INTERNATIONAL STANDARD

ISO/IEC 20243-2

First edition
2018-01

Information technology — 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

Technologies de l'information — Norme de fournisseur de technologie de confiance ouverte (O-TTPS) — Atténuation des produits contrefaits et malicieusement contaminés —

Partie 2: Procédures d'évaluation de l'O-TTPS et l'ISO/IEC 20243-1:2018

Reference number
ISO/IEC 20243-2:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

FOREWORD

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

This document was prepared by The Open Group and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

A list of all parts in the ISO 20243 series can be found on the ISO website.

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.

1.3.5 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] The O-TTPS is freely available at: www.opengroup.org/bookstore/catalog/c147.htm. The O-TTPS is technically identical to ISO/IEC 20243:2015 ISO/IEC 20243-1:2018 and is available at: www.iso.org

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.
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.

General Assessor Requirement No.	Description
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.