ISO/IEC 15408-4:2022-08 (E)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities

Contents

Page

Foreword iv

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 General model of evaluation methods and evaluation activities 1
4.1 Concepts and model 1
4.2 Deriving evaluation methods and evaluation activities 3
4.3 Verb usage in the description of evaluation methods and evaluation activities 5
4.4 Conventions for the description of evaluation methods and evaluation activities 6

5 Structure of an evaluation method 6
5.1 Overview 6
5.2 Specification of an evaluation method 7
5.2.1 Overview 7
5.2.2 Identification of evaluation methods 8
5.2.3 Entity responsible for the evaluation method 9
5.2.4 Scope of the evaluation method 9
5.2.5 Dependencies 9
5.2.6 Required input from the developer or other entities 9
5.2.7 Required tool types 10
5.2.8 Required evaluator competences 10
5.2.9 Requirements for reporting 10
5.2.10 Rationale for the evaluation method 10
5.2.11 Additional verb definitions 12
5.2.12 Set of evaluation activities 12

6 Structure of evaluation activities 12
6.1 Overview 12
6.2 Specification of an evaluation activity 12
6.2.1 Unique identification of the evaluation activity 12
6.2.2 Objective of the evaluation activity 12
6.2.3 Evaluation activity links to SFRs, SARs, and other evaluation activities 13
6.2.4 Required input from the developer or other entities 13
6.2.5 Required tool types 13
6.2.6 Required evaluator competences 13
6.2.7 Assessment strategy 13
6.2.8 Pass/fail criteria 14
6.2.9 Requirements for reporting 15
6.2.10 Rationale for the evaluation activity 15

Bibliography 16