ISO/IEC TS 24462:2024-03 (E)

Information security, cybersecurity and privacy protection - Ontology building blocks for security and risk assessment

Contents

Page

Foreword ... iv

Introduction ... v

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Symbols and abbreviated terms ... 3

5 Background ... 4

6 Methodology ... 4

7 Building blocks: collection and structure ... 7
7.1 General ... 7
7.2 Application security assessment ... 8
7.3 Risk assessment ... 8
7.4 Application security controls validation ... 9
7.5 Risk analysis ... 9

8 Ontology capturing relationships among BBs ... 10
8.1 General ... 10
8.2 Building block: application security assessment ... 13
8.3 Building block: risk assessment ... 13
8.4 Building block: application security audit ... 14
8.5 Building block: application security controls validation ... 14
8.6 Building block: risk analysis ... 14
8.7 Lifecycle of building blocks ... 15
8.8 Using BBs ... 15
8.8.1 General ... 15
8.8.2 Using the ontology to structure an assessment based on an existing standard ... 15
8.8.3 Using the ontology to obtain components for an assessment based on a revised edition of a standard ... 15
8.8.4 Using the ontology to obtain structural components for an assessment based on the first edition of a standard ... 16

9 Standard inventory of uniform components ... 17
9.1 Structural BBs ... 17
9.1.1 Description ... 17
9.1.2 Inventory ... 17
9.2 Semantic BBs ... 18
9.3 Assessment BBs ... 18
9.3.1 Description ... 18
9.3.2 Inventory ... 18
9.4 Assessment component BBs ... 22
9.4.1 Description ... 22
9.4.2 Inventory ... 22

10 Complete XML encoding ... 25

Bibliography ... 39