

ISO/IEC 15408-1:2026-05 (E)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model

Contents

Page

- Foreword..... vi
- Introduction..... vii
- 1 Scope..... 1
- 2 Normative references..... 1
- 3 Terms and definitions..... 1
- 4 Abbreviated terms..... 13
- 5 Overview..... 14
 - 5.1 General..... 14
 - 5.2 ISO/IEC 15408 series audience..... 14
 - 5.2.1 General..... 14
 - 5.2.2 Consumers (Risk owners)..... 14
 - 5.2.3 Developers..... 14
 - 5.2.4 Technical working groups..... 15
 - 5.2.5 Evaluators..... 15
 - 5.2.6 Others..... 15
 - 5.3 Target of evaluation (TOE)..... 17
 - 5.3.1 General..... 17
 - 5.3.2 TOE boundaries..... 18
 - 5.3.3 Different representations of the TOE..... 18
 - 5.3.4 Different configurations of the TOE..... 18
 - 5.3.5 Operational environment of the TOE..... 19
 - 5.4 Presentation of material in this document..... 19
- 6 General model..... 19
 - 6.1 Background..... 19
 - 6.2 Assets and security controls..... 20
 - 6.3 Core constructs of the paradigm of the ISO/IEC 15408 series..... 22
 - 6.3.1 General..... 22
 - 6.3.2 Conformance types..... 23
 - 6.3.3 Communicating security requirements..... 23
 - 6.3.4 Meeting the needs of consumers (risk owners)..... 26
- 7 Specifying security requirements..... 27
 - 7.1 Security problem definition (SPD)..... 27
 - 7.1.1 General..... 27
 - 7.1.2 Threats..... 27
 - 7.1.3 Organizational security policies (OSPs)..... 28
 - 7.1.4 Assumptions..... 28
 - 7.2 Security objectives..... 29
 - 7.2.1 General..... 29
 - 7.2.2 Security objectives for the TOE..... 29
 - 7.2.3 Security objectives for the operational environment..... 29
 - 7.2.4 Relation between security objectives and the SPD..... 30
 - 7.2.5 Tracing between security objectives and the SPD..... 30
 - 7.2.6 Providing a justification for the tracing..... 31
 - 7.2.7 On countering threats..... 31
 - 7.2.8 Security objectives: conclusion..... 31
 - 7.3 Security requirements..... 31
 - 7.3.1 General..... 31

7.3.2	Security Functional Requirements (SFRs)	32
7.3.3	Security assurance requirements (SARs)	34
7.3.4	Security requirements: conclusion	35
8	Security components	36
8.1	Hierarchical structure of security components	36
8.1.1	General	36
8.1.2	Class	36
8.1.3	Family	36
8.1.4	Component	36
8.1.5	Element	36
8.2	Operations	37
8.2.1	General	37
8.2.2	Iteration	37
8.2.3	Assignment	38
8.2.4	Selection	39
8.2.5	Refinement	40
8.3	Dependencies between components	41
8.4	Extended components	42
8.4.1	General	42
8.4.2	Defining extended components	42
9	Packages	43
9.1	General	43
9.2	Package types	44
9.2.1	General	44
9.2.2	Assurance packages	44
9.2.3	Functional packages	44
9.3	Package dependencies	45
9.4	Evaluation method(s) and activities	45
10	Protection Profiles (PPs)	45
10.1	General	45
10.2	PP introduction	46
10.3	Conformance claims and conformance statements	46
10.4	Security assurance requirements (SARs)	48
10.5	Additional requirements common to strict and demonstrable conformance	49
10.5.1	Conformance claims and conformance statements	49
10.5.2	Security problem definition (SPD)	49
10.5.3	Security objectives	49
10.6	Additional requirements specific to strict conformance	49
10.6.1	Requirements for the security problem definition (SPD)	49
10.6.2	Requirements for the security objectives	50
10.6.3	Requirements for the security requirements	50
10.7	Additional requirements specific to demonstrable conformance	50
10.8	Additional requirements specific to exact conformance	50
10.8.1	General	50
10.8.2	Conformance claims and conformance statements	51
10.9	Using PPs	51
10.10	Conformance statements and claims in the case of multiple PPs	52
10.10.1	General	52
10.10.2	Where strict or demonstrable conformance is specified	52
10.10.3	Where exact conformance is specified	52
11	Modular requirements construction	52
11.1	General	52
11.2	PP-Modules	52
11.2.1	General	52
11.2.2	PP-Module Base	53
11.2.3	Requirements for PP-Modules	53
11.3	PP-Configurations	56
11.3.1	General	56
11.3.2	Requirements for PP-Configurations	57
11.3.3	Usage of PP-Configurations	62
12	Security Targets (STs)	65
12.1	General	65

12.2	Conformance claims and conformance statements.....	66
12.3	Assurance requirements.....	68
12.4	Additional requirements in the exact conformance case.....	69
12.4.1	Additional requirements for the conformance claim.....	69
12.4.2	Additional requirements for the SPD.....	69
12.4.3	Additional requirements for the security objectives.....	69
12.4.4	Additional requirements for the security requirements.....	69
12.5	Additional requirements in the multi-assurance case.....	70
13	Evaluation and evaluation results.....	71
13.1	General.....	71
13.2	Evaluation context.....	73
13.3	Evaluation of PPs and PP-Configurations.....	73
13.4	Evaluation of STs.....	74
13.5	Evaluation of TOEs.....	74
13.6	Evaluation methods and evaluation activities.....	75
13.7	Evaluation results.....	75
13.7.1	Results of a PP evaluation.....	75
13.7.2	Results of a PP-Configuration evaluation.....	75
13.7.3	Results of an ST/TOE evaluation.....	75
13.8	Multi-assurance evaluation.....	76
14	Composition of assurance.....	77
14.1	General.....	77
14.2	Composition models.....	77
14.2.1	Layered composition model.....	77
14.2.2	Network or bi-directional composition model.....	78
14.2.3	Embedded composition model.....	79
14.3	Evaluation techniques for providing assurance in composition models.....	79
14.3.1	General.....	79
14.3.2	ACO class for composed TOEs.....	80
14.3.3	Composite evaluation for composite products.....	80
14.4	Requirements for evaluations using composition techniques.....	91
14.4.1	Re-use of evaluation results.....	91
14.4.2	Composition evaluation issues.....	92
14.5	Evaluation by composition and multi-assurance.....	93
	Annex A (normative) Specification of packages.....	94
	Annex B (normative) Specification of Protection Profiles (PPs).....	98
	Annex C (normative) Specification of PP-Modules and PP-Configurations.....	107
	Annex D (normative) Specification of Security Targets (STs) and direct rationale STs.....	121
	Annex E (normative) PP/PP-Configuration conformance.....	132
	Bibliography.....	137