# IIC Security Applicability Task Group


December 2019

Ron Zahavi co-chair SATG

Microsoft

# Security Applicability Task Group

- Purpose
  - Make IISF actionable
- How
  - By defining best practices
  - Creating the IoT Security Maturity Model
  - Capturing use cases
  - Capturing case studies

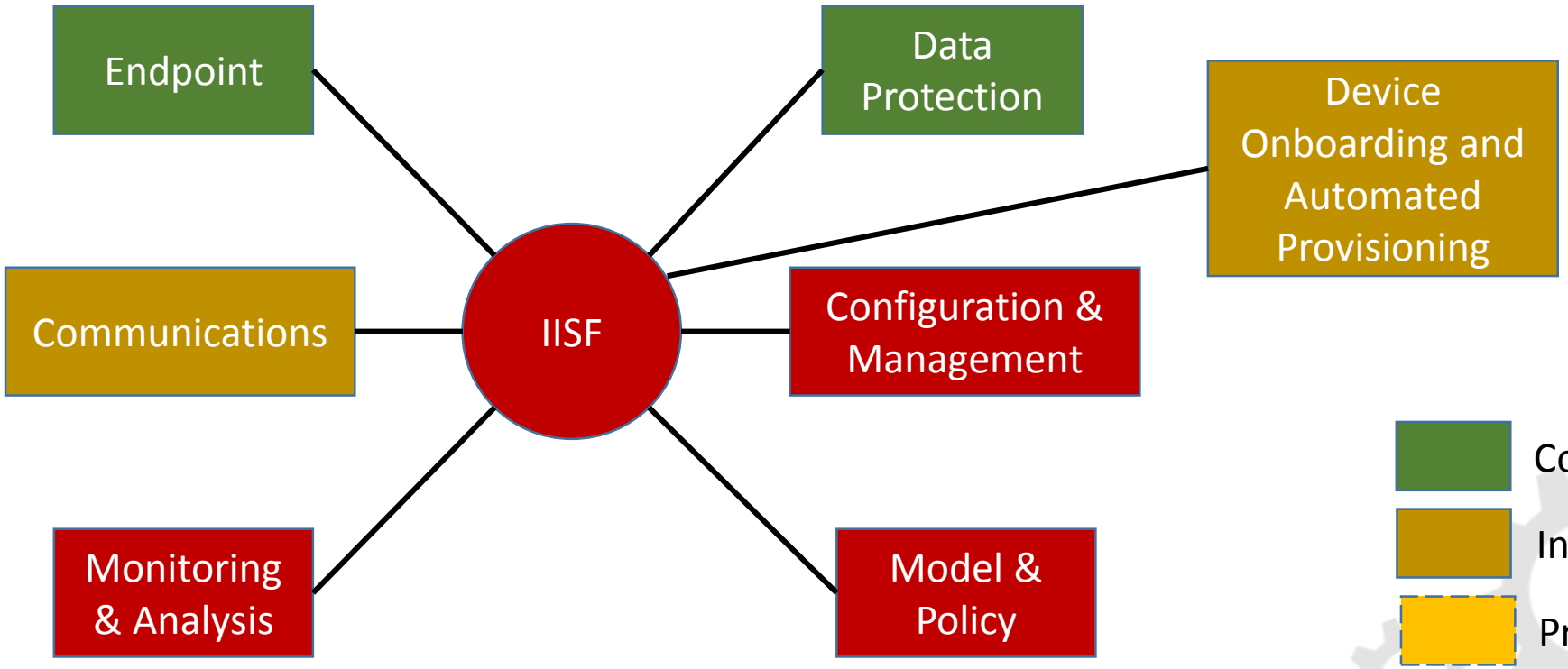
**Our Focus Today**

industrial internet CONSORTIUM

# Best Practices

# How will we develop these Best Practices?

Create one Best Practices document for each of six Building Blocks in IISF



industrial internet CONSORTIUM

# IoT Security Maturity Model (SMM) - Introduction

# Top Security Concerns: What does “system is secure” mean?

- Is my IoT infrastructure developed, deployed and operated securely?
- By deploying IoT which security risks am I taking for the rest of my business?
- Who can evaluate my IoT infrastructure and give me a threat assessment?
- How much should I spend on security for my needs?
- How do I identify actions I need to take including process improvements, security techniques and security mechanisms?

# Not All Systems Need the Same Level of Security

Home smart lighting

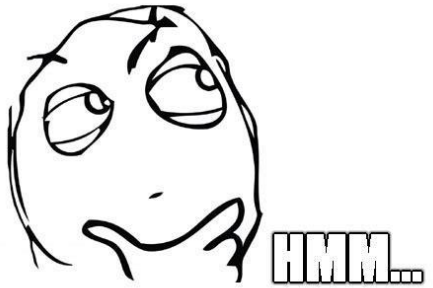
Manufacturing floor

IT security vs. trustworthiness (privacy, safety, etc.)

IT

OT

# Establish and Assess Against a Target



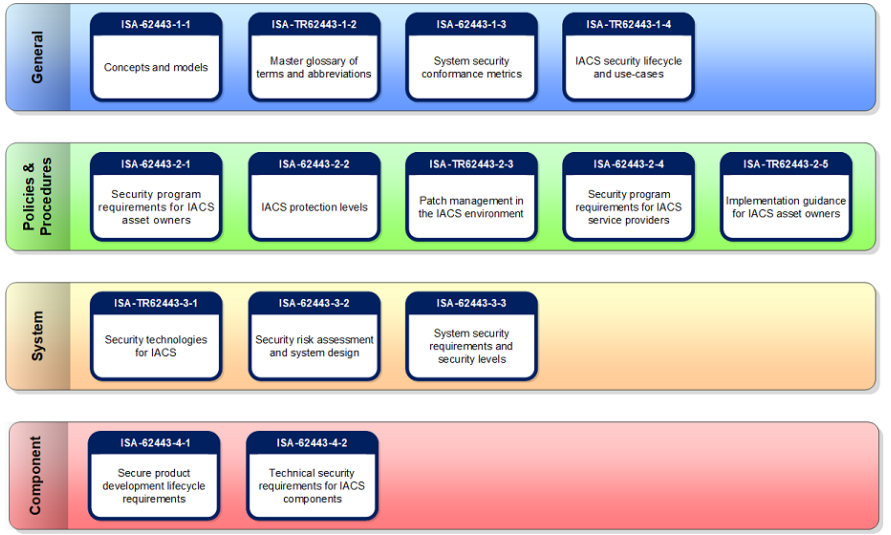

And need consistency in assessing…..


5

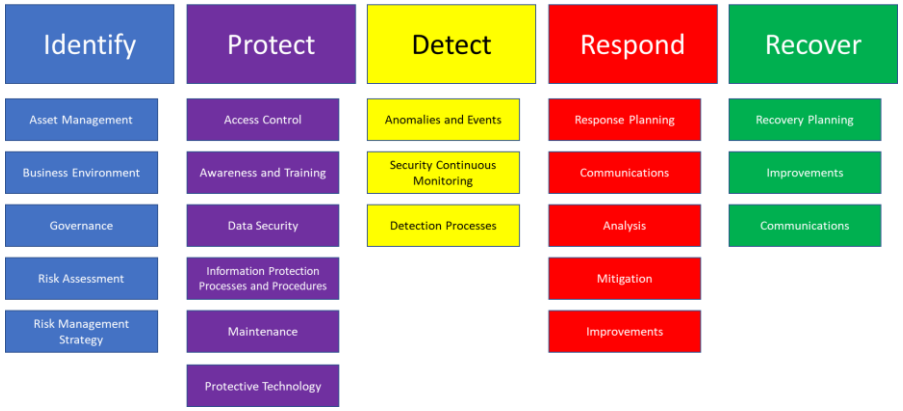
# Many Frameworks but no Single Standard

## Common Criteria

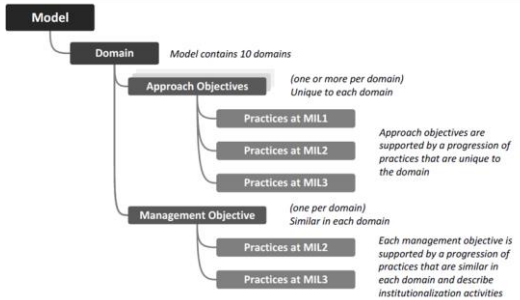
| Level | Description |
|---|---|
| EAL 1 | Functionally tested |
| EAL 2 | Structurally tested |
| EAL 3 | Methodically testbed and checked |
| EAL 4 | Methodically designed, tested, and reviewed |
| EAL 5 | Semiformally designed and tested |
| EAL 6 | Semiformally verified design and tested |
| EAL 7 | Formally verified design and tested |

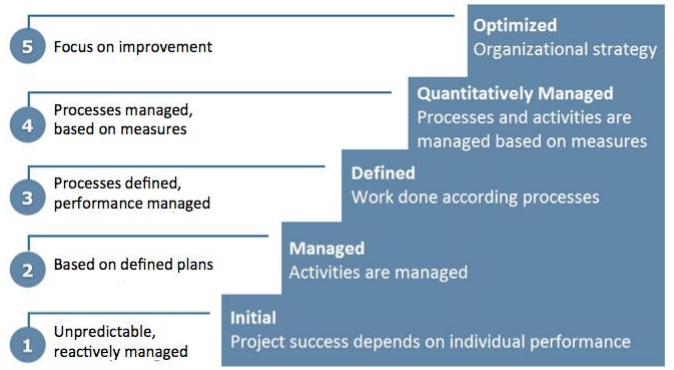



## NIST Cyber Security Framework




## C2M2



# Security Maturity vs. Security Level

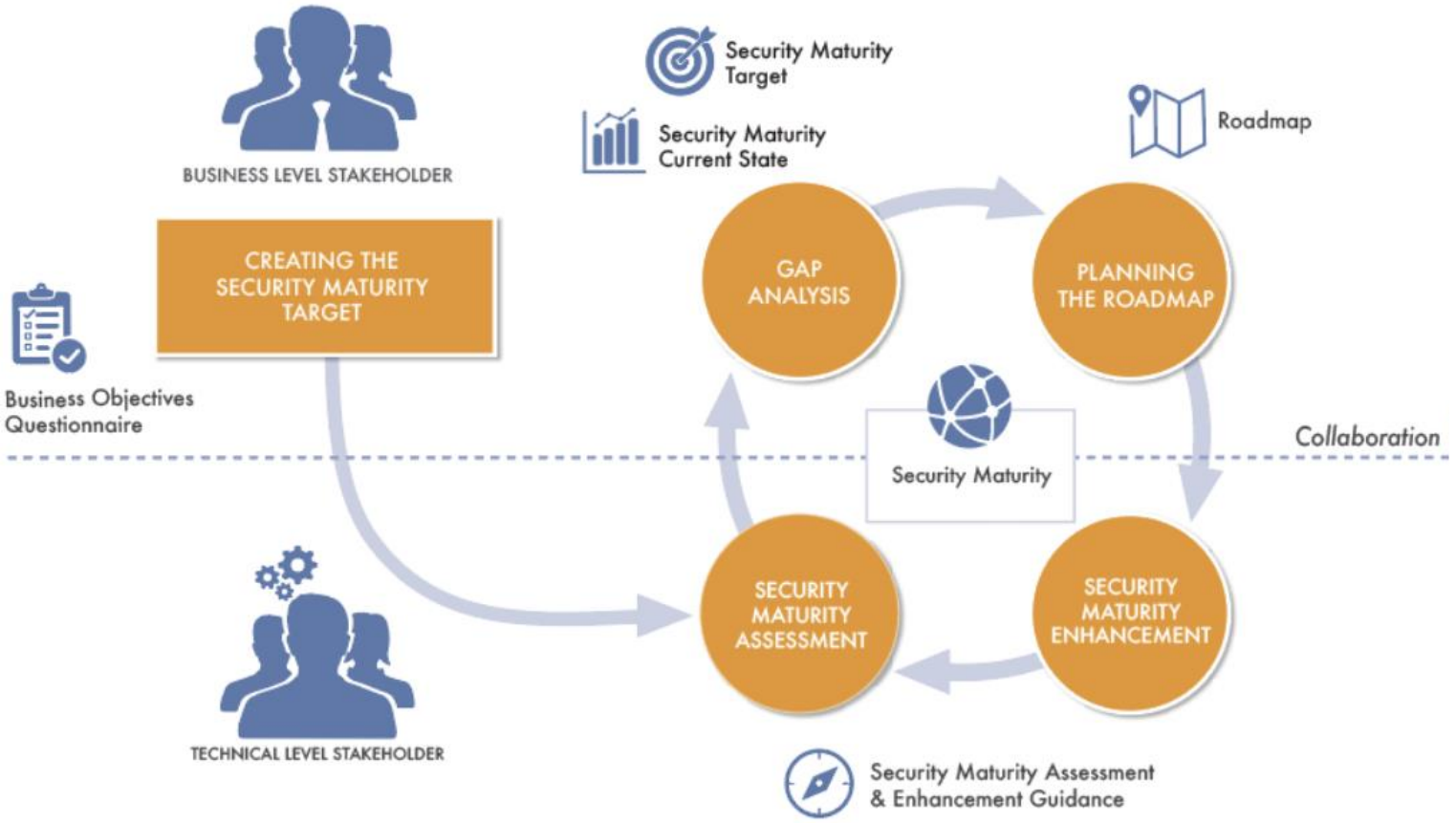
**Security maturity** is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.

| None | Minimum | Ad Hoc | Consistent | Formalized |
|---|---|---|---|---|
| | • Minimum requirements implemented<br>• No assurance activities | • main use cases<br>• well-known security incidents<br>• similar environments<br>• Assurance: ad hoc reviews<br>• baseline mitigations | • Consider best practices, standards, regulations, classifications<br>• Use software and other tools.<br>• assurance: security patterns, secure-by-default designs and known protection approaches and mechanisms | • Well-established process forms the basis<br>• continuous support and security enhancements.<br>• assurance: focus on the coverage of security needs and timely addressing of issues |

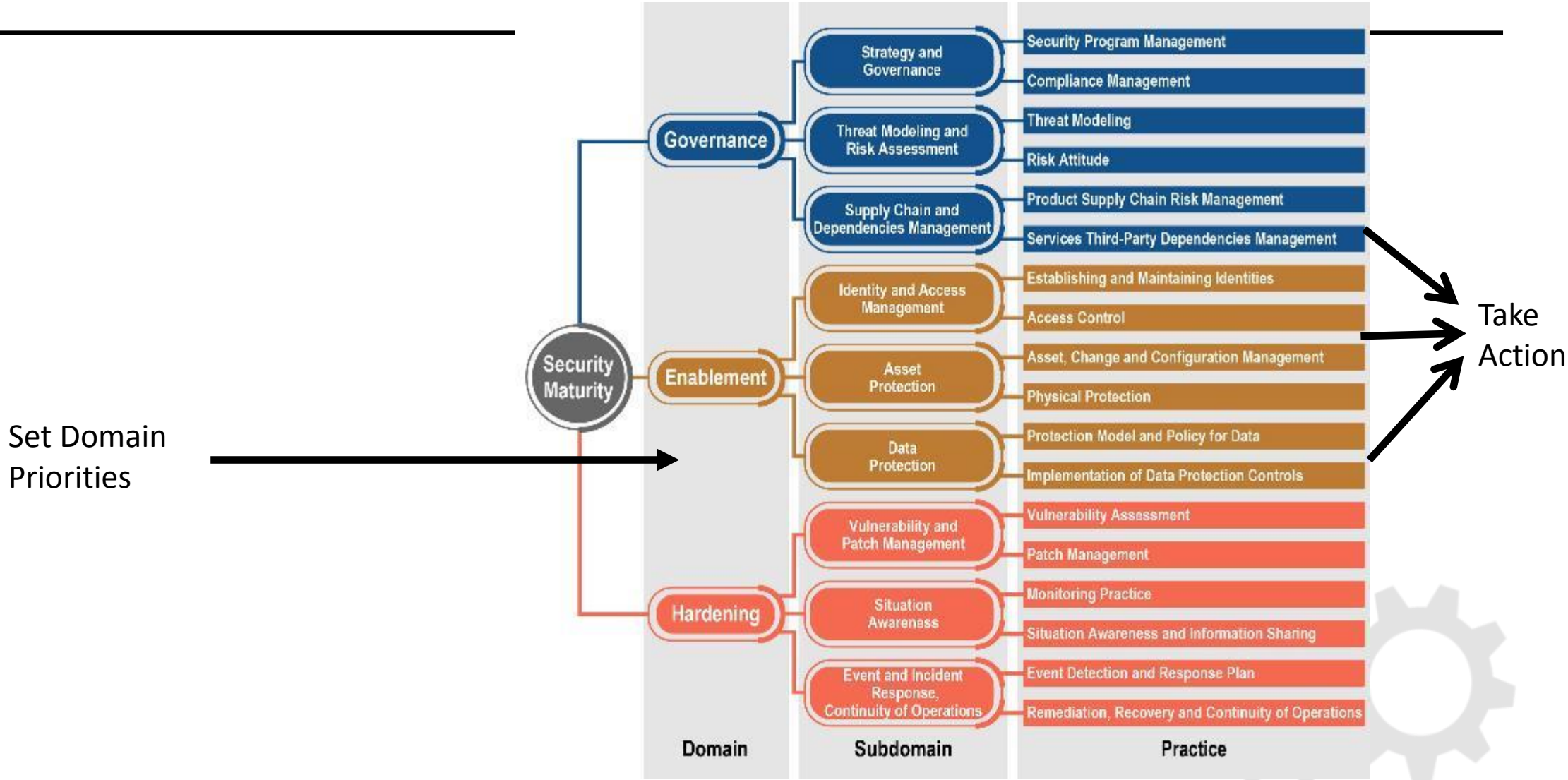
**Security level** is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.

| Security Level (SL) | Description from IEC 62443-1-1 section 10.4.3 |
|---|---|
| 0 | No specific requirements or security protection necessary |
| 1 | Protection against casual or coincidental violation |
| 2 | Protection against intentional violation using simple means with low resources, generic skills and low motivation |
| 3 | Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation |
| 4 | Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation |

# Process


BUSINESS LEVEL STAKEHOLDER
Security Maturity Target
Security Maturity Current State
Roadmap
CREATING THE SECURITY MATURITY TARGET
GAP ANALYSIS
PLANNING THE ROADMAP
Business Objectives Questionnaire
Collaboration
Security Maturity
SECURITY MATURITY ASSESSMENT
SECURITY MATURITY ENHANCEMENT
TECHNICAL LEVEL STAKEHOLDER
Security Maturity Assessment & Enhancement Guidance

# SMM Structure and Tables



# Domain Definitions

**Governance**

- The subdomains and practices that have to do with setting the security strategy, understanding risk, and managing the overall security program

**Enablement**

- The subdomains and practices focused on implementing the policy and controls to manage identity and protect physical assets, digital assets and data

**Hardening**

- The subdomains and practices related to managing security operations, vulnerability and patch management, monitoring and response

# 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 business 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 **how** the practice supports specific security activities.

# Measuring the Security Maturity

**Why do we need measuring?**

(1) To compare with other similar systems

(2) To compare with an “ideal” target

(3) To understand what needs to be done to achieve the target

(4) For consistency of results and presentation

# Two Dimensions

*Comprehensiveness* captures the degree of depth, consistency and assurance of security measures that support security maturity domains, subdomains or practices.

*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, subdomains or practices.

# 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.

# Template and Tables

| **<Practice-Name>** | | | | |
|---|---|---|---|---|
| *<Practice Description>* | | | | |
| | **Comprehensiveness Level 1** | **Comprehensiveness Level 2** | **Comprehensiveness Level 3** | **Comprehensiveness Level 4** |
| **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**<br><br>Considerations | **What needs to be done to achieve this level**<br><br>Considerations | **What needs to be done to achieve this level**<br><br>Considerations | **What needs to be done to achieve this level**<br><br>Considerations |
| | **Indicators of accomplishment**<br><br>Considerations | **Indicators of accomplishment**<br><br>Considerations | **Indicators of accomplishment**<br><br>Considerations | **Indicators of accomplishment**<br><br>Considerations |

Levels include all the considerations of the lower levels

# Profiles

- At a practice level
- Adding information to “what’s needs to be done” and “indicators of accomplishment” that is specific to an industry or system (scopes)
- This extends the tables into a profile
- Profiles can be industry and/or system
- Profiles make the general considerations more specific or provide more detail
- Industry profiles can add information to general scope, or to system scope as well
- Information does not have to be added to all tables

# More detailed General Considerations (1/2)

***Practice: Threat Modeling of Medical Devices including a handheld that collects patient telemetry and a base station aggregates patient vitals and shares data across a hospital network.***

| | ***Comprehensiveness Level 1*** | ***Comprehensiveness Level 2*** | ***Comprehensiveness Level 3*** | ***Comprehensiveness Level 4*** |
|---|---|---|---|---|
| **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.<br><br>**What needs to be done to achieve this level**<br><br>Collect the available information about typical IT security vulnerabilities and incidents, and recognize those which are relevant as threats.<br><br>**Indicators of accomplishment**<br><br>Business level documents mention general security threats, such as sensitive data disclosure, denial of service attacks, or infiltration with malware | At this level, the organization performs an actual vulnerability assessments to understand threats as they pertain to the organization. The organization can discern specific IT vs. IoT threats.<br><br>**What needs to be done to achieve this level**<br><br>Perform a vulnerability assessment for IT, OT, and IoT (at this level they are typically managed separately).<br><br>Use the generally accepted vulnerability evaluation schemes (such as Common Vulnerability Scoring System or CVSS).<br><br>**Indicators of accomplishment**<br><br>- A vulnerability assessment report is available and identifies common and typical threats valid for the | At this level accepted formal threat modeling methodologies are used, and automated tools are used for thread modeling.<br><br>**What needs to be done to achieve this level**<br><br>Describe the threats during the analysis using a generally accepted classifications like CAPEC or OWASP Top10.<br><br>Optionally use the tools to describe the architecture of the system to automatically identify threats and possible resolution.<br><br>Address the IT, OT, and IoT-specific (for example, edge device physical compromise) threats.<br><br>Consider the results of threat modeling and risk assessments as a part of formal processes to address and prevent the identified concerns.<br><br>**Indicators of accomplishment**<br><br>Identified tools and | At this level threat modeling is built into business processes and driven by business goals and risk profile.<br><br>**What needs to be done to achieve this level**<br><br>Validate the security threats against objectives set according to business needs.<br><br>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.<br><br>Organize the particular threats and attack vectors as a consistent hierarchical structure, including all identified security issues<br><br>**Indicators of accomplishment** |

# More detailed General Considerations (2/2)

| | |
|---|---|
| **Industry Specific Considerations** | - **Level 3 and higher: Note: FDA guidance can be interpreted to require that a medical device manufacturer reach or exceed a level 3 comprehensiveness in threat modeling as part of a pre-market submission.**<br>- **The threat model takes into account FDA guidance for post-market management of cybersecurity in medical devices**<br>**FDA requirements for pre-market submissions related to cybersecurity: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf**<br>**FDA post-market guidance on managing cybersecurity in medical devices: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf**<br>- **Level 4: threat model includes not only the device in isolation, but the medical environments in which the device will operate.**<br>- **Level 4: threat model includes scenarios in which the device could allow its users to violate HIPAA standards (such as by leaking PII), and seeks to mitigate those opportunities.** |
| **Handheld Specific Considerations** | - The handheld collects only anonymized patient telemetry data. Its exposed attack surfaces are Bluetooth LE, USB, and physical access. |
| **Base station Specific Considerations** | - The base station aggregates patient telemetry with PII, making the data it stores and transmits HIPAA relevant. Its exposed attack surfaces include Bluetooth LE, USB, Wi-Fi, Ethernet, and physical access. |

# What a Security Maturity evaluation result looks like

We need a representation for the evaluated Security Maturity of the system:

- 18 practices
- Every practice has the comprehensiveness level
- Every practice has the scope

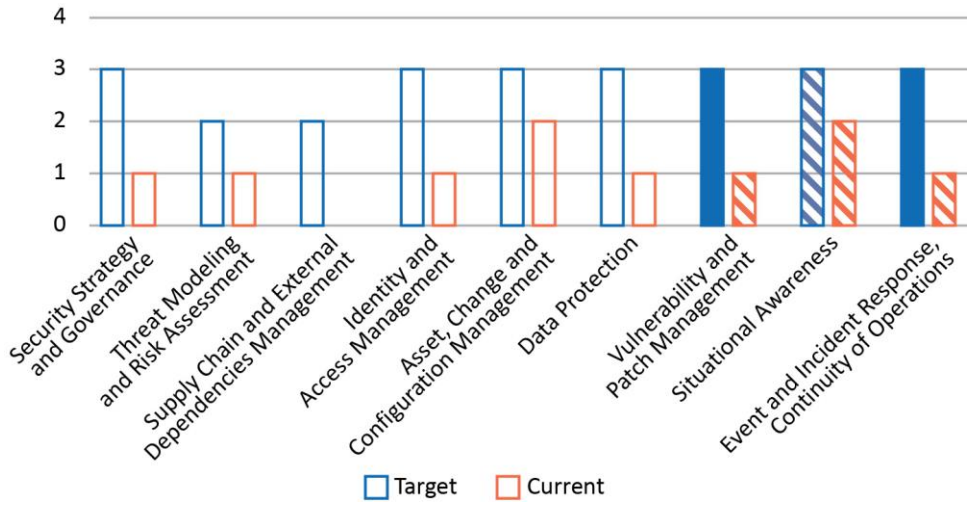
So, this is NOT a single score

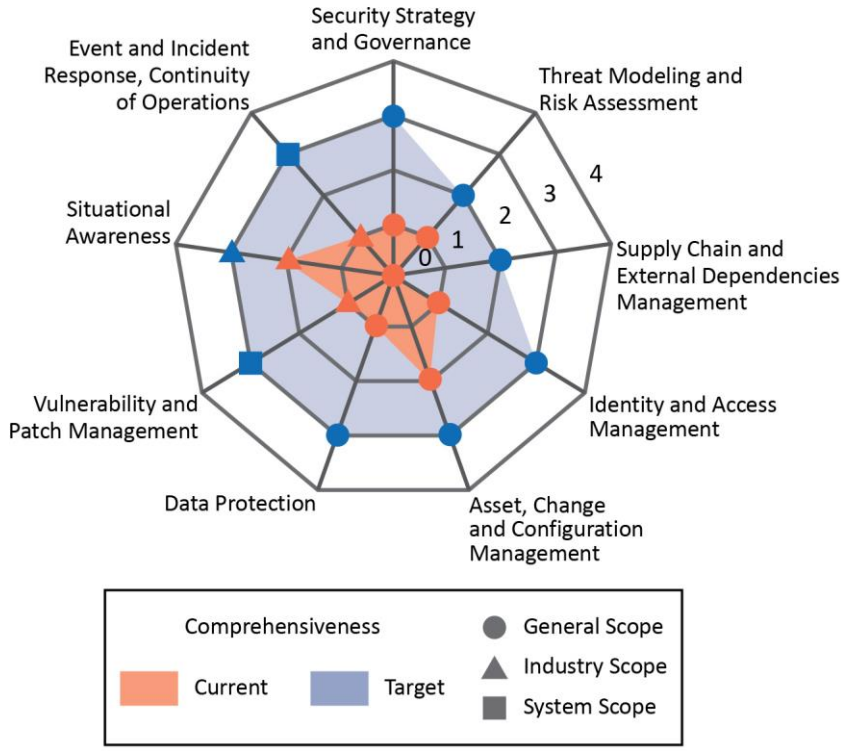
It is the state represented by 36 separate characteristics

We call the “ideal” state the **Security Maturity Target**

# Flexible visualization options

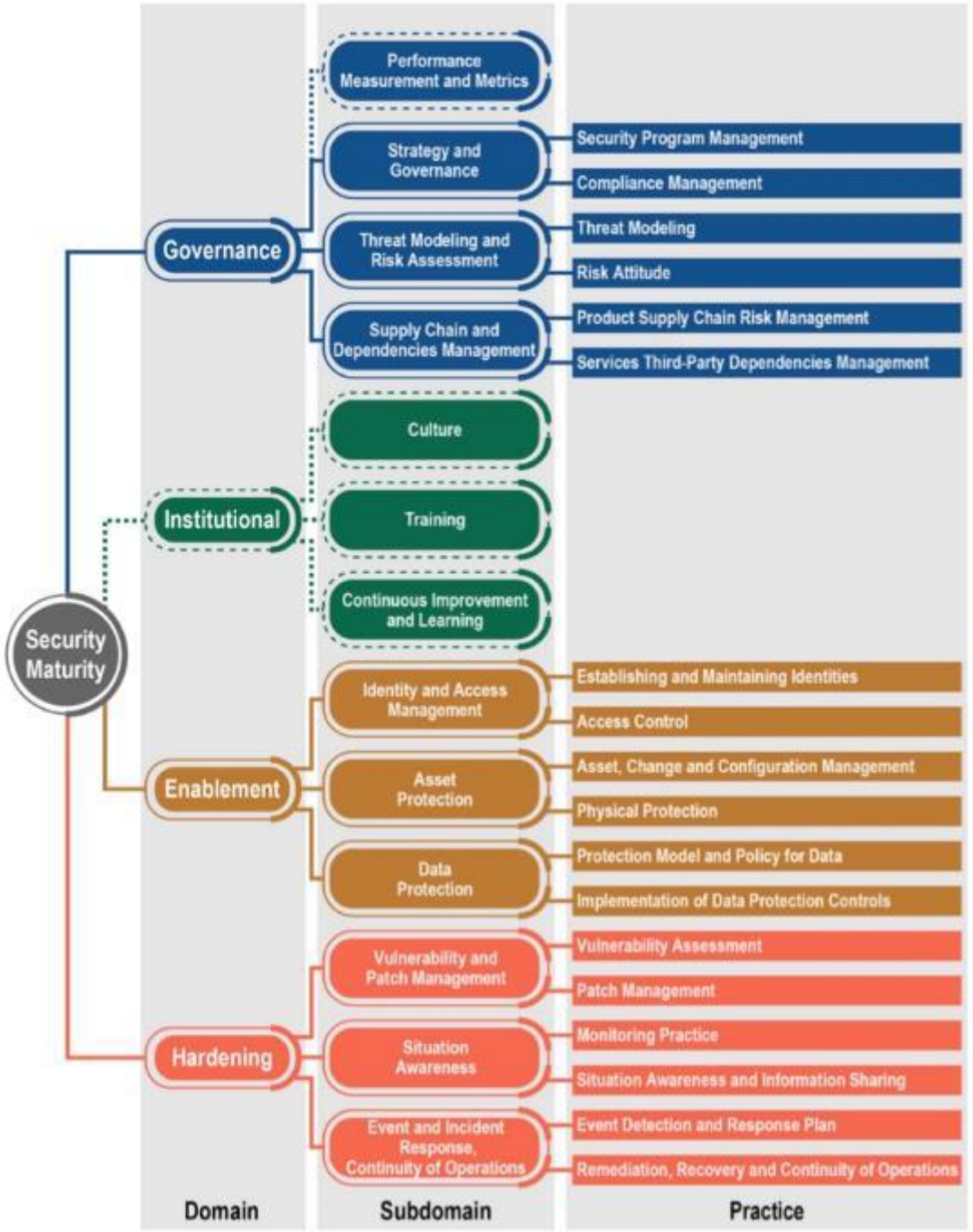
| | Target | Current | Target Scope | Current Scope | Gaps: Comprehensiveness | Gaps: Scope |
|---|---|---|---|---|---|---|
| Security Strategy and Governance | 3 | 1 | 1 | 1 | | |
| Threat Modeling and Risk Assessment | 2 | 1 | 1 | 1 | | |
| Supply Chain and External Dependencies Management | 2 | 0 | 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 | | |



# Security Maturity Model Extends to Trustworthiness

- Concept of maturity and appropriate investment applies
- Organized and effective process toward managing investment
- Comprehensiveness and Scope concepts extended
- New Domains, Subdomains and Practices can be added as needed



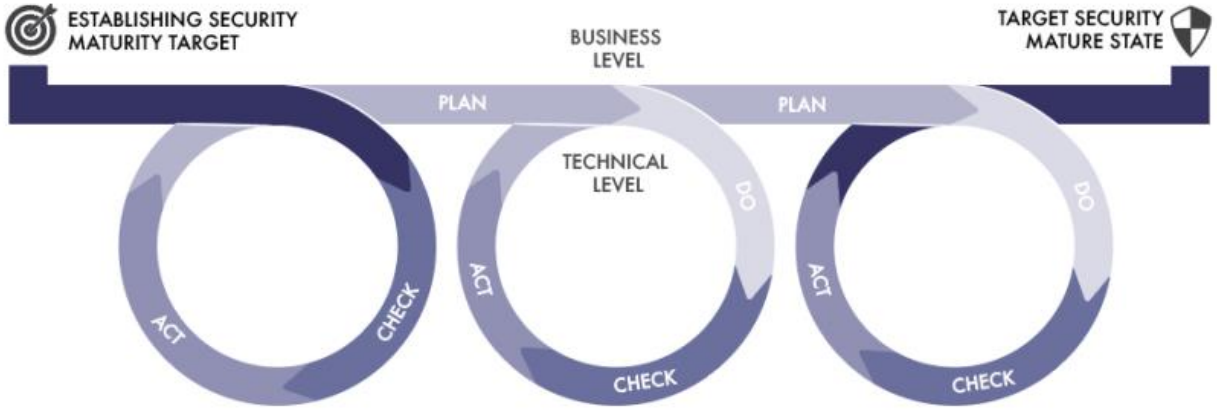
# Mappings

- SMM is a maturity model, does not include specific security controls
- There are other control frameworks (NIST, 62443, etc.)
- Issue: how do you know which controls to use and how much you need?
- We have mapped the SMM to these frameworks
- You can identify your desired maturity level and then trace to the appropriate controls that are relevant

| 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 | | Comprehensiveness Level 2 | | Comprehensiveness Level 3 | | Comprehensiveness Level 4 | |
| | What needs to be done to achieve this level | Indicators of accomplishment | What needs to be done to achieve this level | Indicators of accomplishment | What needs to be done to achieve this level | Indicators of accomplishment | What needs to be done to achieve this level | Indicators of accomplishment |
| **NIST Framework** | | ID.GV-2 PR.AT-5 | | ID.BE-2 PR.AT-4 ID.GV-1 | | ID.GV-3 ID.RM-3 PR.IP-8 | | PR.AT-1 RC.RP-1 |
| **ISO/IEC 27001:2013** | A.6.1.1 A.7.2.1 A.7.2.2 | | A.6.1.1 A.7.2.2 | A.5.1.1 | | A.18.1 A.16.1.6 | | A.16.1.5 |
| **ISA 62443-2-1:2009** | 4.3.2.3.3 4.3.2.4.2 | | | 4.3.2.6 | 4.4.3.7 | | | |
| **NIST SP 800-53 Rev. 4** | PM-1 PS-7 AT-3 PM-13 CP-2 PM-11 | | PM-8, AT-3, PM-13, CP-2, PS-7, PM-11 | | PM-8, PM-9, PM-11, SA-14, AC-21, CA-7, CP-2, PS-7, SI-4 | | AT-2 PM-13 CP-2 | CP-10, IR-4, IR-8 |

DRAFT

# 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

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

**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.

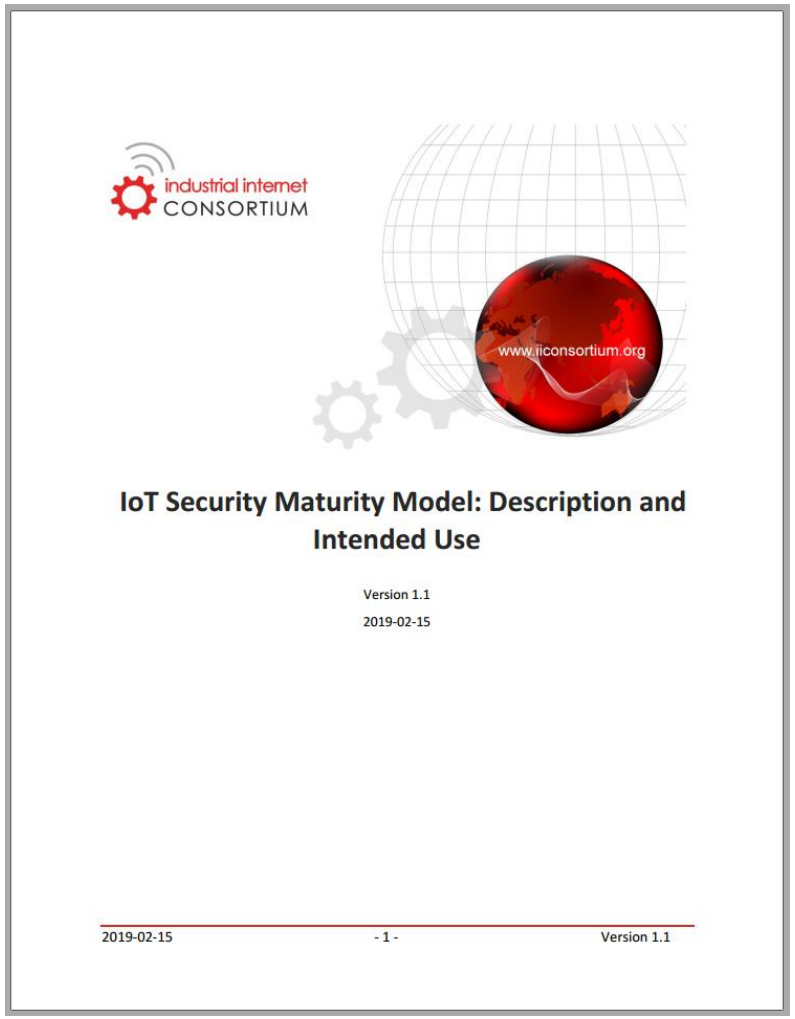
**Assessment for Security Maturity fosters the collaboration of potential users, business stakeholders and high-level technicians/security specialists**

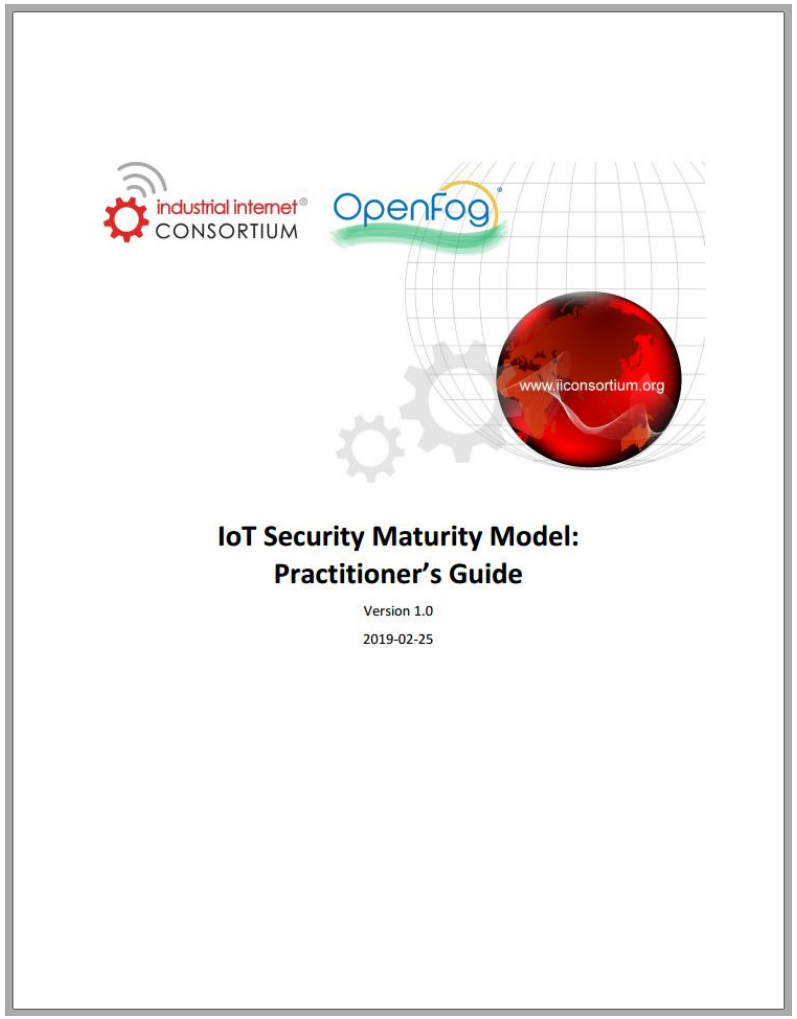
**We do not have to waste the time on assuring the requirements that make no sense in regard to the solution**

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

# Next Steps

1. Do you want to conduct an assessment using SMM?
2. Do you want to start a consulting practice that conducts assessments?
3. Do you want to adapt your existing consulting assessment practice?
4. Are you interested in more hands-on classes and certification?




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


As secure as you need to be!