The Open Group Standard

Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products

Part 2: Assessment Procedures for the O-TTPS and ISO/IEC 20243-1:2018

Version 1.1.1

Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products – Part 2: Assessment Procedures for the O-TTPS and ISO/IEC 20243-1:2018, Version 1.1.1

ISBN: 1-947754-21-8 (Part 2)

Document Number: C185-2

Updated September 2018 to align with ISO/IEC 20243-2:2018.
ISO/IEC 20243-2:2018, technically equivalent to the Assessment Procedures for the O-TTPS and ISO/IEC 20243:2015 V1.1.1 was published by ISO, February 2018.
ISO/IEC 20243-1:2018, technically equivalent to the O-TTPS Version 1.1, was published by ISO, February 2018.
Published by The Open Group, August 2016, and updated in January 2017 to change “Accreditation Program” to “Certification Program”.
ISO/IEC 20243:2015, technically equivalent to the O-TTPS Version 1.1, was published by ISO, September 2015.The previous version of the O-TTPS Assessment Procedures was published by The Open Group, April 2015.
O-TTPS Version 1.1 was published by The Open Group, July 2014.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

1. Introduction

1.1 Scope

This document specifies the procedures to be utilized by an assessor when conducting a conformity assessment to the mandatory requirements in the Open Trusted Technology Provider™ Standard (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.

1.2 Normative References

The following documents, in whole or in part, are normatively referenced within this document. For undated references, the latest edition of the referenced document applies:

- ISO/IEC 20243-1:2018: Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products

1.3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply. For terms not defined here refer to the Glossary in the O-TTPS.

The O-TTPS is technically equivalent to ISO/IEC 20243-1:2018. Throughout this document, the term O-TTPS is used when referring to The Open Trusted Technology Provider Standard (O-TTPS) (ISO/IEC 20243-1:2018).

Note: The terms listed in the following sections are capitalized throughout this document.

1.3.1 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.

1.3.2 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.

1.3.3 Implementation Evidence

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

1.3.4 O-TTPS Requirements

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

[1] The O-TTPS Part 1 is freely available at: www.opengroup.org/library/c185-1. The O-TTPS is technically equivalent to ISO/IEC 20243-1:2018 and is available at: www.iso.org/standard/74399.html.

1.3.5 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.

1.3.6 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.

1.3.7 Process Evidence

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

Note: The Process Evidence shows they have defined/documented processes, the Implementation Evidence (see Section 1.3.3) demonstrates that the defined/documented processes/procedures have been implemented.

1.3.8 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.

1.3.9 Selected Representative Product

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

2. General Concepts

2.1 The O-TTPS

This section is included to provide insight into the structure and the naming conventions of the requirements in the O-TTPS, which are also included in these Assessment Procedures in Section 3.

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 life cycle 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 life cycle. The collection of provider best practices contained in the O-TTPS are those that The Open Group Trusted Technology Forum (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 life cycle activities: Technology Development and Supply Chain Security:

- 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

  — Secure Development/Engineering methods

- 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 life cycle. 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-related requirements: PD
- Secure Development/Engineering methods: SD
- Supply Chain-related requirements: SC

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

These Assessment Procedures introduce 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 life cycle 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.

2.3 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:

- OEM: 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 including both hardware and software technology providers and component suppliers.
- Distributor or Pass-Through Reseller (assumes no value-add to the products/components): In Section 4 it indicates which requirements do not typically apply to this group. In general, none of the Product Development (PD) or Secure Engineering (SE) requirements apply and all of the Supply Chain (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. For this category of technology provider they 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 – those options listed below. 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.

The O-TTPS value-add options list for integrators and VARs (taken from the O-TTPS attributes (high-level categories of requirements in the O-TTPS)):

- PD_DES: Software/Firmware/Hardware Design Process
- PD_CFM: Configuration Management
- PD_MPP: Well-defined Development/Engineering Method Process and Practices
- PD_QAT: Quality and Test Management

- PD_PSM: Product Sustainment Management
- SE_TAM: Threat Analysis and Mitigation
- SE_RTP: Run-time Protection Techniques
- SE_VAR: Vulnerability Analysis and Response
- SE_PPR: Product Patching and Remediation
- SE_SEP: Secure Engineering Practices
- SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape
- SC_RSM: Risk Management
- SC_PHS: Physical Security
- SC_ACC: Access Controls
- SC_ESS: Employee and Supplier Security and Integrity
- SC_BPS: Business Partner Security
- SC_STR: Supply Chain Security Training
- SC_ISS: Information Systems Security
- SC_TTC: Trusted Technology Components
- SC_STH: Secure Transmission and Handling
- SC_OSH: Open Source Handling
- SC_CTM: Counterfeit Mitigation
- SC_MAL: Malware Detection

3. Assessment Requirements

This section contains the general requirements for the assessor that shall be read, understood, and followed during an assessment. Section 4 contains additional specific requirements for the assessor, arranged in table format with specific requirements for assessing each of the O-TTPS Requirements.

3.1 General Requirements for Assessor Activities

This section contains general requirements for all assessor activities.

3.1.1 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 Section 4 is characterized as either requiring Process Evidence, Implementation Evidence, or both. Process Evidence: • The specific types of Process Evidence listed in Section 4 in this document 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 Section 4 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 Section 4 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 Section 4 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 section or in the Process or Implementation Evidence fields in the tables in Section 4 by the following preface: “For integrators and VARs: …”.
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.

4. Assessor Activities for O-TTPS Requirements

This section provides specific assessor activities for each O-TTPS Requirement. The tables in this section 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.
- 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.

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.
- **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.

4.1 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

4.2 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	CD_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 process 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.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 Circuits (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

4.3 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 life cycle.

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 life cycle.
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 life cycle. 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

4.4 PD_QAT: Quality and Test Management

Attribute Definition

Quality and test management is practiced as part of the Product Development/Engineering life cycle.

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 life cycle.
Assessment Type	Implementation Evidence required
Related Requirements	PD_CFM.06, SC_TTC.01

Specific Requirements for Assessor Activities	Note that "full life cycle" should be interpreted as throughout the development/engineering life cycle. 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

4.5 PD_PSM: Product Sustainment Management

Attribute Definition

Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is 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 life cycle 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 life cycle 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

4.6 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)	A 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.

4.7 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, for example, the following: 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.03	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; some examples are: Product Security Incident Response Team (PSIRT) process documentation, PSIRT reports, email records of notifications

4.8 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
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.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; for example, bug and defect reports, change management documentation for resolutions of vulnerability defects, vulnerability checklists, and vulnerability assessment review

4.9 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, 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, zeroing out memory and effective opacity.
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 design process
Evidence of Conformance (Implementation)	Evidence that design practices are implemented such as: results from tooling that enforce secure design practices, results from manual review of the application of secure design practices, design accounts for things like: tagging, tamper detection, deployment of anti-counterfeit technology

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; for example, training certificates, Computer-Based Training (CBT), training attendance statistics

4.10 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

4.11 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	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
Evidence of Conformance (Process)	Risk management 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 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.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

4.12 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 general requirements for Evidence of Conformance within this document for video reference.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Photographs of the relevant physical security controls; for example, cages, doors, loading bays, fences, rooftop, ceiling, cabling, etc., snapshots of audit reports, CCTV video, video of implementation of personnel ingress/egress searches, security logs

4.13 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 IP and over time, during the life cycle.

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 General Requirements for Assessor Activities (Section 3.1) 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.05	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall employ the use of access control auditing.
Assessment Type	Implementation Evidence required
Related Requirements	SC_ISS.01
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

4.14 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 Electronic Industry Citizenship Coalition (EICC) 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 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

4.15 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 practices 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.03, 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

4.16 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

4.17 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

4.18 SC_TTC: Trusted Technology Components

Attribute Definition

Supplied components 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
Evidence of Conformance (Implementation)	Component specifications, component quality conformance reports, identification of high-risk components

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
Evidence of Conformance (Implementation)	None.

4.19 SC_STH: Secure Transmission and Handling

Attribute Definition

Secure transmission and handling of assets and artifacts during delivery is needed to lower the risk of product tampering while in transit to their destination.

O-TTPS Reference

Section 4.2.1.9.

Assessor Activity Tables

SC_STH.01	Secure transmission and handling controls shall be established and documented.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_ISS.01

Specific Requirements for Assessor Activities	Assessors should note that this requirement applies to both receiving components from upstream suppliers as well as delivering items downstream.
Evidence of Conformance (Process)	Risk management process, security controls, secure transmission and handling procedures
Evidence of Conformance (Implementation)	Photos reflecting CCTV use in manufacturing operations and product transfer locations, review of a portion of CCTV video to validate operation of CCTV, evidence of using encrypted transmission, secure File Transfer Protocol (FTP)server logs, secure packaging, trailer seals

SC_STH.02	Secure transmission and handling controls shall be designed to lower the risk of physical tampering with assets and artifacts that are physically transported.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	None.
Specific Requirements for Assessor Activities	NOTE: The assessor is not required to determine the effectiveness of the controls themselves. NOTE: Assets and artifacts include products. NOTE: Physical transport includes movement inside or outside the factory/facility.
Evidence of Conformance (Process)	Risk management process, security controls, secure transmission and handling procedures
Evidence of Conformance (Implementation)	Secure packaging, security tape, shipping logs, badges, guards, bonded transport, photographic evidence, interviews with security staff

SC_STH.03	Secure transmission and handling controls shall be designed to lower the risk of tampering with assets and artifacts that are electronically transmitted.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_CFM.05
Specific Requirements for Assessor Activities	The assessor is not required to determine the effectiveness of the controls themselves. NOTE: Secure handling also includes secure controls applied to data at rest.
Evidence of Conformance (Process)	Risk management process, electronic delivery process, security controls, secure transmission and handling procedures
Evidence of Conformance (Implementation)	Demonstrated use of encryption, secure FTP server logs, access controls, cryptographic hash verification, hash value comparisons

SC_STH.04	Secure transmission and handling controls shall be followed routinely.
Assessment Type	Implementation Evidence required

Related Requirements	SC_STR.01
Specific Requirements for Assessor Activities	NOTE: The assessor should look for evidence that the processes provided for SC_STH.02 and SC_STH.03 are carried out routinely. Refer to item 3 and item 10 in General Requirements for Assessor Activities (Section 3.1) of this document.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	See SC_STH.02 and SC_STH.03.

4.20 SC_OSH: Open Source Handling

Attribute Definition

Open Source components are managed as defined by the best practices within the O-TTPS for Product Development/Engineering methods and Secure Development/Engineering methods.

O-TTPS Reference

Section 4.2.1.10.

Assessor Activity Tables

SC_OSH.02	In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD-CFM.02, PD_CFM.03, PD_DES.02
Specific Requirements for Assessor Activities	Verify that the lineage of Open Source components is tracked and identified in the development life cycle tools.
Evidence of Conformance (Process)	Product development process
Evidence of Conformance (Implementation)	Records of component lineage derivation for the Open Source components

SC_OSH.03	In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_CFM.06, PD_QAT.01, SC_MAL.all
Specific Requirements for Assessor Activities	None.

Evidence of Conformance (Process)	Product test process
Evidence of Conformance (Implementation)	Security and integrity checking might include activities such as checking hash values of included Open Source code, vulnerability analysis, and performing malware checks

SC_OSH.04	For such sourced components, responsibilities for ongoing support and patching shall be clearly understood.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_CFM.03, PD_PSM.all
Specific Requirements for Assessor Activities	From the Distributor or Pass-Through Reseller's perspective, it might not be the "Organization's" (in this case the Distributor/Reseller's) point of contact, it might be a point of contact in the Open Source provider's organization.
Evidence of Conformance (Process)	Product support policy
Evidence of Conformance (Implementation)	An Organization's point of contact for customers to request support and patching, a list of such sourced components and their support contacts, examples of how such sourced components will be supported

4.21 SC_CTM: Counterfeit Mitigation

Attribute Definition

Practices are deployed to manufacture, deliver, and service products that do not contain counterfeit components.

Practices are deployed to control the unauthorized use of scrap from the hardware manufacturing process.

O-TTPS Reference

Section 4.2.1.11.

Assessor Activity Tables

SC_CTM.01	Instances of counterfeit activity relating to products shall be reviewed and an appropriate response sent.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	PD_MPP.02, SC_BPS.01, SE_VAR.03
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	Counterfeit review and response policy

Evidence of Conformance (Implementation)	Records showing the monitoring of grey market activities, copies of portions of investigation reports and action plans upon counterfeit findings, records of appropriate response sent

SC_CTM.04	Techniques shall be utilized as applicable and appropriate to mitigate the risk of counterfeiting, such as security labeling and scrap management techniques.
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_RSM.04. SC_PHS.all, SC_ACC.05
Specific Requirements for Assessor Activities	None.
Evidence of Conformance (Process)	Security controls: risk management process, anti-counterfeit controls
Evidence of Conformance (Implementation)	List of high-risk items that are subject to these controls, scrap handling procedures, demonstrations of use of labeling and photo of labeling, demonstration of results arising from use of anti-counterfeit technology, demonstration/observation/photos of their use, holograms, inks, Radio Frequency Identification (RFID), etc.

4.22 SC_MAL: Malware Detection

Attribute Definition

Practices are employed that mitigate as much as practical the inclusion of malware in components received from suppliers and components or products delivered to customers or integrators.

O-TTPS Reference

Section 4.2.1.12.

Assessor Activity Tables

SC_MAL.01	One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes.
Assessment Type	Implementation Evidence required
Related Requirements	SC_CFM.04, PD_QAT.01
Specific Requirements for Assessor Activities	The processes for this are described in the related requirements. The assessor should ensure that the acceptance criteria include malware detection. Since some systems may be proprietary or otherwise may not have commercial malware detection tools, this is a non-conformity and the rationale for this must be included in the assessment report. NOTE: This requirement is focused on software, including firmware but not pure hardware.
Evidence of Conformance (Process)	None.

Evidence of Conformance (Implementation)	Acceptance procedures requiring the use of malware detection tools, demonstration and/or copies of records showing application of malware detection tools to code in the development stage, up-to-date signatures being used in the detection tool

SC_MAL.02	Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).
Assessment Type	Process Evidence and Implementation Evidence required
Related Requirements	SC_CFM.04, PD_QAT.01, PD_QAT.03, PD_PSM.01
Specific Requirements for Assessor Activities	The processes for this may be described in the related requirements. The assessor should ensure that the criteria for release include malware detection. NOTE: This requirement is focused on software, including firmware but not pure hardware.
Evidence of Conformance (Process)	Quality assurance process
Evidence of Conformance (Implementation)	Release procedures requiring the use of malware detection tools, demonstration and/or copies of records showing application of malware detection tools before final packaging and delivery

A Annex: Assessment Guidance

This section contains guidelines that are not mandatory, but should be read, understood, and considered by assessors when doing O-TTPS assessments.

A.1 Guidance

- There are many security mechanisms that may be used and referenced in the Evidence of Conformance; e.g., digital signatures, encryption, hashing, and bound mechanisms. It is suggested that mechanisms employed by the Organization should be related to the risk analysis of the medium and environment in which the release is made.
- The assessor's records should contain supplementary information about the assessment methodology used for each requirement, such as: who was interviewed (names and roles), on what topic, what evidence was reviewed, evidence identifier, date, and location of the interview, whether the location was physical or virtual.

B Annex: Assessment Report Template

This section contains the Assessment Report Template.

Table 1: Assessment Report Template

Organization	
Authorized Signatory of the Organization	
Report Submission Date	
Acceptance Date	
Assessment Organization Name and ID	
Assessment Team Leader Name and ID	
Assessors who participated in the Assessment	
Version of the Standard to which the Organization is certified	
Assessment Team Recommendation	
Designated Certification Authority Individual	
Approved Assessment Outcome	