IoT Security Maturity Model
Augmented Reality Profile

An AR for Enterprise Alliance White Paper

2024-12-16

Authors
Ron Zahavi (Auron Technologies, LLC), James Cooper (Raytheon, an RTX Company),
Mik Bertolli (Avrio Analytics), Mihir Kamdar (The AREA)

Contents

Figures

Tables

1 THE IOT SECURITY MATURITY MODEL

The goal of an SMM is to provide a path for Internet of Things (IoT) providers to know where they need to be, and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms. It seeks to help organizations identify the appropriate approach for effective enhancement of these practices where needed. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

As an informed understanding of the risks and threats an organization face is the foundation of choosing and implementing appropriate security controls, the model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

Not all IoT systems require the same strength of protection mechanisms and the same procedures to be deemed "secure enough". The organization 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 implementation 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 needs and security-related requirements. Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support. Factors to weigh in such an analysis include the specific threats to an organization's industry vertical, regulatory and compliance requirements, the unique risks present in an environment and the organization's threat profile.

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 not say what the appropriate security level should be; it provides guidance and structure for organizations to identify considerations for different maturity levels appropriate for their industry and system. It provides guidance for defining and accounting for different levels of comprehensiveness and alignment with industry sector and system, including non-industrial systems. Some users of the model will apply its guidance to create industry- and system-specific

[1] Security level according to [*IEC-62443-33*].

profiles, which can then be used by a broader audience, in concert with the model, to help assess maturity in a specific vertical or use case.

The audience for this document includes owners of IoT systems, decision makers, security leaders in various verticals, business risk managers, system integrators, architects, security assessors, analysts, policy and regulatory authorities, and other stakeholders concerned about the proper strategy for the implementation of mature security practices tailored to the needs and constraints of the specific IoT system.

Those using this SMM should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements[2] 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?

1.1 THE SMM PROCESS

Organizational business stakeholders define goals for the security posture of the organization and the systems it owns or operates. These systems may be brand new or brownfield. These goals should be mapped to objectives that tie to the risks. Technical teams within the organization, or third-party assessment vendors, map these objectives into tangible security techniques and capabilities, identifying the appropriate target security maturity state.

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

1.2 UNDERSTANDING THE MODEL

Figure 1-1 illustrates the structure of the SMM and the breakdown of security maturity domains. *Domains* are the high-level views that capture the key aspects of security maturity: governance, enablement and hardening. Each of the domains has different key aspects to it, called *subdomains*. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

[2] Given the organizational requirements, namely, business or mission needs, requirements from regulatory authorities, and other similar factors.

This hierarchical approach enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

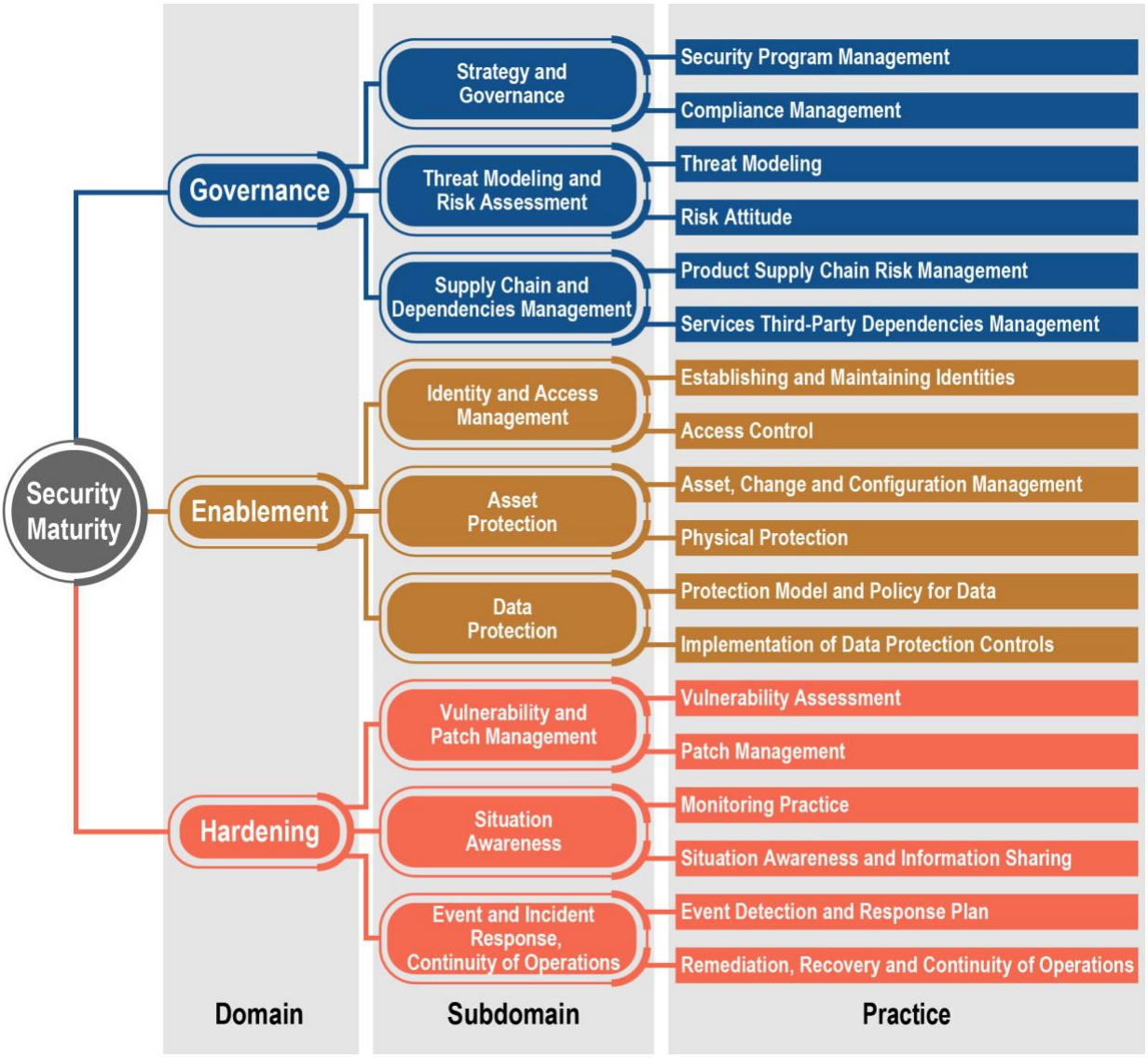

Figure 1-1: SMM hierarchy.

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 subdomains level, the stakeholder identifies the typical needs for addressing security concerns.

1.2.1 SECURITY GOVERNANCE

Figure 1-2 below describes the elements of the governance domain of the SMM.

The security governance domain is the heart of security. It influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation.

Security strategy and the governance subdomain facilitates organizational drivers along with providing security, compliance with regulations, laws and contractual obligations. This also can relate to customer expectations and reputation management.

Security program management practice is vital to the clear planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.	**Compliance management practice** is necessary when strict requirements for compliance with evolving security standards is needed.

Threat modeling and the risk assessment subdomain identifies gaps in specific configurations, products, scenarios and technologies and prioritize countermeasures accordingly.

Threat modeling 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.	**Risk attitude 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.

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

Product Supply chain risk management 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.	**Services Third-Party dependencies management 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.

Figure 1-2: Security governance.

1.2.2 SECURITY ENABLEMENT

Figure 1-3 below describes the elements of the enablement domain of the SMM.

The security enablement domain is based on established security policy and addresses the business risks using the best available means. Security policy and controls are subject to periodic review and assessment.	
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.	
Establishing and maintaining identities practice helps to identify and constrain who may access the system and their privileges.	**Access control practice** 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.
The asset management subdomain is put in place to protect both physical and digital assets. This is an area of strong collaboration between IT and physical security teams.	
Asset, Change and Configuration Management practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.	**Physical protection practice** 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.
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.	
The security model and policy for data practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.	**The implementation of data protection controls practice** describes the preferred application of data protection mechanisms to address confidentiality, integrity, and availability.

Figure 1-3: Security enablement.

1.2.3 SECURITY HARDENING

Figure 1-4 below describes the elements of the security hardening domain of the SMM.

The security hardening domain practices support trustworthiness objectives through the assessment, recognition, and remediation of risks with both organizational and technical countermeasures.	
Vulnerability and the patch management subdomain policies and procedures keep systems up to date and less prone to attacks.	
Vulnerability assessment practice helps to identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.	**Patch management practice** policy 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.
The situational awareness subdomain aims at understanding the current security state enabling an organization to prioritize and manage threats more effectively.	
Monitoring practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.	**Situational Awareness and Information sharing practice** helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.
Event and incident response, continuity of operations subdomain implemented in a combination of policy and technical preparation allows an organization to respond to incidents swiftly and minimize disruption to the rest of the system.	
An event detection and response plan define 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.	**Remediation, recovery, and continuity of operations** represent 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.

Figure 1-4: Security hardening.

1.3 Applying the Model

Two aspects are essential for measuring the maturation progress of IoT systems and prioritizing associated security practices: comprehensiveness and scope. These are considered within the

context of the target and assessment, namely the system of interest, whether end-to-end, a component or a sub-system under consideration.

Comprehensiveness captures the degree of depth, consistency and assurance of security measures that support security maturity domains, subdomains, or practices. 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, subdomains, or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

1.3.1 SCORING AND PRIORITIZATION

Any rigorous security self-assessment procedure, including the SMM, needs a scoring and prioritization method to enable evaluation of the current state and the development of a metrics-based security strategy.

Comprehensiveness and scope, which are orthogonal, help score and prioritize security maturity practices. Certain IoT systems may not require the highly sophisticated or narrowly scoped implementation of all security practices. Such implementation may be over-engineered, given the particular system and the threats that it faces. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

1.3.2 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 of security controls. 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 is null, we shall 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, application of measures learned through successful references may be applied.

- *Level 3, Consistent:* The requirements consider best practices, standards, regulations, classifications, software, and other tools. Using such tools helps to 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 on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. For this assurance, a more complex approach is applied that uses semi-formal to formal methods.

1.3.3 SCOPE

The scope measurement captures the extent to which the specifics of an application, network or system of interest is taken into account during the implementation of the security facet.

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

- *Level 1, General:* This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific 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 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. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

1.3.4 SMM TEMPLATE

All IoT devices, networks and systems do not require the highest comprehensiveness and scope for all security domains, sub-domains, or practices. The security maturity target for the system of interest is defined as the set of all desirable values of comprehensiveness and scope characteristics for every security maturity domain, sub-domain, and practice.

In case of insufficient details about the system-security needs the stakeholders may initially determine the target levels of comprehensiveness and scope just for domains. These levels determine the relative priorities of security governance, enablement and hardening. The levels set for the domains will be inherited by the appropriate sub-domains and then by the practices according to the hierarchy. The stakeholders may modify the levels to match the risks more closely. This is helpful for the step-by-step recognition of an uncertain security maturity target.

The security maturity target by default is defined when referring to the comprehensiveness and scope for security maturity practices as seen in The Security Maturity Model Practitioner's Guide.[3] 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.

	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>

Table 1-1: SMM template.

1.4 SECURITY MATURITY PROFILES

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 AR for Enterprise Alliance 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

[3] The Security Maturity Model Practitioner's Guide, *[IIC-SMMP2020].*

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 1-2 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 1-2: 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.

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.

This Augmented Reality profile provides considerations at the system-specific scope. Augmented Reality devices may be applicable to a variety of industries, yet in each case the concerns about the Augmented Reality system are applicable, since they are system-specific. An industry profile may reference this profile without repeating the system-specific Augmented Reality concerns while elaborating the industry scope considerations.

As the general and industry rows in the table included headings and structure described above, the system row should include a description of the system and how it is used in the larger IoT infrastructure and for a comprehensiveness level with industry-specific considerations:

- What needs to be done to achieve that level and
- Indicators of accomplishment that can assist assessors in identifying if the organization has met the requirements of the 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.

SMM profiles may be used together for systems that span technologies and/or industries. The Digital Twin SMM Profile[4] describes the extensions to the SMM for digital twin systems. This document may be used together with the AR SMM Profile to understand what needs to be done and indicators of achievement for AR used in conjunction with digital twins.

2 AUGMENTED REALITY SECURITY CONSIDERATIONS

2.1 BACKGROUND

Augmented Reality offers the ability to visualize data and instructions overlaying digital assets in the real world in real time. This capability is delivering tremendous benefits to enterprises – increasing productivity, lowering costs, improving safety, enabling expertise to be shared more easily, and more. Organizations of all sizes across industries are taking advantage of AR to drive innovation, increase competitiveness, and accelerate business strategies.

[4] The Digital Twin Security Maturity Model Profile *https://www.digitaltwinconsortium.org/wp-content/uploads/sites/3/2022/06/SMM-Digital-Twin-Profile-2022-06-20.pdf*

Augmented Reality leverages the latest innovations in mobile technology, big data analytics and the Internet to offer new information-rich communication channels for enterprises.

Corporations of all sizes across industries are tapping into the potential of these rapidly expanding and converging fields and communication channels to visualize data and instructions overlaying digital assets in the real world in real time. The value of visualizing information in this manner offers many benefits.[5]

2.2 SCOPE

The scope of this document is limited to augmented reality, whilst there may be some overlap with virtual reality and mixed reality – the sections, maturity stages and writeup has been completed to the AR scope. Key aspects of AR technology encompass:

- **Hardware Diversity:** AR experiences can vary significantly based on the hardware used, including considerations such as field of view, display quality, and form factor. This influences the immersion level and usability of AR applications.
- **Software Tools:** Augmented reality development relies on Software Development Kits (SDKs), which provide the necessary tools, APIs, and frameworks for building applications.
- **Tracking and Localization:** AR systems typically rely on precise tracking and localization mechanisms to accurately map virtual objects onto the real world.
- **Marketplace:** Understanding the dynamics of the AR marketplace is vital for newcomers.
- **Market Momentum:** The AR market is witnessing substantial growth due to technological advancements and increased adoption across industries. Forecasts predict exponential expansion with a projected CAGR of over 40%, presenting ample opportunities.
- **Major Players:** Tech giants such as Apple, Google, Facebook, and Microsoft are heavily invested in AR technology. This concentration of influential players indicates the transformative potential of AR.
- **Challenges**: New practitioners should anticipate challenges such as hardware limitations, content quality, user acceptance barriers, and privacy concerns. Addressing these challenges proactively is essential for sustainable success.[6]

The AREA: The AR for Enterprise Alliance provides the support organizations need to assess, plan, and manage their enterprise Augmented Reality projects. Our up-to-date resources and neutral,

[5] Building a new industry together – Why an Alliance for Augmented Reality? *https://thearea.org/why-ar-for-enterprise/*

[6] AREA FAQ, *https://thearea.org/about-us/area-faq/*

reliable guidance make the path to AR adoption surer, shorter, and smoother. In addition, the AREA works to build and strengthen the AR ecosystem by identifying opportunities and challenges, spearheading research, and facilitating dialogue among AR providers and enterprises.[7]

2.3 AR CONSIDERATIONS

Augmented reality considerations are necessary to familiarize individuals with the technology, its applications, benefits, challenges, and potential impacts. This knowledge empowers people to make informed decisions, explore creative possibilities, and engage meaningfully with the evolving digital landscape:

- **Understanding the Concept:** Providing an introduction helps to define AR as a technology that overlays digital information onto the real world in real-time.
- **Differentiating from Virtual Reality (VR):** An introduction to AR helps clarify the distinction between augmented reality and virtual reality.
- **Applications and Use Cases:** AR has a wide range of applications across various industries. Introducing AR includes highlighting these use cases and envision how the technology can improve their lives or businesses.
- **Consumer Awareness:** As AR becomes more integrated into our daily lives, AR can provide guidance on how to use AR-enabled devices and apps effectively and safely.
- **Educational Opportunities:** Introducing AR in an educational context can introduce new concepts and inspire students to explore technology-related careers and fields.
- **Innovation and Creativity:** By understanding the basics of AR, individuals can start thinking about novel ways to use this technology to solve problems or create unique experiences.
- **Business and Industry Impacts:** For businesses, an introduction to AR can invest in potential revenue streams and competitive advantages.
- **Ethical and Privacy Considerations**: As AR interacts with the real world, issues related to data privacy, security, and potential intrusiveness need to be addressed and understood.
- **Cultural and Social Impact:** As AR becomes more prevalent, it can impact culture and society in various ways. An introduction to AR can help people anticipate and navigate these changes.[8]

[7] Join the AREA, *https://thearea.org/*

[8] What is Augmented Reality?, *https://thearea.org/augmented-reality/*

2.4 AR TECHNOLOGIES

Augmented reality technologies are reshaping industries and enhancing various aspects of our lives, making the world a better place in numerous ways. By seamlessly integrating digital information into the physical environment, AR technologies are transforming industries such as manufacturing and healthcare, and redefining business as we know it.

Some prominent examples:

- Augmented reality technologies are revolutionizing learning and training by offering immersive experiences. Complex concepts can be visualized, historical events can be recreated, and scientific theories can be simulated, enhancing student engagement and understanding. The technology bridges the gap between theoretical knowledge and real-world applications.
- Healthcare professionals can use AR during procedures to overlay important data, such as patient vitals or imaging results, directly onto their field of view, reducing the need to look away from the patient.
- AR technology can guide technicians and engineers in real-time during maintenance and repair tasks. Instructions and diagrams can be overlaid on the physical equipment, reducing errors and improving efficiency. It can also help individuals troubleshoot issues with everyday appliances and devices.
- Architects and designers can use AR to visualize their designs in a real-world context before construction begins. This can lead to better-informed design decisions and a more accurate representation of the final product.
- AR is also reshaping business by enhancing customer experiences. For example, retailers utilize AR to enable customers to virtually try products before purchasing, boosting confidence and reducing returns.

As augmented reality technologies continue to advance, their positive impact on various sectors will likely expand, shaping a more interactive, informed, and interconnected world. The choice of technologies for an enterprise AR project depends on many factors, from planned use cases to the business environment and conditions in the enterprise (e.g., the skills and experience of AR project developers, available tools and processes, deployment methods, etc.).[9]

[9] The Heart of the AR Revolution, *https://thearea.org/ar-technologies/*

2.5 AR USE CASES

Augmented reality use cases are proliferating across industries, as practitioners begin to benefit from the ways that AR enhances user experiences and improves productivity. It enables people to visualize complex structures and execute procedures more effectively.

As AR applications continue to evolve, they promise to reshape numerous industries and further integrate technology into our daily lives. These diverse augmented reality use cases highlight the burgeoning demand for AR technologies, and reflect the current stage of the market, where innovation and adoption are growing rapidly.[10]

2.5.2 TRAINING USE CASE

Augmented Reality-enabled skill development can be delivered to groups or individuals. Digital learning materials delivered via an AR-enabled display can re-use learning assets stored in a corporate knowledge base. The user's interactions and skill mastery can be captured using the AR system and the status stored in the user's learning management system record.

With AR in an environment which the real machine or products are available, the learner can see and hear the real -world circumstances and interact with equipment or other people directly, increasing the kinesthetic learning component. When connected to machines and sensors with live data streams which appear on the AR display in the user's field of view, the learner can make judgements about the duration of the task, the correct level of tension or pressure needed and other real time metrics, avoiding errors and bad habits while learning.

An AR-enabled system can also be worn or used by an expert to create highly compelling and interactive learning materials for playback as video or by other AR-enabled display users. The expert can use gestures or other tools to annotate/enhance the existing training materials with text, graphics, animations or videos. The type of AR display used when developing skills depends on many factors:

- Need for use of both hands to practice or perform a skill
- Room in the vicinity where the training is conducted for another screen pointed directly at the workspace
- Support for introducing new display devices (e.g. projection AR)

Another capability that an AR-enabled training system can support is the real time capture of the learner's achievement of competency. Then, the recording or data about the competency level can be stored in the learning management system.

[10] AR Use Cases, *https://thearea.org/ar-use-cases/*

The benefits of AR-enhanced training include raising the employee's value to the business through increasing workplace competencies, skills and certifications. In some situations, having AR-enabled instructions can reduce or remove the need to train a user in advance of performing a skill or procedure for the first time. An AR-enabled instruction delivery system may substitute reduce or eliminate the time that would be required for the training.

In addition, there can be benefits due to lower training time or on-the-spot lessons, which can translate to higher overall productivity of employees who do not need to stop working to acquire new competencies, skills and certifications.[11]

2.5.3 MAINTENANCE USE CASE

When a technician receives a maintenance work order using an AR-enabled system and display device that is connected to the operational systems and the documentation for the work order, a complete step-by-step maintenance procedures can be provided in real time and digitally registered with the technician's workspace. The type of AR display used by the technician depends on many factors:

- Need for technician to use both hands
- Room in the vicinity where the procedures are performed for another screen pointed directly at the workspace
- Support for introducing new display devices (e.g., projection AR)

Maintenance tasks conducted by a technician with an AR-enabled system reduces the need for the technician to change their focus of attention between the task itself and the documentation (e.g., a manual on screen or printed). The first and every subsequent step in the maintenance process is either automatically detected by the system or manually selected by the technician.

At each step in a maintenance use case, text from documentation (and/or a symbol representing a process) is spatially registered (overlaid) with the part where or on which the user must perform the current task. When a diagnosis or maintenance procedure is completed, the system automatically detects its status and sends a message to the management system, or the technician can confirm completion through voice, gesture or another interaction with the AR system.

Another capability that an AR-enabled system for maintenance can support is access to remote experts who can see what the technician sees. Using AR the remote expert can tell the technician how to detach, remove and replace parts. The remote expert may also use tools to point the technician's attention to special features and to give visual directions.

[11] AR Training Use Case, *https://thearea.org/ar_use_case/training/*

Common roles of users:

- Technicians
- Operations managers
- Inspectors

The benefits of AR-enhanced maintenance can be measured as reduced down time to complete the procedures with lower (or no) errors. Also, the technician's cognitive load would be reduced as a result of not needing to look away from the workspace to the documentation, remember the documentation when focusing on the parts and workspace. In addition, there can be benefits due to lower training time and higher overall productivity of technicians, even if they have not been trained on the specific assembly tasks. Finally, if the technician is unable to complete the maintenance and needs an expert, the remote expert can be called from the AR display and avoid unnecessary travel to the site to complete the maintenance task.[12]

2.6 Secure and Insecure Environments

The term secure environment can hold different meaning in different industries. In the defense industry it may mean a Sensitive Compartmented Information Facility (SCIF) where secret or top-secret information might be processed, to banking and finances where it can be about cybersecurity infrastructure to secure transactions and records, to even law enforcement where it can mean a facility to safeguard those held in lawful custody. Accordingly, operating rules in secure environments can vary widely, from network access to permissible sensors (cameras, microphones, IR), to installed software and updates, and more.

That said, most operating environments will not be secure environments with few or no restrictions on how devices might be used. This could range from your home environment, many commercial environments, or some test labs. While there might be some limitations such as network configurations or operating hours these spaces are largely free of additional restrictions.

As types of secure environments can vary, we will consider them broadly and point to the need for awareness and adherence to specific policies to meet your site security requirements.

2.7 Common AR SMM Comprehensiveness Level Considerations

There are some common themes of how AR considerations relate to the SMM comprehensiveness levels. This is not repeated in every table but is summarized here and can be used as a starting point for which comprehensiveness level is considered in each table.

[12] AR Maintenance Use Case, *https://thearea.org/use_case/maintenance/*

For example, if the intent is to utilize devices of type A, then the SMM Level 1 comprehensiveness level is likely a good starting point when considering each of the eighteen practice tables.

When using this common table or the specific practice tables if one characteristic, such as the complexity of spatial computing suggests a comprehensiveness level (e.g. 3) as a target but another characteristic such as onboard storage suggests a lower level (e.g. 2), the higher target level should be used, not an average.

Similarly, in an assessment, the lower assessed value should be used. The SMM practitioners guide notes that a + notation may be used to indicate that there are some indicators associated with a higher level, but not all criteria of the higher level have been met.

Common AR Comprehensiveness Level Considerations (All Practices)				
The contents of this table should be considered part of all the SMM Practice tables in this AR Profile.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
System-Specific Scope Considerations	Type A: Display with no onboard storage, connectivity or compute capability.	Type B: A more complex device consisting of a display with onboard storage, compute and either connectivity or spatial telemetry.	Type C: A standalone spatial compute device with onboard spatial mapping and full 6DOF tracking along with network connectivity.	Type D: The most flexible and complex device type, that is a general compute device with spatial capabilities. It can serve as a platform for additional hardware and software development, including addition of hardware such as sensors and broadly supported SDKs.
	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**

	The display is driven by a host device (e.g., a phone). The display may accept user input (e.g., via voice, hand gestures or a controller) but inputs are only passed on to the host device.	This type requires no host device. It may be connected to a network with no spatial telemetry (i.e., at most 3DOF tracking, no spatial mapping of physical environment). Alternatively, it may have spatial mapping and reconstructions capabilities as well as full 6DOF tracking, but no network connectivity.	Type C devices are not general compute devices, having custom Operating System implementations, limited or no SDK for development, no support for additional hardware (e.g., additional sensors) or other restrictions on type of software, content or hardware that can be used with the device.	Operating Systems are often open or commonly used platforms (e.g., Android, Windows Mixed Reality) and software or content that can be used with the device is generally unrestricted.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Device is simple and has no networking or storage.	Device may have networking and storage or storage and spatial capabilities, but not both.	Sophisticated devices with a variety of sensors but not a platform where other sensors can be added and no SDK.	Sophisticated device with a platform for hardware and software development and augmentation.

Table 2-1: AR comprehensiveness level considerations for all SMM practices.

The separation between the levels is designed to reflect the fundamental reality that are AR device sophistication can require higher comprehensiveness and maturity. This means that higher levels represent:

- A higher level of control with increased granularity for both flow of data between/across systems, and 3rd party hardware/software,
- A higher capability to deal with increasing device sophistication with added device connectivity and integrated sensors
- A higher level of understanding for system-level capabilities and implementations across both hardware and software with platform capabilities,
- A higher level of device management.

3 PROFILE TABLES

The following tables add the industry and device scope to the general SMM considerations as appropriate.

3.1 Security Program Management

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)**
System-Specific Scope Considerations	Not treated as an AR device. Department level.	AR managed independently from security policy. Organizational level.	Designated individual, subject matter expert, formal organization, skill center, or other governing body exists for AR security. May recommend or require specific training or certification.	AR and security policy integrated enterprise wide.
	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**
	Printed policy or reference to policy is posted in proximity of AR devices. May include check-out log acknowledging policy.	Administrator installs warning notification on device. Notification presents some means to acknowledge receipt.	Non-secure environments: Responsible party is authorized to determine appropriate security posture, communication, deployment, and enforcement. Secure environments: Need to ensure compliance to defined security requirements for operating environment.	Complete program management established across the organization.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

	Policy is visible before checking out AR devices. Check-out log, if present, is signed by users of devices.	Warning is displayed as part of device login. User must indicate understanding of policy before proceeding.	Security requirements and policy are reviewed and updated on recurring basis. All related needs and inquiries are directed to designated party.	Security policy is stored and accessible alongside other enterprise policies.

Table 3-1: Security program management.

3.2 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)**
Technology-Specific Scope Considerations	Not treated as an AR device. Department level.	AR managed independently from compliance. Organizational level.	Centrally managed and industry or government formal.	AR and compliance integrated enterprise wide.
	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**
	Device treated as a mobile device. Must be updated or taken off network (manually). AR compliance is defined at departmental level.	Guidelines for data use are present for what someone can or cannot do (proprietary, etc.) for connectivity, for location. AR compliance is defined at, and managed at, organizational level across different environments (such as secure and insecure).	Export control and safety, and local requirements are applied. AR compliance is managed centrally across different organizations within a company or agency. Industry-specific, such as Aerospace, and government regulations are applied.	AR compliance is enterprise wide and integrated with overall compliance. AR devices must undergo formal certifications required by industry.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

	Mobile device compliance is documented and available at the departmental level.	AR compliance is documented at the organizational level. Documentation outlines procedures for handling AR devices in different types of environments managed by the organization.	A standalone compliance organization exists across the company or agency. Compliance addresses governmental and industry compliance requirements and applies them to AR devices.	A standalone compliance organization exists across enterprise and AR device compliance is integrated. AR devices compliance is performed by 3rd party organizations and status of compliance is recorded and maintained by the organization.

Table 3-2: Compliance management.

3.3 THREAT MODELING PRACTICE

The threat modeling subdomain identifies gaps in specific configurations, products, scenarios, uses and technologies that may lead to varying levels of vulnerabilities and exploits within an organization. Threat modeling allows for a systematic understanding of threat surfaces necessary for prioritizing countermeasures accordingly.

Threat modeling surrounding AR devices includes many considerations beyond general IT security. These considerations vary by the sophistication of the device in question. AR devices with environmental awareness (e.g., spatial mapping, 6 degree-of-freedom spatial tracking), are cyber-physical devices that are capable of collecting data and monitoring physical spaces, often using sensor systems such as LiDAR and infrared. As such, AR may introduce new forms of data to be secured within an IT framework along with new attack vectors. Other data collected for consideration may include user-specific data, such as eye tracking, face tracking or other biometrics, that expose organizational security and privacy attack surfaces.

Furthermore, to attain this environmental awareness many AR devices may employ a unique hardware stack, such as where spatial compute operations are isolated on separate (and frequently proprietary) chipsets from the primary compute hardware. These chipsets may employ different architectures or have a different hardware attack surface from other IT assets. Such variations in hardware/firmware topology and its interfaces with device operating systems and other software should be considered in AR threat modeling.

The use-cases of AR as well as its location of use can introduce additional threat modeling considerations. For example, in the case of wearable AR devices, Environmental Health and Safety (EH&S) may introduce additional threat vectors, such as communicable disease. Similarly, AR content used in operational settings may compose an additional threat vector in the form of content displayed for the purpose of negative impacts on visibility and cognitive state. AR-specific

threat modeling should include assessment of such attack vectors to determine if they pose relevant risks to the organization.

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)**
Technology-Specific Scope Considerations	At this level, there is no consideration of AR-specific threats.	Threat models consider some AR-specific threat vectors related to use and form-factor.	Threat models included availability of spatial telemetry on connected devices.	Threat models consider the full hardware and software stack of AR devices, including systems for spatial tracking and mapping.
	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**
	Device is treated the same as other displays in threat models. There is no distinction for AR displays. Host device considerations are handled separately in their respective threat models.	Threat models include consideration of threat vectors related to display (e.g., portability), distinguishing it from non-wearable/non-portable displays. E.g., consideration of loss of sight during use as a threat surface. Threat models have a concept of content classification and include modeling of on-device security, such as encryption at rest/in transit, accessibility, connectivity and physical access controls/physical security. Attack vectors arising from use of spatial information in applications or content	Attack vectors arising from shared use of spatial information across devices in multiuser sessions applications or content are included in threat models, including attack surfaces related to how that data is made available across networks to applications. Models include consideration of spatial data encryption in transit and whether absolute or relative spatial data is shared across devices. Attack vectors associated with software/hardware installation on the devices, such as the addition of 3rd party	Threat modeling explicitly includes spatial tracking and data through all steps of the modeling process (e.g., through decomposition, ranking and mitigation in OWASP). Models track spatial data usage through the full implementation stack of the device, from acquisition of data via sensors to use in content. Threat modeling of sessions includes spatial tracking, mapping and associated data is performed across user sessions, including spatial telemetry retention policies. Attack vectors associated with device software/hardware development are consistently modeled, including attack vectors at the SDK, development engine/framework and OS level.

		are included in threat models, including attack surfaces related to how that data is made available to applications. Models include consideration of spatial data storage and retention. Threat modeling is performed for multi-user AR sessions, including connectivity among multiple devices.	sensors.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	General IT policies and procedures are applied and used.	Documented scope of threat modeling process includes AR devices and AR-specific threats related to use and form-factor. Documented threat models include where and how AR content is consumed. This may include modeling threats associated with externally observable behaviors when a user interacts with AR content, or the impact of incorrect/malicious content injection during use in a location. Threat model scope and process have a concept of content classification and include modeling of on-device security, such as encryption at rest/in transit, accessibility,	Documented threat models include consideration of attack vectors arising from shared use of spatial information across devices in multiuser sessions, including attack surfaces related to how that data is made available across networks to applications. Spatial data encryption in transit and type of spatial data shared across devices is included in the documented scope of models. Software/hardware installation threat model requirements and considerations are documented.	There is a comprehensive understanding of the hardware-firmware-software stack of the devices in use, such as whether dedicated spatial computing chips are used and how they should be integrated within a model. Models include consideration of spatial data storage and retention Software/hardware development threat model requirements/considerations are documented.

		connectivity and physical access controls/physical security. The documented threat modeling process includes multi-user AR sessions, including connectivity among multiple devices. Threat surfaces considered include how devices authenticate/join a session, where content is rendered amongst devices and what data is shared amongst devices (e.g., only relative states are shared with all content rendered locally vs. shared rendering). Device/user state is modeled distinctly from content. Threat models account for spatial tracking, spatial mapping and the associated collected data. Models include how data might be extracted at runtime or from storage of dedicated spatial processors. Attack vectors arising from use of spatial information in applications or content are included in threat models, including attack surfaces related to how that data is made available to applications.		

		Spatial information is included as appropriate (e.g., as assets, entry points, data flow) in an accepted threat modeling process.		

Table 3-3: Threat modeling.

3.4 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)**
Technology-Specific Scope Considerations	At this level, risk management only includes general IT concern and has no formal consideration of AR.	Risk management considers AR independently. However, risk assessments are ad hoc as AR use-cases are implemented.	Risk assessment and management of AR is conducted consistently and across the organization with quantitative metrics distinguished from other IT risks.	Risk assessment and management details consider specific AR device capabilities as well as implementation/usage within the organization. Restrictions and/or guidance on use of AR are influenced by risk management.
	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**

	Risk management does not have a separate concept of AR.	Risk management policy and procedures include formal treatment of aspects that distinguish AR from other mobile devices, such as wearable devices, device sensors and content.	Risks management and assessments include holistic considerations, including risks to safety, (e.g., such as distraction or obstruction of view). Safety compliance, such as EH&S and OSHA compliance are considered in risk management policies and procedures.	Usage and risks associated with AR are visible to leadership, such as through executive briefings and reporting. Usage of AR satisfies compliance requirements as necessary for a use-case. This compliance is included in risk management policy, procedures and documentation.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	AR is not included within the scope of any risk management documentation, policy or procedure.	Risk management documentation has explicit sections for AR. Risk policies and procedures address AR separately from other mobile devices.	Risk management documentation includes sections for compliance with appropriate policy or regulatory bodies. Risk management procedures explicitly include risks to safety, such as in risk management files and documented processes.	Documented executive reporting on risk management (e.g., presentations, memos, quarterlies) includes AR-specific usage risks.

Table 3-4: Risk attitude.

3.5 Product Supply Chain Risk Management Practice

Product Supply Chain Risk Management				
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)**

Technology - Specific Scope Considerations	System focused considerations.	Subsystems are managed separately by IT.	Review of hardware providers. Holistic system and subsystems.	Separation of external and internal duties.
	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**
	Regular reviews are performed of external components to understand where they are coming from, why they are used, and alternatives are identified if need to replace.	IT reviews are conducted for external connections and include data integrity, data usage, safety, and security specification. Constraints are placed on data to make sure it is safe and not possible to steal by external parties. Information must be stored locally on the device. Data integrity is maintained when used, sent, or retrieved from device. General IT requirements are applied for external suppliers of open source. Organizations have access to the code and perform reviews. If open source is not available organizations must determine a make or buy decision then.	End customer considerations are included for safety of data and usage. Review of export control policy is conducted. Organizations look at provenance of software and hardware and avoid chips from non-approved countries, if used in classified environments. Methods are available to wipe out or remove the storage. Or to ensure data doesn't get out or may need to be destroyed. Several SDKs may need to be integrated. Some SLAs are carved out separately by client rather than by AR device. Multi-group SLAs are defined.	Lifecycle process exists to assign a device to employee, that was assigned to another employee. Data is managed, wiped clean. Alignment exists between the OS provider and organization itself. The organization coordinates updates with enterprise and vendors.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

	A record exists of device component provenance. A catalog of component vendors is kept.	IT Standard operating procedures exist for management of on device data. Procedures exist for reviewing and testing of open source if used by suppliers.	Documentation exists detailing hardware and software components, where they are produced, who produces them and if they comply with export regulations. IT SOPs exist for cleansing of data from devices. Multigroup SLAs exist that incorporate both device manufacturer and client SLAs.	Processes exist to handle scenarios such as device transfer between employees. Procedures are documented to identify responsibilities of organization's staff and OS providers.

Table 3-5: Product supply chain risk management.

3.6 Services Third-Party Dependencies Management Practice

The internet is ubiquitous, yet organizations are still hesitant to go to cloud for any sensitive data. Such organizations first investigate if storage and processing can be performed on premises. They check if it can be cut off and isolated. If not, for defense and aerospace related organizations they may use the government cloud. They use the government cloud for authentication, single sign on, PKI, and tie it to existing mechanisms rather than introduce something new.

Similarly, other industries, such as manufacturing, pharma, have concerns regarding protection of IP, trade secrets, what can be seen, and what cannot. They are very careful regarding what data can be sent and shared and what should not be sent to the cloud.

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)**

Technology - Specific Scope Considerations	Operational isolation.	On premises cloud.	Secure isolated external cloud.	External account verification.
	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**
	Local data and local access only.	Local data and remote access. No ability to differentiate data for local vs. remote use.	Hybrid data and air gap clouds are used. Only non-identifiable information is sent to the cloud. Data can be separated to local data and external data. Cloud processing of connectivity and interaction of devices. Computer vision is still a vulnerability (algorithms) even if on device and not shipped.	External cloud with cloud/scalability and rigor of evaluations. Multi-party client SLAs for GIS, software, algorithms, AR device.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Devices do not have removable storage or networking capabilities.	Devices do not have removable storage but have networking capabilities. or spatial capabilities. There is no separation of data between on premise or remote storage.	Documentation exists that clearly states what data should remain on the device and what data can be sent to the cloud. Test results are available to demonstrate that no PII information is transmitted or stored remotely.	Verification of services such as backup and failover conducted on a regular basis and results compared to SLAs.

Table 3-6: Services third-party dependencies management.

3.7 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)**
Technology - Specific Scope Considerations	Managed shared account.	Device local accounts with access levels.	Organizationally managed mobile device management (MDM) solution.	MDM tied into networked enterprise user authentication system.
	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**
	Administrator sets up each device with shared account, sets configuration, and installs tools.	User accounts are created on the device and user roles are set. Any account or inventory changes must be manually deployed across all devices.	User profiles are deployed to device-level from centralized system.	MDM is installed on all devices and connected to enterprise network. Authorized user accounts are authenticated on network and profiles are downloaded to the device.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Devices require no user-specific authentication, configuration, or installation. Device can readily be used by anybody.	Users must log into individual account and do not have access beyond their role and their activity can be reviewed by the administrator. Environment and tools may be tailored to fit user roles.	All accounts and device configuration are in sync as of most recent update across devices.	All accounts and device configuration are in sync and connected to the network.

Table 3-7: Establishing and maintaining identities.

3.8 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)**
Technology - Specific Scope Considerations	Physically isolated and disconnected devices. Physically controlled.	Devices are connected locally.	Process exists for different security classification levels.	AR devices integrated with IT/OT.
	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**
	Designation of which people have access, and which don't. Devices have single account, or no accounts. Non-removable storage. Devices are disabled outside secure environment or not removed from the secure environment. Physical log of who signs out the device. Individuals are responsible for devices.	Networked devices are evaluated to make sure they don't have controlled information. Devices can support multiple accounts with an admin account to manage them. Devices may have removable storage. Devices cannot be used at lower security levels and may need to be destroyed. Custom system to track devices (e.g. QR code), device must be signed out.	Device classification can be reduced. Devices are part of mobile device management. Organizational and individual responsibility for devices.	AR devices part of overall lifecycle and managed according to the operational environment in which they are used and with safety considerations.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

	A list exists of who is allowed to use the device. Logs are kept of who has signed out or is using the device and when it is returned.	Reports exists for device reviews. Device logs exist for multiple accounts and devices can be traced on the network. If device isn't networked, a system must exist or physical evidence as to usage.	Devices can be identified as part of the mobile device centralized management at the organizational level.	Separate procedures exist for secure and insecure environment usage and implemented consistently across the enterprise.

Table 3-8: Access control practice.

3.9 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)**
Technology - Specific Scope Considerations	General access.	Administrative and individual accounts.	A Formal governing body exists within the organization.	Governed by enterprise-wide policies.
	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**
	Devices are not formally-managed assets and may be separately inventoried. Devices are disconnected from operational systems and networks.	Administrative accounts on local device manage all configuration changes. Administrator determines changes allowed and scheduling of updates. Device-level user accounts with established roles.	Mobile Device Management (MDM) software is used to deploy and schedule changes. Change review board, or similar, determines changes allowed and scheduling. If the device is not updated as required it will be removed from	Non-secure environments: Device may always be connected to a company or public network or can go online whenever a connection is available allowing for regular MDM administration of changes. Secure environments: Device may require a tethered connection to a secure PC for changes,

			access.	connection to an air-gapped network, or other means for secure change administration.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Users are able to freely install, update, modify and remove applications.	Standard users are unable to effect change and must request changes with administrators. Administrators may have the option to have the user install configuration updates.	Accounts, configuration, and changes are managed through MDM. All changes can be traced to meeting minutes, action items, or other board artifacts.	Management of devices is consistent with enterprise practices and policy.

Table 3-9: Asset, change and configuration management.

3.10 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)**
Technology - Specific Scope Considerations	Baseline control limited physically/locally and no knowledge of device location.	Identity and role based but still local. Can identify device location.	Limited remote capability with ability to identify device location and operating environment. Export/import issues and use outside certain countries.	Devices managed by location with automatic recognition and use of sophisticated authentication methods.
	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**
	Devices may need to be placed in lockers to prevent access.	Role of person (project access, guest, partner, etc.) and usage	Device can identify where it is. This may mean beacon/GPS	Device can use user biometrics for identification.

	Simple devices (no memory, no networking) are used.	environment (training, classified, etc.) is considered. Consideration if person using device can be observed, and who may observe. Control over who can access and remove memory or connect to network. Devices are classified by type. Specialized functions, such as spatial computing, should be on separate processors. At least logically separated.	capability, network location finding, or other means of geolocation. Device is able to load and execute location-based policy.	Device can perform system management tasks autonomously. Devices can automatically be turned off and confirm remote wipes.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Physical, lockable storage space exists.	Training documentation exists for handling the devices in different environments. Logs exist recording who has access to the device and can remove memory or connect to the network. Inventory system shows classification of devices by type.	A log exists on the device indicating location and position. Device limits what can be accessed or displayed by location or role.	User authentication is logged including method of authentication.

Table 3-10: Physical protection.

3.11 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)**
Technology - Specific Scope Considerations	Basic security settings and restrictions available.	All security settings and restrictions available.	Enterprise management of devices (MDM) of security settings and restrictions.	Approved as a standard enterprise device or service
	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**
	Scope of policy may vary based on features and capability of deployed AR technology. Device is used for Testing and evaluation only and not approved for use with any sensitive information. PIN or passcode to unlock device Encryption of data at rest.	Manual configuration and no enterprise management. Limited pilot use with sensitive information allowed with additional processes and controls in place Password length, complexity, reuse Configure screen lock time Throttling of failed login attempts.	Approved for general use. Some security or capability gaps require risk acceptance.	Authentication integrated with enterprise identity and access management (AD/AAD/LDAP/SSO). All significant security and capability gaps addressed. Device requests and enterprise enrollment processes can be automated. No additional dedicated support required for standard compliant deployments logging.

			All devices managed through MDM All level 2 security settings and restrictions available through MDM. Remote visibility into device compliance status (settings, OS version, last check-in with MDM). Remote wipe capability. General deployments may require additional support through technical support staff and knowledgebase articles.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Policy exists on allowable applications, data, use cases, locations (onsite/offsite). A record is kept for device PINs or passcodes and data is encrypted at rest.	Rules exist for password creation, timeout, locking after failed attempts and are enforced on the device.	Devices are managed centrally by MDM and associated procedures are documented.	Devices are managed across the enterprise and officially recognized by IT management.

Table 3-11: Protection model and policy for data.

3.12 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)**
Technology - Specific Scope Considerations	Defined by IT policy.	Isolated accounts used.	Protected data partitioned storage on the device.	Secure network storage used.
	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**
	Data to be used on device must be defined so usage category can be determined.	Individual passworded accounts on the device are used. Password requirements must be established.	Partitioned data space and/or chipsets for encryption protected data must exist. Some or all data must be selectable to be encrypted.	Protected data can be stored on secure company network storage. Data sync capability over authenticated network connection. Option might exist to wipe local data on sync to network.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Data protection guidance is available and accessible. Data is correctly handled as defined by the policy.	Users have access to only their protected data.	All protected data is encrypted and/or stored in a separate partition from unprotected data. Any unauthorized data access attempts are flagged.	Protected data is automatically synced to secure, encrypted network storage upon connection.

Table 3-12: Implementation of data protection practices.

3.13 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)**
Technology - Specific Scope Considerations	Vulnerability assessments are conducted on devices when new systems are procured and prior to installation within the operating environment.	Vulnerability assessments are conducted on devices used with critical infrastructure as part of maintenance activities as well as on equipment in regular use within the operating environment.	Vulnerability assessments on the entire IIoT system are conducted according to industry standards such as the Common Vulnerability Scoring System (CVSS).	Vulnerability assessments are done on all systems within the organization taking into consideration the internal as well as external federated systems.
	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**

	In compliance with the threat assessment conducted, potential vulnerabilities are assessed and catalogued manually and on new equipment that is to be introduced into the operating environment. Physical tracking and inventory of physical devices done locally. Likely isolated to nonsecure environments. May be cleared for secure environments if sensors, networking, and other capabilities can be adequately disabled.	Vulnerability assessment includes potential zero-day vulnerabilities emergent over time requiring patching/updates on critical infrastructure and contractor equipment that is regularly introduced into the operating environment.	Scheduled physical security assessments and hardening of critical infrastructure are prioritized according on the level of importance and vulnerability as determined by standard vulnerability assessment scoring system.	Vulnerability assessment conducted autonomously with threat detection software with generation of real-time assessment and action report.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Vulnerability assessment report for introduction of a new system into an operating environment, associated risk strategy and mitigation plan to be compiled and implemented opportunistically. Device locations are tracked and known.	Vulnerability assessment report to include assessment of maintenance risk, mitigation strategy and potential frequency required for operating environment. Documentation of highly critical devices and systems, the number and location of restricted access points within highly critical systems and security	Vulnerability assessment report developed according to relevant standard reporting and scoring with focus on IT/OT risk.	Vulnerability assessment report available in real-time through continuous scanning by threat detection software with action report from highest to lowest risk.

		implemented to reduced vulnerability presented by the access points is regularly generated and updated.		

Table 3-13: Vulnerability assessment.

3.14 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)**
Technology - Specific Scope Considerations-	Basic patching.	Manual patching based on environment and usage considerations.	Policy and law impact considered.	Classification based patch management.
	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**
	IT based patching.	For secure environments patches go through review by security team. Critical patches put on quick path in unclassified environments. Air gapped devices may not get updated. Dependent on device type and capability. Ad-hoc management and patching in lab environment.	Centrally managed devices are updated OTA. Safety compliance considered. Devices may undergo certification. Depending on environment, may require OHSA (or similar) compliance.	Patching classified based on the usage environment and type of class of user.

	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment
	A record exists and maintained by IT as to patches implemented on a device.	A record exists and maintained by IT as to patches implemented on a device by environment.	Automated system records exist showing deployed patches on each device. Compliance and certification records exist for devices.	Classification exists for devices based on the usage environment and type of class of user.

Table 3-14: Patch management.

3.15 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)**
Technology - Specific Scope Considerations	Device logging is used.	Custom logging and monitoring are applied	Integrated logging and monitoring are applied.	Sophisticated logging and monitoring are applied.
	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**
	Manual logs are kept for devices that do not offering logging. For devices that offer logging, certain industries may require that logging is turned on by default. However, logging cannot be enforced.	Manual management and enforcement are applied within secure facilities. Logs are maintained across sharing of the device. Logs are wiped manually and not retained due to retention period policies and to avoid improper exposure and contamination.	3rd party tools are used to monitor the state of the device (e.g. proper settings, patch versions, state of compliance, etc.). Dedicated monitoring may be used, depending on end user policies. Devices must be disconnected from the network automatically if non-compliant.	Logs and policies are checked and managed on a regular basis and based on identity lifecycle management. Logs are wiped automatically and correspond to identity record changes.

		Caches, repositories and backups are also managed.	Specific implementations are introduced to handle safety concerns.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Manual or device logs are available.	Retention and backup policies are documented.	Records exist that demonstrate when devices are set up or when there were wiped. Intermittent testing records are available to verify devices were handled correctly. Operational policies are available for safety concerns.	Intermittent testing is performed to ensure logs are indeed wiped when employees depart.

Table 3-15: Monitoring practice.

3.16 Situational Awareness and Information Sharing Practice

Enterprises that host both secure and non-secure operating environments may have separate pathways to handle these functions. For instance, in non-secure operating environments vulnerability notifications or other situational awareness may be sent out to IT and general personnel via email, text message, or other intra-company messaging. However, with secure environments the notification may be flowed out to lab managers who then have the responsibility to see the information disseminated within the secure space. Further, the means available within the secure space may vary.

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)**

Technology - Specific Scope Considerations	IT shares relevant information with groups that it can access.	IT shares relevant information with lab managers and ensures information is shared also with environments where special access is needed to apply a fix.	Subscription to vulnerability database (i.e., CERT or consortium-based) containing updates for AR devices and ecosystem. Relevance and criticality of vulnerability is formalized to aid in prioritization and scheduling of updates.	Sharing across the enterprise.
	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**
	IT and specialized secure environment staff: do not share information	Vulnerability communications are monitored and tracked for AR content. IT and specialized environment staff share but manage separately (timing of action, what action to take, etc.).	Centralized sharing and actions are coordinated.	Information is shared with business partners.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Threat information is shared with some groups but possibly not all groups.	Threat information is shared with lab managers who flow information out as needed.	Threat information is automatically shared to all subscribed parties.	Information is sent to and received across the enterprise and business partners.

Table 3-16: Situational awareness and information sharing practice.

3.17 Event Detection and Response Plan Practice

Today devices are mostly isolated, and it is very difficult to identify related events. Most devices have cameras, but this may be overlooked. Some scenarios may influence safety. There could be some incidents of interference or “Denial of service”, scope and response related to cameras. Focus should be on what the AR scenario is and if there is additional data, such as 3D which needs to be protected, and what environment the device is being used in.

A barrier for event detection are the many sensors that are found on these devices, IR for example, is a challenge. Denial of service in hazardous environments is also serious. Need to consider:

1. The environment
2. Type of event
3. Features of devices (with cameras and 3D chips)

Huge effort for organizations to have network and device logging for AR devices.

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)**
Technology - Specific Scope Considerations	General IT event detection and response are applied.	Custom and separate event detection and response are applied.	Integrated event detection and response are applied.	Sophisticated device capability for event detection and response.
	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**
	No specialized event detection for AR devices. Upon a noticed event, the AR device is checked by IT security.	The organization has its own custom and separate device management strategy for event detection. These may be different for secure and insecure environments. Events are contextual. An event is generated if the wrong role is using the device, or if it is being used in the wrong location. Events are local to the device, environment or facility. Type of user should be defined, such as	Integrated event detection for AR devices with other types of devices across the enterprise. Improper access is detected automatically, and events are generated accordingly. Events and logs are managed centrally.	The device itself is able to detect conditions that warrant the generations of certain events. For example, the device can contextually recognize improper scenario use and activation of certain sensors in the wrong environment.

		administrator, end user, etc. Conditions happening to the device are detected, such as the device being moved or denial of service.		
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Procedures are outlined for IT to manage the device when certain events occur.	A custom system exists for managing events and documentation exists for how to handle each event.	An automated centralized enterprise system exists with logs and history of events.	Device-specific events are part of the automated system and can be differentiated.

Table 3-17: Event detection and response plan.

3.18 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)**
Technology - Specific Scope Considerations	Basic backup and recovery.	Use case-based processes.	Separate remediation for different secure environments. (In SCIF and not).	Automated backup and recovery
	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**

	Device can use app- or OS-defined automatic cloud backup or needs to be manually synced with PC or cloud, if available. Backup data may be encrypted and/or separately partitioned. Remediation plan defined in event of missing, outdated, or corrupted backup? Consideration might be given to data backup needs (i.e. what data must be backed up).	Defined use case scenarios based on the environment where the device is used, the device sophistication, who is using it (role), where and how and backup and recovery processes for each scenario. Must differentiate data restoration requirements based on scenario, operational environment, or other factors (ex. training vs. operations).	Organizationally managed Mobile Device Management (MDM) is running. Unclassified can sync to PC or cloud. In SCIF, have to turn off broadcast, may need to sync to air-gapped system. A central organization may make decision, but execution may be local depending on operational requirements. For limited or no connectivity environments devices may automatically sync outside of operating environment.	Management of devices is consistent with enterprise practices and policy.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Periodic backups exist.	Backups are created per defined requirements for given use cases.	Backups are automated per the tools. Central vs. local decision-making and execution (i.e. lower levels restore is manual vs. higher levels is automated). Backup materials may be stored offsite to meet security requirements.	Systems automatically load scheduled backups from enterprise repository to restore continuity of operation.

Table 3-18: Remediation, recovery, and continuity of operations.

Annex A ACRONYMS

AIC Availability, Integrity, Confidentiality
CAPEC Common Attack Pattern Enumeration and Classification
CPS Cyber-Physical Systems
DMR Department of Mineral Resources
DWS Department of Water and Sanitation
EA Environmental Authorizations
EIAS Environmental Impact Assessments
EMP Environmental Management Plans
GPS Global Positioning System
ICS Industrial Control System
ICT Information and Communications Technology
IIC Industry IoT Consortium
IIRA Industrial Internet Reference Architecture
IISF Industrial Internet Security Framework
(I)IoT (Industrial) Internet of Things
IT Information Technology
ISO International Standards Organization
LHD Load Haul Dump
MHSA Mine Health and Safety Act
MitM Man-in-the-Middle
MPRDA Mineral and Petroleum Resources Development Act
NEMA National Environmental Management Act
OHSA Occupational Health and Safety Act
OT Operational Technology
OWASP Open Web Application Security Project
PLC Programmable Logic Controller
POPIA Protection of Personal Information Act
PPE Personal Protective Equipment
SCADA Supervisory Control and Data Acquisition
SLA Service Level Agreement
TMM Trackless Mobile Machine
WAN Wide Area Network

Annex B DEFINITIONS

The following terms, specific to the context of the SMM, are defined here:

- *Security level* is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.
- *Security maturity* is a measure of an understanding of the current Security Level, its necessity, benefits, and cost of its support.
- *Domains* are the strategic-level priorities for security maturity. In the SMM, there are three domains: Governance, Enablement, and Hardening.
- *Subdomains* refer to the basic means to address a domain at the planning level. Each domain currently defines three subdomains.
- *Security practices* are the typical activities performed for a given subdomain; they provide the deeper detail necessary for planning. Each subdomain has a set of practices.
- *Comprehensiveness* is a measure of the completeness, consistency and assurance of the implementation of measures supporting the security maturity domain, subdomain or practice.
- *Scope* is a measure of the applicability to a specific vertical or system.
- *Security maturity target* is the desired "end state" 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 by the business objectives of the organization or group.

Annex C REFERENCES

[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-IIRA2019]

Industry IoT 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-IIV2019]

Industry IoT 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-IISF2016]
Industry IoT Consortium: The Industrial Internet of Things Volume G4: Security Framework Version 1.0, 2016-September-26 *http://www.iiconsortium.org/IISF.htm*

[IIC-SMMD2020]
Industry IoT 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

[IIC-SMMP2020]
Industry IoT Consortium: IoT Security Maturity Model: Practitioner's Guide, Version 1.2, 2020-05-05, retrieved 202-05-05
https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

[RFC 2119]
S. Brander. IETF. "Key Words for Use in RFCs To Indicate Requirement Levels." March 1997. Best Current Practice. *https://ietf.org/rfc/rfc2119.txt*

4 AUTHORS & LEGAL NOTICE

This document is a work product of The AREA Security Committee, chaired by James Cooper.

Authors: The following persons contributed substantial written content to this document: Ron Zahavi (Auron Technologies, LLC), James Cooper (Raytheon, an RTX Company), Mik Bertolli (Avrio Analytics), Mihir Kamdar (The AREA).

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document: Tangi Meyer (Dassault Systems), Adam Greenbaum (Lockheed Martin), Mark Sage (The AREA).