

# ISO/IEC 20243-2:2018-01 (E)

## 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

---

### Contents

- 1. Introduction ..... 1
  - 1.1 Scope ..... 1
  - 1.2 Normative References ..... 1
  - 1.3 Terms and Definitions ..... 1
    - 1.3.1 Distributor ..... 1
    - 1.3.2 Evidence of Conformance ..... 1
    - 1.3.3 Implementation Evidence ..... 1
    - 1.3.4 O-TTPS Requirements ..... 1
    - 1.3.5 Organization ..... 1
    - 1.3.6 Pass-Through Reseller ..... 2
    - 1.3.7 Process Evidence ..... 2
    - 1.3.8 Scope of Assessment ..... 2
    - 1.3.9 Selected Representative Product ..... 2
- 2. General Concepts ..... 3
  - 2.1 The O-TTPS ..... 3
  - 2.2 Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products ..... 3
  - 2.3 Relevance of IT Technology Provider Categories in the Supply Chain ..... 4
- 3. Assessment Requirements ..... 6
  - 3.1 General Requirements for Assessor Activities ..... 6
    - 3.1.1 General Requirements for Evidence of Conformance ..... 6
- 4. Assessor Activities for O-TTPS Requirements ..... 8
  - 4.1 PD\_DES: Software/Firmware/Hardware Design Process ..... 8
  - 4.2 PD\_CFM: Configuration Management ..... 9
  - 4.3 PD\_MPP: Well-defined Development/Engineering Method Process and Practices ..... 11
  - 4.4 PD\_QAT: Quality and Test Management ..... 11
  - 4.5 PD\_PSM: Product Sustainment Management ..... 13
  - 4.6 SE\_TAM: Threat Analysis and Mitigation ..... 14
  - 4.7 SE\_VAR: Vulnerability Analysis and Response ..... 16
  - 4.8 SE\_PPR: Product Patching and Remediation ..... 17
  - 4.9 SE\_SEP: Secure Engineering Practices ..... 17
  - 4.10 SE\_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape ..... 19
  - 4.11 SC\_RSM: Risk Management ..... 20
  - 4.12 SC\_PHS: Physical Security ..... 21
  - 4.13 SC\_ACC: Access Controls ..... 22
  - 4.14 SC\_ESS: Employee and Supplier Security and Integrity ..... 23
  - 4.15 SC\_BPS: Business Partner Security ..... 24
  - 4.16 SC\_STR: Supply Chain Security Training ..... 24
  - 4.17 SC\_ISS: Information Systems Security ..... 25
  - 4.18 SC\_TTC: Trusted Technology Components ..... 25
  - 4.19 SC\_STH: Secure Transmission and Handling ..... 26
  - 4.20 SC\_OSH: Open Source Handling ..... 28
  - 4.21 SC\_CTM: Counterfeit Mitigation ..... 29
  - 4.22 SC\_MAL: Malware Detection ..... 30
  - A.1 Guidance ..... 32