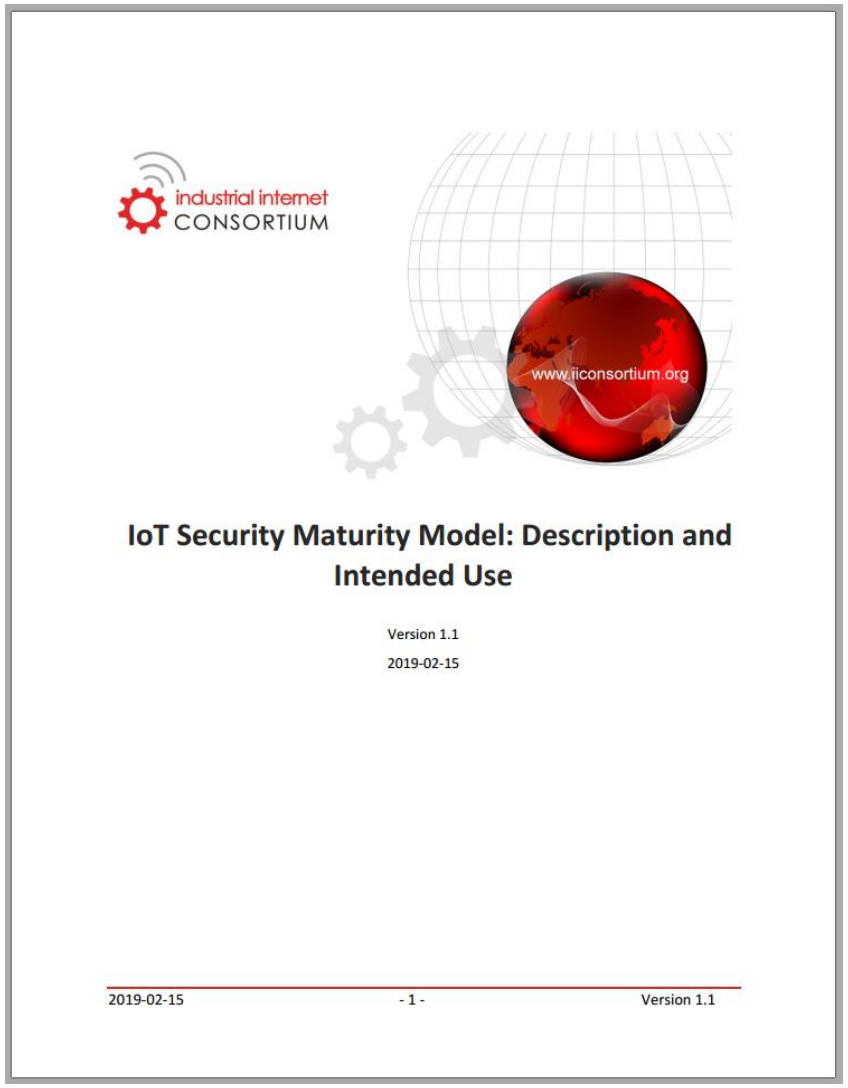
industrial internet CONSORTIUM

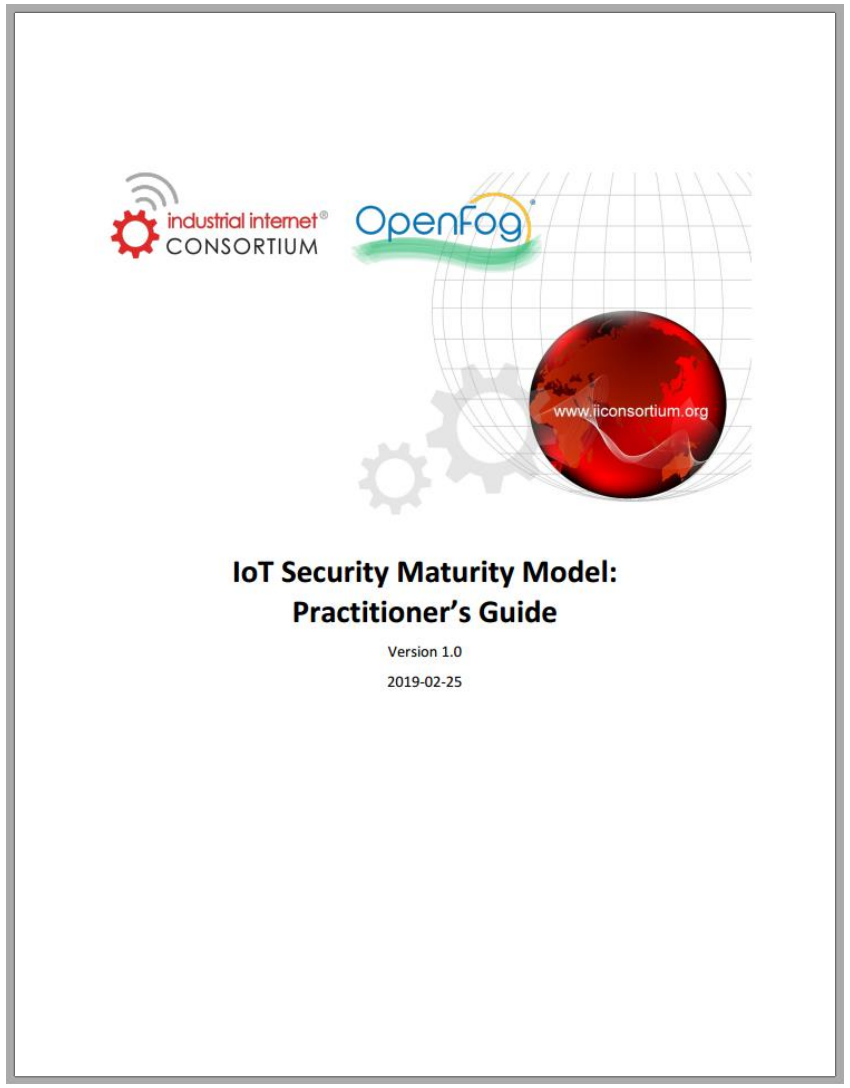
IoT Security Maturity Model: Nudge for the Security of the Internet of Things

Ekaterina Rudina, Kaspersky Lab

2019

industrial internet CONSORTIUM





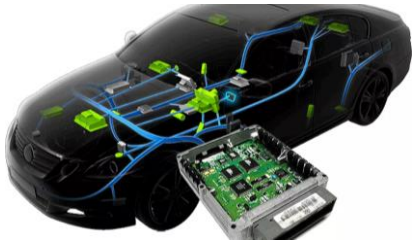
https://www.iiconsortium.org/smm.htm

https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf

https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf

What does it mean “to be secure”…

For a production line



For an automotive ECU

For a surveillance camera

For a fitness bracelet

For a nuclear facility

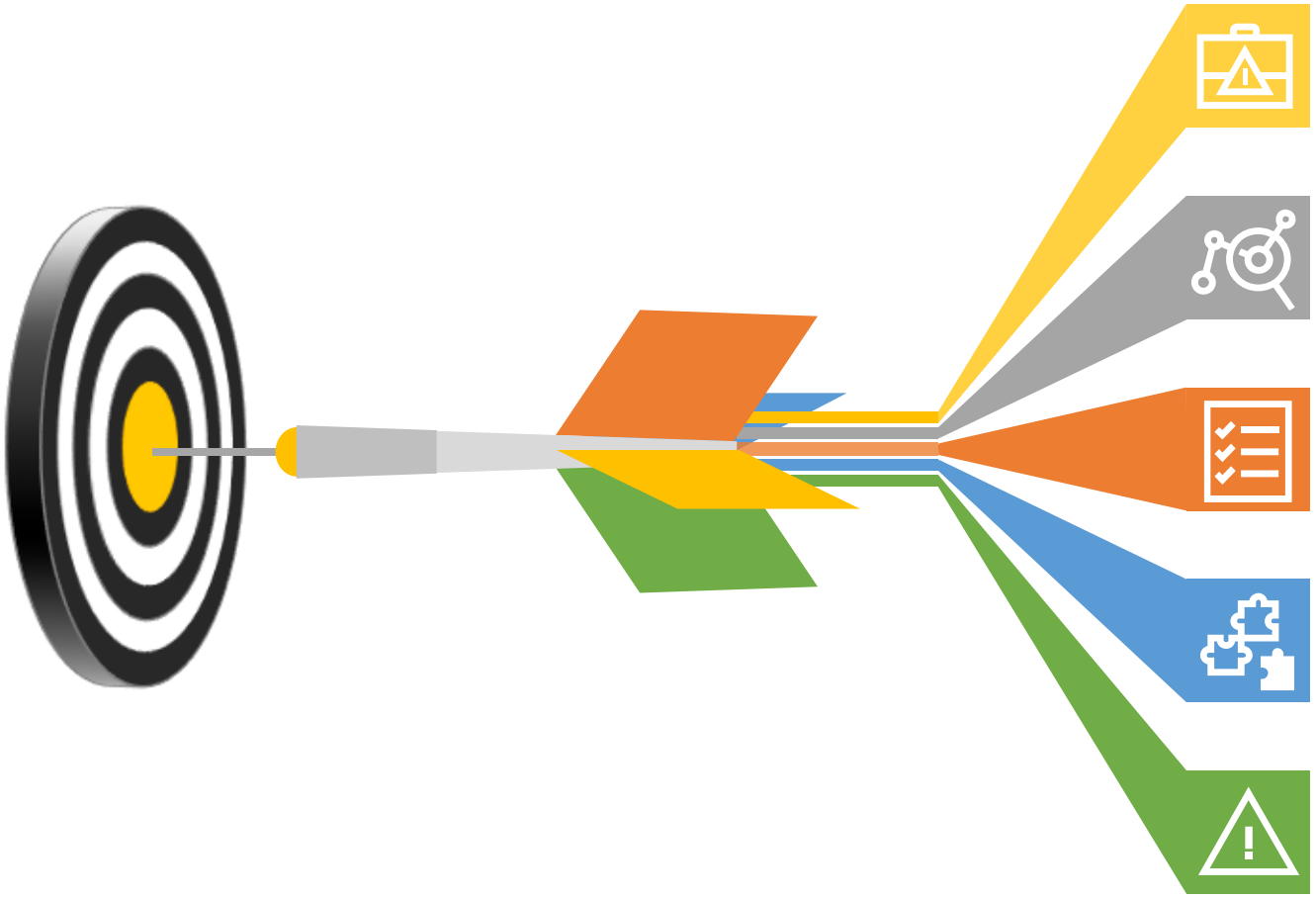
Security challenges for (not only) IoT solutions

Rigid requirements to the security levels describing the comprehensiveness of security measures

Specificity of some areas and particular systems in regard to security may **constrain** the implementation of security measures or require some that are out-of-scope for the standard/regulatory requirements

As a result, it is hard to understand what is required to **guarantee that the system is secure enough** but not more

The Mature Security Solution in IoT addresses



Business Context

Size and coverage, project timing, competing solutions…

Threats and risks

Known threats, threat sources, worst threat impact …

Expectations and priorities

Objectives, indicators, extent of improvement

Available and already implemented practices

What has been done

Industry and System Constraints

Safety, service continuity, type of lifecycle

What is Security Maturity

Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.

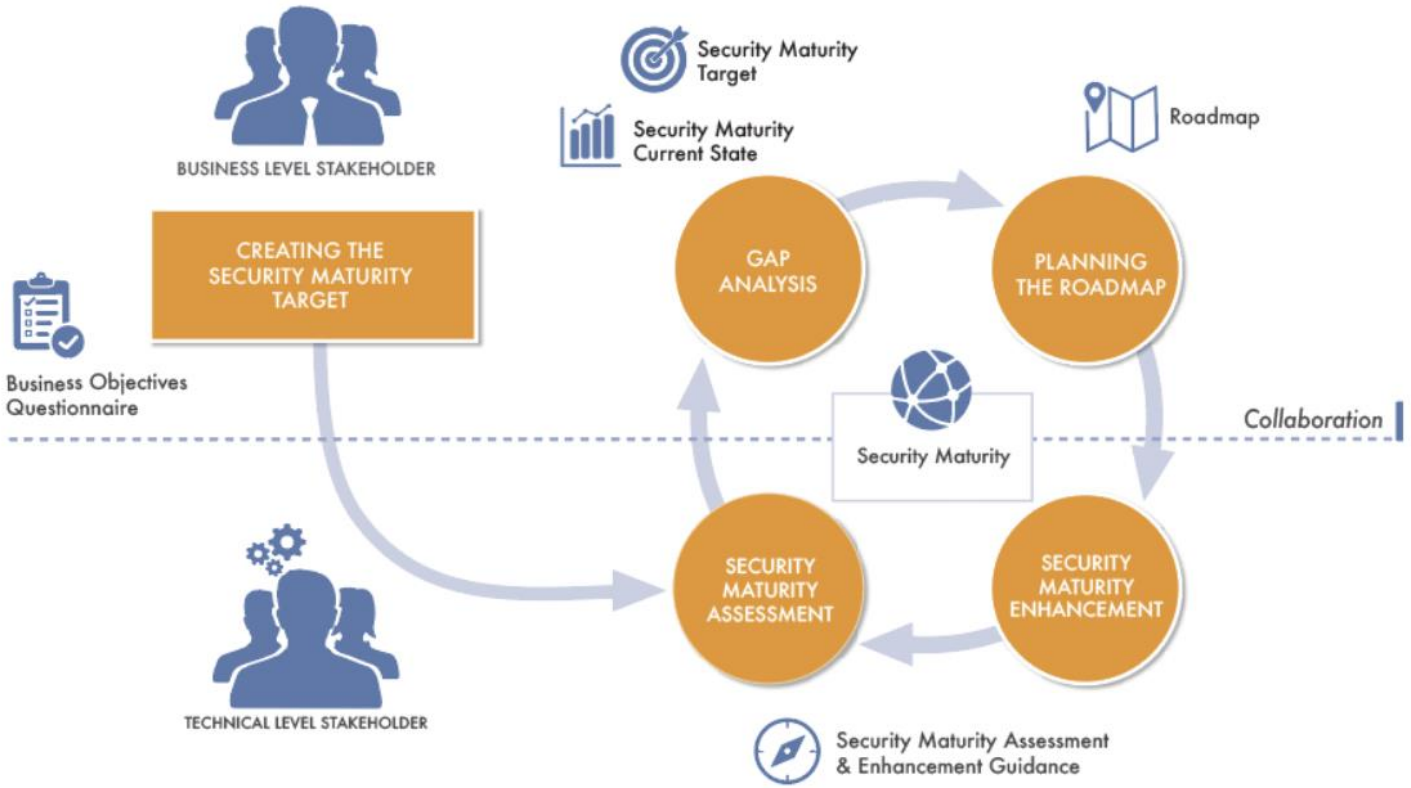
Security level, on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.

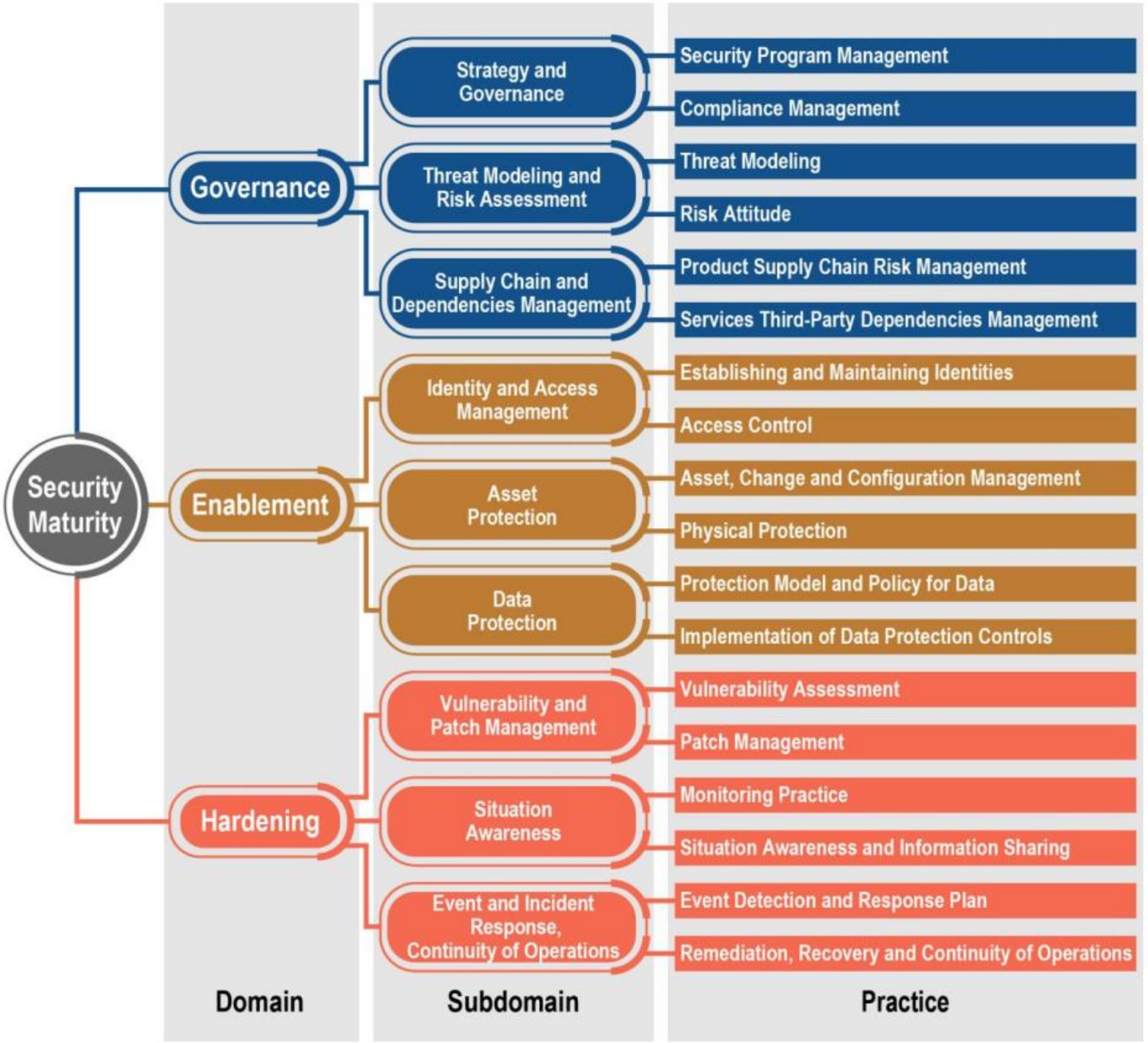
Those using the Security Maturity Model should be able to determine and clearly communicate to management the answers to the following questions:

- 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?

Security Maturity Model for Strategy and Priority setting

The process of security maturity assessment and enhancement

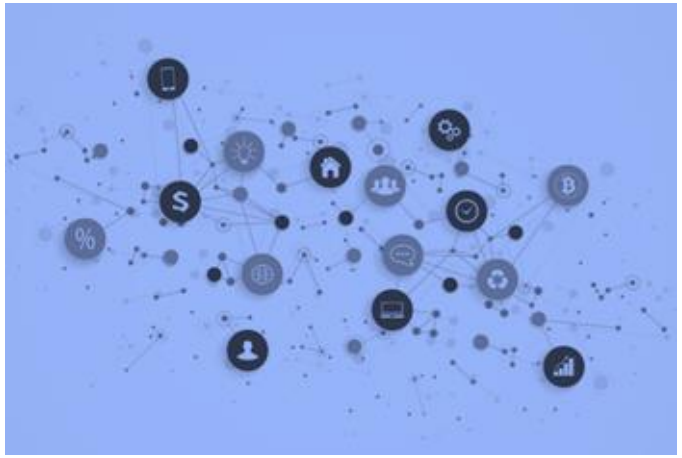




The Security Practices catalogue

The assessment for each given practice can be performed separately, making the input into the whole scoring of Security Maturity

The Hierarchy: Domains, Subdomains, Practices



Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.

At the domains level, the stakeholder determines the **priorities** of the direction in improving security

Subdomains reflect the basic means of obtaining these priorities at the planning level.

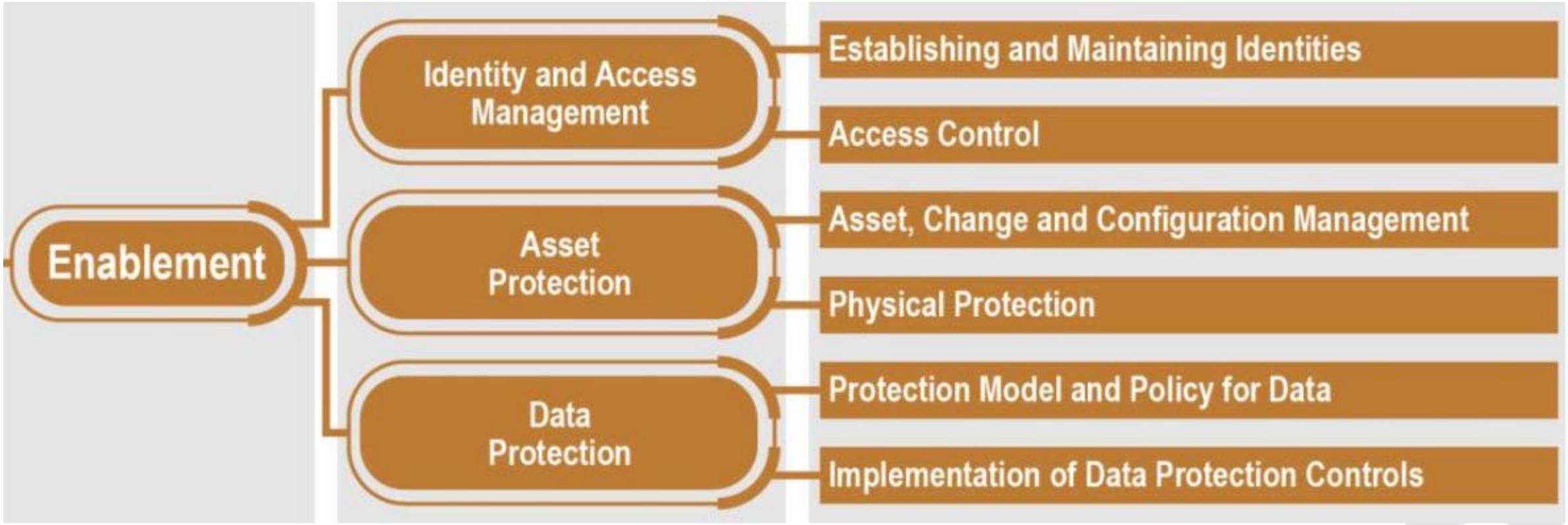
At the sub domains level, the stakeholder identifies the typical **needs** for addressing security concerns.

Practices define typical activities associated with sub domains and identified at the tactical level.

At the practices level, the stakeholder considers the **purpose** of specific security activities.

Governance Domain

Enablement Domain



Hardening Domain

Scoring. Comprehensiveness levels

Level 0, None:

There is no common understanding of how the security practice is applied and no related requirements are implemented

Level 1, Minimum:

The minimum requirements of the security practice are implemented. There are no assurance activities for the practice implementation

Level 2, Ad hoc:

The requirements for the practice cover main use cases and well-known security incidents in similar environments. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks

Level 3, Consistent:

The requirements consider best practices, standards, regulations, classifications, software and other tools. The assurance validates the implementation against security patterns, secure-by-default designs and known protection approaches and mechanisms

Level 4, Formalized:

A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest.

Scoring. 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 IoT sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

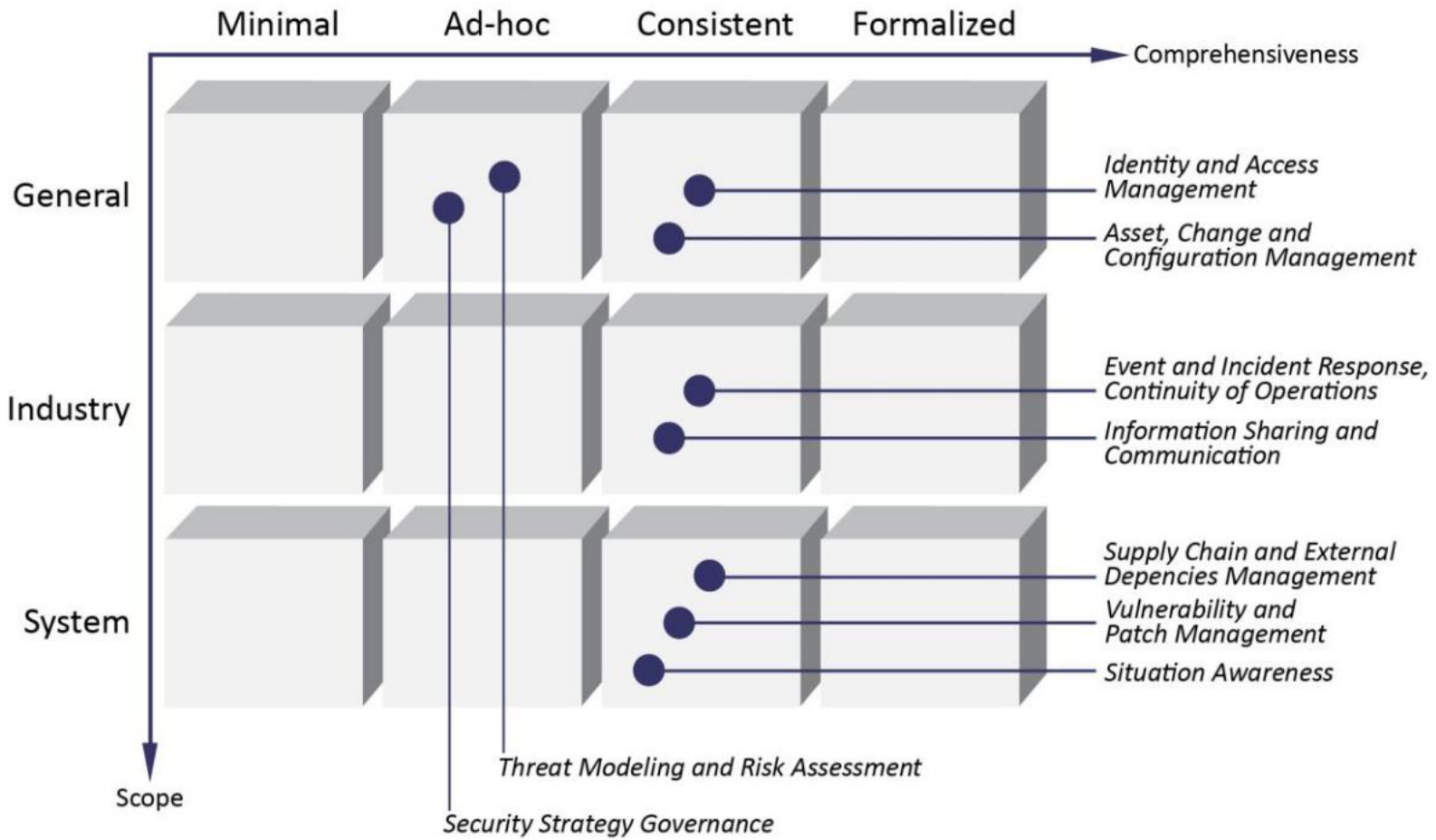
- **Level 2, Industry specific**

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 took 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. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

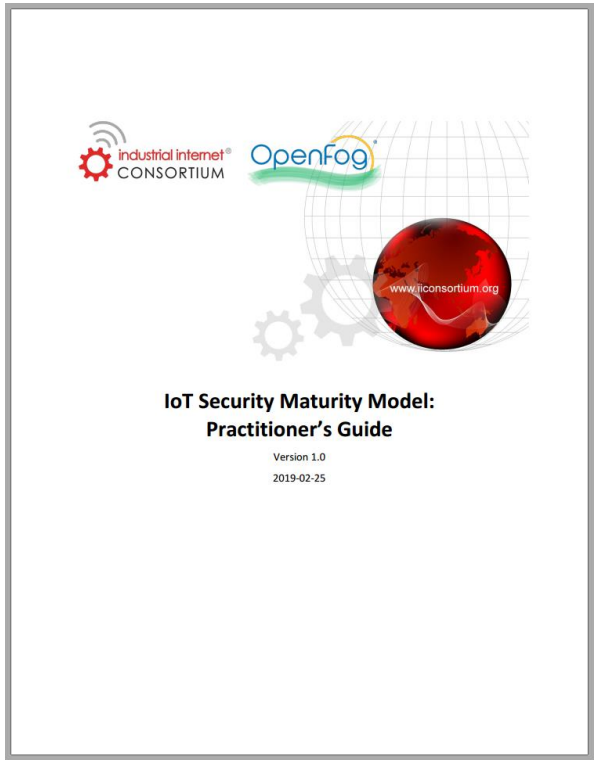
Two-dimensional approach



Setting up the Security Maturity Profile

1. Background and problem description
2. Factors for consideration
3. Prioritization of goals at the security domains level.
4. Validation of the security needs for subdomains.
5. Validation of security practices purpose.

See the Section 10 of IoT SMM Practitioners Guide

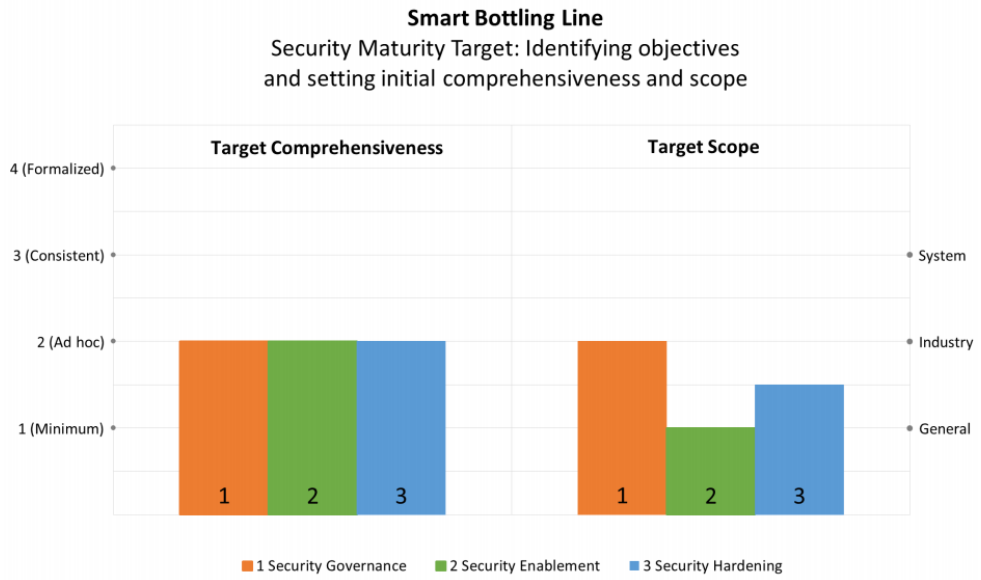


PRIORITIZING THE SECURITY DOMAINS

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, *basic* and *general* scope (which would grow to *general+* as industry-specific scope is assigned to the particular practices)



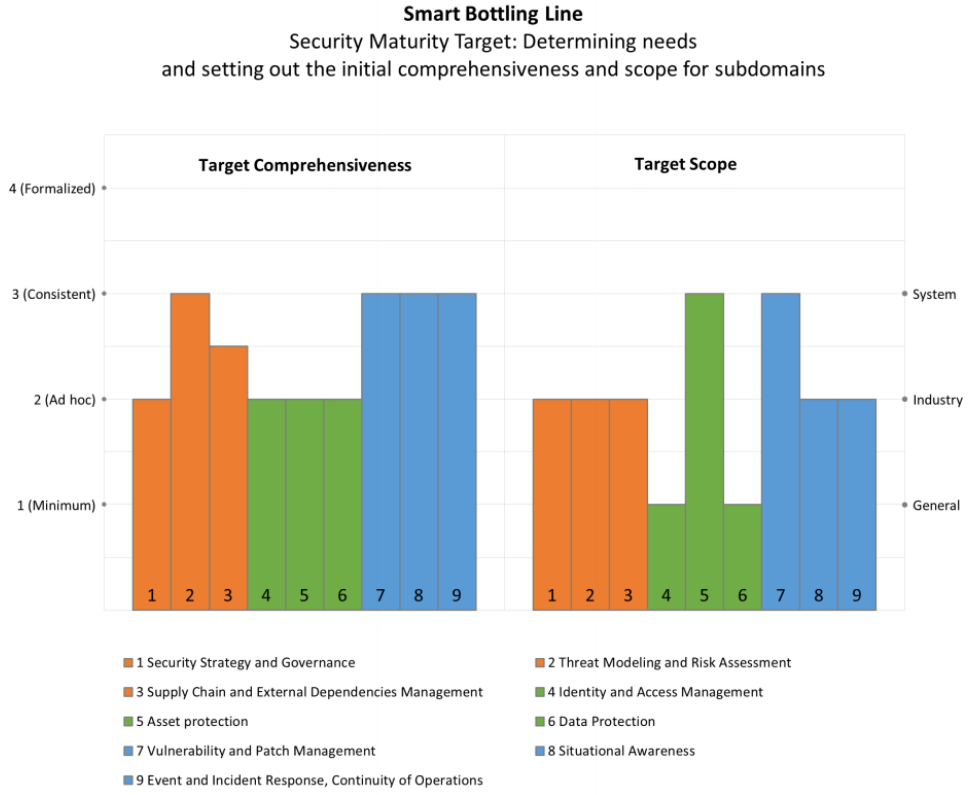
CONSIDERING THE SECURITY NEEDS FOR SUBDOMAINS

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.

etc

etc



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*.

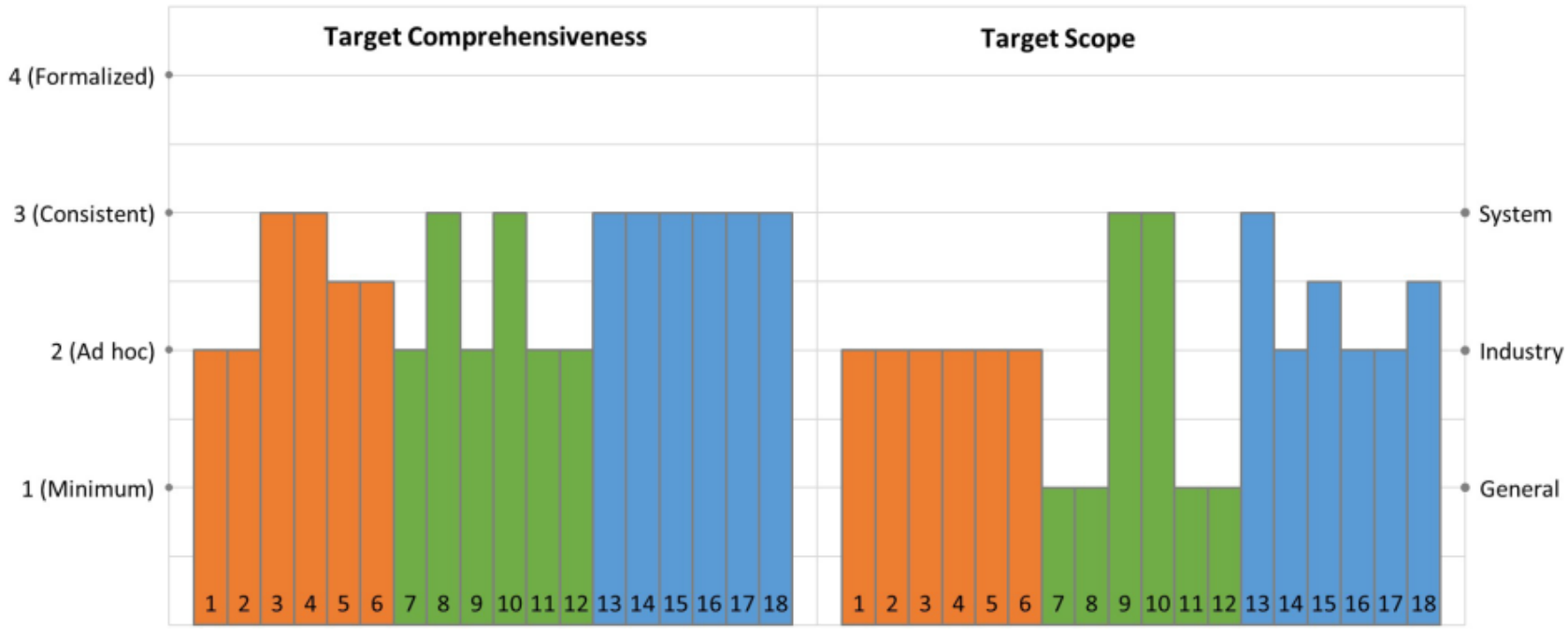
Risk attitude: An approach to characterizing risks focuses on the process continuity and integrity. Where possible, a quantitative estimation of risk is performed. The estimation of risk usually depends on the size of facility, production output, internal dependencies and other factors. The other part 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*.

etc

etc

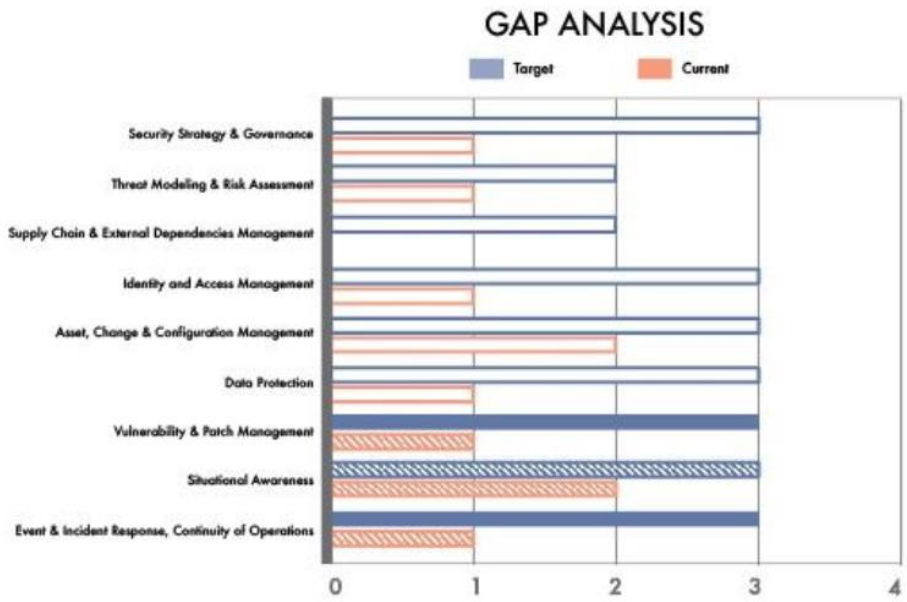
Smart Bottling Line

Security Maturity Target: Detailed Target for Security Practices



- 1 Security Program Management
- 2 Compliance Management
- 3 Threat Modeling
- 4 Risk Attitude
- 5 Supply Chain Risk Management
- 6 Third-Party Dependencies Management
- 7 Establishing and Maintaining Identities
- 8 Access control
- 9 Asset, Change and Configuration Management
- 10 Physical Protection
- 11 Security Model and Policy for Data
- 12 Implementation of Data Protection Controls
- 13 Vulnerability Assessment
- 14 Patch Management
- 15 Audit
- 16 Information Sharing and Communication
- 17 Event Detection and Response Plan
- 18 Remediation, Recovery, and Continuity of Operation

Gap Analysis



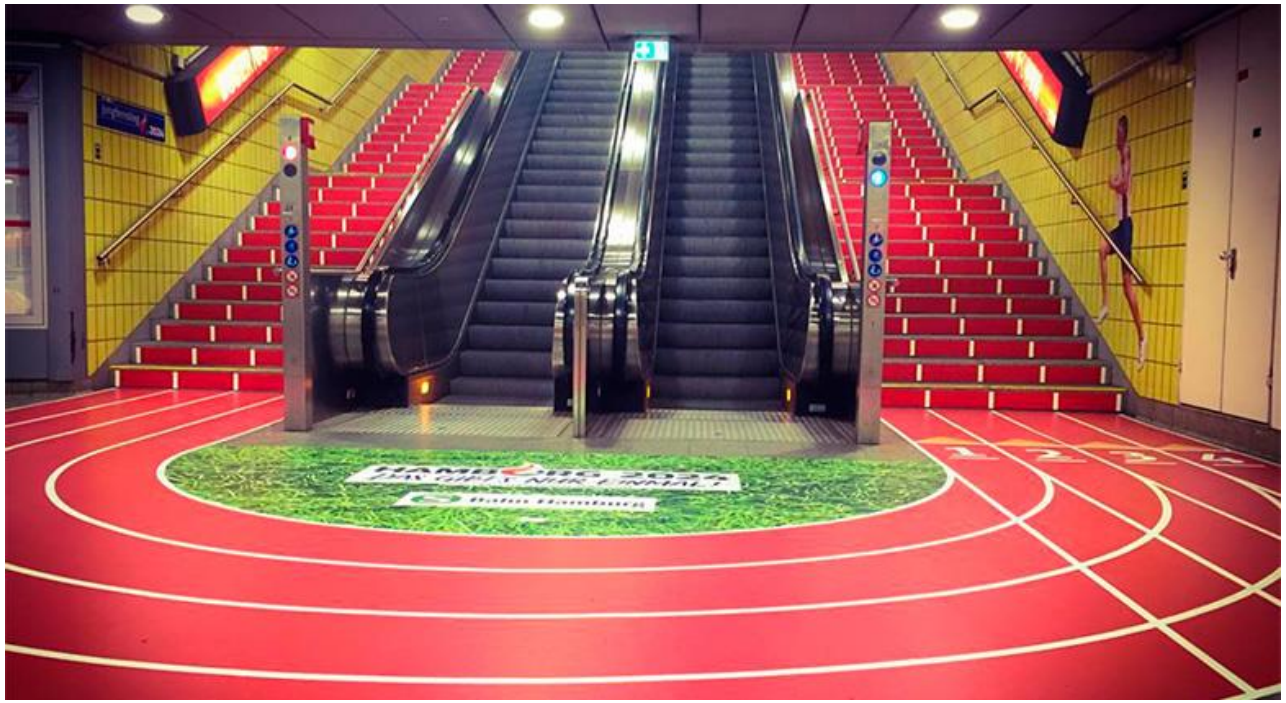
General Scope Industry Scope System Scope

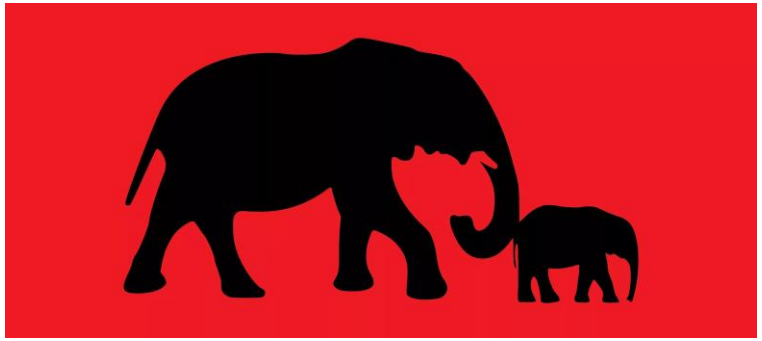
	Target	Current	Target Scope	Current Scope	Comprehensiveness Gap	Scope Gap
Security Strategy & Governance	3	1	1	1		
Threat Modeling & Risk Assessment	2	1	1	1		
Supply Chain & External Dependencies Management	2	0	1	1		
Identity and Access Management	3	1	1	1		
Asset, Change & Configuration Management	3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

We apply the known techniques to the assessment of required practices and perform gap analysis to demonstrate how the Profile is covered in the current implementation

Why I call this NUDGE for the IoT Cybersecurity?

Nudge is a concept in behavioral science, political theory and behavioral economics which proposes positive reinforcement and indirect suggestions as ways to influence the behavior and decision making of groups or individuals.





Nudge is already widely applied to address health, safety, environment concerns and many others

In cybersecurity we still observe almost all currently known cognitive biases, e.g. endownment effect (inefficient DLP bought some years ago), IKEA effect (proprietary encryption), …

Thaler and Sunstein in
Nudge: Improving Decisions about Health, Wealth, and Happiness
discuss the following "nudges"

iNcentives

Understand mappings choice/welfare

Defaults / Least resistance

Give feedback

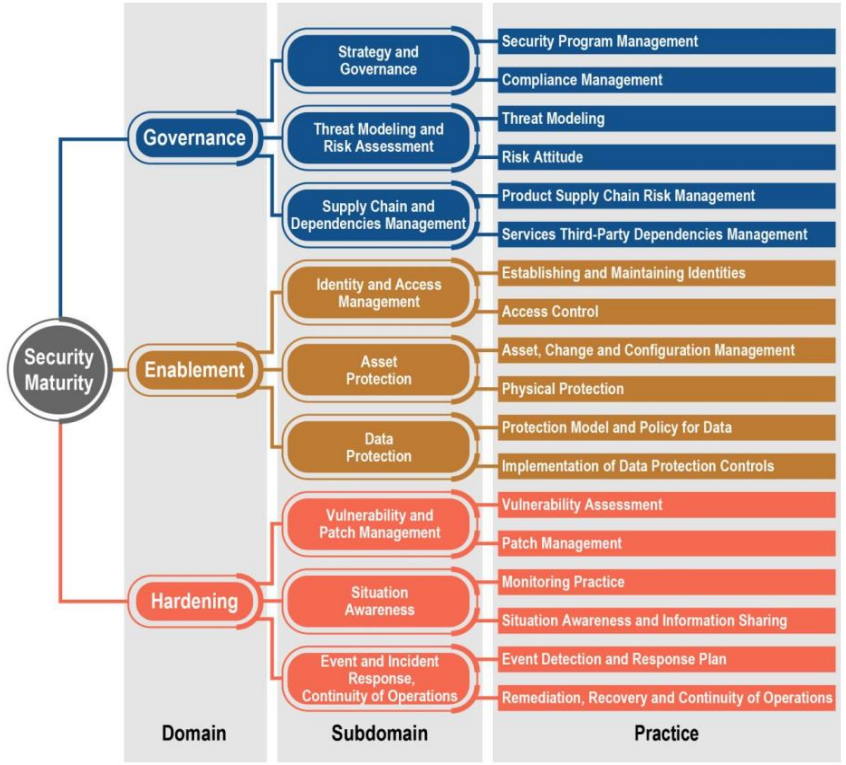
Expect error

Structure the choices

Structure complex choices

As choices become more numerous, though, good choice architecture will provide structure, and structure will affect outcomes

SMM provides the practices hierarchy as a choice architecture for cybersecurity



iNcentives

Understand mappings choice/welfare

Defaults / Least resistance

Give feedback

Expect error

Structure the choices

Understand Mappings choice/welfare

Some tasks are easy like choosing a flavor of an ice cream. Other tasks are hard like choosing a medical treatment

IoT SMM Practitioners Guide establishes connections between levels and goals/needs/practice purpose, and between levels and actions to be done, thus clearly mapping actions to high-level goals

Practice	Typical purpose definition	Comprehensiveness Level
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	4 / Formalized

Goal – concern – practice purpose – what needs to be done

iNcentives

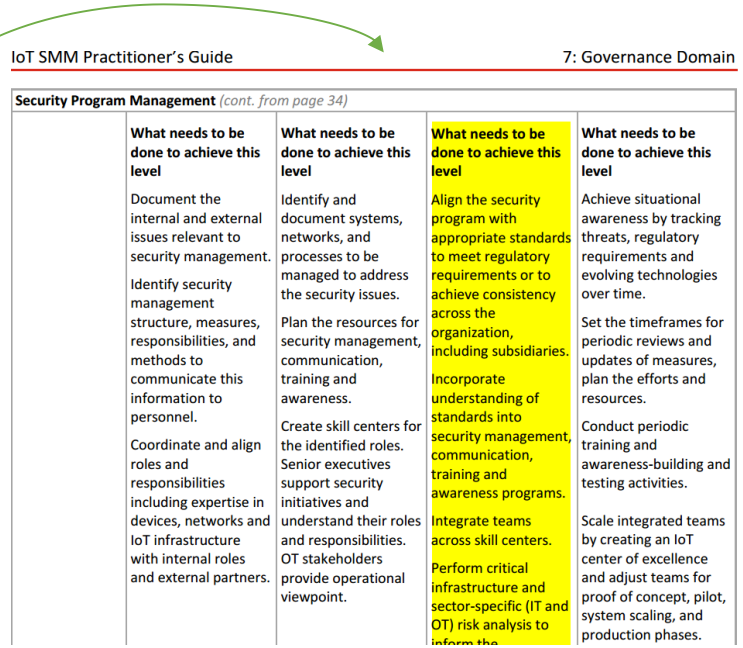
Understand mappings choice/welfare

Defaults / Least resistance

Give feedback

Expect error

Structure the choices



IoT SMM Practitioner's Guide 7: Governance Domain

Security Program Management *(cont. from page 34)*

	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**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.	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. Senior executives support security initiatives and understand their roles and responsibilities. OT stakeholders provide operational viewpoint.	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	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.

Defaults

Defaults are important because of

- Inertia
- Status quo bias
- “Yeah, whatever” heuristic

IoT SMM Practitioners Guide helps to set up the meaningful defaults depending on the results of the very simple initial interview about the goals

Goal definition sets up

- The level of comprehensiveness for domain
- The initial level of comprehensiveness for subdomain (“concern by default”)
- The initial level of comprehensiveness for practice (“practice purpose by default”)
- Actions to be done by default

iNcentives

Understand mappings choice/welfare

Defaults / Least resistance

Give feedback

Expect error

Structure the choices

Give feedback and Expect error

Well-designed systems tell people when they are doing well and when they are making mistakes. A well-designed system expects its users to err and as is forgiving as possible

In IoT SMM, the processes are repeated and duplicated.

The practices hierarchy do not allow to assign the inconsistent requirements to the practices implementation

(e.g., impossible to assign poor requirements to patch management if the system requires hardening)

iNcentives

Understand mappings choice/welfare

Defaults / Least resistance

Give feedback

Expect error

Structure the choices

iNcentives

The proposed way on how to think about incentives:

Who pays?

Who chooses?

Who pays?

Who profits?

The IoT SMM helps to set up the dialogue about incentives valid for all parties and agree on the solution that fits most of them

The cybersecurity market (as many others) is replete with incentives conflict:

- Possible losses from attacks
- Requests on efficient and secure solutions
- Short time-to-market for IoT products
- Regulatory requirements
- …

iNcentives

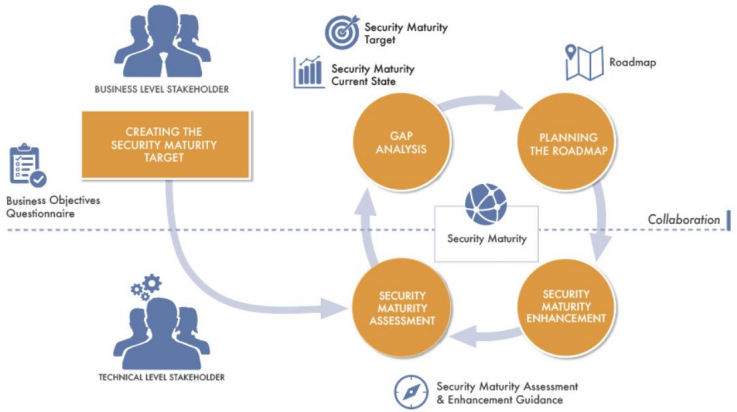
Understand mappings choice/welfare

Defaults / Least resistance

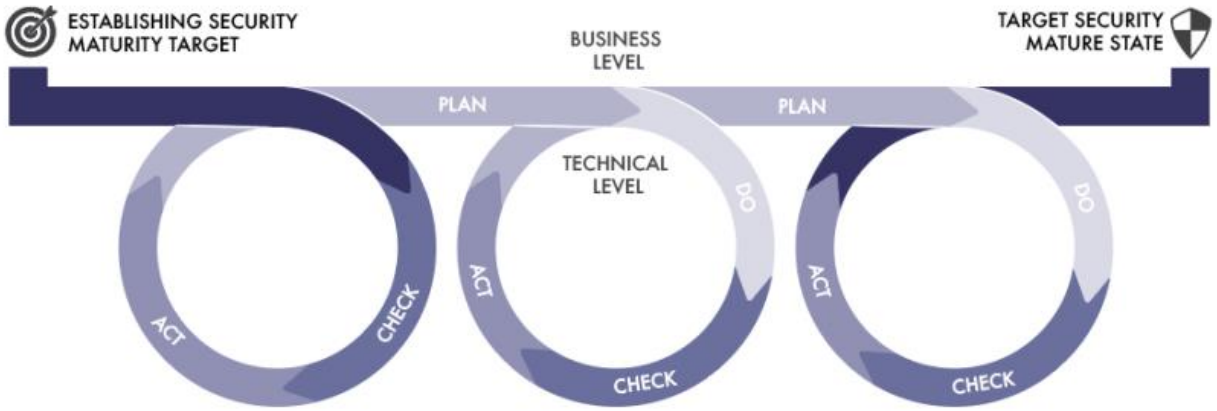
Give feedback

Expect error

Structure the choices



The advantages of using IoT SMM Approach



The **Security Maturity Profile** plays a role of the security standard for the solution and helps the stakeholders to align their security concerns and appropriate measures to address these concerns

Assessment for Security Maturity fosters the collaboration of potential users, business stakeholders and high-level technicians/security specialists

Security requirements can be tailored to the **specific needs** of particular solution and organized according to the recognized framework

We do not have to waste the time on assuring the requirements that make no sense in regard to the solution

Scoring and roadmap planning are covered by the method. Lifecycle-based approach helps with setting the priorities and enhancement of Security Maturity for the selected security practices.

The method does not separate security enhancement and security evaluation, thus making the process much more effective

Thank You