

ISO/IEC 20243-2:2023-11 (E)

Information technology - Open Trusted Technology Provider™ Standard (O-TTPS) - Part 2: Assessment procedures for the O-TTPS

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