BS ISO/IEC 20243-2:2023

BSI Standards Publication

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

Part 2: Assessment procedures for the O-TTPS

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20243-2:2023

National foreword

This British Standard is the UK implementation of ISO/IEC 20243-2:2023. It supersedes BS ISO/IEC 20243-2:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee ICT/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 25703 8

ICS 13.310; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2023.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20243-2:2023

INTERNATIONAL STANDARD

ISO/IEC 20243-2

Second edition
2023-11

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

Part 2: Assessment procedures for the O-TTPS

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

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: BS ISO/IEC 20243-2:2023

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20243-2:2023

Contents

Page

Foreword ... iv
Preface ... vi
Trademarks ... viii
Introduction ... ix
1 Scope ... 1
1.1 Conformance ... 1
1.2 Future Directions ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
4 General Concepts ... 3
4.1 The O-TTPS ... 3
4.2 Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products ... 4
4.3 Relevance of IT Technology Provider Categories in the Supply Chain ... 4
5 Assessment Requirements ... 5
5.1 General Requirements for Assessor Activities ... 5
5.1.1 General Requirements for Evidence of Conformance ... 5
6 Assessor Activities for O-TTPS Requirements ... 8
6.1 PD_DES: Software/Firmware/Hardware Design Process ... 9
6.2 PD_CFM: Configuration Management ... 10
6.3 PD_MPP: Well-Defined Development/Engineering Method Process and Practices ... 14
6.4 PD_QAT: Quality and Test Management ... 14
6.5 PD_PSM: Product Sustainment Management ... 16
6.6 SE_TAM: Threat Analysis and Mitigation ... 18
6.7 SE_VAR: Vulnerability Analysis and Response ... 20
6.8 SE_PPR: Product Patching and Remediation ... 23
6.9 SE_SEP: Secure Engineering Practices ... 25
6.10 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape ... 26
6.11 SC_RSM: Risk Management ... 28
6.12 SC_PHS: Physical Security ... 30
6.13 SC_ACC: Access Controls ... 31
6.14 SC_ESS: Employee and Supplier Security and Integrity ... 34
6.15 SC_BPS: Business Partner Security ... 36
6.16 SC_STR: Supply Chain Security Training ... 37
6.17 SC_ISS: Information Systems Security ... 38
6.18 SC_TTC: Trusted Technology Components ... 38
6.19 SC_STH: Secure Transmission and Handling ... 40
6.20 SC_OSH: Open Source Handling ... 42
6.21 SC_CTM: Counterfeit Mitigation ... 44
6.22 SC_MAL: Malware Detection ... 46
Annex A ASSESSMENT GUIDANCE ... 48
Annex B ASSESSMENT REPORT TEMPLATE ... 49
Bibliography ... 50

Documents
Document Sharing Hub

© ISO/IEC 2023 – All rights reserved

Full document details: BS ISO/IEC 20243-2:2023

Foreword

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

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

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

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

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

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

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

The main changes are as follows:

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

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

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

— PD_DES.01 has become a mandatory requirement.

— PD_CFM.04 has become a mandatory requirement.

— The attribute definition of PD_QAT has been clarified.

— The attribute definition of PD_PSM has been clarified.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

— SE_PPR.02 has become a mandatory requirement.

— SE_PPR.04 has become a mandatory requirement.

— SC_RSM.05 has become a mandatory requirement.

— SC_ACC.04 has become a mandatory requirement.

— SC_ESS.02 has become a mandatory requirement.

— SC_ESS.03 has become a mandatory requirement.

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

— SC_BPS.02 has become a mandatory requirement.

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

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

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

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

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

Preface

The Open Group

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

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

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

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

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

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

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

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

This Document

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

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

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

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

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

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

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

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

Intended Audience

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

Trademarks

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

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

Introduction

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

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

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

Documents
Document Sharing Hub

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

Part 2: Assessment procedures for the O-TTPS

1 Scope

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

1.1 Conformance

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

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

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

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

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

1.2 Future Directions

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

2 Normative references

There are no normative references in this document.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

3 Terms and definitions

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub

© ISO/IEC 2023 – All rights reserved

Full document details: BS ISO/IEC 20243-2:2023

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

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

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

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

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

4 General Concepts

4.1 The O-TTPS

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

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

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

— **Technology Development**

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

— **Supply Chain Security**

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

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

— Product Development/Engineering Method-related requirements: PD

— Secure Development/Engineering Method-related requirements: SD

— Supply Chain Security Method-related requirements: SC

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

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

— An individual product

— All products within one product-line

— All products within a business unit, or

— All products within an entire organization

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

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

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

4.3 Relevance of IT Technology Provider Categories in the Supply Chain

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

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

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

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

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

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

5 Assessment Requirements

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

5.1 General Requirements for Assessor Activities

This clause contains general requirements for all assessor activities.

5.1.1 General Requirements for Evidence of Conformance

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023

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

6 Assessor Activities for O-TTPS Requirements

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

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

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

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

Each table also includes the following fields:

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

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20243-2:2023