INTERNATIONAL STANDARD

ISO/IEC 20243-2

Second edition
2023-11

Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) —

Part 2: Assessment procedures for the O-TTPS

Reference number
ISO/IEC 20243-2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by The Open Group [as Open Trusted Technology Provider Standard (O-TTPS) V1.2, Part 2: Assessment Procedures for the O-TTPS] and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 20243-2:2018), which has been technically revised.

The main changes are as follows:

— Wording has been changed throughout the document, including in introductory materials, attribute definitions and requirements, as necessary to improve clarity and/or concision.

— The definition of “component” has been clarified to include both hardware and software.

— A definition for “security-critical” has been added.

— PD_DES.01 has become a mandatory requirement.

— PD_CFM.04 has become a mandatory requirement.

— The attribute definition of PD_QAT has been clarified.

— The attribute definition of PD_PSM has been clarified.

— The SE_VAR requirements have been largely reworked and reorganized, with a new mandatory requirement being added and several existing requirements becoming mandatory.

— SE_PPR.02 has become a mandatory requirement.

— SE_PPR.04 has become a mandatory requirement.

— SC_RSM.05 has become a mandatory requirement.

— SC_ACC.04 has become a mandatory requirement.

— SC_ESS.02 has become a mandatory requirement.

— SC_ESS.03 has become a mandatory requirement.

— SC_ESS.04 has been completely rewritten and has become a mandatory requirement.

— SC_BPS.02 has become a mandatory requirement.

— The SE_STH requirements have been largely reworked and reorganized, with a new requirement being added and an existing requirement becoming mandatory.

— SC_CTM.02 has been revised heavily and has become a mandatory requirement.

— SC_MAL.02 has been heavily revised and has become a mandatory requirement.

A list of all parts in the ISO/IEC 20243 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. With more than 870 member organizations, we have a diverse membership that spans all sectors of the technology community – customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

— Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices

— Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies

— Offering a comprehensive set of services to enhance the operational efficiency of consortia

— Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

This Document

The Open Group Open Trusted Technology Forum (OTTF) is a global initiative that invites industry, government, and other interested participants to work together to evolve the O-TTPS and other OTTF deliverables.

This document is Part 2 of the Open Trusted Technology Provider Standard (O-TTPS). It has been developed by the OTTF and approved by The Open Group, through The Open Group Company Review process. There are two distinct elements that should be understood with respect to this document: the O-TTPF (Framework) and the O-TTPS (Standard).

The O-TTPF (Framework): The O-TTPF is an evolving compendium of organizational guidelines and best practices relating to the integrity of Commercial Off-The-Shelf (COTS) Information and Communications Technology (ICT) products and the security of the supply chain throughout the entire product lifecycle.

An early version of the O-TTPF was published as a White Paper in February 2011, revised in November 2015, and has since been updated and published as a Guide in September 2021 (see Referenced Documents). The O-TTPF serves as the basis for the O-TTPS, future updates, and additional standards. The content of the O-TTPF is the result of industry collaboration and research as to those commonly used commercially reasonable practices that increase product integrity and supply chain security. The members of the OTTF will continue to collaborate with industry and governments and update the O-TTPF as the threat landscape changes and industry practices evolve.

The O-TTPS (Standard): The O-TTPS is an open standard containing a set of guidelines that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of COTS ICT products. Part 1 of the O-TTPS (this document) provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

The O-TTPS, Part 2: Assessment Procedures for the O-TTPS (see Referenced Documents) provides assessment procedures that may be used to demonstrate conformance with the requirements provided in Clause 6 of the O-TTPS, Part 1.

Using the guidelines documented in the O-TTPF as a basis, the OTTF is taking a phased approach and staging O-TTPS releases over time. This staging will consist of standards that focus on mitigating specific COTS ICT risks from emerging threats. As threats change or market needs evolve, the OTTF intends to update the O-TTPS by releasing addenda to address specific threats or market needs.

The O-TTPS is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors recognize the value that it can bring to governments and commercial customers worldwide, particularly those who adopt procurement and sourcing strategies that reward those vendors who follow the O-TTPS best practice requirements and recommendations.

NOTE Any reference to “providers” is intended to refer to COTS ICT providers. The use of the word “component” is intended to refer to either hardware or software components.

Intended Audience

The O-TTPS is intended for organizations interested in helping the industry evolve to meet the threats in the delivery of trustworthy COTS ICT products. It is intended to provide enough context and information on business drivers to enable its audience to understand the value in adopting the guidelines, requirements, and recommendations specified within. It also allows providers, suppliers, and integrators to begin planning how to implement the O-TTPS in their organizations. Additionally, acquirers and customers can begin recommending the adoption of the O-TTPS to their providers and integrators.

Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo are trademarks of The Open Group.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Introduction

Part 2 of the O-TTPS specifies the procedures to be utilized by an assessor when conducting a conformity assessment to the mandatory requirements in the O-TTPS.[1)]

These Assessment Procedures are intended to ensure the repeatability, reproducibility, and objectivity of assessments against the O-TTPS. Though the primary audience for this document is the assessor, an Information Technology (IT) provider who is undergoing assessment or preparing for assessment, may also find this document useful.

[1)] The O-TTPS Part 1 is freely available at: www.opengroup.org/library/c185-1.

Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products —

Part 2:
Assessment procedures for the O-TTPS

1 Scope

The Assessment Procedures defined in this document are intended to ensure the repeatability, reproducibility, and objectivity of assessments against the O-TTPS. Though the primary audience for this document is the assessor, an Information Technology (IT) provider who is undergoing assessment or preparing for assessment, may also find this document useful.

1.1 Conformance

The Open Group has developed and maintains conformance criteria, assessment procedures, and a Certification Policy and Program for the O-TTPS as a useful tool for all constituents with an interest in supply chain security.

The conformance requirements and assessment procedures are available in the O-TTPS, Part 2: Assessment Procedures for the O-TTPS.

Certification provides formal recognition of conformance to the O-TTPS, which allows:

— Providers and practitioners to make and substantiate clear claims of conformance to the O-TTPS

— Acquirers to specify and successfully procure from providers who conform to the O-TTPS

1.2 Future Directions

Refer to the O-TTPS, Part 1: Requirements and Recommendations.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

Shall	Indicates an absolute, mandatory requirement that has to be implemented in order to conform to this document and from which no deviation is permitted. Do not use "must" as an alternative for "shall". (This will avoid any confusion between the requirements of a document and external statutory obligations.)
Shall not	Indicates an absolute preclusion, and if implemented would represent a non-conformity. Do not use "may not" instead of "shall not" to express a prohibition.
Should	Indicates a recommendation among several possibilities that is particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.
Should not	Indicates a practice explicitly recommended not to be implemented, or that a certain possibility or course of action is deprecated but not prohibited. To conform to the O-TTPS, an acceptable justification must be presented if the requirement is implemented.
May	Indicates an optional requirement to be implemented at the discretion of the practitioner. Do not use "can" instead of "may" in this context.
Can	Used for statements of possibility and capability, whether material, physical, or causal.

Throughout this document, the term O-TTPS is used when referring to The Open Trusted Technology Provider Standard.

NOTE The terms listed in the following clauses are capitalized throughout this document.

3.1
Distributor
Distributors and Pass-Through Resellers distribute products, but do not modify the product or augment the physical composition of the product as they distribute it. Distributors and Pass-Through Resellers do have responsibility for mitigating risk to the physical and logical access to the product.

3.2
Evidence of Conformance
Evidence submitted to the assessor performing the assessment to demonstrate conformance to the O-TTPS Requirements within an Organization's declared Scope of Assessment.

3.3
Implementation Evidence
Artifacts that show the required process has been applied to the Selected Representative Products.

3.4
O-TTPS Requirements
All of the mandatory (i.e., Shall) requirements in the O-TTPS.

3.5
Organization
A technology provider being assessed for conformance to the O-TTPS Requirements; e.g., Original Equipment Manufacturer (OEM), Original Design Manufacturer (ODM), hardware and software component supplier, integrator, Value-Add Reseller (VAR), Distributor, or Pass-Through Reseller.

3.6
Pass-Through Reseller
Pass-Through Resellers distribute products, but do not modify the product or augment the physical composition of the product as they distribute it. Distributors and Pass-Through Resellers do have responsibility for mitigating risk to the physical and logical access to the product.

3.7
Process Evidence
The evidence/artifacts listed in this document as required to demonstrate that the Organization has the required processes/procedures defined.

Note 1 to entry: The Process Evidence shows they have defined/documented processes, the Implementation Evidence demonstrates that the defined/documented processes/procedures have been implemented.

3.8
Scope of Assessment
A description by the Organization of the products, product lines, business units, and/or geographies, which optionally could encompass an entire organization.

3.9
Selected Representative Product
A set of products that is a representative sample of all the products from within the Scope of Assessment.

4 General Concepts

4.1 The O-TTPS

This clause is included to provide insight into the structure and the naming conventions of the requirements in the O-TTPS, which are also included in the Assessment Requirements in Clause 5.

The O-TTPS is a standard containing a set of requirements that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of commercial Off-The-Shelf (COTS) Information and Communication Technology (ICT) products. It provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. The assessor shall only assess conformance against the mandatory requirements, the (shall) requirements, in the O-TTPS and shall not assess conformance to guidelines or recommendations.

The O-TTPS is described in terms of the provider's product lifecycle. The collection of provider best practices contained in the O-TTPS are those that the OTTF considers best capable of influencing and governing the integrity of a COTS ICT product from its inception to proper disposal at end-of- life. These provider practices are divided into two basic categories of product lifecycle activities: Technology Development and Supply Chain Security:

— **Technology Development**

  The provider's Technology Development activities for a COTS ICT product are mostly under the provider's in-house supervision in how they are executed. The methodology areas that are most relevant to assuring against tainted and counterfeit products are: Product Development/Engineering Methods and Secure Development/Engineering Methods.

— **Supply Chain Security**

The provider's Supply Chain Security activities focus on best practices where the provider must interact with third parties who produce their agreed contribution with respect to the product's lifecycle. Here, the provider's best practices often control the point of intersection with the outside supplier through control points that may include inspection, verification, and contracts.

The O-TTPS is structured by prefacing each requirement with the associated activity area described above. The naming convention is reflected in the O-TTPS and in this document and is listed below:

— Product Development/Engineering Method-related requirements: PD

— Secure Development/Engineering Method-related requirements: SD

— Supply Chain Security Method-related requirements: SC

4.2 Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products

This document introduces the concepts of "Scope of Assessment" and "Selected Representative Products". Rather than assuming an Organization would only request assessment for conforming to the requirements in the O-TTPS for one specific product, these Assessment Procedures allow for the possibility of an Organization to identify their desired Scope of Assessment, which could be:

— An individual product

— All products within one product-line

— All products within a business unit, or

— All products within an entire organization

If an Organization wants to be assessed for conforming to the O-TTPS Requirements throughout a larger scope, then the concept of Selected Representative Products becomes useful. Depending on the size of the product-line, business unit, or organization, it would likely not be practical or affordable for the Organization to demonstrate conformance on every product in a product-line, business unit, or in an entire organization. Instead, the Organization may identify a representative subset of products from within the Scope of Assessment. It is this set of Selected Representative Products which would then be used to generate Evidence of Conformance to each of the O-TTPS Requirements.

However, if an Organization decides to be assessed for conforming to the O-TTPS Requirements for an individual product, then they are free to do so. In that case, the Scope of Assessment would be that one product and there would be only one Selected Representative Product to be assessed.

NOTE Throughout these Assessment Procedures, what is being assessed is the conformance to the O-TTPS Requirements which are, in general, a set of process requirements to be deployed throughout a product's lifecycle from design through to disposal. Assessors are not assessing the products; they are using the products to aid in demonstrating conformance to the O-TTPS Requirements for the defined and implemented processes.

4.3 Relevance of IT Technology Provider Categories in the Supply Chain

The Assessment Procedures contained herein are applicable to all types of Organizations who are ICT technology providers. The nature of the Organization as it applies to their Scope of Assessment is relevant and should be specified by the Organization being assessed and recorded by the assessor. The category selections include:

— **Original Equipment Manufacturer (OEM) or Original Design Manufacturer (ODM)**

Indicating product provider or component supplier and whether the product(s)/component(s) in the Scope of Assessment are primarily hardware or software or both. All of the O-TTPS Requirements are applicable to OEMs and ODMs, including both hardware and software technology providers and component suppliers.

— **Distributor or Pass-Through Reseller (assumes no value-add to the products/components)**

Clause 6 indicates which requirements do not typically apply to this group. In general, none of the Product Development/Engineering Method (PD) or Secure Development/Engineering Method (SE) requirements apply, and all of the Supply Chain Security Method (SC) requirements do apply.

— **Integrator/Value-Add Reseller (VAR)**

These are integrators or resellers who do add value to the product before they distribute it or resell it. This category of technology provider would need to indicate the type of value they add to the product before reselling or distributing it. This value-add should be relevant to the technology within their Scope of Assessment. These technology providers indicate their value-add by choosing one or more of the attribute categories from the O-TTPS. This additional declaration provides the assessor with a better understanding of the Organization's value-add and, therefore, the Organization will be better informed about the particular requirements that will apply, and the type(s) of evidence that should be provided.

5 Assessment Requirements

This clause contains the general requirements for the assessor that shall be read, understood, and followed during an assessment. Clause 6 contains additional specific requirements for the assessor, arranged in table format with specific requirements for assessing each of the O-TTPS Requirements.

5.1 General Requirements for Assessor Activities

This clause contains general requirements for all assessor activities.

5.1.1 General Requirements for Evidence of Conformance

The Evidence of Conformance, demonstrating the existence of a process and the implementation of a process provided by the Organization, shall meet the following requirements:

General Assessor Requirement No.	Description
1	There are two categories of evidence required: Process Evidence and Implementation Evidence. Each requirement in Clause 6 is characterized as either requiring Process Evidence, Implementation Evidence, or both. Process Evidence: — The specific types of Process Evidence listed in Clause 6 are required. This is because these specific types of Process Evidence are generally considered to be paramount in demonstrating conformance and will help assure consistency across all assessments. — When a specific process is cited in the Evidence of Conformance by an Organization and it is different from the process name specified in the assessor activities in Clause 6 under Process Evidence, the assessor should accept this provided the intent of the requirement is met. The assessor shall record those instances and shall include a rationale for acceptance. Implementation Evidence: — Implementation Evidence shows the process has been applied to the Selected Representative Products. Acceptable types of evidence/artifacts are listed in the assessor activities in Clause 6 under Implementation Evidence. This is because each Organization will likely have different ways of demonstrating implementation of the processes, which may include a wide variety of types of evidence. — In certain instances, the types of acceptable Implementation Evidence may differ based on whether the Selected Representative Product being assessed is primarily a hardware or software component/product. Therefore, in some instances, the types of recommended evidence in the Assessment Procedures include options for both hardware and software-related evidence, to be provided as appropriate.
2	The Implementation Evidence shall be related to the Selected Representative Products.
3	The Implementation Evidence and Process Evidence provided shall be sufficient to demonstrate conformance to the requirement and shall be retained by the assessor.
4	The evidence provided shall cover the period of time for which the claimed process has been implemented for the product(s) in the Scope of Assessment.

General Assessor Requirement No.	Description
5	There may be one or more processes identified for each attribute; this will be evident from the Evidence of Conformance. Therefore, in some cases it is acceptable for a requirement to be met by evidence from more than one formal process.
6	Evidence specified in the tables in Clause 6 indicates the expectations of content. The specific names of items and the location of information and document names used within the supplied Evidence of Conformance may vary and is acceptable as long as conformance to the requirement is shown.
7	Terminology used in identifying evidence by Organizations may differ from that used by the O-TTPS provided the terms are understood by the Organization and the assessor.
8	The nature of the Organization as it applies to their Scope of Assessment must be specified by the Organization being assessed and recorded by the assessor. The options include the primary categories of technology providers in the supply chain. Below are the category options and any associated requirements that might be associated with those categories: — **OEMs** All of the requirements apply equally to software or hardware providers. Therefore, if the technology providers that are being assessed are considered to be OEMs, then all of the requirements shall apply and a response of Not Applicable (N/A) is not acceptable based solely on whether a product is primarily hardware or software. — **Distributors or Pass-Through Resellers (with no value-add)** There are certain cases where requirements do not apply. For those cases in the specific guidelines of those requirements, it will state: "NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable". — **Integrators or Value-Add Resellers (VARs)** Depending on the value added for the Selected Representative Product(s) being assessed, different requirements could apply. In instances where the type of evidence required may be slightly different from that required for OEMs, or known by a different name, that evidence is indicated in the specific requirements clause or in the Process or Implementation Evidence fields in the tables in Clause 6 by the following preface: "For integrators and VARs: …".

General Assessor Requirement No.	Description
9	For those O-TTPS Requirements related to training programs, the purpose of receiving the training artifacts evidence is to ensure that the training occurs, not to judge the effectiveness of the training.
10	The term "routinely" is used occasionally in the O-TTPS. For assessment purposes, the assessor shall check that the period is defined. However, the Organization shall provide a rationale for the stated period.
11	When photographic or video evidence is provided as Evidence of Conformance, it shall be current and be indicative of how an Organization is currently applying its processes.
12	The assessor shall record their activities and findings such that the assessment can be repeated and reviewed should the need arise.
13	In instances where the Organization indicates that the requirement is non-applicable, the assessor shall request the rationale for non-applicability in place of evidence, which shall be recorded.

6 Assessor Activities for O-TTPS Requirements

This clause provides specific assessor activities for each O-TTPS Requirement. The tables in this clause are arranged as follows:

— There is an overall heading for each O-TTPS attribute, which includes the name and acronym for the attribute, the definition of the attribute, and a reference to where in the O-TTPS the attribute and associated requirements can be found within the O-TTPS (not this document)

— Under each attribute heading there are tables for every O-TTPS Requirement associated with that attribute – each table contains the acronym for the O-TTPS Requirement, along with the exact wording of the O-TTPS Requirement

NOTE Part 1 of the O-TTPS contains all O-TTPS Requirements, whether mandatory (designated "shall") or recommended (designated "should"). Part 2 of the O-TTPS contains only the mandatory requirements from Part 1.

Each table also includes the following fields:

— Assessment Type: indicates whether the Evidence of Conformance to be provided/assessed is Process Evidence, Implementation Evidence, or both

— Related Requirements: indicates which other O-TTPS Requirements shall be considered in the assessment of this requirement; indicates which Requirements may have overlap or relationship to consider when preparing for assessment

— Specific Requirements for Assessor Activities: provides additional assessor requirements for the specific O-TTPS Requirement – if any

— Evidence of Conformance (Process): indicates the Process Evidence that shall be provided for each requirement

— Evidence of Conformance (Implementation): indicates the types of Implementation Evidence that are acceptable

6.1 PD_DES: Software/Firmware/Hardware Design Process

Attribute Definition

A formal process exists that defines and documents how requirements are translated into a product design.

O-TTPS Reference

Section 4.1.1.1.

Assessor Activity Tables

PD_DES.01	A process shall exist that assures the requirements are addressed in the design.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_TAM.02
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product requirements management process, product design process
Evidence of Conformance (Implementation)	Design artifacts, requirements traceability report, quality assurance, audit reports, reports produced by tracking system

PD_DES.02	Product requirements shall be documented.
Assessment Type	Implementation Evidence required
Related Requirements	SC_OSH.02
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.

Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Product requirements document

PD_DES.03	Product requirements shall be tracked as part of the design process.
Assessment Type	Process Evidence and Implementation Evidence Required
Related Requirements	PD_DES.01, PD_DES.02
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product requirements management process, product design process
Evidence of Conformance (Implementation)	Product requirements document

6.2 PD_CFM: Configuration Management

Attribute Definition

A formal process and supporting systems exist which assure the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.

O-TTPS Reference

Section 4.1.1.2.

Assessor Activity Tables

PD_CFM.01	A documented formal process shall exist which defines the configuration management process and practices.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	None.

Specific Requirements for Assessor Activities	The configuration management process shall include change management or separate process documentation shall exist that covers change management. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Configuration Management (CM) process
Evidence of Conformance (Implementation)	CM reports, build reports, CM tooling, CM artifacts, CM applications, tools, build tools, change control applications, reports produced from change boards

PD_CFM.02	Baselines of identified assets and artifacts under configuration management shall be established.
Assessment Type	Implementation Evidence required
Related Requirements	PD_MPP.02
Specific Requirements for Assessor Activities	Baselines shall be current and include the artifacts that constitute each product. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Product baselines in the CM system

PD_CFM.03	Changes to identified assets and artifacts under configuration management shall be tracked and controlled.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_OSH.03

Specific Requirements for Assessor Activities	Starting with a change request to the Selected Representative Product(s) trace that the process for change management has been implemented. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Change management process
Evidence of Conformance (Implementation)	Problem reports, change reviews, build reports, requests for changes, build/scope review

PD_CFM.04	Configuration management shall be applied to build management and development environments used in the development/engineering of the product.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	Implementation Evidence may consist of screenshots from a CM application. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	CM process
Evidence of Conformance (Implementation)	Evidence from CM application (for software or hardware)

PD_CFM.05	Access to identified assets and artifacts and supporting systems shall be protected and secured.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_ACC.all

Specific Requirements for Assessor Activities	An access control policy shall exist and it shall describe the access control policy for each of the artifacts and assets identified in the assessment of PD_CFM.02 and supporting systems. This includes physical access control policies and logical access control policies. The assessor shall check that the evidence demonstrates that the access control policy has been implemented. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Security controls: access control policies and procedures
Evidence of Conformance (Implementation)	Security audit reports, CM access control, problem tracking access control, build management access control, assembly management access control, access controls to physical artifacts, role-based or identity-based access controls, list of supporting systems

PD_CFM.06	A formal process shall exist that establishes acceptance criteria for work products accepted into the product baseline.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_QAT.all
Specific Requirements for Assessor Activities	The acceptance criteria for each artifact and asset (configuration item) that forms part of the baseline should be defined. NOTE: Types of artifacts and assets may include, but are not limited to: source code, open source code, binary code, hardware or Integrated Circuit (IC) specifications, components, sub-assemblies, drivers, and documentation such as product manuals and configuration guides. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product development process
Evidence of Conformance (Implementation)	Signed or acknowledged acceptance and compliance records, reports or output from the process gate reviews, business process flows

6.3 PD_MPP: Well-Defined Development/Engineering Method Process and Practices

Attribute Definition

Development/engineering processes and practices are documented, and managed and followed across the lifecycle.

O-TTPS Reference

Section 4.1.1.3.

Assessor Activity Tables

PD_MPP.02	The development/engineering process shall be able to track, as appropriate, components that are proven to be targets of tainting or counterfeiting as they progress through the lifecycle.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_CFM.03, SC_MAL.01, SC_RSM.04
Specific Requirements for Assessor Activities	The process should cover identifying and labeling components that are judged by the Organization as requiring tracking throughout the development/engineering lifecycle. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add this requirement is not applicable.
Evidence of Conformance (Process)	Product development process
Evidence of Conformance (Implementation)	List of components that have been identified as requiring tracking targets of tainting/counterfeiting, CM tool

6.4 PD_QAT: Quality and Test Management

Attribute Definition

Quality and test management is practiced as part of the product development/engineering lifecycle. Changes in the product are validated as part of the nominal process of product development/engineering.

O-TTPS Reference

Section 4.1.1.4.

Assessor Activity Tables

PD_QAT.01	There shall be a quality and test product plan that includes quality metrics and acceptance criteria.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_MPP.02, SC_TTC.01
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Quality Assurance (QA) process, product test process
Evidence of Conformance (Implementation)	Quality and test product plan, documented acceptance criteria

PD_QAT.02	Testing and quality assurance activities shall be conducted according to the plan.
Assessment Type	Implementation Evidence required
Related Requirements	SE_TAM.03, SC_TTC.01
Specific Requirements for Assessor Activities	The assessor reviews the Evidence of Conformance related to QA of the work products under development. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Test reports which address the acceptance criteria, QA audit report, QA tracking, QA and test plan

PD_QAT.03	Products or components shall meet appropriate quality criteria throughout the lifecycle (i.e., at appropriate stages).
Assessment Type	Implementation Evidence required

Related Requirements	PD_CFM.06, SC_TTC.01
Specific Requirements for Assessor Activities	Note that "full lifecycle" should be interpreted as throughout the development/engineering lifecycle (i.e., at appropriate stages). NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Test reports, QA audit report, QA tracking, QA plan

6.5 PD_PSM: Product Sustainment Management

Attribute Definition

Product support, release maintenance (i.e., changes/updates to an existing product), and defect management are product sustainment services managed throughout the lifecycle of the product and made generally available.

O-TTPS Reference

Section 4.1.1.5.

Assessor Activity Tables

PD_PSM.01	A release maintenance process shall be implemented.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_QAT.03, PD_CFM.03, SC_MAL.02
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product release maintenance process
Evidence of Conformance (Implementation)	Design change requests, product update descriptions, defect reports, product lifecycle management tooling reports

PD_PSM.02	Release maintenance shall include a process for notification to acquirers of product updates.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_BPS.01
Specific Requirements for Assessor Activities	NOTE: The type of notification may be called something different for hardware (e.g., notification of a new version *versus* notification of an update, which is more often the case with software). NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product release maintenance process
Evidence of Conformance (Implementation)	Acquirer notification example

PD_PSM.03	Release maintenance shall include a product update process, which uses security mechanisms.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_RSM.all, SC_STH.all
Specific Requirements for Assessor Activities	NOTE: The type of process may be called something different for hardware (e.g., new version release or new bill of materials for a new release *versus* product update process, which is more often the case with software). NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product defect management process, product lifecycle management processes, or release management processes and practices
Evidence of Conformance (Implementation)	Security audit report that covers updates, new version release or new bill of materials for a new release, representative updates showing the Organization's security mechanisms being used

PD_PSM.04	A defect management process shall be implemented.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product defect management process
Evidence of Conformance (Implementation)	Evidence of a defect management process, defect reports

PD_PSM.05	The defect management process shall include a documented feedback and problem reporting process.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_MPT.02, SC_RSM.all, PD_DES.01
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Problem reporting process, product defect management process
Evidence of Conformance (Implementation)	Product failure reports, problem reports, change requests, product QA reports, component QA reports

6.6 SE_TAM: Threat Analysis and Mitigation

Attribute Definition

Threat analysis and mitigation identify a set of potential attacks on a particular product or system and describe how those attacks might be perpetrated and the best methods of preventing or mitigating potential attacks.

O-TTPS Reference

Section 4.1.2.1.

Assessor Activity Tables

SE_TAM.01	Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_RSM.all, PD_DES.all
Specific Requirements for Assessor Activities	The assessor should determine whether the Organization has a process in place to assess their product architecture and design against the threat landscape – and that they have implemented the process. The assessor should not attempt to assess the Organization's understanding of the threat landscape. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product design process
Evidence of Conformance (Implementation)	List of known potential attacks, threat assessment against product architecture and design, vulnerability analysis during all phases, relevant threat analysis reports

SE_TAM.02	Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_DES.01
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product development process
Evidence of Conformance (Implementation)	Process and method artifacts

SE_TAM.03	Threat analysis shall be used as input to the creation of test plans and cases.
Assessment Type	Process Evidence required
Related Requirements	PD_QAT.02
Specific Requirements for Assessor Activities	The assessor may choose to consider how threat analysis, from SE_TAM.01, is used as input to the creation of test plans and cases during the analysis of PD_QAT.01. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product test process
Evidence of Conformance (Implementation)	None.

6.7 SE_VAR: Vulnerability Analysis and Response

Attribute Definition

Vulnerability analysis is the process of determining whether a product contains vulnerabilities and categorizing their potential severity.

O-TTPS Reference

Section 4.1.2.3.

Assessor Activity Tables

SE_VAR.01	Techniques and practices for vulnerability analysis shall be utilized. Some techniques include: code review, static analysis, penetration testing, white/black box testing, etc.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_TAM.01, SE_PPR.03

Specific Requirements for Assessor Activities	According to the attribute, the definition of vulnerability analysis is the process of determining whether a product contains vulnerabilities and categorizing their potential severity; therefore, the potential severity of vulnerabilities should be categorized. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Vulnerability analysis process
Evidence of Conformance (Implementation)	Attacks, identified in SE_TAM.01, must be reflected in the vulnerability analysis, using the appropriate techniques and practices (e.g., static analysis reports, white/black box testing reports, code scanning reports, build reports, code review documentation, penetration testing reports, test results, probing, x-ray, tamper detection techniques, hardware penetration testing, solder examination, checking for signal integrity, checks for power consumption, validation of product to spec, side-channel analysis, review of known vulnerability repositories)

SE_VAR.02	A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_BPS.01
Specific Requirements for Assessor Activities	The governing process should include a description of who should be notified. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Vulnerability analysis process
Evidence of Conformance (Implementation)	List of newly discovered exploitable product vulnerabilities and evidence of the appropriate distribution (e.g., Product Security Incident Response Team (PSIRT) process documentation, PSIRT reports, records of notifications)

SE_VAR.04	The impact of published vulnerabilities to the product of the organization being assessed for conformance shall be analyzed and mitigated.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_VAR.01
Specific Requirements for Assessor Activities	There may be cases where no published, exploitable vulnerabilities have been identified for a product or a product line. In this case, an organization may instead provide a rationale explaining why Implementation Evidence is not available. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Vulnerability analysis and mitigation process
Evidence of Conformance (Implementation)	List of exploitable product vulnerabilities and evidence of the appropriate analysis and mitigation (e.g., PSIRT process documentation, PSIRT reports, records of analysis and mitigation)

SE_VAR.05	Vulnerability analysis and response (PSIRT) shall feed into the processes for ongoing product development, product patching, and remediation.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_VAR.01, SE_PPR.01
Specific Requirements for Assessor Activities	Refer to SE_VAR.04. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	PSIRT documentation, PSIRT policy, policy for product lifecycle or product development process
Evidence of Conformance (Implementation)	Examples of remediated product vulnerabilities submitted through PSIRT process

6.8 SE_PPR: Product Patching and Remediation

Attribute Definition

A well-documented process exists for patching and remediating products. Priority is given to known severe vulnerabilities.

O-TTPS Reference

Section 4.1.2.4.

Assessor Activity Tables

SE_PPR.01	There shall be a well-documented process for patching and remediating products.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_CFM.03, PD_PSM.all, SE_VAR.05
Specific Requirements for Assessor Activities	For hardware: the patching and remediation process could be firmware patching or product recall/swapping/repair of components/products. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product patching and remediation process
Evidence of Conformance (Implementation)	Problem reports, patching schedules, release roadmap, release notifications, change requests, etc.

SE_PPR.02	There shall be a process for informing an acquirer of mechanisms for notification and remediation.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Notification process documentation

Evidence of Conformance (Implementation)	Documentation of remediation instructions on website page, in email communications, blog posts, supplemental product documentation, etc.

SE_PPR.03	Remediation of vulnerabilities shall be prioritized based on a variety of factors, including risk.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_PSM.all, SC_RSM.all, SC_VAR.01
Specific Requirements for Assessor Activities	As stated in the attribute definition, vulnerability assessment review should utilize the criteria for prioritization of the remediation of vulnerabilities that are defined by the Organization. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Vulnerability remediation process
Evidence of Conformance (Implementation)	Implementation Evidence as defined in the process documentation (e.g., bug and defect reports, change management documentation for resolutions of vulnerability defects, vulnerability checklists, and vulnerability assessment review)

SE_PPR.04	Documented development and sustainment practices (e.g., ensuring updates to the project are managed, new capabilities are provided, and continuous roll-forward updates occur) shall be followed when implementing product remediation.
Assessment Type	Process Evidence required
Related Requirements	PD_DES.all, PD_CFM.all, PD_MPP.all, PD_QAT.all, PD_PSM.all
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Documentation indicating development processes used to create products are also used for patch and product update development processes

Evidence of Conformance (Implementation)	None.

6.9 SE_SEP: Secure Engineering Practices

Attribute Definition

Secure engineering practices are established to avoid common engineering errors that lead to exploitable product vulnerabilities.

O-TTPS Reference

Section 4.1.2.5.

Assessor Activity Tables

SE_SEP.01	Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabilities; for example, user input validation, use of appropriate compiler flags, etc.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_TAM.all, SE_VAR.all
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Product development process
Evidence of Conformance (Implementation)	Acceptable coding patterns, user input validation, use of appropriate compiler flags, results from tooling that enforces coding patterns, results from manual code reviews, minimize footprint

SE_SEP.02	Secure hardware design practices (where applicable) shall be employed; for example, secure boot, zeroing out memory, effective opacity, etc.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_TAM.all, SE_VAR.all

Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable. NOTE: Not applicable outside secure hardware development, design, and manufacturing.
Evidence of Conformance (Process)	Product design process
Evidence of Conformance (Implementation)	Evidence that design practices are implemented (e.g., zeroing out of memory and effective opacity, secure boot, results from tooling that enforce secure design practices, results from manual review of the application of secure design practices, artifacts and/or assets indicating use of tagging, tamper detection, deployment of anti-counterfeit technology, etc.)

SE_SEP.03	Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_SEP.all, SE_TAM.01, SE_MTL.02
Specific Requirements for Assessor Activities	NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Training process
Evidence of Conformance (Implementation)	Evidence that training has been provided such as training artifacts (e.g., training certificates, Computer-Based Training (CBT), training attendance statistics)

6.10 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape

Attribute Definition

The threat landscape is monitored and the potential impacts of changes in the threat landscape are assessed on development/engineering practices, tools, and techniques.

O-TTPS Reference

Section 4.1.2.6.

Assessor Activity Tables

SE_MTL.02	Changes to the development/engineering practices, tools, and techniques shall be assessed in light of changes to the threat landscape.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_TAM.01, PD_CFM.03
Specific Requirements for Assessor Activities	There may or may not have been changes, but a process should exist to govern such change. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Process improvement process
Evidence of Conformance (Implementation)	Quality engineering/management review, changed secure engineering practices, the applicant's assessment of the development/engineering practices, tools, and techniques in light of changes to the threat landscapes, internal responses for dealing with notification from vendors and monitoring of security forums

SE_MTL.03	The cause of product vulnerabilities shall be evaluated and appropriate changes to the development/engineering practices, tools, and techniques identified to mitigate similar vulnerabilities in the future.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SE_VAR.01
Specific Requirements for Assessor Activities	There may or may not have been changes, but a process should exist to govern such change. NOTE: For Distributors and Pass-Through Resellers, where there is no value-add, this requirement is not applicable.
Evidence of Conformance (Process)	Vulnerability root cause analysis process, process improvement process

Evidence of Conformance (Implementation)	Changed secure engineering practices, the applicant's assessment of the development/engineering practices, tools, and techniques in light of changes to the vulnerability analysis

6.11 SC_RSM: Risk Management

Attribute Definition

The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks.

O-TTPS Reference

Section 4.2.1.1.

Assessor Activity Tables

SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_MPP.02
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	Risk management and prioritization process
Evidence of Conformance (Implementation)	Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents

SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.
Assessment Type	Implementation Evidence required
Related Requirements	PD_RSM.02
Specific Requirements for Assessor Activities	None.

Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Mitigation plan, output from the risk identification assessment

SC_RSM.04	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be followed routinely.
Assessment Type	Implementation Evidence required
Related Requirements	SC_CTM.04
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Evidence that the risk management plan has been followed, component qualification data/reports, snapshot of applicable risk management tools, change history on risk assessment plan, evidence supporting the frequency of updates/reviews matches that described in the risk management process

SC_RSM.05	The mitigation plan shall be reviewed periodically by practitioners, including management, and revised as appropriate.
Assessment Type	Implementation Evidence required
Related Requirements	SC_RSM.03, SC_RSM.04
Specific Requirements for Assessor Activities	If the mitigation plan is new enough not to have been reviewed yet, the Organization may provide a timeline for reviewing the mitigation plan and revising as appropriate.
Evidence of Conformance (Process)	None.

Evidence of Conformance (Implementation)	Evidence that the mitigation plan has been reviewed and, if revisions were found to be appropriate, updates were made to the mitigation plan

SC_RSM.06	Supply chain risk management training shall be incorporated in a provider's organizational training plan, which shall be reviewed periodically and updated as appropriate.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_STR.01
Specific Requirements for Assessor Activities	The purpose of receiving the training artifacts evidence is to ensure that the training occurs, not to judge the effectiveness of the training.
Evidence of Conformance (Process)	Training process/policy
Evidence of Conformance (Implementation)	Training plan includes supply chain training

6.12 SC_PHS: Physical Security

Attribute Definition

Physical security procedures are necessary to protect development assets and artifacts, manufacturing processes, the plant floor, and the supply chain.

O-TTPS Reference

Section 4.2.1.2.

Assessor Activity Tables

SC_PHS.01	Risk-based procedures for physical security shall be established and documented.
Assessment Type	Process Evidence required
Related Requirements	SC_RSM.all
Specific Requirements for Assessor Activities	None.

Evidence of Conformance (Process)	Risk management process: physical security
Evidence of Conformance (Implementation)	None.

SC_PHS.02	Risk-based procedures for physical security shall be followed routinely.
Assessment Type	Implementation Evidence required
Related Requirements	SC_STR.01
Specific Requirements for Assessor Activities	The evidence supplied should be related to the procedures; e.g., if the procedure says Closed Circuit TV (CCTV) is a control, then appropriate CCTV video would be expected to be provided as Evidence of Conformance. Refer to Section 5.1.1 (General Requirements for Evidence of Conformance) within this document for video reference.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	See Specific Requirements for Assessor Activities above. Photographs of the relevant physical security controls (e.g., cages, doors, loading bays, fences, rooftop, ceiling, cabling), snapshots of audit reports, CCTV video, video of implementation of personnel ingress/egress searches, security logs

6.13 SC_ACC: Access Controls

Attribute Definition

Proper access controls are established for the protection of product-relevant intellectual property against the introduction of tainted and counterfeit components where applicable in the supply chain. Access controls may vary by type of intellectual property and over time, during the lifecycle.

O-TTPS Reference

Section 4.2.1.3.

Assessor Activity Tables

SC_ACC.01	Access controls shall be established and managed for product-relevant intellectual property, assets, and artifacts; assets and artifacts include controlled elements related to the development/manufacturing of a provider's product.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_MPP.02, SC_RSM.all, SC_ISS.01
Specific Requirements for Assessor Activities	The assessor is not required to determine the effectiveness or appropriateness of access policy. Note that the following requirements are to be viewed as a whole; the intent is to show that access policies are in place and are being followed.
Evidence of Conformance (Process)	Security controls: access control policies and procedures
Evidence of Conformance (Implementation)	System password and access policies, actual audit reflecting an individual's use of access controls, actual audit reflecting badge-based physical access, transport tracking, inventory account reports

SC_ACC.02	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be documented.
Assessment Type	Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Supplier premises logs, access control lists, access logs, Non-Disclosure Agreements (NDAs)

SC_ACC.03	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be followed routinely.

Assessment Type	Implementation Evidence required
Related Requirements	SC_ISS.01
Specific Requirements for Assessor Activities	Refer to Section 5.1.1 (General Requirements for Evidence of Conformance) within this document regarding “routinely”.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Photographs, CCTV video, video of implementation of personnel ingress/egress searches, access logs, badges, time clock reports, split key reports

SC_ACC.04	Access to product-relevant intellectual property, assets, and artifacts shall be reviewed periodically by practitioners, including management; access controls shall be revised and remediated as appropriate.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_ISS.01, SC_ACC.05
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	Policy describing access control review process
Evidence of Conformance (Implementation)	Evidence that the access controls have been reviewed and, if determined to be appropriate, revisions and/or remediations have been applied to the access controls

SC_ACC.05	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall employ the use of access control auditing.
Assessment Type	Process and Implementation Evidence required
Related Requirements	SC_ISS.01, SC_ACC.04
Specific Requirements for Assessor Activities	None.

Evidence of Conformance (Process)	Security controls: access control audit process
Evidence of Conformance (Implementation)	Audit reports or communications to management of audit results or internal SC security metric reports For physical assets and artifacts, this may include a sign-in or sign-up sheet For electronic assets and artifacts, this may include audit records from an application/tool used to manage/record access

6.14 SC_ESS: Employee and Supplier Security and Integrity

Attribute Definition

Background checks are conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities.

A provider has a set of applicable business conduct guidelines for their employee and supplier communities.

A provider obtains periodic confirmation that suppliers are conducting business in a manner consistent with principles embodied in industry conduct codes, such as the Responsible Business Alliance (RBA) Code of Conduct.

O-TTPS Reference

Section 4.2.1.4.

Assessor Activity Tables

SC_ESS.01	Proof of identity shall be ascertained for all new employees and contractors engaged in the supply chain, except where prohibited by law.
Assessment Type	Process Evidence and practicable Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	Typically, this may be part of the hiring process, but needs to be explicitly part of that process. Assessors are checking identity not legality. Implementation Evidence may be varied by country.
Evidence of Conformance (Process)	Human Resources (HR) identity check process

Evidence of Conformance (Implementation)	Evidence that the identity is verified by the Organization

SC_ESS.02	Background checks shall be conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities (within reason given local customs and according to local law).
Assessment Type	Process Evidence and Implementation Evidence (as allowed by local law) required
Related Requirements	SC_ESS.01
Specific Requirements for Assessor Activities	Assessors verify that background checks are performed in accordance with local customs and law of the country in which the background check is being performed. Implementation Evidence may vary by country.
Evidence of Conformance (Process)	Policy for background checks
Evidence of Conformance (Implementation)	Evidence that policy for background checks has been followed

SC_ESS.03	A set of business conduct guidelines applicable to its employees and contractors shall exist, consistent with principles embodied in industry conduct codes (e.g., the RBA Code of Conduct).
Assessment Type	Process Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	Employee handbook containing business conduct guidelines
Evidence of Conformance (Implementation)	None.

SC_ESS.04	Training on business conduct guidelines shall routinely be provided to employees.
Assessment Type	Process Evidence required
Related Requirements	SC_ESS.03
Specific Requirements for Assessor Activities	The training policy should describe the nature and frequency of the training.
Evidence of Conformance (Process)	Training policy
Evidence of Conformance (Implementation)	None.

6.15 SC_BPS: Business Partner Security

Attribute Definition

Relevant business partners follow the recommended supply chain security best practice requirements specified by the O-TTPS.

Periodic confirmation is requested that business partners are following the supply chain security best practice requirements specified by the O-TTPS.

O-TTPS Reference

Section 4.2.1.5.

Assessor Activity Tables

SC_BPS.01	Supply chain security best practices (e.g., O-TTPS) shall be recommended to relevant business partners.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_CTM.01, SE_VAR.02, PD_PSM.02
Specific Requirements for Assessor Activities	The Assessment Procedures should be interpreted to mean that O-TTPS is preferred but not required. The assessor, in any event, should follow the requirement, which cites the O-TTPS only as an example.

Evidence of Conformance (Process)	Supplier and customer communication process
Evidence of Conformance (Implementation)	Communication reflecting recommended practices, security requirements for suppliers, list of relevant business partners and best practices

SC_BPS.02	Legal agreements with business partners shall reference applicable requirements for supply chain security practices (e.g., O-TTPS).
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_BPS.01
Specific Requirements for Assessor Activities	The required evidence may be the same or similar to the evidence provided for SC_BPS.01.
Evidence of Conformance (Process)	Legal agreement template
Evidence of Conformance (Implementation)	Signed legal agreement

6.16 SC_STR: Supply Chain Security Training

Attribute Definition

Personnel responsible for the security of supply chain aspects are properly trained.

O-TTPS Reference

Section 4.2.1.6.

Assessor Activity Tables

SC_STR.01	Training in supply chain security procedures shall be given to all appropriate personnel.
Assessment Type	Implementation Evidence required
Related Requirements	SC_ACC.03, SC_PHS.02, SC_RSM.06
Specific Requirements for Assessor Activities	The assessor does not need to determine what “appropriate” means; this is defined by the Organization.

Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Training materials, minutes or materials from informational, training artifacts, training attendance statistics, training certificates, computer-based training, a list of appropriate personnel

6.17 SC_ISS: Information Systems Security

Attribute Definition

Supply chain information systems properly protect data through an appropriate set of security controls.

O-TTPS Reference

Section 4.2.1.7.

Assessor Activity Tables

SC_ISS.01	Supply chain data shall be protected through an appropriate set of security controls.
Assessment Type	Implementation Evidence required
Related Requirements	SC_ACC.all
Specific Requirements for Assessor Activities	Supply chain data may include electronic transactions, orders, routing and transit information, and specifications.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	List of the types of supply chain data that are protected, list of associated security controls, examples of access controls on applications that process supply chain data

6.18 SC_TTC: Trusted Technology Components

Attribute Definition

Supplied components, whether hardware or software, are evaluated to assure that they meet component specification requirements.

Suppliers follow the supply chain security best practices with regard to supplied components (e.g., O-TTPS).

O-TTPS Reference

Section 4.2.1.8.

Assessor Activity Tables

SC_TTC.01	The quality of supplied components shall be assessed against the component specification requirements.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_RSM.02, PD_QAT.all
Specific Requirements for Assessor Activities	For Distributors and Pass-Through Resellers, where there is no value-add, they should at least be making sure that the component specifications which were ordered match what they are receiving from the supplier and delivering to the customer.
Evidence of Conformance (Process)	Quality assurance process, quality assurance process for third-party software, Software Development Life Cycle (SDLC) for external development
Evidence of Conformance (Implementation)	For supplied hardware components, this may include component specifications, component quality conformance reports, identification of high-risk components, etc. For supplied software components, this may include output from the quality assurance process for third-party software, code review of supplied software components for development where access to source code is allowed, adherence to SDLC for externally developed software, etc.

SC_TTC.02	Counterfeit components shall not knowingly be incorporated into products.
Assessment Type	Process Evidence required
Related Requirements	PD_MPP.02, SC_RSM.all, SC_CTM.all
Specific Requirements for Assessor Activities	Note that it is not possible to assess whether the policy has been implemented. Use of an Approved Supplier List (ASL) may support the intention of the policy.
Evidence of Conformance (Process)	Policy on use of authentic components or policy to prevent the use of counterfeit components