Open Trusted Technology Provider™ Standard (O-TTPS)

Assessment Procedures

Version 1.1
April 2015

Open Trusted Technology Provider™ Standard (O-TTPS):
Assessment Procedures

Document Number: X1316

Published by The Open Group, April 2015.

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

The Open Group, 8 New England Executive Park, Burlington, MA 01803, United States

or by electronic mail to:

ogspecs@opengroup.org

Contents

1. Introduction

This document defines the procedures that must be utilized by an O-TTPS Recognized Assessor when conducting an Assessment for conformance to the Open Trusted Technology Provider Standard (O-TTPS) requirements.

For a complete understanding of the O-TTPS Accreditation Program and to see where the O-TTPS Assessment component fits in the process, the reader should refer to the O-TTPS Accreditation Policy. Additionally, readers should familiarize themselves with all of the Referenced Documents. The O-TTPS, Conformance Statement Questionnaire, ISCA Document, and Accreditation Package Document will be utilized during the Assessment.

The primary audience for this document is the Assessor; however, an Organization that is undergoing Assessment and needs to understand the requirements for accreditation in more depth may also find this document useful.

1.1 Terminology

Refer to the Glossary in the O-TTPS.

1.2 Referenced Documents

The following documents are referenced within this document and can be found here: ottps-accred.opengroup.org/home-public:

- Accreditation Package Document
- Accreditation Policy
- Accreditation Requirements
- Conformance Statement Questionnaire
- Implementation Selection Criteria Application (ISCA) Document
- Open Trusted Technology Provider™ Standard (O-TTPS)
- O-TTPS Recognized Assessor Agreement
- Trademark License Agreement

2. General Concepts

This section contains general but important context-setting information for the Assessment. Some of these concepts are defined in greater detail in the O-TTPS Accreditation Policy, ISCA Document, Conformance Statement, and Accreditation Package Document. For the avoidance of doubt, where some of these concepts may also be addressed in the O-TTPS and the O-TTPS Accreditation Policy, those documents are the definitive sources and take precedence over this document.

2.1 The O-TTPS

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). 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.

These provider practices are divided into two basic categories of product life cycle activities: Technology Development and Supply Chain Security:

- Technology Development
  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
- Supply Chain Security
  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 these Assessment Procedures and is listed below:

- PD: Product Development/Engineering-related requirements
- SD: Secure Development/Engineering methods
- SC: Supply Chain-related requirements

2.2 Relevance of Scope of Assessment and Selected Representative Products

These Assessment Procedures utilize the concepts of "Scope of Assessment" and "Selected Representative Products", which are described more fully in the O-TTPS Accreditation Policy, the ISCA Document, and the Accreditation Package Template.

The Scope of Accreditation is specified in the Conformance Statement and further elaborated on in the ISCA Document. If an Organization requests 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 shall identify a representative subset of products, from within the Scope of Assessment, as defined in the ISCA Document and which are approved by the Accreditation Authority as defined in the Accreditation Policy. 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 Accreditation would be that one product and there would be only one Selected Representative Product to be assessed.

Please Note: Throughout these Assessment Procedures, what is being assessed is the conformance to the O-TTPS Requirements, which are a set of process requirements to be deployed throughout a product's life cycle from design through disposal. Assessors are not assessing the products; they are using the products to aid in demonstrating conformance to having the required processes in place and for implementing those processes.

2.3 Relevance of IT Technology Provider Categories in the Supply Chain

These Assessment Procedures are applicable to all types of Organizations who are providers of ICT: Original Equipment Manufacturers (OEMs), including product and component suppliers (hardware and software), Distributors and Pass-Thru Resellers (non-value-add resellers), and Integrators and Value-Add Resellers (VARs). Variances in the procedures can depend on the type of Organization and their degree of value added; allowed variances are described in the Assessor requirements table (#14) in Section A.1.

A Assessment Guidelines

The activities expected of Assessors are described in this appendix. This appendix contains general guidelines for the Assessor that should be read, understood, and followed during an Assessment. Appendix B contains additional specific guidelines for the Assessor, arranged in table format with specific guidelines for assessing each of the O-TTPS Requirements.

A.1 General Guidance for Assessor Activities

This section contains general guidance for all Assessor activities. In Appendix B there is specific guidance associated with each requirement.

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:

Reqmt. No.	Description
1	There are two categories of evidence required: process and implementation. For process evidence, the types of evidence/artifacts listed in this document and in the ISCA Document, Appendix B are required. This is because these types are generally cited as being required in the O-TTPS and therefore are considered to be paramount in demonstrating conformance and will help assure consistency across all accreditation applications. When a specific process is cited in the Accreditation Package by an Organization and it is different from the process name specified in the Assessor Activities (Appendix B) under Process Evidence, the Assessor may accept this as long as the intent of the requirement is met and the Assessor notes those instances in the Accreditation Package Template with a rationale for acceptance. As long as the process evidence is acceptable it does not have to be structured in accordance with the definition in the Assessment Procedures nor have the same name. For implementation evidence – that is, evidence that shows the process has been applied to the Selected Representative Products – the types of evidence/artifacts listed in this document are suggested/recommended types of 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.
2	The implementation evidence shall be related to the Selected Representative Products.
3	The implementation and process evidence provided must be sufficient to demonstrate conformance to the requirement.
4	The evidence provided should cover the period of time for which the claimed process has been implemented for the Selected Representative Product.
5	There may be one or more processes identified for each attribute; this will be evident from the Attribute to Process Mapping tables in the Accreditation Package Document. 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 within this document 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 so long as conformance to the requirement is shown.

Reqmt. No.	Description
7	Terminology used in identifying Evidence of Conformance by Organizations may differ from that used by the O-TTPS provided that the terms are understood by the Organization and the Assessor.
8	For some requirements, there are specific guidelines included in Appendix B. This guidance is there to aid the Assessor. Since some of the specific guidelines may be non-normative as they relate to the requirement, failure to provide evidence to meet the specific guidance is not necessarily a non-conformance if appropriate alternate evidence is provided. However, the Assessor should consider whether the evidence provided is sufficient and, if not, then a non-conformance may be appropriate. As a minimum, the Assessor should note an observation that the guidance was not followed.
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 you should check that the period is defined. However, the Organization should provide a rationale for the stated period.
11	When photographic or video evidence is provided as Evidence of Conformance, it should be current and be indicative of how an Organization is currently applying its processes.
12	There are many security mechanisms that could be used and referenced in the Evidence of Conformance; e.g., digital signatures, encryption, hashing, and bound mechanisms. The mechanism employed by the Organization should be related to the risk analysis of the medium and environment in which the release is made.
13	The Assessor must maintain a log of their activities, which will be made available to the Accreditation Authority upon request, such that the Assessment is able to be repeated. The log 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 as indicated in the evidence tables, date, and location of the interview, whether the location was physical or virtual.
14	The nature of the Organization as it applies to their Scope of Accreditation will be specified in the ISCA Document [or the Conformance Statement] by the Organization being accredited. The options include: • OEMs indicating they are a product provider or component supplier. All of the O-TTPS Requirements are applicable to OEMs including both hardware and software technology providers and component suppliers. • Distributor or Pass-Thru Reseller (assumes no value added to the products/components). In general, none of the Product Development (PD) or Secure Engineering (SE) requirements apply and all of the Supply Chain (SC) requirements apply to this group. • Integrators/VARs indicating they are adding value to the technology within their Scope of Accreditation. The Organization will be asked to indicate which O-TTPS attributes apply to their value-add. (See O-TTPS attributes listed below.) This is to provide the Assessor with a better understanding of which requirements will apply and what type of evidence should be provided. Typically all Supply Chain (SC)-related requirements are applicable. The requirements for Product Development (PD) and Secure Engineering (SE) may be applicable depending on the Organization's value-add and their role in the supply chain. O-TTPS attributes: • PD_DES: Software/Firmware/Hardware Design Process • PD_CFM: Configuration Management • PD_MPP: Well-defined Development/Engineering Method Process and Practices

Reqmt. No.	Description
	• 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 All of the O-TTPS Requirements are applicable to OEMs including both hardware and software technology providers and component suppliers. In certain instances the types of implementation evidence required 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. Furthermore, if the technology providers that are being assessed are considered to be OEMs, then all of the requirements apply and a response of N/A is not acceptable based solely on whether a product is primarily hardware or software. If Organizations are considered to be Distributors or Pass-Thru Resellers (specifically not VARs), then there are certain cases where requirements do not apply. For those cases in the specific guidelines of those requirements, it will state: "NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable." If Organizations are considered to be Integrators or VARs, then depending on the value added for the Selected Representative Product 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 guidelines of the requirement or in the process or implementation evidence fields by the following preface: "For Integrators and VARs: …".
15	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 the Assessor shall then include in the final report.

A.2 Recognized External Certifications

Where the OTTF provides a mapping table from another standard to the O-TTPS Assessment Procedures, (e.g., CC_O-TTPS Mapping Table) then those mapping tables will provide additional specific

information on accepting evidence and assessments or compensating activities that shall be followed by the Assessor.

Audit reports are acceptable types of evidence for all requirements, even if this is not explicitly stated in the evidence section of the Evidence of Conformance table. However, Assessors must be satisfied that the audit results are comprehensive (they cover all of the O-TTPS Requirements) and complete, and that identified corrective actions have been cleared in a timely fashion. In addition, the Assessor must spot check a minimum of 10% of the requirements.

In all cases, when audit reports are submitted as Evidence of Conformance the Assessor shall ensure that:

- The audits were performed by an auditor that is independent from the process being assessed.
- The scope of the audit includes examination of the process and implementation evidence associated with the Selected Representative Products.
- The audit reports address relevant O-TTPS Requirements and attributes.
- The Selected Representative Products are included in the scope of the audits.
- The audit reports must have been issued within 24 months prior to this Assessment.

The audit report indicates that the requirements are met successfully or that any identified corrective actions have been addressed (i.e., have been cleared or in the process of being cleared).

B Assessor Activities for O-TTPS Requirements

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

- There is an overall heading for each 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 should be considered in the Assessment of this requirement.
- **Specific Guidelines for Assessor Activities**: Provides additional guidance for the specific requirement – if any.
- **Evidence of Conformance (Process)**: Indicates the *types* of process evidence that must be provided for each requirement.
- **Evidence of Conformance (Implementation)**: Indicates the *types* of implementation evidence that are suggested/recommended.

B.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 and Implementation
Related Requirements	SC_TAM.02
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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
Related Requirements	SC_OSH.02
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Product requirements document

B.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 and Implementation
Related Requirements	None.
Specific Guidelines for Assessor Activities	The configuration management process should include change management or separate process documentation should exist that covers change management. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable.
Evidence of Conformance (Process)	Configuration Management 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
Related Requirements	CD_MPP.02
Specific Guidelines for Assessor Activities	Baselines should be current and include the artifacts that constitute each product. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation

Related Requirements	SC_OSH.03
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SC_ACC.all
Specific Guidelines for Assessor Activities	An access control policy 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	PD_QAT.all
Specific Guidelines 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 IC specifications, components, sub-assemblies, drivers, and documentation such as product manuals and configuration guides. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	PD_CFM.03, SC_MAL.01, SC_RSM.04
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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	Implementation
Related Requirements	PD_MPP.02, SC_TTC.01
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable.
Evidence of Conformance (Process)	Quality Assurance 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
Related Requirements	SE_TAM.03, SC_TTC.01
Specific Guidelines for Assessor Activities	The Assessor reviews the Evidence of Conformance related to QA of the work products under development. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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
Related Requirements	PD_CFM.06, SC_TTC.01

Specific Guidelines for Assessor Activities	Note that "full life cycle" should be interpreted as throughout the development/engineering life cycle. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Test reports, QA audit report, QA tracking, QA plan

B.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 and Implementation
Related Requirements	PD_QAT.03, PD_CFM.03, SC_MAL.02
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SC_BPS.01
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation

Related Requirements	SC_RSM.all, SC_STH.all
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	None.
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	PD_MPT.02, SC_RSM.all, PD_DES.01
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	SC_RSM.all, PD_DES.all
Specific Guidelines for Assessor Activities	The Assessor shall 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	PD_DES.01
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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
Related Requirements	PD_QAT.02
Specific Guidelines for Assessor Activities	The Assessor shall 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that this requirement is not applicable.
Evidence of Conformance (Process)	Product Test Process
Evidence of Conformance (Implementation)	None.

B.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 and Implementation
Related Requirements	SE_TAM.01, SE_PPR.03
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SC_BPS.01
Specific Guidelines for Assessor Activities	The governing process should include a description of who should be notified. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	PD_CFM.03, PD_PSM.all
Specific Guidelines for Assessor Activities	For hardware: the patching and remediation process could be firmware patching or product recall/swapping/repair of components/products. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	PD_PSM.all, SC_RSM.all, SC_VAR.01
Specific Guidelines 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: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	SE_TAM.all, SE_VAR.all
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SE_TAM.all, SE_VAR.all
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SE_SEP.all, SE_TAM.01, SE.MTL.02
Specific Guidelines for Assessor Activities	NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	SE_TAM.01, PD_CFM.03
Specific Guidelines for Assessor Activities	There may, or may not have been changes, but a process should exist to govern such change. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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 and Implementation
Related Requirements	SE_VAR.01
Specific Guidelines for Assessor Activities	There may, or may not have been changes, but a process should exist to govern such change. NOTE: It is typically the case, for Distributors and Pass-Thru Resellers, where there is no value-add, that 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

B.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 and Implementation
Related Requirements	PD_MPP.02
Specific Guidelines 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
Related Requirements	PD_RSM.02
Specific Guidelines 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

Related Requirements	SC_CTM.04
Specific Guidelines 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 and Implementation
Related Requirements	SC_STR.01
Specific Guidelines 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

B.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
Related Requirements	SC_RSM.all
Specific Guidelines 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
Related Requirements	SC_STR.01
Specific Guidelines for Assessor Activities	The evidence supplied should be related to the procedures; e.g., if the procedure says 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

B.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 and Implementation
Related Requirements	PD_MPP.02, SC_RSM(ALL), SC_ISS.01
Specific Guidelines 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
Related Requirements	None.
Specific Guidelines for Assessor Activities	None.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	Supplier premises logs, access control lists, access logs, NDA agreements

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

Assessment Type	Implementation
Related Requirements	SC_ISS.01
Specific Guidelines for Assessor Activities	Refer to 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.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
Related Requirements	None.
Specific Guidelines 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

B.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 and Implementation
Related Requirements	None.
Specific Guidelines 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)	HR Identity Check Process
Evidence of Conformance (Implementation)	Evidence that the identity is verified by the Organization

B.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 and Implementation
Related Requirements	SC_CTM.01, SE_VAR.03, PD_PSM.02
Specific Guidelines 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

B.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
Related Requirements	SC_ACC.03, SC_PHS.02, SC_RSM.06
Specific Guidelines 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

B.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
Related Requirements	SC_ACC.all
Specific Guidelines 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

B.18 SC_TTC: Trusted Technology Components

Attribute Definition

Supplied components are evaluated to assure that they meet component specification requirements.

Suppliers follow 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 and Implementation
Related Requirements	SC_RSM.02, PD_QAT.all
Specific Guidelines for Assessor Activities	For Distributors and Pass-Thru 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
Related Requirements	PD_MPP.02, SC_RSM.all, SC_CTM.all
Specific Guidelines 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.

B.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 and Implementation
Related Requirements	SC_ISS.01
Specific Guidelines 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 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 and Implementation
Related Requirements	None.
Specific Guidelines 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 and Implementation

Related Requirements	PD_CFM.05
Specific Guidelines 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, SFTP 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
Related Requirements	SC_STR.01
Specific Guidelines 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 of Section A.1 of this document.
Evidence of Conformance (Process)	None.
Evidence of Conformance (Implementation)	See SC_STH.02 and SC_STH.03.

B.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 and Implementation
Related Requirements	PD-CFM.02, PD_CFM.03, PD_DES.02
Specific Guidelines 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 sourced 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 and Implementation
Related Requirements	PD_CFM.06, PD_QAT.01, SC_MAL.all
Specific Guidelines 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 and Implementation

Related Requirements	PD_CFM.03, PD_PSM.all
Specific Guidelines for Assessor Activities	From the Distributor or Pass-Thru 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

B.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 and Implementation
Related Requirements	PD_MPP.02, SC_BPS.01, SE_VAR.03
Specific Guidelines 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 and Implementation
Related Requirements	SC_RSM.04. SC_PHS.all, SC_ACC.05
Specific Guidelines for Assessor Activities	None.
Evidence of Conformance (Process)	Security Controls: Risk Management Process, Anti-counterfeit Controls
Evidence of Conformance (Implementation)	List of high-risk item 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, RFID, etc.

B.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
Related Requirements	SC_CFM.04, PD_QAT.01
Specific Guidelines 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 and Implementation
Related Requirements	SC_CFM.04, PD_QAT.01, PD_QAT.03, PD_PSM.01
Specific Guidelines 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

C Recording Assessment Findings

To help assure consistency across O-TTPS accreditation applications, the guidelines in this section should be followed.

C.1 Recording Final Observations

Below is an example of one requirement table from the Accreditation Package Document, which will initially be completed by the Organization with information on where the Assessor can find the applicable Evidence of Conformance for each item/row. The last column "Assessor Comment" is where the Assessor will record their Assessment findings for each item in the table. The Assessor may use this table to record and revise their findings throughout the Assessment process should they choose to, but they must record their final findings in the Assessor Comment Column in the final Accreditation Package Document before submitting it to the Accreditation Authority.

During the Assessment, if the finding is that the evidence provided indicates conformance, the Assessor will indicate this by completing the mandatory Assessor Comment column.

The minimum content of the Assessor Comment column for each requirement is:

- Date conformance was established
- Assessor or Assessor(s) responsible for the specific finding
- Evidence assessed (which of the recommended types of evidence was examined, or if alternative evidence was considered why it was determined to be equivalent)
- Assessment method employed (e.g., documentation audit, direct inspection, face-to-face interview, web conference, interview conference call, photograph inspection, video recording, online system audit)
- Rationale for PASS

PD_DES.01		A process shall exist that assures the requirements are addressed in the design.			
Required Types of Process Evidence		Product Design Process, Product Requirements Management Process			
Recommended/Suggested Types of Implementation Evidence		Design artifacts, requirements traceability report, quality assurance, audit reports			
Process ID	**Product No**	**Evidence File Name**	**Description of Evidence**	**Pointer within Evidence**	**Assessor Comment**
Process Evidence					
Product Design Process					
Product Requirements Process					

			[Add more rows if needed]		
Implementation Evidence for each Selected Representative Product					
	P1				
			[Add more rows if needed]		
	P…				
			[Add more rows if needed]		

C.2 Determining the Assessment Outcome

For each and every requirement, the Assessor must determine whether a PASS finding can be asserted and, if so, completes the Assessor Comment column to record the basis of that finding.

C.3 Completing the Assessment Report

The final step is to complete the Assessment Report, which is part of the Assessment Package Document – and is included here for illustration. The Assessor completes all of the fields, with the information described below and submits it to the Accreditation Authority.

Table 1: Assessment Report Template

Organization	[As defined in the Conformance Statement.]
Authorized Signatory of the Organization	[Printed name and signature of Authorized Signatory. The Signature means that the Organization has reviewed the report and concurs with the findings.]
Report Submission Date	[The date the report is submitted to the Accreditation Authority.]
Acceptance Date	[The date the report is approved by the Accreditation Authority.]
Assessment Organization Name and ID	[Must be an O-TTPS Recognized Assessor (Company)]
Assessment Team Leader Name and ID	[Printed name and signature of Assessment Team Leader. This is the individual who will "sign-off" on the Assessment Report. Must have met the O-TTPS Assessor criteria, passed the O-TTPS Assessor Examination, and be employed or contracted by an O-TTPS Recognized Assessor (Company).]
Assessors who participated in the Assessment	[Names of all of the Assessors who participated in the Assessment. Must have met the O-TTPS Assessor criteria, passed the O-TTPS Assessor Examination, and be employed or contracted by an O-TTPS Recognized Assessor (Company).]
O-TTPS Accreditation Requirements Version	[O-TTPS Accreditation Requirements version number]
O-TTPS Version	[O-TTPS version number]

O-TTPS Assessment Procedures Version	[O-TTPS Assessment Procedures version number]
O-TTPS Accreditation Policy Version	[O-TTPS Accreditation Policy version number]
O-TTPS Conformance Statement Version	[O-TTPS Conformance Statement version number]
Assessment Team Recommendation	
Designated Accreditation Authority Individual	[Approving report]
Approved Assessment Outcome	