. Share incident information about general security	**What needs to be done to achieve this level** Analyze which types of security incidents may particularly affect the system or organization. Provide appropriate instructions on when to share information on incidents, to whom, and how. Devices produce failure reports and a mechanism exists for	**What needs to be done to achieve this level** Maintain subscriptions to security advisories, mailing lists of vendors, sector communities to keep the situational awareness about security issues arising in the particular sector or relevant to the used technologies.	**What needs to be done to achieve this level** Share the zero-day vulnerabilities with the vendor of the software or equipment and inform the relevant authorities, agencies and security companies to enable joint work to mitigate the effect of possible future exploitation of these vulnerabilities in the wild.

Situational Awareness and Information Sharing				
	incidents with external parties. General security incidents include malware infection, unauthorized access to the service or software, compromised credentials, use of unauthorized equipment or media, etc. Include into the appropriate instructions the recommendations on the means and process of the communication regarding security issues (the intended recipients, way of communication, etc.). Awareness and communication of the security incidents is need-to-know. Keep abreast of product recalls and news.	sharing the logs and events.	Obtain information from software and services, including anti-malware solutions and other security software that perform monitoring of the security state automatically sending reports about detected security events and vulnerabilities upon appearance this information. Devices automatically produce failure reports that can be shared with manufacturers and central management systems. Include into the instructions for the personnel and guidance for the configuration of monitoring software the recommendations on the means and process of the communication (the intended recipients, way of communication, etc.) and the general strategy in disclosure of vulnerabilities to the external agents (e.g., responsible disclosure).	Define the policy describing the appropriate use of data about security incidents, discovered vulnerabilities, and applied practices from other participants of IoT community and specifying how and when to collaborate with regulatory authorities, standardization committees, and voluntary organizations for providing the feedback on the regulatory acts, guidelines, standards, and recommendations. Create an on call "ready team" prepared to quickly address issues as they arise.
	Indicators of accomplishment Recommendations on sharing information about security incidents clarify	**Indicators of accomplishment** Clarity on the when, with whom, and how to communicate	**Indicators of accomplishment** Systematic approaches to situational awareness are in place.	**Indicators of accomplishment** Information sharing about zero-day vulnerabilities is

Situational Awareness and Information Sharing				
	sharing practices while limiting sharing as much as possible, but decisions are made ad hoc.	security incidents is provided in the policy. Personnel are aware of general news about incidents.	Information sharing policies support responsible disclosure.	codified in policy and practice.

Table 9-4: Situational Awareness and Information Sharing

Example

A retailer determines that its comprehensiveness target for situational awareness and information sharing for its stores should be at level 2, *ad hoc*, based on the need to generally protect consumer information at the point of sale. As it introduces new technology involving facial recognition that is connected to the cloud, the retailer recognizes the need to consider policies for consumer privacy data for storage and transmission and sets its comprehensiveness target at level 3, *consistent*.

9.3 Event and Incident Response, Continuity of Operations subdomain

Event and incident response subdomain comprises a combination of policy and technical activities designed to allow an organization to respond to incidents swiftly and to minimize disruption to the organization enabling the organization to continue its core business.

9.3.1 Event Detection and Response Plan Practice

Event Detection and Response Plan				
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Define incidents and basic response actions.	Provide guidance on how to detect and respond to incidents that can impact critical components.	Set up the basis for the automatic execution of response procedures within the organization.	Include partners and other organizations in an incident response approach that also has a view beyond isolated incidents, enabling the organization to detect early stages of an attack as well as prevent incidents.
General considerations	This level supports sharing of zero-day vulnerabilities and is applicable if the security assessment and testing activities are implemented	At this level, individual departments implement their own incident response plans to establish and document the procedures and	The organization has a unified and automated (or semi-automated) cycle of incident detection, response, and support of operations continuity.	The organization has an integrated incident-response program that includes partners and other organizations. This level enables the monitoring and analysis of additional

Event Detection and Response Plan *(cont. from page 72)*				
	within the organization.	actions to respond to defined types of significant incidents that can impact critical components.		data that can be used to detect an attack at early stages or to provide responses to prevent the exploitation of vulnerabilities.
	What needs to be done to achieve this level The policy addresses well-known incidents by type and responsible personnel. These incidents may include denial-of-service attacks, unauthorized access to networks, accessing protected and private information, defacing web pages, misuse of services, etc. Base the detection actions for every type of security incident on clear indicators of security violation. Consider the information about information flows and general use of IT components for incident examination. Define the basic response plan that does not consider any deviations from the prescribed actions.	**What needs to be done to achieve this level** Determine which security incidents may require immediate reaction, enumerate the types, and outline the steps that should be taken to respond to the incident and mitigate damage. Describe the personnel roles and order of operations when a response is needed. Employ basic analysis, including manual deep examination of the incident-related data for certain use cases. Perform analysis as a part of forensics activities. Align the notification actions with situational awareness policy. Prescribe the response that includes the actions for the system recovery, remediation, and support of operations continuity also	**What needs to be done to achieve this level** Use advanced monitoring techniques and automated solutions such as network and device logging, intrusion detection system/intrusion prevention system, next generation firewall for incident detection and analysis. Implement automated notification about the security incident including all relevant information delivered to those responsible for system recovery, remediation and maintaining continuous system operation. Integrate the incident response with Situational Awareness as well as the Remediation, Recovery, and Continuity of Operations SMM practices.	**What needs to be done to achieve this level** Consider the secondary symptoms of the security violation or system misuse such as unusually heavy traffic or high CPU usage, locked-up accounts, cleared log file, unexpected changes in configuration, and correlate these symptoms. Optionally implement an approach based on the correlation of symptoms to prevent the incident. Precisely define the notion of a security-relevant event that is typically wider than a security violation. Implement the response to prevent such events.

Event Detection and Response Plan *(cont. from page 72)*				
		aligned with appropriate policy.		
	Indicators of accomplishment Individuals are aware of the need to respond to security events based on clear indicators of security violations.	**Indicators of accomplishment** Departments have a systematic and documented approach to incidents with varying degrees of manual analysis of indicators. Incident response plan is accepted.	**Indicators of accomplishment** Unified approach to incident detection and response. Advanced tools and some degree of automation of incident detection and analysis has been implemented. Incident response and recovery plans are tested. Incident response and recovery plans incorporate lessons learned from incidents and response strategies are updated appropriately. Public relations are managed for incidents.	**Indicators of accomplishment** Shared approach to incidents with partners and other third parties. Analysis approach goes beyond individual incidents, creating broader understanding and supporting the ability to detect and respond to secondary indicators of an attack that may be precursors to a security violation.

Table 9-5: Event Detection and Response Plan

Example

A healthcare provider determines that their target comprehensiveness level is 2, *ad hoc*, as they would like to have an internal organization with clear roles that can address incidents, perform analysis and generate a response. Upon review of their current state they determine that they have some individuals across the organization that respond to incidents in their respective areas when an incident is detected. They determine that they are at a comprehensiveness level 1, basic, and that they need to establish a more formal organization and document procedures.

9.3.2 Remediation, Recovery and Continuity of Operations Practice

Remediation, Recovery and Continuity of Operations				
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	Provide basic instructions for the system recovery.	Define a policy and plans to handle possible known incidents and to confirm the complete recovery of the system.	Enable automated remediation and recovery procedures.	Support technical and organizational measures to facilitate quick system recovery and establish policies and technologies to enable forensic investigations.
General considerations	This level defines the concrete actions for the remediation and recovery of the most critical components.	This level supports continuity of operations by simple redundancy measures such as data backups and has a documented plan for remediation and recovery.	This level uses automation to enable remediation and recovery.	This level includes regular periodic testing of remediation and recovery procedures to verify the ability to maintain continuity of operations. It also includes technical and policy approaches to enable forensic examination of systems following an incident.
	What needs to be done to achieve this level Identify critical components and provide basic instructions for recovery based on general mechanisms.	**What needs to be done to achieve this level** Define a remediation and recovery policy, establish contingency plans for particular use case scenarios. Maintain all backup systems to the same level as the primary systems. Establish measures to confirm complete recovery. Consider additional approaches to recovery such as using redundant components or on-	**What needs to be done to achieve this level** Automated removal of malware, restoring backup data to databases, systematically removing temporary containment actions, and restarting all operational systems and applications. Define procedures for operational continuity. Upon detection of a security incident these mechanisms immediately enable	**What needs to be done to achieve this level** Establish the policy for regular and planned testing of continuous operation at a scheduled time to verify that the backup and fail-over systems will work properly when called upon and that the system can be restored to a pre-incident state. Support automated operations continuity, enabling the use of redundant mechanisms and data upon receiving information

Remediation, Recovery and Continuity of Operations *(cont. from page 75)*				
		demand data recovery. Devices can be automatically restored to a secure state following a compromise. Compartmentalization through hardware-enforced barriers between software components prevent a breach in one from propagating to others.	the secondary mechanisms. Support operations continuity based on user observation (after-the-fact approach). Note, that this approach can carry number of adverse risks. In particular it does not prevent damage to the primary equipment or other consequences of the incident while preventing the interruption.	about the possible interrupt or damage of primary ones. Ensure that recovery both restores the system and makes it more secure by keeping the same operational capabilities and protecting against the exploit that caused the incident. Establish the policies and technologies to enable forensic examinations.
	Indicators of accomplishment Documented instructions for recovery of individual components.	**Indicators of accomplishment** A documented remediation and recovery policy supported by functioning backup systems and redundant components used to enable recovery of IT and OT components. Incidents are contained and mitigated. Newly identified vulnerabilities are mitigated or documented as accepted risk.	**Indicators of accomplishment** Use of automated mechanisms to maintain continuity, including fail-over. Business system availability metrics are established and supported with processes and technologies.	**Indicators of accomplishment** Planned and periodic testing of recovery procedures, use of automation and techniques to improve system resilience. Policies and technologies in place to enable forensic investigations to enable learning and system improvement. Reputation is managed for incidents.

Table 9-6: Remediation, Recovery and Continuity of Operations

Example

A city traffic department determines that they need to be able to recover quickly from any possible disruption to the system and to be able to have processes that enable them to maintain continuity of operations, learn and improve over time. They identify their target comprehensiveness as level 4, *formalized*. The current state assessment identifies automated recovery systems, but they are disconnected and localized damage can occur. They rate their current comprehensiveness level as 3, *consistent*.

Part III: Comprehensiveness Level Definition Guide

10 Comprehensiveness Level Definition Guide

This guide recommends for consideration the following domain goals corresponding to the comprehensiveness levels for these domains.

The goal of **Security Governance** is to		
	set up a general base for security considerations	1 / Minimum
	establish baseline security measures	2 / Ad-hoc
	facilitate implementation of security capabilities	3 / Consistent
	set a clear governance structure and processes	4 / Formalized
The goal of **Security Enablement** is to		
	enable the use of available security controls	1 / Minimum
	implement security controls according to the known usage scenarios	2 / Ad-hoc
	employ both built-in and additional mechanisms to cover the known risks	3 / Consistent
	establish the process to address the risks by the best available means	4 / Formalized
The goal of **Security Hardening** is to		
	apply the recognized practices of cyber hygiene	1 / Minimum
	improve system protection according to its needs and priorities	2 / Ad-hoc
	employ the well-recognized methods and tools enabling trustworthiness	3 / Consistent
	establish the continuous process of supporting the trustworthiness objectives	4 / Formalized

Table 10-1: Comprehensiveness Level Definition Guide

This guide recommends for consideration the following typical needs corresponding to the comprehensiveness levels for subdomains.

Strategy and Governance refers to the need for		
	vision, scope and security objectives	1 / Minimum
	the most appropriate best practices	2 / Ad-hoc
	well-recognized approaches and standards	3 / Consistent
	support of business processes, legal, operational, and other issues	4 / Formalized
Threat Modeling and Risk Assessment refers to the need for		
	review of current threat landscape	1 / Minimum
	understanding the system and technology vulnerabilities	2 / Ad-hoc
	comprehensive description of relevant risks	3 / Consistent
	a holistic and systematic approach to risk management	4 / Formalized
Supply Chain and External Dependencies Management refers to the need for		
	a reputation check for suppliers and contractors	1 / Minimum
	security assurance artifacts for the supply chain	2 / Ad-hoc
	certificates and other guarantees by trusted authorities	3 / Consistent
	control of exposure to possible harm from suppliers and contractors	4 / Formalized
Identity and Access Management refers to the need for		
	supporting elementary entities for the basic usage scenario	1 / Minimum
	differentiating the actors for the general access scenarios	2 / Ad-hoc
	employing best practices for supporting sophisticated access scenarios	3 / Consistent
	comprehensive protection against the risks connected to unauthorized access	4 / Formalized
Asset Protection refers to the need for		
	accounting for the use of both digital and physical assets	1 / Minimum
	monitoring of the assets on a use case basis	2 / Ad-hoc
	managing and protecting the assets of various types	3 / Consistent
	assurance of the enforcement of asset management policies	4 / Formalized
Data Protection refers to the need for		
	the general maintenance of data confidentiality and integrity	1 / Minimum

	an increased level of assurance for some data	2 / Ad-hoc
	the implementation of recognized data protection policies and methods	3 / Consistent
	assurance of protection of critical business information both in transit and at rest	4 / Formalized
Vulnerability and Patch Management refers to the need for		
	keeping the systems up to date and less prone to attacks	1 / Minimum
	enforcing a regular update policy for critical components	2 / Ad-hoc
	supporting automated updates configured specifically for the case	3 / Consistent
	planning both a regular update process and emergency scenarios for critical zero-days	4 / Formalized
Situational Awareness refers to the need for		
	keeping minimal awareness of the security-related events	1 / Minimum
	specific attention to some kinds of security events	2 / Ad-hoc
	comprehensive monitoring and regular sharing of security related information	3 / Consistent
	providing and managing all information relevant to trustworthiness aspects	4 / Formalized
Event and Incident response, Continuity of Operations refers to the need for		
	checking for system recovery after incidents	1 / Minimum
	ensuring the recovery of separate system components or processes	2 / Ad-hoc
	supporting an automatic recovery procedure where possible and having appropriate reporting	3 / Consistent
	having swift incident response and reducing harm to the business both by technical and organizational means	4 / Formalized

Table 10-2: Comprehensiveness Level Definition Guide

This guide recommends for consideration the following practice purpose definitions corresponding to the comprehensiveness levels for these practices.

The purpose of **Security Program Management** is to		
	describe the general security provisions	1 / Minimum
	reference the relevant security objectives and how they are addressed	2 / Ad-hoc
	cover the general topics of recognized security management standards	3 / Consistent
	implement the clear planning, timely provision and control of security activities	4 / Formalized
The purpose of **Compliance Management** is to		
	be aware of compliance drivers	1 / Minimum
	consider some optional compliance requirements for implementation	2 / Ad-hoc
	implement obligatory compliance requirements	3 / Consistent
	monitor evolving standard requirements for compliance	4 / Formalized
The purpose of **Threat Modeling** is to		
	refer to general IT security issues as threats	1 / Minimum
	identify and describe threats in an ad-hoc manner	2 / Ad-hoc
	describe and classify threats in an accurate (optionally formal) way	3 / Consistent
	reveal and clearly describe IT factors both known and specific that may put the system at risk	4 / Formalized
The purpose of **Risk Attitude** is to		
	informally define the notion of risk	1 / Minimum
	differentiate the importance of risks	2 / Ad-hoc
	measure and appropriately manage the risks	3 / Consistent
	use a risk management framework and processes	4 / Formalized
The purpose of **Product Supply Chain Risk Management** is to		
	monitor the vulnerabilities and patches for the supplied components	1 / Minimum
	implement some security testing for the supplied components	2 / Ad-hoc
	obtain certificates or other security assurance artifacts for the essential components	3 / Consistent
	apply a supply chain risk management policy	4 / Formalized
The purpose of **Services Third-Party Dependencies Management** is to		
	monitor the reputation of contractors	1 / Minimum
	provide for quality of services through contractual agreements	2 / Ad-hoc

	obtain third-party evidence of the service quality	3 / Consistent
	apply as uniform trustworthiness management policy to contractors	4 / Formalized
The purpose of **Establishing and Maintaining Identities** is to		
	maintain one or several accounts in the same or a very similar way	1 / Minimum
	manage the identities for several groups of people, systems or things	2 / Ad-hoc
	support a diverse range of identities leveraging automated mechanisms	3 / Consistent
	maintain and control the use of identities of people, systems and things throughout their lifecycle	4 / Formalized
The purpose of **Access Control** is to		
	only constrain the ability of external agents to access the system	1 / Minimum
	consider the role of the subject and control the appropriate access rights	2 / Ad-hoc
	Use available access control policies with a proper level of assurance	3 / Consistent
	maintain an authorization scheme strictly aligned with business needs and constraints	4 / Formalized
The purpose of **Asset, Change and Configuration Management** is to		
	track the infrequent changes in assets and configurations	1 / Minimum
	follow some specific rules to manage possible changes to the system	2 / Ad-hoc
	support change management procedures for the number of assets and/or configurations	3 / Consistent
	regulate the process for the lifecycle of assets from provisioning to replacement, including emergency changes	4 / Formalized
The purpose of **Physical Protection** is to		
	generally constrain the access to physical assets	1 / Minimum
	customize the access constraints to consider time and manner of physical access	2 / Ad-hoc
	automate adjustable physical access control using specific identity tokens	3 / Consistent
	address all aspects of physical security and safety, prevent theft, and ensure ongoing safe operation	4 / Formalized
The purpose of **Security Model and Policy for Data** is to		
	declare that data should be protected from unauthorized access	1 / Minimum
	set simple data categorization and appropriate constraints	2 / Ad-hoc

	define the particular approach and roles/attributes for controlling the access to data	3 / Consistent
	categorize and consistently protect the data according to the requirements of stakeholders	4 / Formalized
The purpose of **Implementation of Data Protection Controls** is to		
	take advantage of built-in protection controls (OS, network, services)	1 / Minimum
	configure built-in controls and ensure that their usage fits the data protection goals	2 / Ad-hoc
	support the proper application of data controls according to recognized standards	3 / Consistent
	ensure the required protection of each data item both in transit and at rest	4 / Formalized
The purpose of **Vulnerability Assessment** is to		
	consider whether widely known vulnerabilities are relevant to the system	1 / Minimum
	check whether the specified components are prone to attacks	2 / Ad-hoc
	get an objective third-party evaluation of vulnerabilities and exposures	3 / Consistent
	perform regular deep customized security inspections	4 / Formalized
The purpose of **Patch Management** is to		
	consider the security advisories issued by vendors and install the appropriate patches	1 / Minimum
	check that specified components are protected against the most probable attacks	2 / Ad-hoc
	establish automatic update procedures where possible	3 / Consistent
	enforce a system policy to guarantee the continuous protection against known attacks	4 / Formalized
The purpose of **Monitoring Practice** is to		
	from time to time check the system logs for diagnostic purposes	1 / Minimum
	periodically check events indicating how properly the critical processes execute	2 / Ad-hoc
	collect and analyze security relevant information both with built-in and specifically designed tools	3 / Consistent
	act as catalyst and capacity-builder for the continuous system protection	4 / Formalized
The purpose of **Situation Awareness and Information Sharing** is to		
	obtain some relevant external information on an ad-hoc basis	1 / Minimum

	enable personnel to consistently use relevant external information feeds	2 / Ad-hoc
	consider on a case basis sharing internal data with authorities and community	3 / Consistent
	establish a two-way sharing of zero-days and incidents across the industry	4 / Formalized
The purpose of **Event Detection and Response Plan** is to		
	define specific incidents and basic actions to react	1 / Minimum
	provide guidance for critical components on how to detect and respond to incidents	2 / Ad-hoc
	set up the basis for automatic execution of response procedures	3 / Consistent
	create controls to detect incidents, assign them for investigation and escalate as needed	4 / Formalized
The purpose of **Remediation, Recovery, and Continuity of Operations** is to		
	give basic instructions for system recovery	1 / Minimum
	handle known incidents and check whether the system is completely recovered	2 / Ad-hoc
	Enable automatic execution of remediation and recovery procedures	3 / Consistent
	support a combination of both technical and organizational measures facilitating quick system recovery	4 / Formalized

Table 10-3: Comprehensiveness Level Definition Guide

Part IV: Case Studies

To increase the usefulness of the SMM, we include several case studies for:

- a smarter data-driven bottling line,
- an automotive gateway supporting OTA updates and
- consumer (residential) security cameras.

The organization of the case study material is consistent, as described below.

11 Case Study Approach

Each case study presents the relevant use case descriptions, SMM profiles and explanation of the identification of comprehensiveness levels and scope for each domain, subdomain and practice. The explanation of the purpose and form of the content is not repeated in the case studies.

Each case study is organized as follows:

- Case study background and problem description.
- Factors to consider in the case study system analysis.
- The prioritization of the security domains.
- The security needs for subdomains.
- How to validate the purpose of security practices.

11.1 Case Study Background and Problem Description

Each case study starts with the description of its background, the problem the SMM aims to solve and the approach taken. This is followed by a section on establishing the security maturity target.

11.2 Factors to Consider in the Case Study System Analysis

To apply the security maturity model, analyze use cases to determine the relevant concerns, risks, and constraints and identify and describe all security assumptions, goals, and requirements. Then prioritize activities and perform a security maturity evaluation and enhancement.

The analysis of a new or an existing deployed system should consider the following factors:

Size and coverage: Estimate how big the organization or system is, or how many consumers will have access to the device, solution or system under examination.

Exposure: Estimate how many kinds of external connections exist and how they might be compromised. Enumerate the external connections. Find out whether there are security vulnerabilities or natural exposures for similar systems or organizations.

Threat landscape: Evaluate the threat environment, the types of threat actors, and how aggressive the threat actors in the environment for the given system are.

Best practices: Find out whether there are known best practices for improving security for similar systems or organizations.

Experience. Find out whether there are known security incidents for similar systems or organizations.

Urgency: Evaluate the urgency of threats and risks and prioritize according to urgency.

Threat impact: Consider the extent of consequences related to the threats. Do they affect safety, the environment, community or "only" production? Trustworthiness aspects such as safety and privacy should be considered.

Constraints: Identify the constraints that functional and non-functional requirements may pose on the implementation of security practices. Evaluate the trade-offs.

Trust: How many people require extended privileges to enable the system to function and how does this vary during the lifecycle of the project (during installation, maintenance, everyday work, etc.)? How many people have physical and other privileged access to sensitive physical components or sensitive information? What are the identity management requirements? How is trust in people established and managed?

Timeline: Establish times and expected results for every milestone and plan for a repeated improvement lifecycle.

Expected results: Articulate the goals of the security maturity evaluation and enhancement.

Dependencies: Outline project dependencies, including the specifics of the interdependencies of the security functions to be implemented.

11.3 Prioritizing the Security Domains

Once a clearly written description of all the assumptions, goals, and requirements of the system has been created, the next step is to evaluate the priority and goals for the security maturity domains. The idea is to set up a basic comprehensiveness level for each domain (governance, enablement and hardening) according to the general goal connected to the appropriate type of activities. This comprehensiveness level may then be increased for certain subdomains and practices but should not be decreased to maintain the domain level at the target.

Similarly, the scope should be defined with clarity on whether the general scope is acceptable or an industry- or system-specific scope is necessary. The scope may then be tailored for subdomains and practices as appropriate. The rationale should be documented.

The comprehensiveness levels for each domain correspond to the general goals as follows:

For the security governance domain:

- Follow general basic security considerations (minimum level).
- Implement security measures based on requirements (ad hoc level).
- Facilitate implementation of consistent security capabilities (consistent level).
- Establish a clear governance structure and associated processes (formalized level).

For the security enablement domain

- Enable the use of some security controls (minimum level).
- Implement security controls according to known security scenarios (ad hoc level).
- Employ both built-in and additional mechanisms to cover the known risks (consistent level).
- Establish a process to address risks by the best available means (formalized level).

For the security hardening domain:

- Apply recognized practices of cyberphysical hygiene (minimum level).
- Improve system protection according to its particular needs and priorities (ad hoc level).
- Employ well-recognized methods and tools for enabling trustworthiness (consistent level).
- Establish a continuous process of supporting the trustworthiness objectives (formalized level).

These domain comprehensiveness-level definitions also apply to subdomains and practices and are relevant when considering the security needs for subdomains and the purpose of every security practice.

11.4 Validating the Security Needs for Subdomains and Practices

Once the goals and corresponding comprehensiveness levels have been established for the domains, the target comprehensiveness for the subdomains should be reviewed and enhanced as appropriate. The scope of the subdomains should also be reviewed. This validation is based on the *Comprehensiveness Level Definition Guide* using the following questions:

For security needs for governance:

- How can the needs for security strategy and governance be described?
- How can the needs for threat modeling and risk assessment be described?
- How can the needs for supply chain and external dependencies management be described?

For security needs for enablement:

- How can the needs for identity and access management be described?
- How can the needs for asset protection be described?
- How can the needs for data protection be described?

For security needs for hardening:

- How can the needs for vulnerability and patch management be described?
- How can the needs for situational awareness be described?
- How can the needs for event and incident response, continuity management be described?

Validating the purpose of security practices: After validating the security needs corresponding to the subdomains, the purpose of every security practice should be reviewed to validate the target comprehensiveness and scope for practices implementation or change them. This validation is based on the *Comprehensiveness Level Definition Guide* using the following questions:

- What is the purpose of security program management?
- What is the purpose of compliance management?
- What is the purpose of threat modeling?
- What is the purpose of setting out the risk attitude?
- What is the purpose of product supply-chain risk management?
- What is the purpose of services third-party dependencies management?
- What is the purpose of establishing and maintaining identities?
- What is the purpose of access control?
- What is the purpose of asset, change and configuration management?
- What is the purpose of physical protection?
- What is the purpose of establishing the protection model and policy for data?
- What is the purpose of implementation of data protection practices?
- What is the purpose of vulnerability assessment?
- What is the purpose of patch management?
- What is the purpose of security audit?
- What is the purpose of information sharing and communication?
- What is the purpose of an event detection and response plan?
- What is the purpose of supporting remediation, recovery, and continuity of operations?

12 Case Study 1: Smarter Data-Driven Bottling Line

The goal for the project is to reduce operating costs and increase efficiency of a legacy bottling line through adaptive management of production output.

12.1 Background, Problem Description and Approach Using SMM

A mid-tier system integrator implements solutions for beverage production lines. The integrator is proud of their packaging expertise and technical know-how in this area. Their solutions are efficient, robust, reliable and easy to operate. They currently provide maintenance and support to their customers.

Now the time has come to propose something completely new: a single platform for monitoring all phases of the operating cycle (including sale, delivery and return of final product), business performance tracking, reporting and analytics. The declared objective is to implement and maintain an adjustable production cycle depending on the past and ongoing requests from purchasers, return percentage, seasonal changes and new marketing opportunities.

They use barcode and RFID scanners to track the incoming raw materials, production batches, packaged product and particular shipments. Scanners are used with legacy equipment to provide live tracking, operational support, reporting and analytics for ongoing business decisions.

As the system integrator does not have much IT experience, they engage an outsourcing company for development of the portal. A key function is to provide an easy-to-use platform for monitoring business operations that includes the technological process. It is customizable to some extent and may be supplemented with additional applications, such as performance tracking, quality monitoring, order and returns management, maintenance, fleet management and extensions for marketing research.

The various applications use data from sensors at the production line and may also control the parameters of the process. The portal is available remotely via the Internet, so security is a concern regarding possible impact on the production line.

The business-level stakeholders at the integrating company have to establish the appropriate security requirements for the platform and the applications that will run on it. They use the SMM for describing their concerns. With the help of an outside security architect developing the platform and various applications, these concerns are formulated as security objectives.

12.2 Factors to Consider in the Case Study System Analysis

- The system integrator considers the solution that would be used by its major clients and would attract new customers who want to enhance the efficiency and operational agility of their manufacturing processes. The planned number of installations would grow from a few dozen in the first year up to perhaps two hundred in three years. The preferred relationship with customers is to supply a solution with a long-term contractual commitment for its support and maintenance. The implementation of practices may be provided by third parties while the integrator establishes appropriate requirements and makes the appropriate security tradeoffs against costs and other concerns.

- The most likely security vulnerabilities and attacks are expected to be on the software and external services, such as the commercial off-the-shelf operating system that may have vulnerabilities exploited by malware. As the production line becomes connected, these vulnerabilities are exposed to the external world.
- The threat environment is typical for connected manufacturing. For computers that are part of the manufacturing infrastructure, the internet remains the main source of attacks and risks of malware infections.
- Best practices for the target environment include network segmentation, using firewalls, keeping the passwords for the operators' machines and servers secure, and installing software patches as they are issued or at least once a month.
- While targeted attacks for the food and beverage manufacturing are not be relevant, typical attacks (e.g., *WannaCry* malware) have already hurt similar environments.
- The urgency of risks must be determined according to their effect on the execution and availability of main services. From this perspective, prevention and prompt incident response play major roles in security processes.
- While safety remains a concern for any manufacturing plant, an important focus of security is on service availability and the integrity of the process. Personnel safety is supported by traditional approaches such as safety instructions but should be considered as the solution is developed. Safety of the product is supported by maintaining process integrity. Privacy is not an issue for this application as it does not work with personal data.
- The typical constraint on security practices is the necessity of integration with (usually) brownfield environment that may not support some necessary practices. The system integrator considers the risks and trade-offs and will provide procedures for risk acceptance when appropriate.
- As the production line gets smarter, planning and design of the system should include the active involvement of service providers to ensure the security and overall trustworthiness of the system. This requires a clear understanding of the typical process, the adjustable parameters and the maximum level of trust that would be assigned to each service.

12.3 Prioritizing the Security Domains

Security governance: The goal for governance is to establish governance practices based on the needs of the typical use cases for the beverage production line. The governance scenarios require alignment with specific needs of smart manufacturing. Therefore, the basic comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

Security enablement: The goal for security enablement is to implement security controls to known use cases. There are no industry- or system-specific requirements; general techniques like password-based authentication and separation of privilege fit the needs. The basic comprehensiveness level is 2, *ad hoc* and the scope is *general*.

Security hardening: The goal is to address the risks arising from connecting to the internet. This requires particular attention to hardening practices such as timely software patching, periodic security audits, maintenance and prompt incident response. There are some Industry-level requirements but not across the board. We have the comprehensiveness level 2, *ad hoc* and *general* scope (which would grow to *general+* as industry-specific scope is assigned to the particular practices).

The initial diagram for the priorities across the domains is shown below.

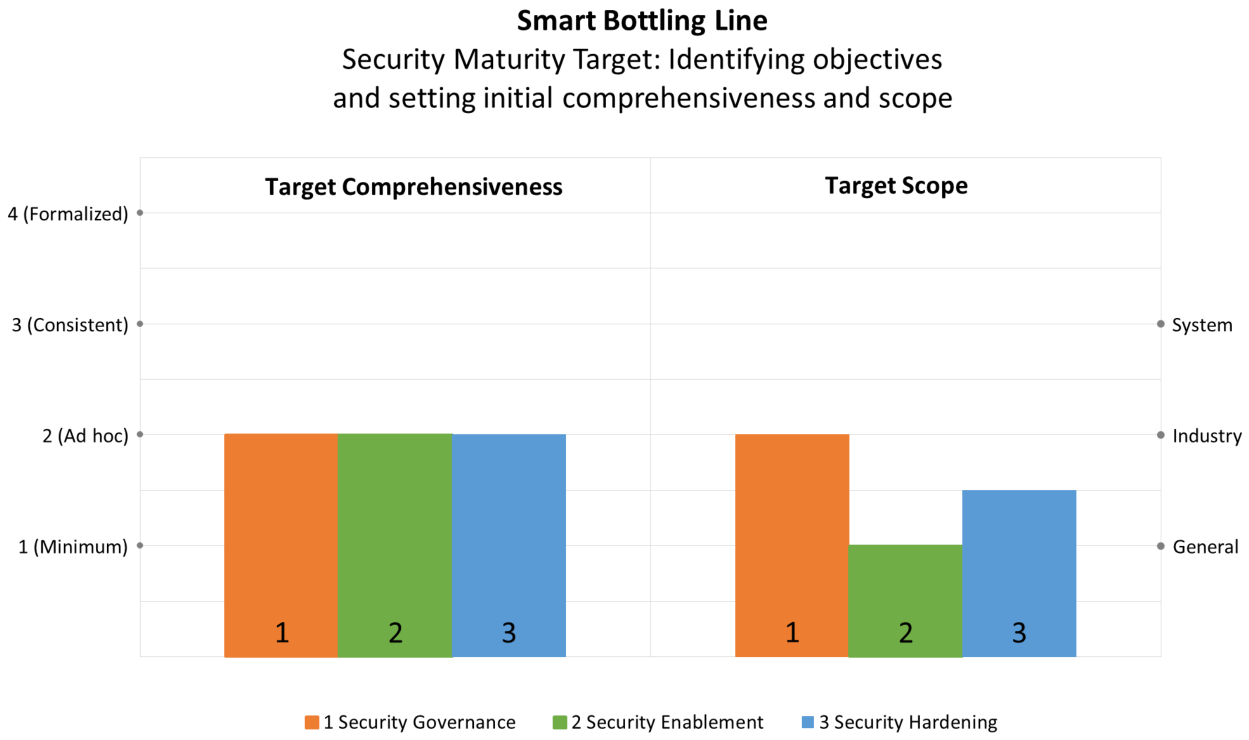


Figure 12-1: Initial target values for security domains

12.4 Considering the Security Needs for Subdomains

12.4.1 Security Needs for Governance

Strategy and governance are guided by the most appropriate best practices. The comprehensiveness level remains 2 and the scope remains *industry* as for the corresponding domain.

Threat modeling and risk assessment for smart manufacturing needs to take into consideration the risks for manufacturing process. To make the threat model and the appropriate risk definitions consistent the analyst uses the tools and methods for investigating the exposures and flaws of the typical solution deployment. Thus, the comprehensiveness level for this subdomain is 3 and the scope remains *industry*. The corresponding domain will be adjusted to the comprehensiveness level 2+ to reflect that some subdomains are greater than 2.

Supply chain and external dependencies management: Using externally provided services and the third-party-supplier networking infrastructure is a source of security risk, but a requirement of security-certification guarantees issued by trusted authorities for all third parties would significantly increase the cost, so the comprehensiveness level remains at 2, with strengthened requirements to some selected providers (depending on risks) leading to a 2+. This is acceptable since remaining risks are covered by hardening practices implemented within the solution and during its support and maintenance. The scope is *industry*.

12.4.2 Security Needs for Enablement

Access management suggests using the typical roles for the definition of responsibilities and allowed access. The set of roles and access control scheme for the installation may slightly change from case to case. This enables using a use case-based approach to access management without the need of enhanced procedures for introducing new roles. Thus, the comprehensiveness level is 2, the scope is *general*.

Asset protection management is a key practice for supporting the reliable and secure functioning of a production line with similar types of assets for different installations. Properly implemented procedures for use, maintenance and support of assets minimize the risks from the majority of threats. Some devices and software are specific to the solution. The comprehensiveness level is 2, the scope is *system specific*. The corresponding domain thus has *general+* scope.

Data protection: Some data for the smart production line affects how the process executes, so integrity and availability of this data is important. These aspects are implemented according to the use case and using general approaches. The comprehensiveness level is 2, the scope is *general*.

12.4.3 Security Needs for Hardening

Vulnerability and patch management is of highest priority given the use of commercial platforms supplemented with custom applications for smart manufacturing. Support of the consistent vulnerability and patch management and specific attention to industry and system vulnerabilities give us the comprehensiveness level 3 and *system* scope. The scope value for the corresponding domain is set to *industry+*.[1]

Situational awareness: Practices for maintaining situational awareness are planned according to the current threat landscape for industrial sector and smart manufacturing in particular. Reports on the current security state for that domain are periodically issued by authoritative agencies, CERTs and security companies. The initial guide for obtaining the information from these sources and its further analysis should underlie the situational awareness approach. The solution should provide the ability to audit security-related events with optional delivery of such reports to the solution support center. The comprehensiveness level is 3, the scope is *industry*.

Event and incident response: Any security incident at the smart production line must be handled immediately as the possible compromise of the process bears significant financial risks and reputation losses. The response process should address the needs of typical manufacturing

[1] Providing software patching as a part of the whole maintenance and support service can be presented as one of the advantages of the "full package" purchase from the system integrator as opposed to just initial installation.

process. The comprehensiveness level is 3, the scope is *industry*. The comprehensiveness level for the corresponding domain is *consistent* and the scope is *industry+*.

The refined security maturity target for subdomains is illustrated by the diagram below.

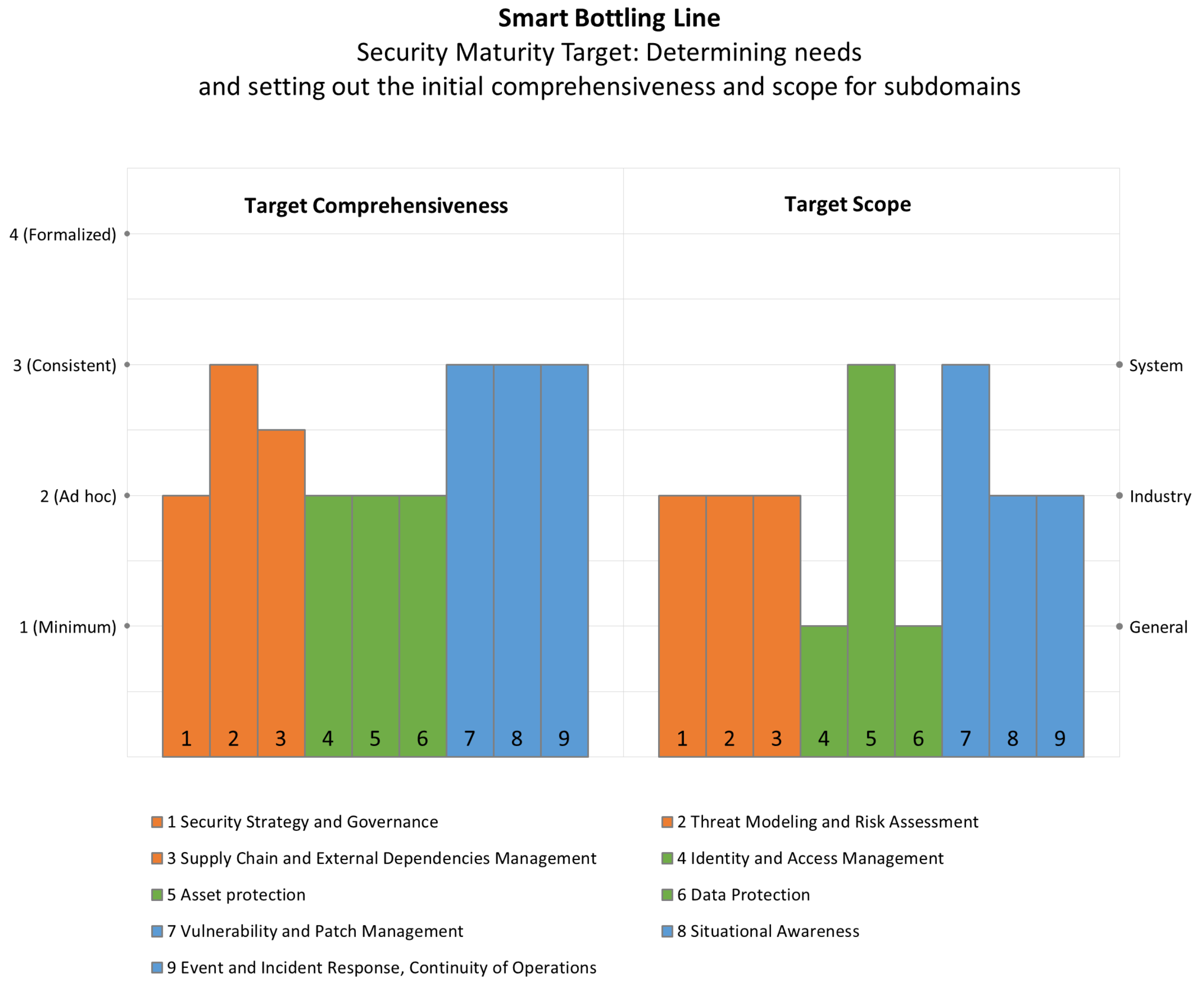


Figure 12-2: Refined target values for security subdomains

12.5 Validating the Purpose of Security Practices

Security program management: The system integrator defines the policies and procedures addressing the security objectives, such as preventing unauthorized control of the line and maintaining the confidentiality of the recipes and know-how. As the implementation of the practice is performed *ad hoc*, the comprehensiveness level remains 2. Since security objectives are not expected to go beyond the needs of similar facilities, the scope remains *industry*.

Compliance management: The system integrator performs the ad hoc assessment for the external compliance with outsourcing of the appropriate assurance activities. The preferred way of providing compliance is through demonstrating evidence of the existing practices correspondence to the compliance requirements. The comprehensiveness level remains 2 and the scope is *industry*.

Threat modeling: The purpose is to describe systematically the threats that may violate the security objectives. The analyst considers the generic landscape and recommendations from security and industry-regulating authorities. Additional sources include consideration of threats for separate assets and boundaries and technology-specific classifications like OWASP Top 10. The comprehensiveness level for this threat modeling is 3 and the scope is *industry*.

Risk attitude: An approach to characterizing risks focuses on the process continuity and integrity. Where possible, a quantitative estimation of risk is performed. The estimation of risk usually depends on the size of facility, production output, internal dependencies and other factors. The other part is elaboration on the strategy for risk mitigation, avoidance or acceptance, and preparing the appropriate procedures. The comprehensiveness level for the practice is 3 and the scope is *industry*.

Product supply chain risk management: The purpose of supply chain risk management is to elaborate the measures taken for every piece of software used as a part of the provided solution. For some components evidence provided by third parties may be required (e.g., certification results). These cases must be documented and controlled contractually. The comprehensiveness level for the practice is 2+, and the scope is *industry*.

Third-party dependencies management: The purpose of the practice is to establish and manage the quality and security commitments for the service-level agreements storing and exchanging the information in cloud and hosting the web services by external providers. Some guarantees may require confirmation of third parties (issued by third parties licenses or certificates), some may be provided by service supplier. The comprehensiveness level for the practice is 2+, and the scope is *industry*.

Establishing and maintaining identities: The purpose of establishing and maintaining identities for the portal is to identify the typical roles for the system managing and controlling the manufacturing process. These procedures are implemented in a way similar to any IT system. The comprehensiveness level for the practice is 2, the scope is *general*.

Access control: The purpose of access control practice is to restrict the access of unauthorized people or systems. Documenting and assessing variously implemented access controls are necessary for timely identification of the weakest links in the solution perimeter. Finally, all controls should be managed consistently. The comprehensiveness level for the practice is 3, the scope is *general*.

Asset, change and configuration management: The purpose of this practice is to tailor the solution for every given installation to maximize efficiency. While the solution remains the same, the asset, change and configuration management implementation will be different from case to case. The assets and some software are specific to the solution. The comprehensiveness level is 2, the scope is *system specific*.

Physical protection is intended to withstand direct attacks on the system by physical means. This includes physical damage and more complicated attacks such as forging RFID labels. The practice should be implemented by traditional means and the protection scenarios are case-based so the comprehensiveness level is 3 and the scope is *system specific*.

Security model and policy for data classifies the data valuable to the manufacturing process and considers how important its confidentiality and integrity are at different stages of the process. The classification is case-based. The comprehensiveness level remains 2 and the scope is *general*.

The purpose of *implementation of data protection controls* is to apply widely accepted mechanisms such as data encryption or controlling the access to data storage. Most built-in controls in COTS software are sufficient to support the required level of assurance. The comprehensiveness level remains 2 and the scope is *general*.

The purpose of *vulnerability assessment* is to perform holistic vulnerability analysis of the system using automation and third-party evaluations. The important role for the system plays the absence of specific flaws, which may allow fraud. The systematic approach and specific security test cases lead to the level 3 *consistent* comprehensiveness and *system* scope for this practice.

The purpose of *patch management* is to implement a centralized and automated process for patch updates for COTS components, manufacturing firmware and software and specifically designed components that make the solution “smart”. The comprehensiveness level is 3 and the scope is *industry*.

The purpose of *auditing* is to record security related events with optional delivery of reports to the solution support center. For this purpose, information from various monitoring sources are consolidated and managed holistically, including the process-related events. The comprehensiveness level is 3 and the scope is *system*. The scope for the upper subdomain and domain is *industry+*.

The purpose of *information sharing and communication* is to learn about vulnerabilities, threat landscape and external incidents. This includes maintaining subscriptions to security advisories, mailing lists of vendors and sector communities to keep the situational awareness about security issues. The comprehensiveness level is 3 and the scope is *industry*.

The purpose of an *event detection and response plan* is a unified cycle of incident detection, response, and support of operations continuity across all installations. This requires automated notification about the security incident including all relevant information delivered to those who are responsible for system recovery, remediation and maintaining continuous system operation. The comprehensiveness level is 3, the scope is *industry*.

The measures for the *remediation and recovery and continuity of operations* after the incident at the manufacturing line must be regulated by the instructions and guidelines and inspired by the industry practices. The comprehensiveness level is 3 and the scope is *industry*.

The detailed security maturity target at the level of required practices implementation maturity is shown at the diagram below.

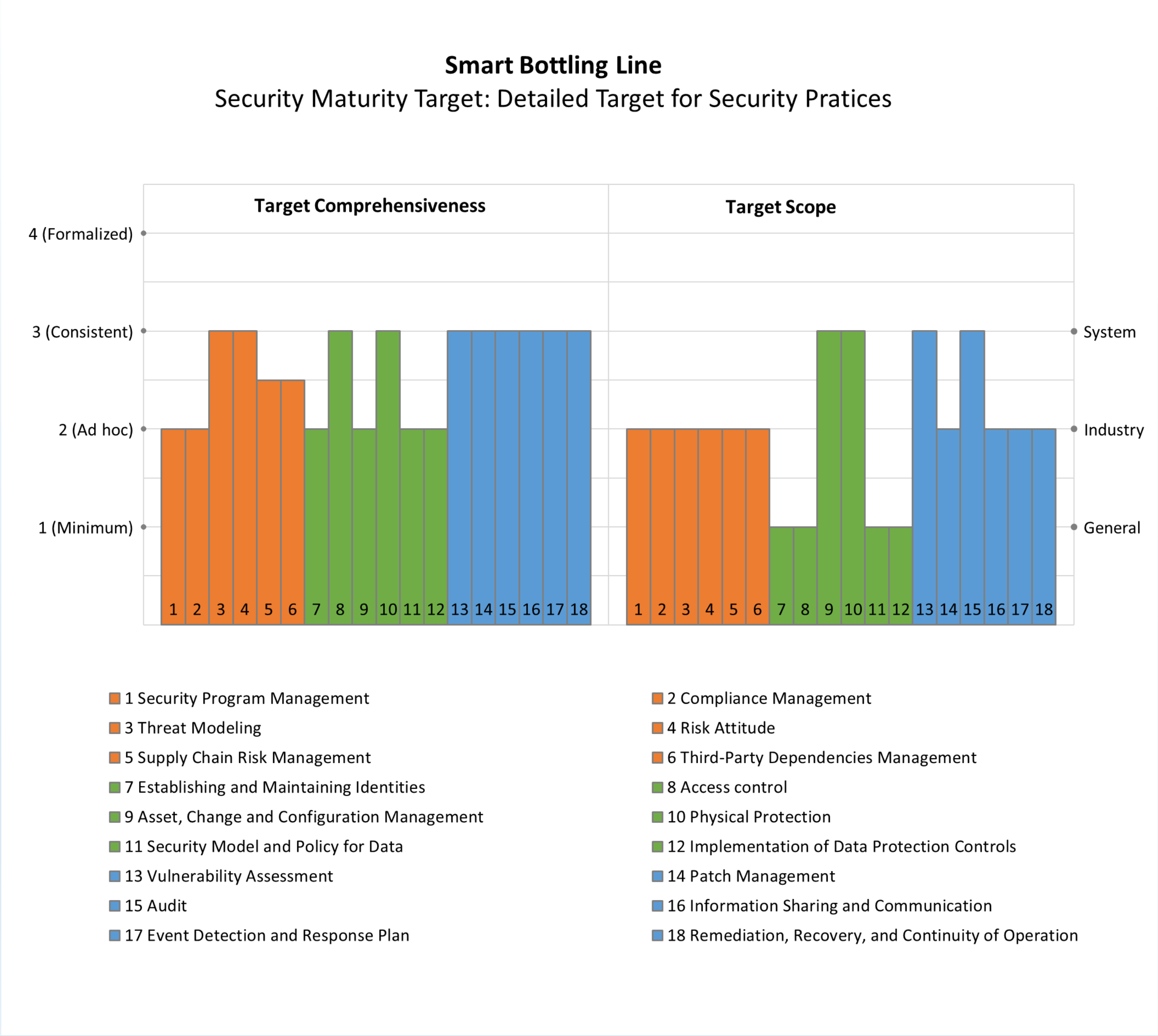


Figure 12-3: Target values for the Security Practice

After validation, the security maturity target at the level of domains has changed. The final diagram illustrating the target values for comprehensiveness and scope is shown below.

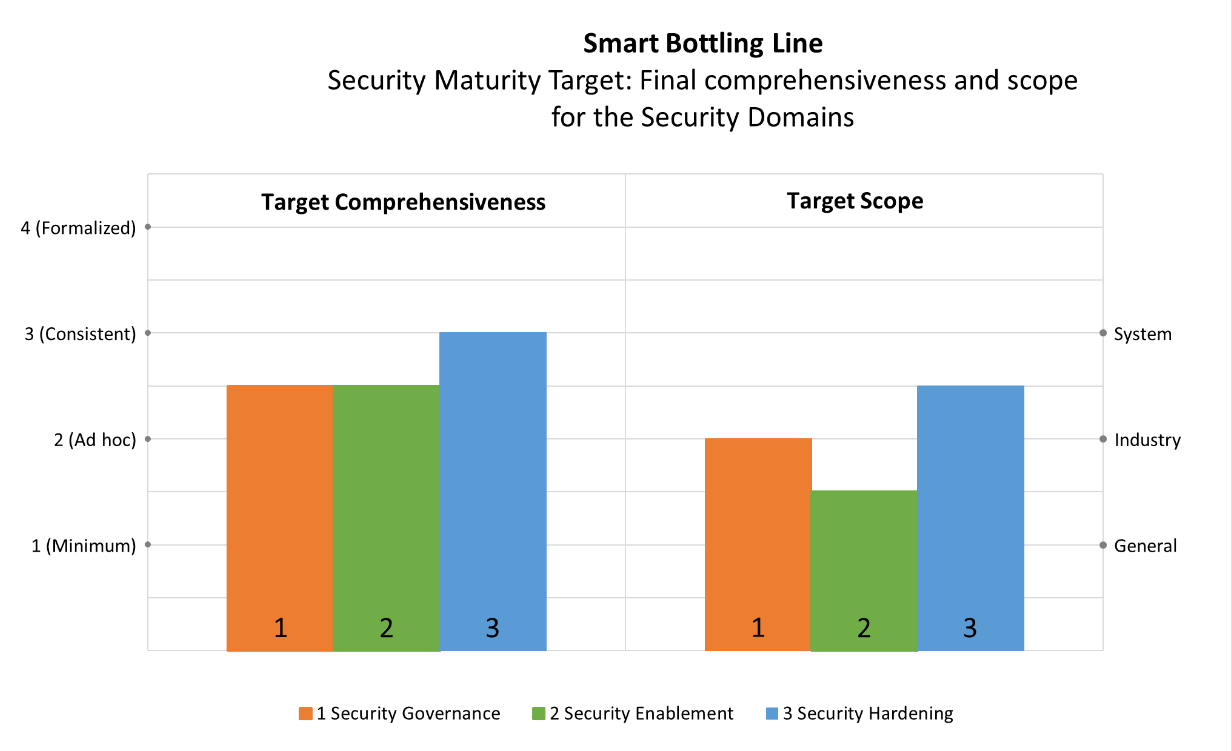


Figure 12-4: Validated security maturity target at the level of security domains

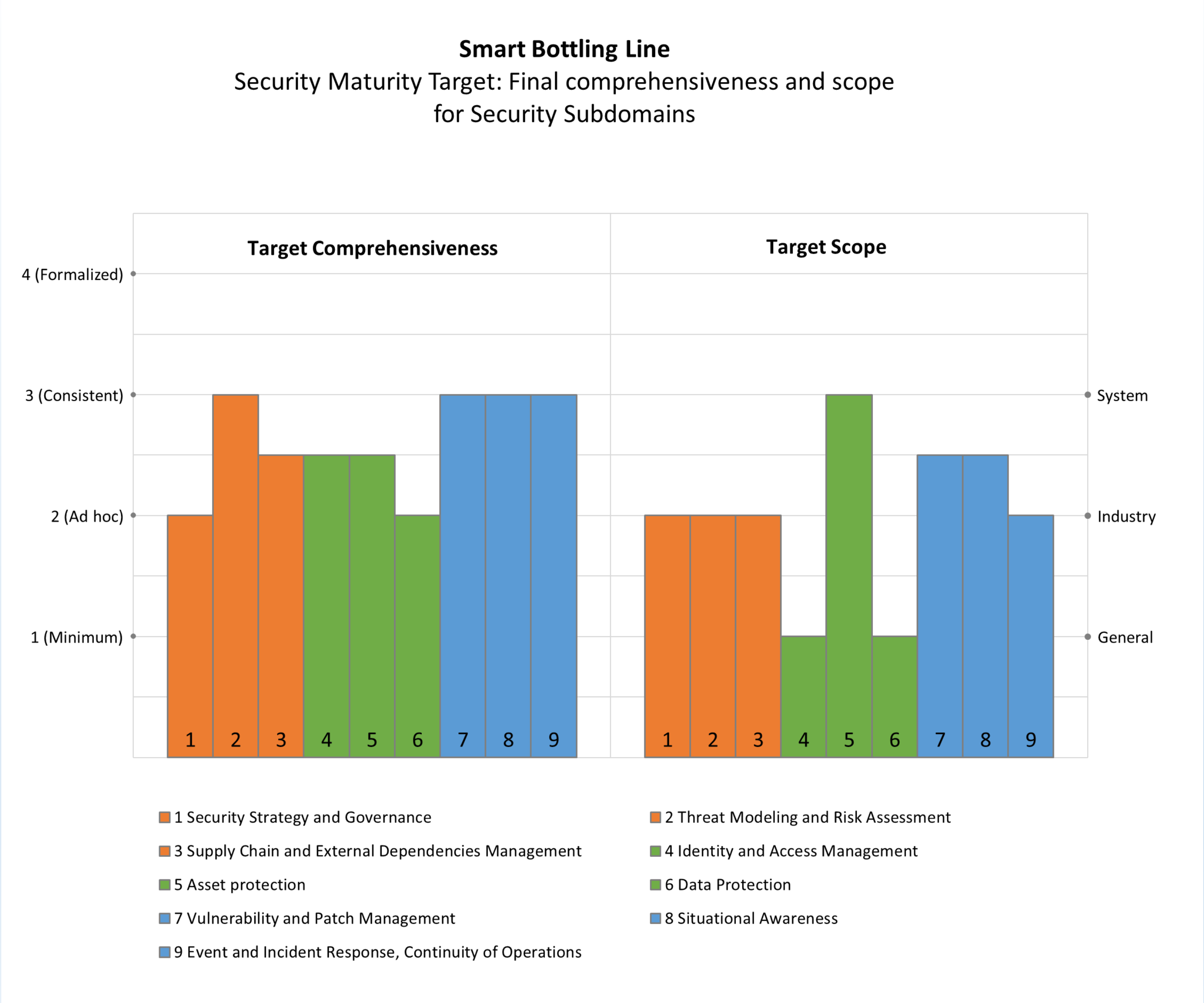


Figure 12-5: Validated security maturity target at the level of security subdomains

The summary of the created security maturity target is given in the table below.

Target	Comprehensiveness	Scope
Security Governance	2 (Ad hoc)+	Industry
Security Strategy and Governance	2 (Ad hoc)	Industry
Security Program Management (P1)	2 (Ad hoc)	Industry
Compliance Management (P2)	2 (Ad hoc)	Industry
Threat Modeling and Risk Assessment	3 (Consistent)	Industry
Threat Modeling (P3)	3 (Consistent)	Industry
Risk Attitude (P4)	3 (Consistent)	Industry
Supply Chain and External Dependencies Management	2 (Ad hoc)+	Industry
Supply Chain Risk Management (P5)	2 (Ad hoc)+	Industry
Third-Party Dependencies Management (P6)	2 (Ad hoc)+	Industry
Security Enablement	2 (Ad hoc)+	General+
Identity and Access Management	2 (Ad hoc)+	General
Establishing and Maintaining Identities (P7)	2 (Ad hoc)	General
Access control (P8)	3 (Consistent)	General
Asset protection	2 (Ad hoc)+	System
Asset, Change and Configuration Management (P9)	2 (Ad hoc)	System
Physical Protection (P10)	3 (Consistent)	System
Data Protection	2 (Ad hoc)	General
Security Model and Policy for Data (P11)	2 (Ad hoc)	General
Implementation of Data Protection Controls (P12)	2 (Ad hoc)	General
Security Hardening	3 (Consistent)	Industry+
Vulnerability and Patch Management	3 (Consistent)	Industry+
Vulnerability Assessment (P13)	3 (Consistent)	System
Patch Management (P14)	3 (Consistent)	Industry
Situational Awareness	3 (Consistent)	Industry+
Audit (P15)	3 (Consistent)	System
Information Sharing and Communication (P16)	3 (Consistent)	Industry
Event and Incident Response, Continuity of Operations	3 (Consistent)	Industry
Event Detection and Response Plan (P17)	3 (Consistent)	Industry
Remediation, Recovery, and Continuity of Operation (P18)	3 (Consistent)	Industry

Table 12-1: Created security maturity target summary

13 CASE STUDY 2: AUTOMOTIVE GATEWAY SUPPORTING OTA UPDATES

The goal for this automotive project is to assess and improve the security for over-the-air (OTA) updates to the in-vehicle firmware and transmission of diagnostic and operational data from on-board systems according to the business concerns of the tier-1 supplier. This should include ongoing support for this security through situational awareness and other dimensions.

13.1 BACKGROUND, PROBLEM DESCRIPTION AND APPROACH USING SMM

The tier-1 automotive supplier implemented the solution for enabling OTA update for ECU firmware and transmitting diagnostic and operational data from on-board systems and components. Motivation for the solution is to enable vehicle connectivity to reduce recall expense for OEMs, shorten response time for clients' calls, continuously improve product quality and operational efficiency, and deliver post-sale vehicle performance and feature enhancements.

As similar solutions were already in the market, the development timeframe was tight and not much attention was paid to security requirements. Now the supplier wants to reconsider the security concerns and check whether it is necessary to add security mechanisms.[1] It is possible to use the OTA update capabilities to improve the security features of already supplied devices.

The tier-1 and interested OEM-level stakeholders discuss the relevant security concerns for the solution. Then the tier-1 supplier developing the solution needs to elaborate the security maturity target covering both technical security measures and organizational support of the proper level of its security and relevant trustworthiness aspects (primarily safety and privacy). Based on this SMM target the developer then conducts a gap analysis for the already supplied samples and provides a roadmap for security enhancement and continuous support of solution trustworthiness. After implementing the appropriate features, the supplier maintains the solution over its usage lifecycle according to established agreements with the OEM.[2]

13.2 FACTORS TO CONSIDER IN THE CASE STUDY SYSTEM ANALYSIS

The main factors affecting the security maturity target for the device begin with objective factors:

Coverage. The device is expected to be installed in vehicles of at least one manufacturer and used around the world.

Exposure. Several vectors for device compromise may be easily identified: through the internet (the channels for images supply), via short-range wireless communication interfaces, via physical access through on-board diagnostics (OBD) interface.

Threat landscape. Currently the interest to the security of connected vehicles is particularly high, and we can expect the attempts of attacks on the device in the wild.

[1] "Adding security" is never ideal since it should be by default and by design.

[2] This prevents the OEM from requiring disproportionate security requirements and enables dialogue about reasonable risk and cost for security.

Relevance. A new type of device intended for connected vehicles. The appropriate area is still under research. Best practices do not exist, and there are no applicable regulatory or standards requirements for security.

Pertinence. The security incidents for this kind of devices were not disclosed. A few security incidents connected to exploiting the flaws in electronic car equipment, or to the failures of this equipment are publicly discussed.

Urgency. Security vulnerabilities of devices of this type are not known. At the same time, the technologies that may be used for its implementation such as securing communications require particular attention.

Threat impact. A successful attack may cause the failure of car equipment or even affect car safety. As we consider the vehicles, individual privacy is also in focus (for example, car tracking).

Constraints. Safety poses constraints on functionality and security. Safety requirements may substantially influence the design and implementation of security practices.

Trust. The trust is distributed. Car service technicians require privileged access to the device for its maintenance. Car owners may also access the device or allow access to unauthorized maintainers. This may require regulation.

Timeline. The time and resources for development, and the resulting cost of the device are constrained due to the increased competition in the market. The timeline is divided into the big stages: prototype, pilot and production, for which the security maturity prioritizing may change.

Expected results. For the prototype it is important to pay attention to designing the security mechanisms according to the expected threats independently of the currently known incidents or technology vulnerabilities. Threat modeling and security enablement practices are prioritized. As the prototyping stage is successfully completed, we adjust the maturity of hardening practices by implementing infrastructure services. Then, for the mass production it is important to regulate the trust by establishing the security program according to the final risk assessment results.

Dependencies. As this is the device of a new kind, hardening practices implementation will rely on enablement practices, and the governance may be used to compensate for flaws associated with excessive trust.

13.3 Prioritizing the Security Domains

Security governance: The goal for governance is to establish the baseline security measures based on use cases for the device. Some governance scenarios may require alignment with industry practices. Therefore, the basic comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

Security enablement: The goal for security enablement is to implement security controls according to the known security scenarios. There are no specific industry-specific requirements for IT security, thus, general techniques may fit the needs of the solution security. The basic comprehensiveness level is 2, *ad hoc* and the scope is *general*.

Security hardening: The goal is to improve the system protection according to its particular needs and priorities. The industry poses constraints on applying additional hardening activities. We have the comprehensiveness level 2, *ad hoc* and *industry* scope.

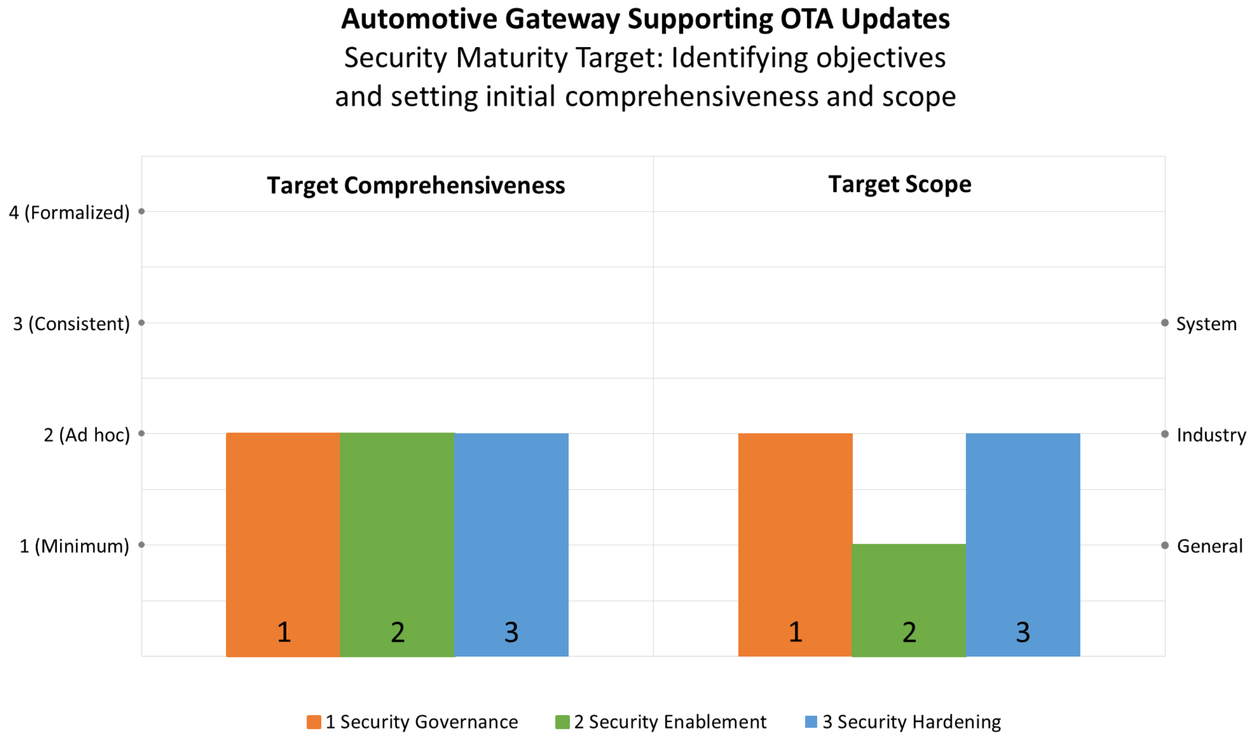


Figure 13-1: Initial target values for security domains for the Automotive Gateway Supporting OTA Updates case study

13.4 Considering the Security Needs for Subdomains

13.4.1 Security Needs for Governance

Strategy and governance are guided by the most appropriate best practices as there no well recognized approaches and security standards for this type of devices. The comprehensiveness level is 2, *ad hoc* and the scope is *industry* as for the upper domain.

Consistent *threat modeling and risk assessment* are important as they help to understand possible system and technology vulnerabilities. The comprehensiveness level is 3, *consistent*. The scope remains *industry*. The comprehensiveness level for the upper security governance domain grows up to 2+.

Supply chain and external dependencies management: As the development of IT-related features of the device is rarely a core activity for a Tier-1 automotive supplier, it will reuse the existing software solutions and involve contractors. Focus on security for these third parties is particularly needed. A use case-based approach works better than IT based certificates or typical policies for supply chain management. The comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

13.4.2 Security Needs for Enablement

Identity and access management: The typical use of the device prescribes the strict regulation of who, how and under what circumstances its functions may be accessed. The set of roles and access control scheme based on this role distribution will not change over time. The use case-based approach for access management is sufficient and does not need enhanced procedures to introduce new identities or change the access control rules. The comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

Asset protection management plays a particular role for device security. Properly implemented procedures for the everyday use, maintenance and repair of the vehicle and control of their enforcement minimizes the risk of the majority of threats. These procedures must be consistent with the car maintenance lifecycle. The comprehensiveness level is 3, *consistent* and the scope is *industry*.

Data protection: As the purpose of the device is to implement over-the-air updates for the ECU firmware it works with at least one kind of sensitive data (firmware update images). The device may also have a unique identifier transferred over the open channels and linked to the owner data, potentially causing privacy issues such as tracking the car. Therefore, the data protection for that device requires a comprehensiveness level increase from 2, *ad hoc* to 3, *consistent*. We set the overall comprehensiveness to 2+ and the scope to *industry*. We also change the comprehensiveness level for the upper security enablement domain to 2+.

13.4.3 Security Needs for Hardening

Vulnerability and patch management: As vulnerable gateways create risks for all the devices for which they provide update services, vulnerability and patch management should be a matter of the utmost priority. The comprehensiveness level is 4, *formalized* and the scope is *industry*.

Situational awareness: Practices keeping the situational awareness are planned according to the current threat landscape and trends in security research of connected vehicles. The main role plays the information sharing and communication across the industry while the security audit for the separate vehicles supports the ongoing security maintenance. The comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

Event and incident response: A security incident is a demonstration of the violation of one or more security objectives. The information of any security incident must be handled immediately as the possible compromise of the devices bears significant reputation risks. The comprehensiveness level is 4, *formalized* and the scope is *industry*. The comprehensiveness for the upper security hardening domain grows up to 2+.

The refined security maturity target for subdomains is illustrated by the diagram below.

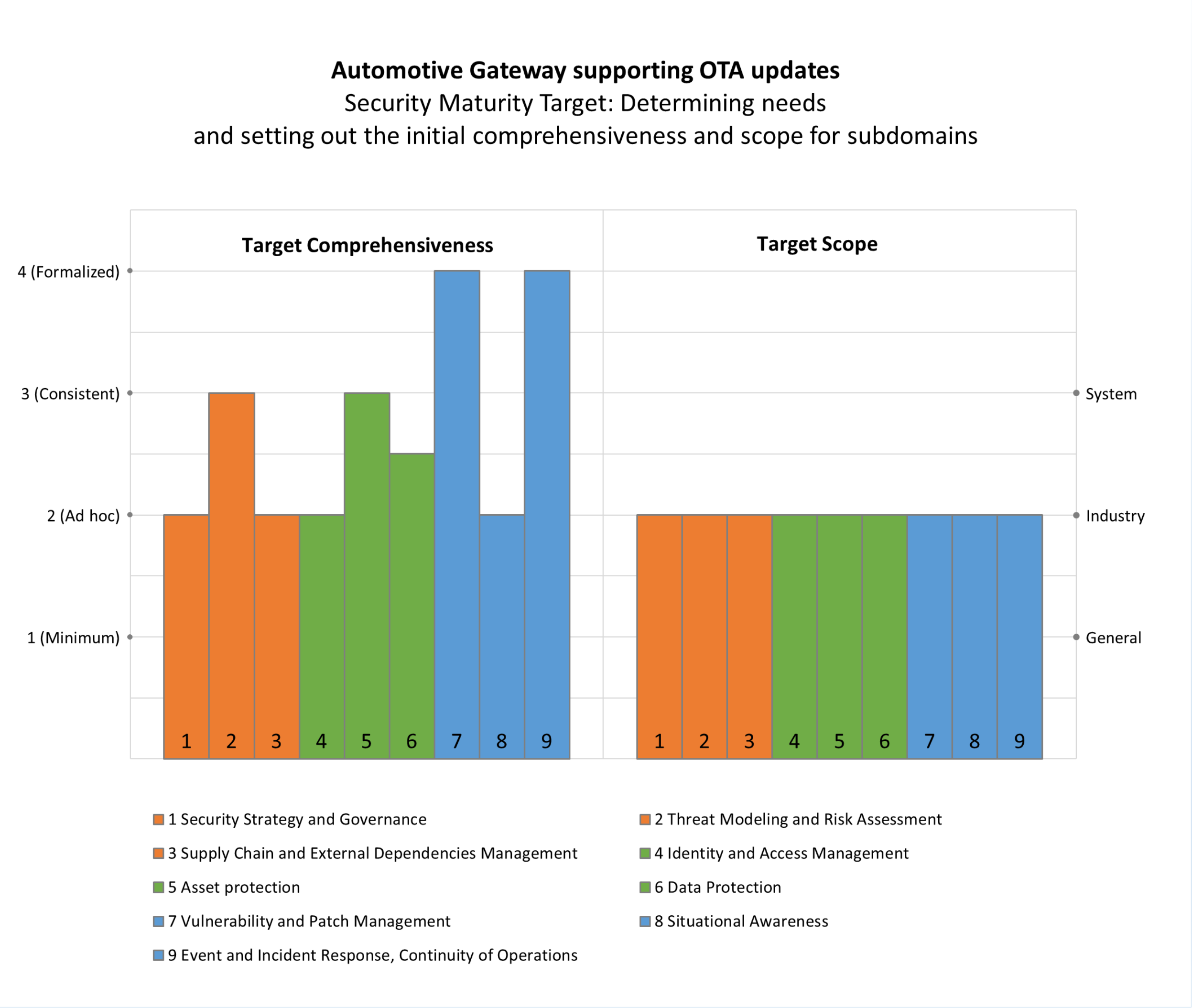


Figure 13-2: Refined target values for security subdomains for the Automotive Gateway Supporting OTA Updates case study

13.5 VALIDATING THE PURPOSE OF SECURITY PRACTICES

Security program management: The purpose of security program management is to provide the vision of what the security should be for this kind of device. As the opportunities provided by the market for the automotive gateway and the appropriate challenges are still under investigation, the stakeholders should focus on the use cases for the device to make the process of establishing the security objectives agile. Premature actions to establish guidelines and processes for security management may hinder prompt changing of the security strategy for the device according to the market response.

The scope is *system* since the risks (such as an unauthorized person taking over control of the car or someone tracking it) are specific to this kind of automotive system. The comprehensiveness level remains 2, *ad hoc* but the scope grows up to *system* level.

Compliance management determines which general and sector-specific standards are applicable, and which level of conformance to these standards is required. At the moment, security standards and regulatory requirements for embedded vehicle devices do not exist. Hence, we consider some requirements from the security standards for embedded devices for optional implementation, tailoring them to the *industry* demands at comprehensiveness level 2 *ad hoc*.

Threat modeling must describe and classify threats in an accurate, optionally formal way. Use the recognized tools and methods to identify and describe all threats reveal the IT factors that may put the system at risk. The threat model must be reconsidered every time the requirements change. This brings us to comprehensiveness level 4, *formalized*. The scope is *system* because of the combination of traditional demands of automotive industry and challenges posed by the newly introduced functions. The upper threat modeling and risk assessment subdomain target levels become 3+ and *industry+*. (The '+' indicates that a subdomain could have one practice at industry scope and another at system scope.)

Risk attitude: The business-level stakeholders need clear understanding of the risk level for all identified threats associated with a device. The risk attitude covers evaluation and measurement, both quantitative and qualitative. The generally accepted approach may be applied to manage them. The approach to evaluating and measuring the risks does not change with the threat model to keep backward compatibility with previous assessments. Thus, the comprehensiveness targets level 3, *consistent*. The scope should be aligned with industry-accepted practices to compare different risks by their severity, so *industry* scope is appropriate.

Product supply chain risk management: Before contracting a supplier, it makes sense to apply well-known approaches such as a search of published vulnerabilities and consider them in view of identified threats. Identify the particular cases to be controlled at the contractual level such as issuing patches for newly discovered vulnerabilities if they pose a particular risk. This is a level 2, *ad hoc* comprehensiveness approach. Product supply chain risk management should follow the industry-accepted practices to simplify the operations, resulting in *industry* scope.

Third-party dependencies management: Third-party threats should be included in the threat model and security policies, and should detail timeframes, commitment for updates, patches, and maintenance of supplied components. This is a comprehensiveness of level 2, *ad hoc*. Dependencies management should follow the industry-accepted practices to simplify the operations, an *industry* scope.

Establishing and maintaining identities: Managing the identities for the device is performed according to the key scenarios defined in the supporting guidelines. The maintenance procedures are implemented in car service only. The unauthorized implementation of such procedures is restricted by the terms of warranty maintenance and repair. The set of identities corresponds to the roles for the industry including car owner, drivers, and authorized personnel of maintenance service and so on, so this is *industry* scope. Since role-based and attribute-based access control models fall under *ad hoc*, comprehensiveness level is 2, *ad hoc* and the scope is *industry*.

Access control: Access to the system functions is performed according to the use case scenarios. Access to the device functions through IT interfaces and through direct connection to on-board diagnostics (OBD) interface is managed separately. This is level 2, *ad hoc,* since it may not be consistent. There is no guarantee that the car owner will not violate the access control. Some access control scenarios require consideration of specific ways to access the device, so this practice implementation is *industry* specific. The upper subdomain grows up to *industry* as well.

Asset, change, and configuration management: During the design and implementation of the device, it is desirable to configure systems to provide only essential capabilities. The developed guidelines for the use, maintenance and repair of the vehicle and its components provide clear instructions and set the warranty and other constraints if these instructions are not followed. The need for a *consistent* approach gives a target of level 3, *consistent*. As the device goes into mass production, the comprehensiveness level may be increased to level 4, *formalized*. The operations prescribed by the practice should be aligned with typical operations for maintenance in the industry, an *industry* scope.

Physical protection: The device and its interfaces must be physically protected from access from the car interior. The device must be tamper-resistant. The personnel of the car service accessing the device to perform the maintenance and repair procedures must have the authorization by the vendor or OEM (depending on the policy of car maintenance). A *consistent* level 3 approach is important. Physical protection and restriction on physical access to the device are to be provided using the regulating principles typical for the automotive industry, so this is *industry* scope. The comprehensiveness level for the upper subdomains grows up to 3+, and for the domain grows up to 2+.

Security model and policy for data: The possibility of tracking the car is a relevant threat, so the data protection policy comprehensiveness level is to be set to level 3, *consistent* to provide privacy. The objectives are specific to the system, so we set the scope level to *system*. Considering the scope of the other subdomain practices, the scope for the upper subdomain and domain are therefore *industry+*.

Implementation of data protection controls follows both general and industry-specific considerations and therefore the scope level is set to *industry*.

As the policy does not change significantly over time and is driven by the use cases, the data protection measures focus on restricting data access, constraining data flow and monitoring data access and use. Regulations do not prescribe specific requirements for such devices but we consider proper implementation of data protection measures as critical for the device promotion at the market; therefore, we set the comprehensiveness level to 2+.

A *vulnerability assessment* before entering the market prevents mitigates the risk that competitors and researchers find previously unknown flaws. Implementation of this assessment by third parties reveals hidden threats and prevents conflicts of interest among developers. This brings us to comprehensiveness level 3, *consistent*. The device is planned to evolve; thus, the vulnerability assessment should be planned regularly. For continuing development after entering the market the comprehensiveness level of vulnerability assessment should be improved to level 4, *formalized*. Vulnerabilities are evaluated and rated according to the system-specific security objectives. Therefore, the scope level for this practice is *system*. The scope level for the upper subdomain and domain grows up to *industry+*.

Patch management, similar to vulnerability assessment, should be established regularly and synchronized with the development lifecycle during the mass production stage. Before entering the market, patches may be managed in an ad hoc way to save time and resources. Patch management addresses issues discovered during testing, security testing and vulnerability assessment phases. This *formalized* approach is level 4. According to the specific requirements of the industry, regular patch management is to be aligned with the automotive industry production V-cycle, resulting in *industry* level for the scope. The upper subdomain gains level 4 comprehensiveness too.

Auditing describes security objectives and identifies threats to provide a base for the identification of events types to be monitored. Deep analysis of monitoring information at a central database from a variety of sources is good during the testing phase; for everyday functioning the amount of data coming from many cars is hard to analyze and store. They may also cause additional issues with privacy. Therefore, we focus on the events that may have most significant impact on normal device functioning. This corresponds to the comprehensiveness level 2, *ad hoc*. As the monitored events are specific to automotive the scope level for this practice is *system*.

Information sharing and communication on the vulnerabilities and threats for the emerging technologies prevent significant risks connected to their use. The proper organization of this process is particularly important for the automotive area where even the unapproved information on possible threat to human safety may cause huge reputational loss. Process-based monitoring and sharing the information among industry peers helps all parties to be better prepared to respond to all kinds of risks. Therefore, the level 4, *formalized* comprehensiveness level is applied here. For information sharing and communication it makes sense to track the news about the trends in automotive industry, incidents, vulnerabilities in design and implementation of protocols for the communication of in-vehicle equipment, newly appeared threats and other security research results for the industry. Thus, the scope is *industry specific*.

Event detection and response plan: The implementation of this practice identifies and classifies security events and describes the requirements to the personnel involved in an incident, the appropriate procedures to be followed, and interaction algorithms and time constraints. Security event response and handling safety incidents are interconnected in an appropriate way. All countermeasures up to the recall of cars are accurately regulated by the established procedures. The comprehensiveness level is 4, *formalized*.

All event response operations should be tailored to the specific risks for the system. Thus, the scope level is *system*. The resulting scope level for the upper domain is *industry+*.

The measures for the *remediation, recovery and continuity of operations* after the incident or device failure are usually taken at the car service. The provided instructions and guidelines must include all procedures including feedback that may help to improve the device. All interactions are made according to the formally defined procedure that may change over time to enhance the experience of all parties and elaborate on the best practices. The operations for remediation, recovery and continuous support are inspired by the industry practices similar to the cases of electronic equipment failure. The comprehensiveness level is 4, *formalized* and the scope is *industry*.

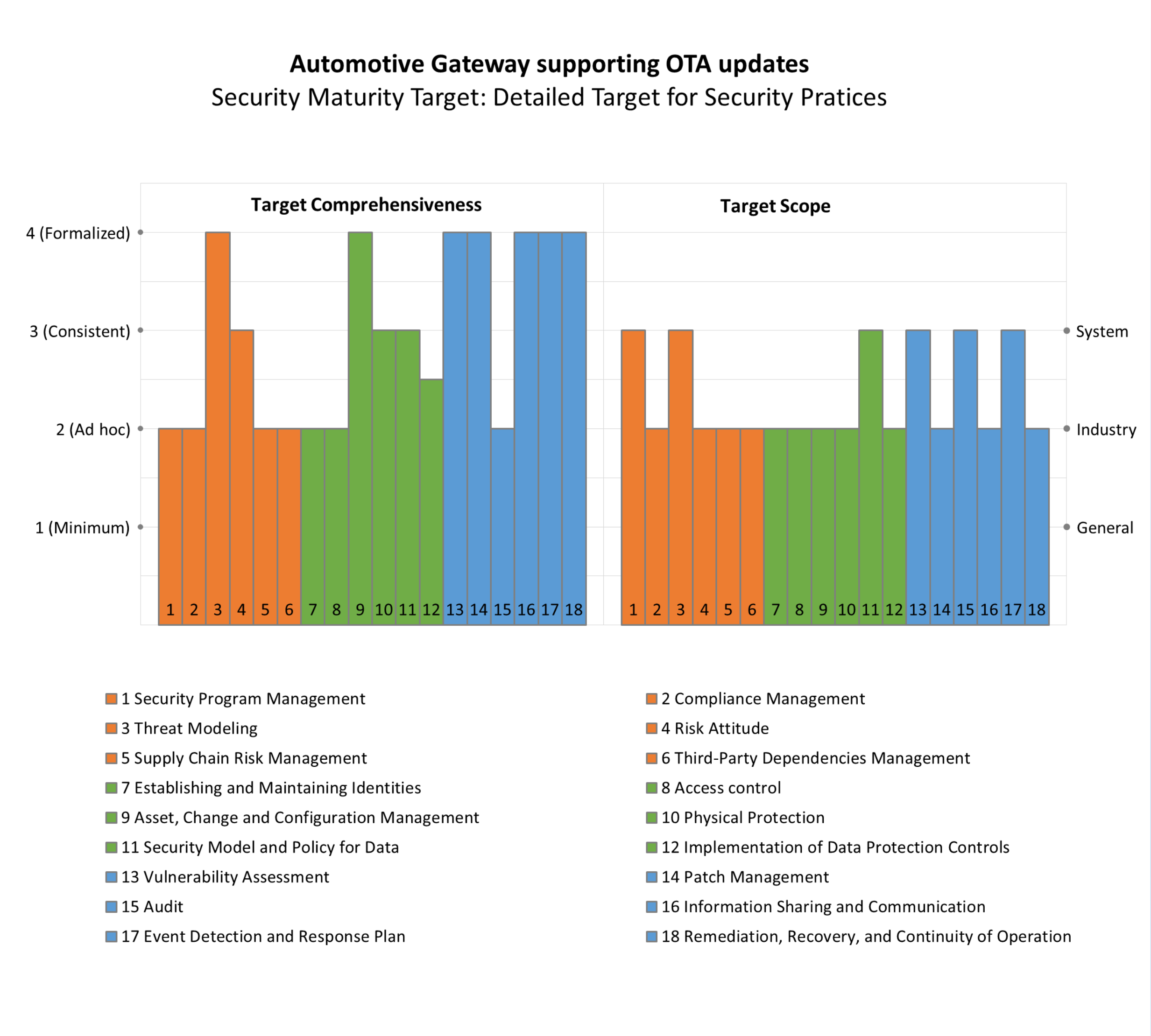


Figure 13-3: Target values for the Security Practices for the Automotive Gateway Supporting OTA Updates case study

After the validation, the security maturity target at the level of domains has changed. The final diagram illustrating the target values for comprehensiveness and scope is shown below.

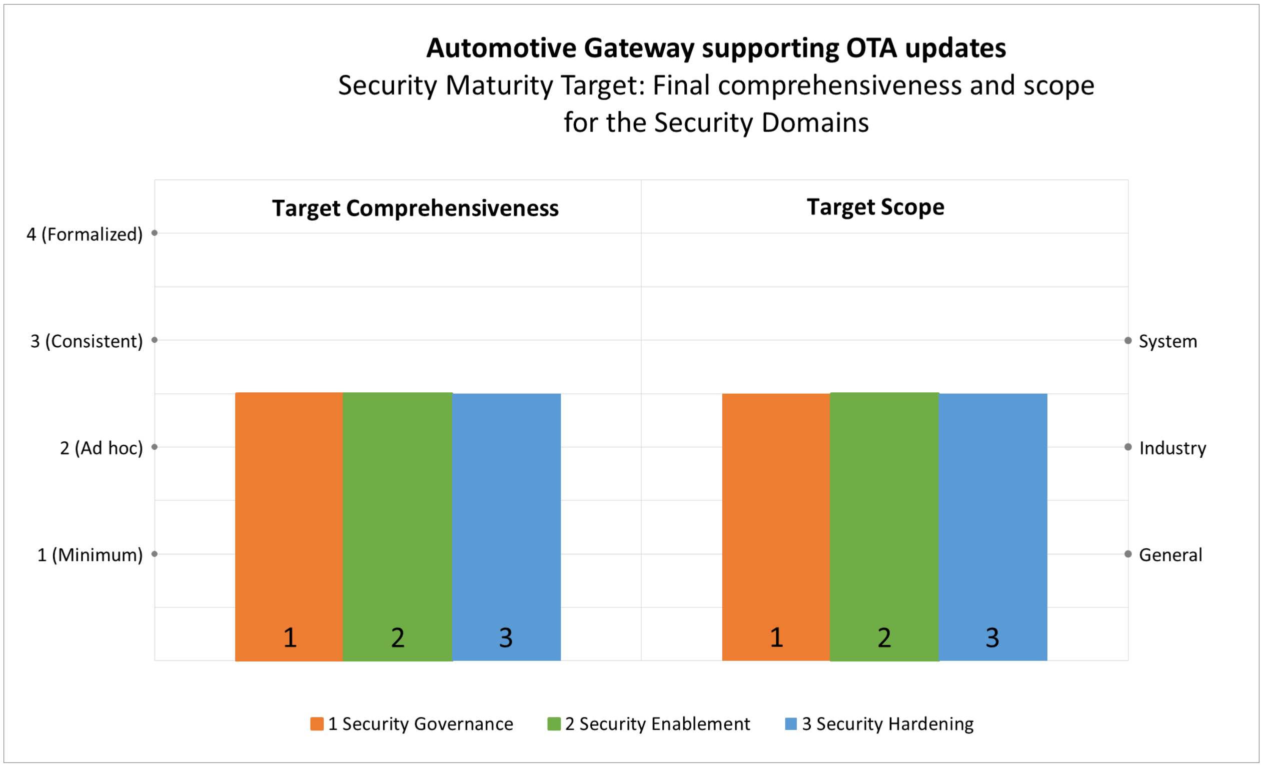


Figure 13-4: Validated security maturity target at the level of security domains for the Automotive Gateway Supporting OTA Updates case study

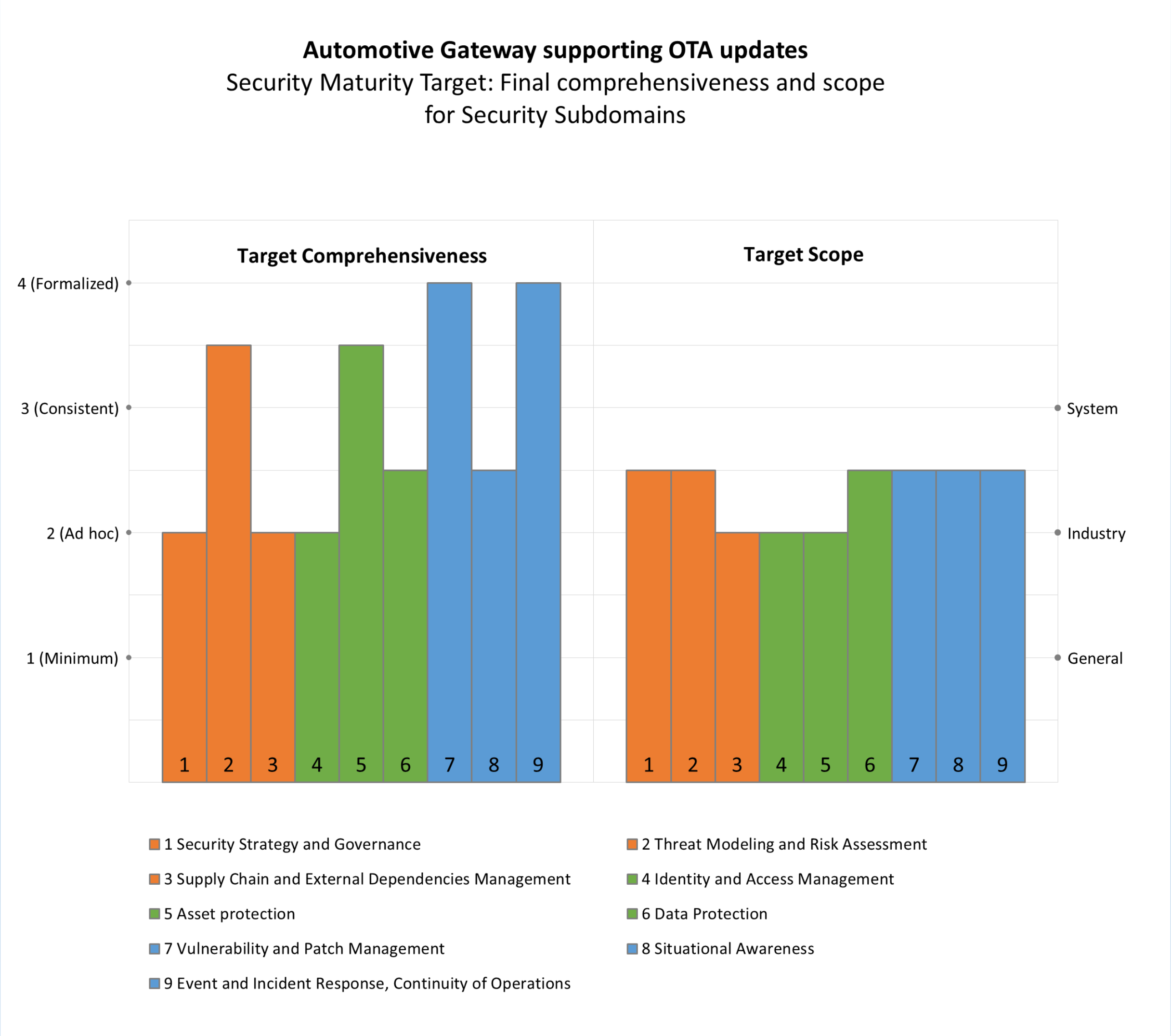


Figure 13-5: Validated security maturity target at the level of security subdomains for the Automotive Gateway Supporting OTA Updates case study

The summary of the created security maturity target is given in the table below.

Target	Comprehensiveness	Scope
Security Governance	2 (Ad hoc)+	Industry+
Security Strategy and Governance	2 (Ad hoc)	Industry+
Security Program Management (P1)	2 (Ad hoc)	System
Compliance Management (P2)	2 (Ad hoc)	Industry
Threat Modeling and Risk Assessment	3 (Consistent)+	Industry+
Threat Modeling (P3)	4 (Formalized)	System
Risk Attitude (P4)	3 (Consistent)	Industry
Supply Chain and External Dependencies Management	2 (Ad hoc)	Industry
Supply Chain Risk Management (P5)	2 (Ad hoc)	Industry
Third-Party Dependencies Management (P6)	2 (Ad hoc)	Industry
Security Enablement	2 (Ad hoc)+	Industry+
Identity and Access Management	2 (Ad hoc)	Industry
Establishing and Maintaining Identities (P7)	2 (Ad hoc)	Industry
Access control (P8)	2 (Ad hoc)	Industry
Asset protection	3 (Consistent)+	Industry
Asset, Change and Configuration Management (P9)	4 (Formalized)	Industry
Physical Protection (P10)	3 (Consistent)	Industry
Data Protection	2 (Ad hoc)+	Industry+
Security Model and Policy for Data (P11)	3 (Consistent)	System
Implementation of Data Protection Controls (P12)	2 (Ad hoc)+	Industry
Security Hardening	2 (Ad hoc)+	Industry+
Vulnerability and Patch Management	4 (Formalized)	Industry+
Vulnerability Assessment (P13)	4 (Formalized)	System
Patch Management (P14)	4 (Formalized)	Industry
Situational Awareness	2 (Ad hoc)+	Industry+
Audit (P15)	2 (Ad hoc)	System
Information Sharing and Communication (P16)	4 (Formalized)	Industry
Event and Incident Response, Continuity of Operations	4 (Formalized)	Industry+
Event Detection and Response Plan (P17)	4 (Formalized)	System
Remediation, Recovery, and Continuity of Operation (P18)	4 (Formalized)	Industry

Table 13-1: Created security maturity target summary

14 Case Study 3: Consumer (Residential) Security Cameras

A producer of IoT security cameras seeks to use the SMM to create an appropriate security program.

14.1 Background, Problem Description and Approach using SMM

The organization performing this SMM benchmark offers a line of security (video) cameras intended to be used in residential settings. The ecosystem includes mobile applications customers can use to view video and control their cameras, and a cloud infrastructure that stores video and relays communication from mobile apps to cameras. While the product line development and marketing were all focused on residential use, the products have also become popular with small businesses.

Having begun life as a startup, the organization is growing and maturing as its customer base expands. As part of that process, the organization wants to build a more mature security program, and that desire was cemented after recent media coverage of security weaknesses in a competitor's products. Previously the organization's security-related efforts have been ad hoc and driven by individuals within the company, rather than being a strategic, company-wide program. The organization has decided it must protect customers from attacks through devices, ensure customer privacy, and protect the company from brand and reputational damage.

Security best practices were explicitly considered during the design of the organization's products, so product security features are well documented in their specifications. In every other aspect of security, though, the company has no documentation or formal policies.

The organization wants to understand the appropriate level of investment to meet these goals. The company leadership are genuine in their desire to build an appropriate security program, but the threat profile of their customers means that it is unlikely that deployment of its products needs to be hardened sufficiently to protect against advanced, persistent threats. The organization wants to adopt an appropriate level of security, without over investing in ways that would reduce margins or increase product costs without appreciable benefit. The company's leadership decides the SMM is an appropriate framework to help them make related decisions.

The organization starts the process by deciding what its target state should be.

14.2 Factors to Consider in the Case Study System Analysis

The following considerations drive the organization's decisions as they determine their target state in the various subdomains:

- Customers install the organization's products in and around their homes, leading to significant privacy implications if a product were compromised. Consequently, the organization wants to place emphasis on secure design and endpoint hardening to minimize the risk present in their released devices.
- Related to this, the company believes that they would experience significant brand and reputational damage if their products suffered from a high-profile security incident. The

organization's products compete in a crowded marketplace and they expect that consumers will avoid products with publicized shortcomings.

- The organization assesses that the most advanced threat actors to target their products will likely be security researchers. There is no clear monetary benefit to be gained from exploiting the product. Similarly, the product is unlikely to be installed in locations that would be of interest to sophisticated, nation-state actors.
- Finally, the organization needs to build their security program from a starting point of zero. Their target state needs to be pragmatic about what activities will yield the most improvement in terms of security and reduction of risk.

As the stakeholders develop their security maturity model benchmark, they opt not to include the element of scope. They make this decision based on two factors. First, their industry has no specific regulatory or compliance requirements that need to be considered. Second, they are developing the benchmark for themselves. That being the case, the scope for all practices is level 4. Given the consistency of scope across the benchmark, the stakeholders decide not to focus on it in their exercise.

14.3 Prioritizing the Security Subdomains

With the factors described above in mind, organization stakeholders work to determine their target state. Again, while ideally all practices would operate at a level 4, the purpose of this exercise is to assign relative priority to the various domains, subdomains, and practices. This process recognizes that not all security practices are equal in all scenarios, and investment of time and resources should be made based on what will lead to the greatest increase in security. Initially security enablement and hardening target comprehensiveness level is 3, and they are prioritized over security governance which has the target comprehensiveness level 2. The target scope for all domains is general.

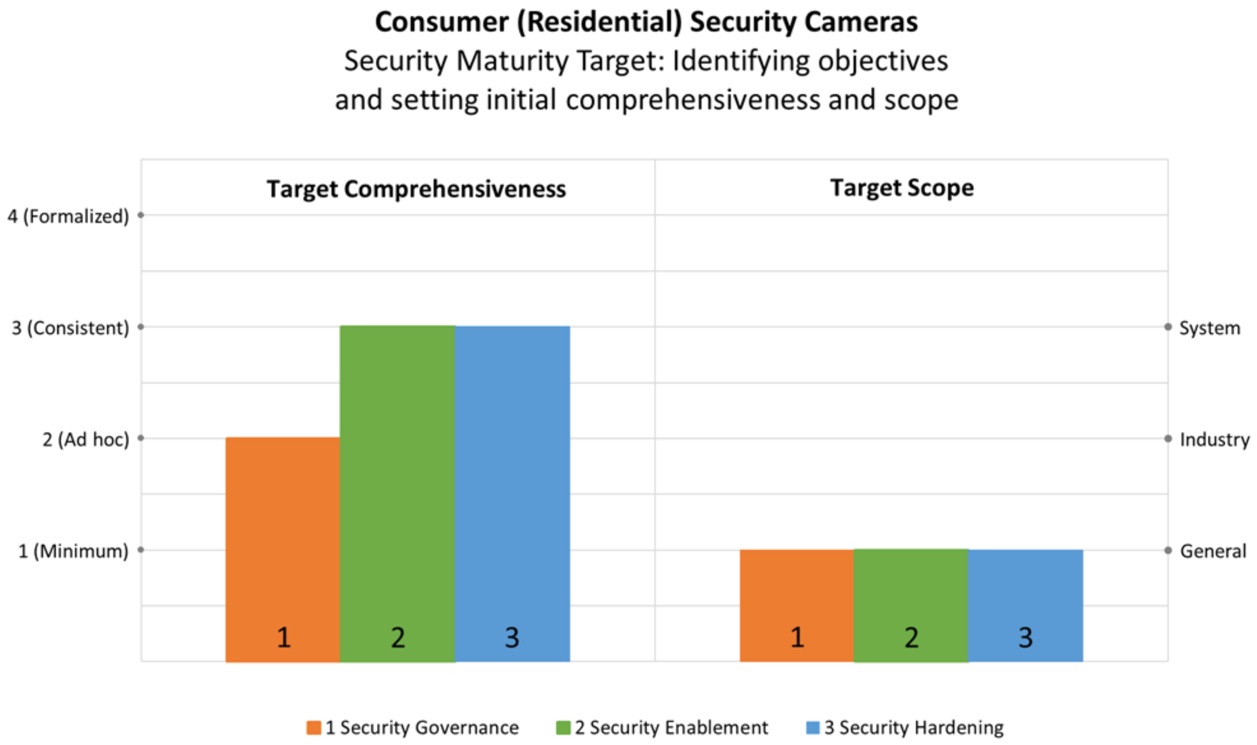


Figure 14-1: Initial target values for security domains for the Consumer Security Cameras case study

14.4 Considering the Security Needs for Subdomains

14.4.1 Security Needs for Governance

At this early stage, without an existing program, the organization seeks to establish baseline measures of security, consistent with a level 2 target state.

Security strategy and governance: As the organization lacks the foundation for a security program, their goal to provide a vision and then roll out basic security best practices, consistent with a level 2 target state.

Threat modeling and risk assessment: The crowded market in which the organization competes causes it to put significant emphasis on the security of its production devices. Consequently, the organization wants to prioritize threat modeling and risk assessment as tools its developers can use to help prevent the inclusion of vulnerabilities in its products, consistent with a level 3 target.

Supply chain and external dependencies management: The company builds its products from commodity components so needs to be sure they do not have vulnerabilities that can impact its products. The stakeholders consequently decide that their risk profile does not require more than a level 0 target.

14.4.2 Security Needs for Enablement

Decisions made in the enablement domain have implications for the security of stored data, and consequently for user privacy. Given the company has a goal of protecting the privacy of their users (the confidentiality of video feeds) a level 3 target is appropriate.

Identity and access management: The company's products only support a single user role. Given the lack of complexity in their access model, the organization decides a level 2 target is appropriate as they only need to differentiate access based on individual users.

Asset protection management is fundamental to the security of hosts storing user information. The company stores user videos on a cloud platform, which transfers much of the responsibility to the cloud provider. Given the number of security incidents that have stemmed from misconfigurations in a cloud backend the company still believes this should be an important area. They consequently decide on a level 3 target for this subdomain.

Data protection: To protect user data, the company chooses a level 4 target for this subdomain. The organization needs to classify all the information that can relate to an identified or an identifiable person and to the video data it holds, and then specify adequate controls for each level of classification. The organization also needs to ensure that its controls protect data in transit, at rest, and while being processed. This should include protection from malicious insiders.

14.4.3 Security Needs for Hardening

The hardening domain prevents attacks against endpoints and backend systems. They are willing to make the investment to have situational awareness and be able to respond to an attack against its assets. It consequently chooses a level 3 target for the hardening domain.

Vulnerability and patch management: The company wants to ensure that known vulnerabilities do not persist in their products or infrastructure. To prevent this possibility, they want to institute automated path management for their deployed products (i.e., OTA updates) and backend infrastructure. They also want to pair patch management with a vulnerability management program to provide feedback and verify the security of managed assets. These goals are consistent with a level 3 target.

Situational awareness: The organization wants to have sufficient monitoring of security events so that signs of malicious activity can be detected and prevented in near real-time. For awareness and information sharing, the company's staff want to understand the state-of-the-art in terms of threats but are unlikely to encounter situations in which they would seek to share their own threat data with law enforcement. Although the specific goal for the monitoring practice is consistent with a level 2, the organization sets an overall goal of level 3 for the subdomain.

Event and incident response: To preserve its professional reputation and revenue stream, the company needs to be able to restore services as fast as possible after an incident. If the organization's products can't store customer video for a sustained period, the company anticipates it would quickly lead to a consumer backlash. This goal of an automatic, swift, and coordinated business response to an incident is consistent with a level 4 goal.

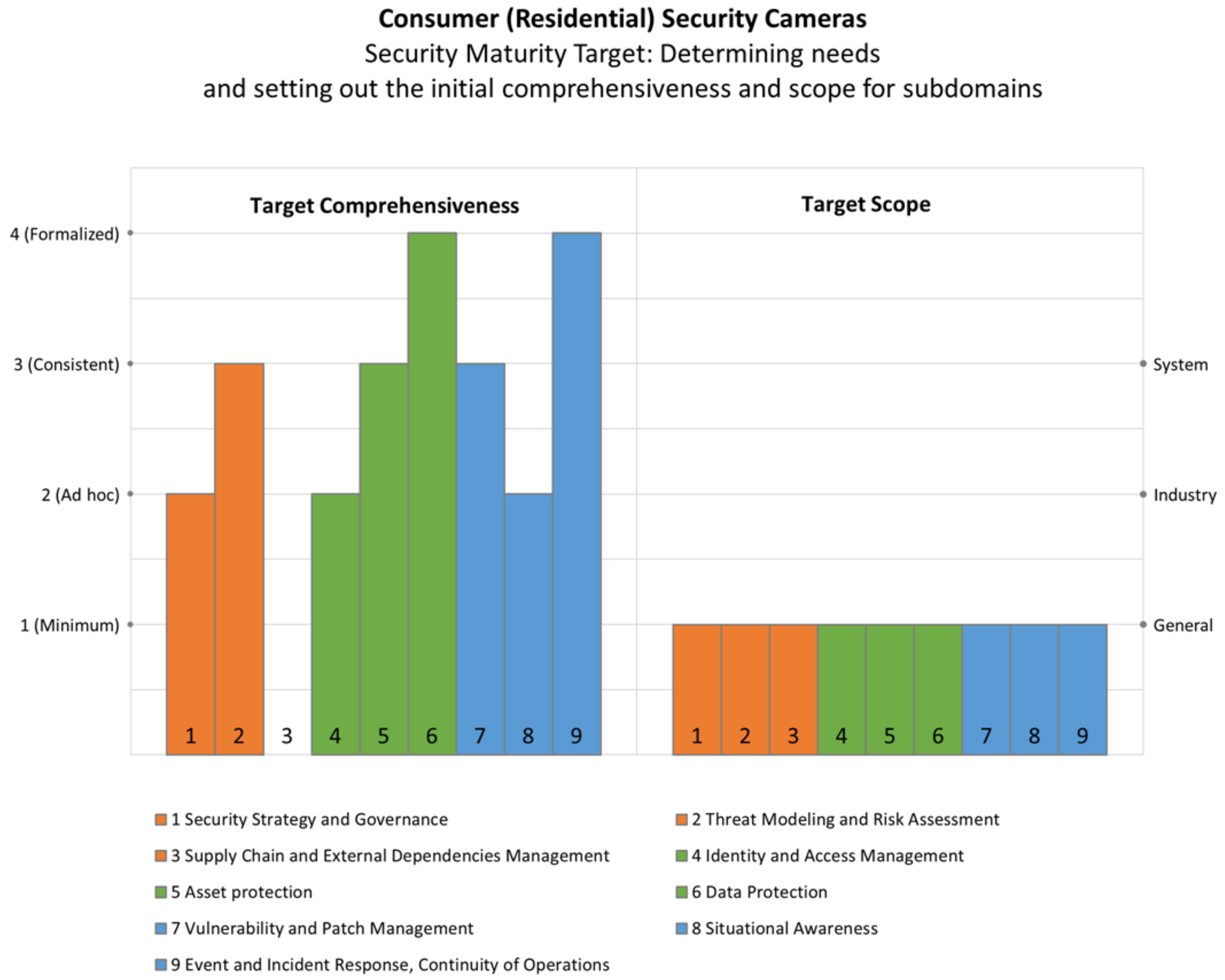


Figure 14-2: Initial target values for security subdomains for the Consumer Security Cameras case study

14.5 Validating the Purpose of Security Practices

After having established the target state for each subdomain, the organization takes stock of its current state in an offsite two-day leadership workshop. The company brings in a third-party security expert to facilitate the process and provide an impartial assessment of current state, based on information provided by the respective team leaders. There is some inherent bias in this process, as allowing team leaders to self-report creates the potential for inflating existing controls, but decided it was adequate for this first iteration through the security maturity model. For future iterations, the company would like to have an independent third-party perform a security assessment to determine the target state objectively for each practice.

Security program management: After a long, uncomfortable conversation, the leadership team acknowledges that they had no existing security program whatsoever. The stakeholders had all assumed that a security policy had been documented *somewhere,* but a review of the company's documentation and wiki found that none existed, although several other documents referenced a security policy. The stakeholders set their current state as level 0.

Compliance management: The stakeholders identified that they have no mature compliance programs. After verifying that they do not process or store any PII data, they believe they do not have any compliance requirements. They consequently rate their current compliance management state as level 1.

Threat modeling: The stakeholders determine that one of their development teams, focused on the cloud-side services, had been conducting routine threat models with formal methods. No other development teams have used threat modeling during the development processes. The stakeholders consequently rate their current state as 2 given its ad hoc nature.

Risk attitude: As a corollary of the lack of security policy, the organization also lacks a sense of risk. No organized effort exists to understand risks and differentiate their relative severities. The stakeholders consequently categorize themselves as a level 1.

Product supply chain risk management: The company lacks a supply chain security program. No one in their development or engineering teams has inventoried third-party provided software and hardware components, and there is no effort to stay informed of vulnerabilities in any third-party components. The organization consequently categorizes itself as a level 0.

Third-party dependencies management: The organization relies on a single third party for ongoing operations, their cloud service provider. Their provider is a market leader and has received multiple certifications for various compliance regimes. They provide these documents to the organization annually, so the stakeholders find themselves at level 3 for this practice.

Establishing and maintaining identities: The company's products currently support a single user role. This allows the developer team to treat all users similarly and puts their current and target states at level 1.

The organization's *access control* requirements are more nuanced than their identity management. The organization needs to ensure that access to PII and stored videos is secure from other users and its own employees. Before performing a requested action, their system's authorization infrastructure currently verifies user authentication and that a request is for data owned by the requester. The stakeholders consequently set their current state as level 2, but acknowledge they need to do more to provide assurance, particularly as it relates to a potential malicious insider.

Asset, change and configuration management: The stakeholders realize that there's no process in place to track changes in system configurations. Their ops team maintain documents in a collaboration system that details how different ecosystem components *should* be configured, but there is no process to ensure the implementations match that or any alerting to note when a change occurs. They consequently benchmark themselves as a level 0 for current state.

Physical protection: The physical assets hosting sensitive information (PII and video) are all operated by the cloud provider who has extensive physical security protections. Physical access to the organization's offices and workstations is controlled with ID cards, which are issued to specific individuals and audited. The organization rates its current state as level 3 for this practice.

Security model and policy for data: As an exception to the organization's lack of official security policies, they do have a well-documented security model and policy for access to data. As part of their first product's design, the team worked out which assets in the ecosystem would process and store which kinds of data and developed their architecture to ensure the security and privacy of stored video feeds and PII. Given the documentation and implementation that defines specific roles, assets, and services that can process or store different types of data, they assess their current state as level 3.

Implementation of data-protection controls: Related to the above architecture plan, the company has a mature solution for securing sensitive data. The architecture provides controls for unauthorized access from malicious insiders and ensures sensitive information is only stored in a well-secured location with the cloud provider. Further, encryption is implemented throughout the architecture, for data in motion and at rest. The stakeholders assess this domain as level 3.

Vulnerability assessment: The company has not performed any sort of vulnerability assessment on their products. They have conducted occasional, irregular vulnerability scans of pieces of their infrastructure. They consequently self-assess their current state as level 1.

Patch management: The organization has no process to push patches to its deployed products, consistent with a level 0 current state, but servers and systems in their backend infrastructure are automatically patched and managed by the cloud provider. The current state for backend systems would be level 3. The organization gives itself a conservative current state assessment of level 1 for this practice for this separate system.

Auditing: The development and ops teams occasionally review logs while troubleshooting, but there is no routine or systematic log review. Moreover, logs are not proactively reviewed for security-relevant events. The organization consequently identifies its current state as level 1.

Information sharing and communication: Members of the organization receive information on security developments relevant to their industry through Twitter and media reports. The stakeholders are unaware of anyone in the organization that routinely monitors threat intelligence feeds; they are certain that no one is responsible for maintaining awareness of new, relevant threats. They assess their current state as level 1.

Event detection and response plan: A search of the organization's document repositories fails to yield any documented incident-response plan. They assess level 0 for their current state.

Remediation, recovery and continuity of operations: The organization's engineering team does maintain documentation addressing how to restore operations in the event of a handful of incident types. For those types of incidents, the team has created detailed instructions. In one instance the team successfully used these procedures to restore services during a cloud provider outage. The organization assesses as a level 2 because these plans only included members of the engineering team and did not include other stakeholders, such as public relations or legal.

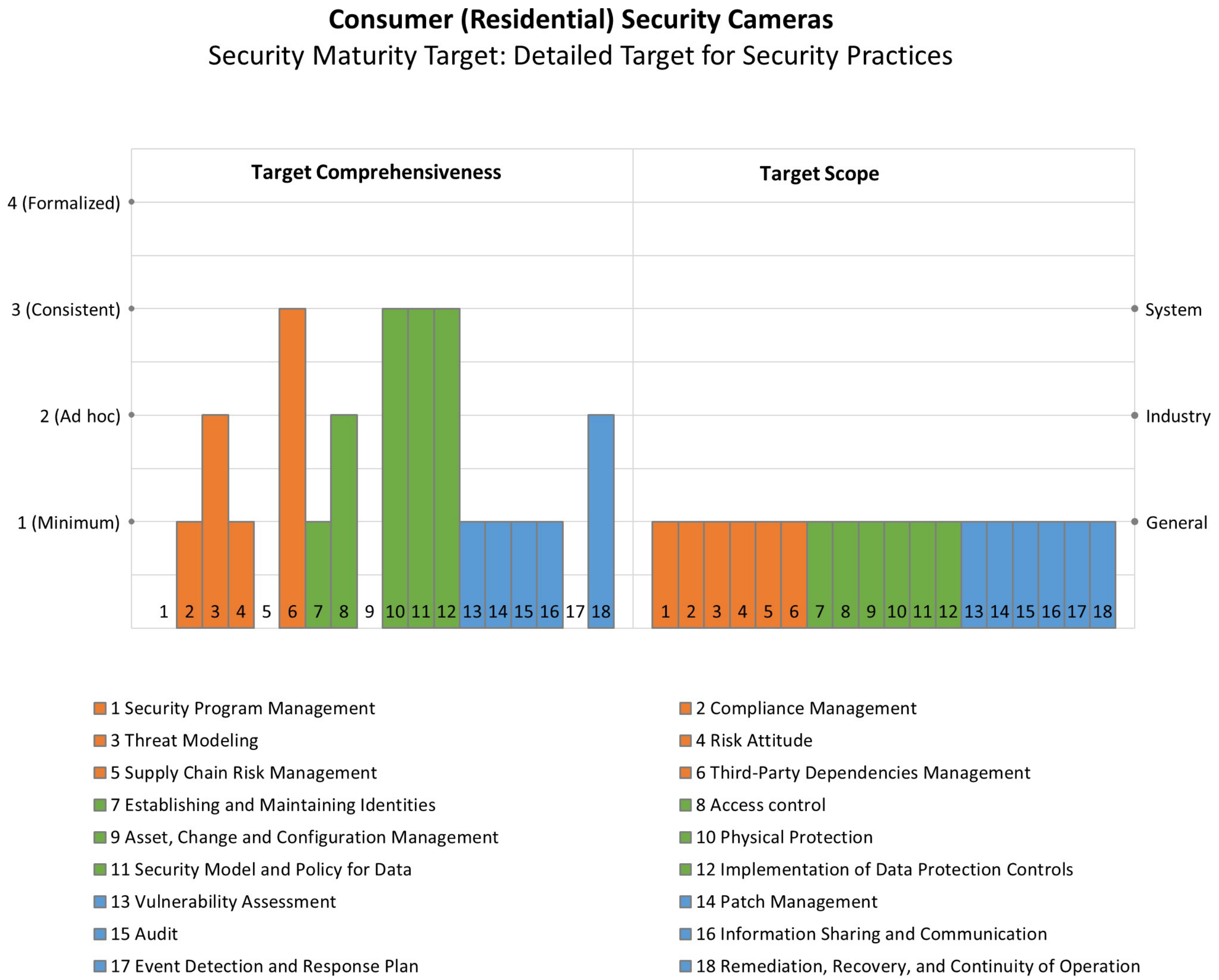


Figure 14-3: Target values for the Security Practices for the Consumer Security Cameras case study

As the target comprehensiveness levels have changed significantly after the detailed consideration of security practices, the higher-level targets for subdomains and domains are aligned with their new values.

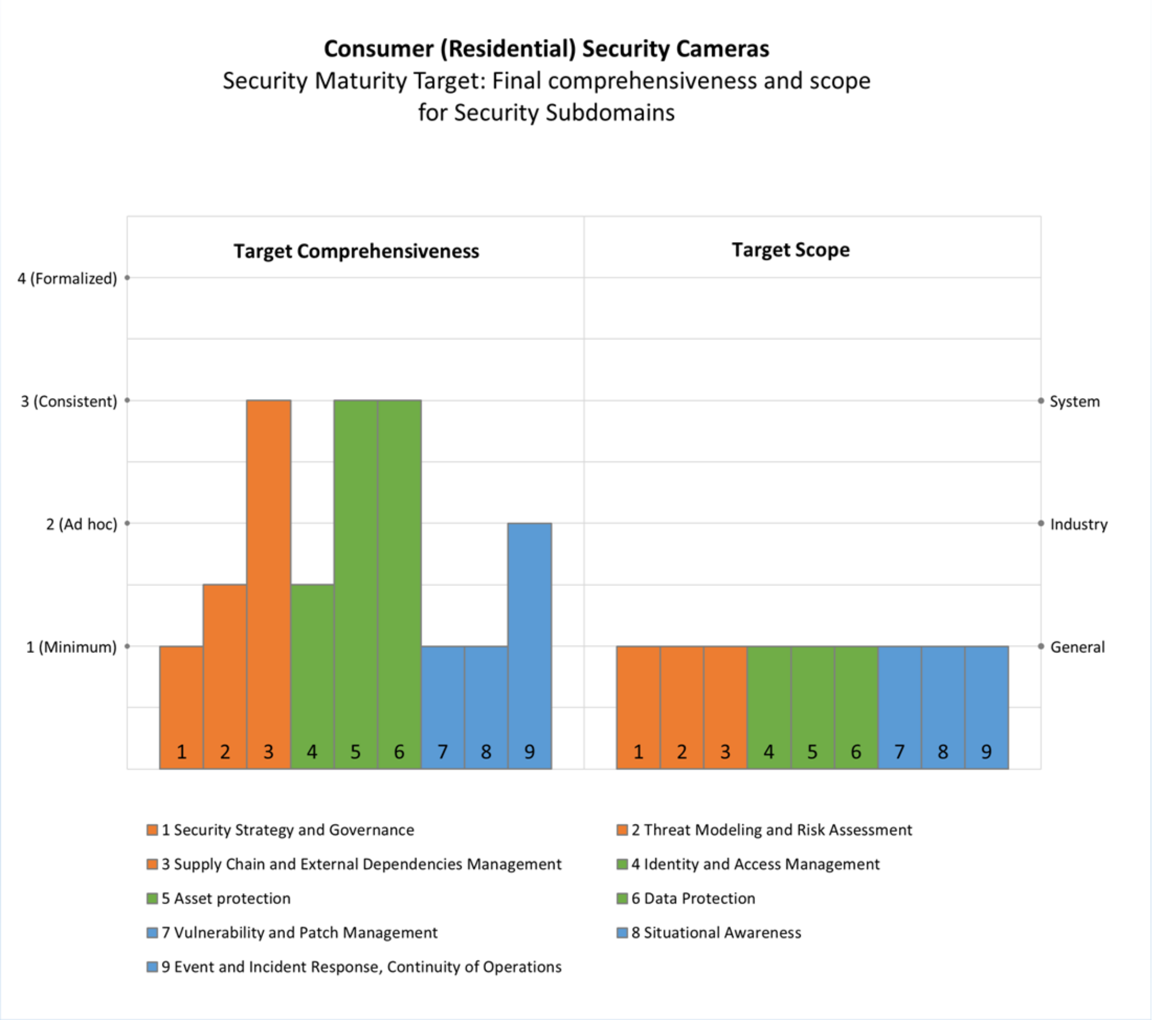


Figure 14-4: Refined values for the Subdomains for the Consumer Security Cameras case study

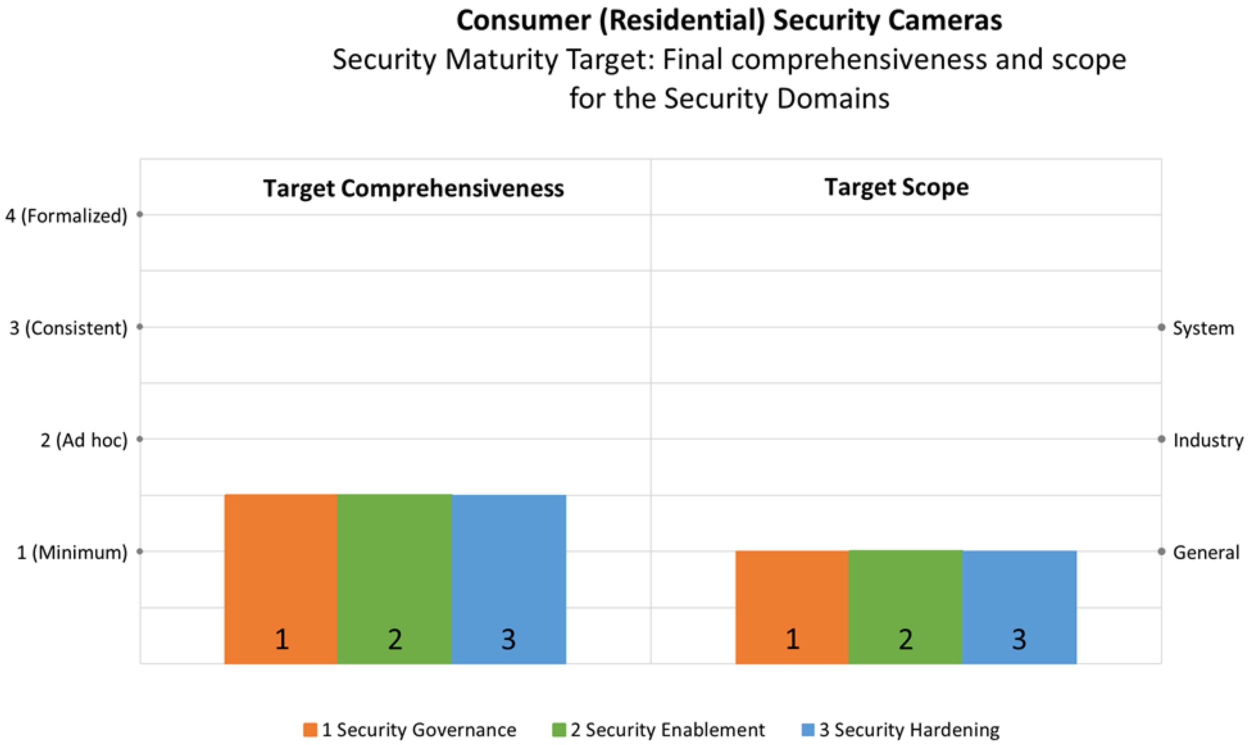


Figure 14-5: Refined values for the Domains for the Consumer Security Cameras case study

14.6 Defining Next Steps and Roadmap

With the target and current states defined, the next phase of the process is for the organization to identify those practices that fell below the target. For each of those practices the organization determines the additional measures necessary to move that practice to target state. After this list of additional controls is developed, the organization then prioritizes each change based on its cost in terms of time, resources, and money relative to the improvement in security that change would bring. The organization also keeps in mind the stakeholders responsible for each change and the capacity of each stakeholder to implement change. With these considerations enumerated, the organization develops its roadmap to improve its overall security maturity and move towards target state.

Part V: Annexes

Annex A Revision History

Revision	Date	Editor	Changes Made
V1.0	2019-02-25	Carielli, Hirsch, Rudina, Zahavi	Initial Release
V1.1	-	-	Skipped 1.1 release to align version numbers with Description and Intended Use Paper
V1.2	2020-05-05	Carielli, Eble, Hirsch, Rudina, Zahavi	Minor update with clarifications and corrections

Annex B ACRONYMS

BSIMM	Building Security in Maturity Model
C2M2	Cyber-Security Capability Maturity Model
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CISO	Chief Information Security Office
DLP	Data Loss Prevention
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architecture
IISF	Industrial Internet Security Framework
IIoT	Industrial Internet of Things
IT	Information Technology
IoT	Internet of Things
NGFW	Next Generation Firewall
OBD	On Board Diagnostics
OEM	Original Equipment Manufacturer
OT	Operational Technology
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RFC	Request for Comment
SIEM	Security Information and Event Management
TLS	Transport Layer Security
US	United States

Annex C 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 Industrial Internet Vocabulary Technical Report.

Comprehensiveness

captures the degree of depth, consistency and assurance of security measures that support security maturity domains, subdomains or practices. There are five comprehensiveness levels, from level 0 to level 4, with larger numbers indicating a higher degree of comprehensiveness of security controls.

Current state

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

Domain

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

Industrial Internet Consortium (IIC)

an open membership, international not-for-profit consortium that is setting the architectural framework and direction for the Industrial Internet. Founded by AT&T, Cisco, GE, IBM and Intel in March 2014, the consortium's mission is to coordinate vast ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards.

Industrial Internet of Things (IIoT)

describes systems that connects and integrates industrial control systems with enterprise systems, business processes, and analytics.
Note 1: Industrial control systems contain sensors and actuators.
Note 2: Typically, these are large and complicated system.

Maturity

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.

Practice

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

Security maturity profile

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.

Scope

reflects the degree of fit to the industry or system needs. It captures the degree of customization of the security measures that support security maturity domains, subdomains or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system. There are three levels of scope for every security facet, from level 1 to level 3, with higher numbers indicating a narrower and more specific scope.

Security level

is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.

Subdomain

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

Target state

The security maturity target 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.

Annex D REFERENCES

[BSIMM] Building Security in Maturity Model (BSIMM), retrieved 2019-01-24
https://www.bsimm.com/download.html
from
https://www.bsimm.com

[CVSS] Common Vulnerability Scoring System (CVSS), V3, 2015, retrieved 2019-01-24
https://www.first.org/cvss/

[ENER-C2M2] Office of Electricity Delivery & Energy Reliability: Cybersecurity Capability Maturity Model (C2M2), retrieved 2016-09-26
https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf
from
https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

[IEC-62443-21] IEC 62443-2-1 2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, 2010
https://webstore.iec.ch/publication/7030

[IEC-62443-33] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013
https://webstore.iec.ch/publication/7033

[IIC-DPBP2019] Industrial Internet Consortium: Data Protection Best Practices, Version 1.0. Bassam Zarkout, Apurva Mohan, Niheer Patel, 2019-07-15, retrieved 2019-11-03
https://www.iiconsortium.org/pdf/Data_Protection_Best_Practices_Whitepaper_2019-07-22.pdf

[IIC-ESMM2018] Extending the IIC IoT Security Maturity Model to Trustworthiness, Frederick Hirsch, Sandy Carielli, Matt Eble, Ekaterina Rudina, Ron Zahavi, in Ninth Edition of the Journal of Innovation: Trustworthiness, September 2018, retrieved 2019-11-03 *https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI-Extending-the-IIC-Security-Maturity-Model-to-Trustworthiness.pdf*

[IIC-IIRA2019] Industrial Internet Consortium: The Industrial Internet, Volume G1: Reference Architecture Technical Report, version 1.9, 2019-06-19, retrieved 2020-04-29
https://www.iiconsortium.org/IIRA.htm

[IIC-IISF2016] Industrial Internet Consortium: Industrial Internet of Things Volume G4: Security Framework, 2016-09-26, retrieved 2019-01-24
https://www.iiconsortium.org/IISF.htm

[IIC-IIV2019] Industrial Internet Consortium: The Industrial Internet, Volume G8: Vocabulary Technical Report, version 2.2, 2019-11-06, retrieved 2020-01-24 *https://www.iiconsortium.org/vocab/index.htm*

[IIC-SMMD2020] Industrial Internet Consortium: IoT Security Maturity Model: Description and Intended Use, version 1.2, 2020-05-05, retrieved 2020-05-05 *https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf*

Annex E INDEX

Annex F AUTHORS AND LEGAL NOTICE

ACKNOWLEDGEMENTS

This document is a work product of the Industrial Internet Consortium Security Applicability Task Group, co-chaired by Ron Zahavi (Microsoft) and James Clardy (Net Foundry), which is a subgroup of the Security Working Group, co-chaired by Sven Schrecker (Trust Driven Solutions), Jesus Molina (Waterfall Security Solutions) and John Zao (NTCU PET Lab).

AUTHORS

The following persons contributed substantial written content to this document:

Sandy Carielli (Entrust Datacard), Matt Eble (Praetorian), Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft)

CONTRIBUTORS

The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document:

Marcellus Buchheit (Wibu-Systems), Steve Clark (WISeKey).

TECHNICAL EDITOR

Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.

IIC ISSUE REPORTING

All IIC documents are subject to continuous review and improvement. As part of this process, we encourage readers to report any ambiguities, inconsistencies or inaccuracies they may find in this Document or other IIC materials by sending an email to admin@iiconsortium.org.

USE OF INFORMATION—TERMS, CONDITIONS AND NOTICES

This is an Industrial Internet Consortium document (the "Document") and is to be used in accordance with the terms, conditions and notices set forth below. This Document does not represent a commitment by any person to implement any portion or recommendation contained in it in any products or services. The information contained in this Document is subject to change without notice.

LICENSES

The companies who contributed content to this Document ("Contributing Companies") have granted to the Industrial Internet Consortium (the "IIC"), a program of Object Management

PATENTS

Compliance with or adoption of any advice, guidance or recommendations contained in any IIC reports or other IIC documents may require use of an invention covered by patent rights. *OMG and its IIC program are not responsible for identifying patents for which a license may be required* to comply with any IIC document or advice, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. IIC documents are informational and advisory only. Readers of this Document are responsible for protecting themselves against liability for infringement of patents and other intellectual property that may arise from following any IIC recommendations or advice. OMG and its IIC program disclaim all responsibility for such infringement.

GENERAL USE RESTRICTIONS

DISCLAIMER OF WARRANTY

WHILE THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PROVIDED “AS IS” AND MAY CONTAIN ERRORS OR MISPRINTS. OMG (INCLUDING ITS IIC PROGRAM) AND THE CONTRIBUTING COMPANIES MAKE NO WARRANTIES, REPRESENTATIONS OR CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE OR USE, OR AGAINST INFRINGEMENT. OMG (INCLUDING ITS IIC PROGRAM) MAKES NO REPRESENTATIONS, WARRANTIES, GUARANTIES, OR CONDITIONS AS TO THE QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT.

IN NO EVENT SHALL OMG (INCLUDING ITS IIC PROGRAM) OR ANY OF THE CONTRIBUTING COMPANIES BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, RELIANCE OR COVER DAMAGE, OR DAMAGE FOR LOSS OF PROFITS, REVENUE, DATA OR USE, HOWEVER IT ARISES, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, INCURRED BY ANY USER OR ANY THIRD PARTY IN CONNECTION WITH THE FURNISHING, PERFORMANCE, REPRODUCTION, DISTRIBUTION OR USE OF THIS MATERIAL, EVEN IF PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The entire risk as to the quality and performance of any software or technology developed using this Document is borne by you. This disclaimer of warranty constitutes an essential part of the Permission granted to you to use this Document.

LIMITED RIGHTS NOTICE

This Document contains technical data that was developed at private expense and (i) embodies trade secrets, or (ii) is confidential and either commercial or financial. This document was not produced in the performance of a government contract and is not in the public domain. The use, duplication or disclosure of this Document by the U.S. Government is subject to the restrictions set forth in 48 C.F.R. 52.227-14–Rights in Data “Limited Rights Notice (Dec. 2007) (a) and (b),” or as specified in 48 C.F.R. 12.211 of the Federal Acquisition Regulations and its successors, as applicable. This data may only be reproduced and used by the U.S. Government with the express limitation that it will not, without written permission of the copyright owners, be used for purposes of manufacture nor disclosed outside the Government. The copyright owners are as indicated above and may be contacted through Object Management Group, Inc., 109 Highland Avenue, Needham, MA 02494, U.S.A.

TRADEMARKS

The trademarks, service marks, trade names and other special designations that appear on and within the Document are the marks of OMG, the Contributing Companies and possibly other manufacturers and suppliers identified in the Document and may not be used or reproduced without the express written permission of the owner, except as necessary to reproduce, distribute and refer to this Document as authorized herein.