

# ISO/IEC 15408-1:2022-08 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		vi
Introduction .....		viii
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Abbreviated terms .....	13
5	Overview .....	15
5.1	General .....	15
5.2	ISO/IEC 15408 series description .....	15
5.2.1	General .....	15
5.2.2	Audience .....	16
5.3	Target of evaluation (TOE) .....	19
5.3.1	General .....	19
5.3.2	TOE boundaries .....	19
5.3.3	Different representations of the TOE .....	20
5.3.4	Different configurations of the TOE .....	20
5.3.5	Operational environment of the TOE .....	20
5.4	Presentation of material in this document .....	21
6	General model .....	21
6.1	Background .....	21
6.2	Assets and security controls .....	21
6.3	Core constructs of the paradigm of the ISO/IEC 15408 series .....	24
6.3.1	General .....	24
6.3.2	Conformance types .....	24
6.3.3	Communicating security requirements .....	24
6.3.4	Meeting the needs of consumers (risk owners) .....	27
7	Specifying security requirements .....	29
7.1	Security problem definition (SPD) .....	29
7.1.1	General .....	29
7.1.2	Threats .....	29
7.1.3	Organizational security policies (OSPs) .....	30
7.1.4	Assumptions .....	30
7.2	Security objectives .....	31
7.2.1	General .....	31
7.2.2	Security objectives for the TOE .....	31
7.2.3	Security objectives for the operational environment .....	31
7.2.4	Relation between security objectives and the SPD .....	32
7.2.5	Tracing between security objectives and the SPD .....	32
7.2.6	Providing a justification for the tracing .....	33
7.2.7	On countering threats .....	33
7.2.8	Security objectives: conclusion .....	33
7.3	Security requirements .....	33
7.3.1	General .....	33

7.3.2	Security Functional Requirements (SFRs) .....	34
7.3.3	Security assurance requirements (SARs) .....	36
7.3.4	Security requirements: conclusion .....	37
8	Security components .....	38
8.1	Hierarchical structure of security components .....	38
8.1.1	General .....	38
8.1.2	Class .....	38
8.1.3	Family .....	39
8.1.4	Component .....	39
8.1.5	Element .....	39
8.2	Operations .....	39
8.2.1	General .....	39
8.2.2	Iteration .....	40
8.2.3	Assignment .....	40
8.2.4	Selection .....	41
8.2.5	Refinement .....	43
8.3	Dependencies between components .....	44
8.4	Extended components .....	44
8.4.1	General .....	44
8.4.2	Defining extended components .....	45
9	Packages .....	45
9.1	General .....	45
9.2	Package types .....	46
9.2.1	General .....	46
9.2.2	Assurance packages .....	46
9.2.3	Functional packages .....	47
9.3	Package dependencies .....	47
9.4	Evaluation method(s) and activities .....	47
10	ProtectionProfiles(PPs) .....	48
10.1	General .....	48
10.2	PP introduction .....	48
10.3	Conformance claims and conformance statements .....	48
10.4	Security assurance requirements (SARs) .....	51
10.5	Additional requirements common to strict and demonstrable conformance .....	51
10.5.1	Conformance claims and conformance statements .....	51
10.5.2	Security problem definition (SPD) .....	51
10.5.3	Security objectives .....	52
10.6	Additional requirements specific to strict conformance .....	52
10.6.1	Requirements for the security problem definition (SPD) .....	52
10.6.2	Requirements for the security objectives .....	52
10.6.3	Requirements for the security requirements .....	52
10.7	Additional requirements specific to demonstrable conformance .....	53
10.8	Additional requirements specific to exact conformance .....	53
10.8.1	General .....	53
10.8.2	Conformance claims and statements .....	53
10.9	Using PPs .....	54
10.10	Conformance statements and claims in the case of multiple PPs .....	54
10.10.1	General .....	54
10.10.2	Where strict or demonstrable conformance is specified .....	54
10.10.3	Where exact conformance is specified .....	54
11	Modular requirements construction .....	54
11.1	General .....	54
11.2	PP-Modules .....	55
11.2.1	General .....	55
11.2.2	PP-Module Base .....	55
11.2.3	Requirements for PP-Modules .....	55
11.3	PP-Configurations .....	59

11.3.1	General .....	59
11.3.2	Requirements for PP-Configurations .....	59
11.3.3	Usage of PP-Configurations .....	65
12	Security Targets (STs) .....	68
12.1	General .....	68
12.2	Conformance claims and statements .....	68
12.3	Assurance requirements .....	71
12.4	Additional requirements in the exact conformance case .....	71
12.4.1	Additional requirements for the conformance claim .....	71
12.4.2	Additional requirements for the SPD .....	71
12.4.3	Additional requirements for the security objectives .....	72
12.4.4	Additional requirements for the security requirements .....	72
12.5	Additional requirements in the multi-assurance case .....	72
13	Evaluation and evaluation results .....	74
13.1	General .....	74
13.2	Evaluation context .....	76
13.3	Evaluation of PPs and PP-Configurations .....	77
13.4	Evaluation of STs .....	77
13.5	Evaluation of TOEs .....	77
13.6	Evaluation methods and evaluation activities .....	78
13.7	Evaluation results .....	78
13.7.1	Results of a PP evaluation .....	78
13.7.2	Results of a PP-Configuration evaluation .....	78
13.7.3	Results of a ST/TOE evaluation .....	78
13.8	Multi-assurance evaluation .....	79
14	Composition of assurance .....	80
14.1	General .....	80
14.2	Composition models .....	81
14.2.1	Layered composition model .....	81
14.2.2	Network or bi-directional composition model .....	82
14.2.3	Embedded composition model .....	82
14.3	Evaluation techniques for providing assurance in composition models .....	83
14.3.1	General .....	83
14.3.2	ACO class for composed TOEs .....	83
14.3.3	Composite evaluation for composite products .....	84
14.4	Requirements for evaluations using composition techniques .....	95
14.4.1	Re-use of evaluation results .....	95
14.4.2	Composition evaluation issues .....	96
14.5	Evaluation by composition and multi-assurance .....	97
	Annex A (normative) Specification of packages .....	98
	Annex B (normative) Specification of Protection Profiles (PPs) .....	102
	Annex C (normative) Specification of PP-Modules and PP-Configurations .....	112
	Annex D (normative) Specification of Security Targets (STs) and Direct Rationale STs .....	125
	Annex E (normative) PP/PP-Configuration conformance .....	136
	Bibliography .....	141