ISO/IEC TR 15443-2:2012-11 (E)

Information technology - Security techniques - Security assurance framework - Part 2: Analysis

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms, definitions and abbreviated terms 1

4 A framework for the analysis of IT security assurance 2

5 Criteria for the analysis SACA paradigms 2
5.1 Availability of recognition agreements and arrangements 2
5.1.1 Discussion 2
5.1.2 Criteria 2
5.2 Geographical and political considerations 3
5.2.1 Discussion 3
5.2.2 Criteria 3

6 Criteria for the analysis of SACA schemes and SACA systems 3
6.1 Independence 3
6.1.1 Discussion 3
6.1.2 Criteria 3
6.2 Scheme competence 4
6.2.1 Discussion 4
6.2.2 Criteria 4
6.3 Assessment conformity 4
6.3.1 Discussion 4
6.3.2 Criteria 5
6.4 Support to security assurance users and providers 5
6.4.1 Discussion 5
6.4.2 Criteria 5
6.5 Provision of interpretations of standards and methods 5
6.5.1 Discussion 5
6.5.2 Criteria 5
6.6 Scheme related policies 6
6.6.1 Discussion 6
6.6.2 Criteria 6
6.7 SACA systems 6
6.7.1 Discussion 6
6.7.2 Criteria 6
6.8 Commercial considerations 6
6.8.1 Discussion 6
6.8.2 Criteria 7
6.9 SACA results 7
6.9.1 Discussion 7
6.9.2 Criteria 7
6.10 SACA Marks and symbols 7
6.10.1 Discussion 7
6.10.2 Criteria 7

7 Criteria for the analysis of SACA bodies 8
7.1 Independence 8
7.1.1 Discussion 8
7.1.2 Criteria 8
7.2 Accreditation 9
7.2.1 Discussion 9
7.2.2 Criteria 9
7.3 SACA body competence 9
7.3.1 Discussion 9
7.3.2 Criteria 9
7.4 Commercial considerations 10
7.4.1 Discussion 10
7.4.2 Criteria 10

8 Criteria for the analysis of SACA methods 11
8.1 General criteria for SACA methods 11
8.1.1 Discussion 11
8.1.2 Criteria 11
8.2 Confidence in the assurance method 11
8.2.1 Discussion 11
8.2.2 Criteria 11
8.3 Independent Confirmation 12
8.3.1 Discussion 12
8.3.2 Criteria 12
8.4 Trust Policies 12
8.4.1 Discussion 12
8.4.2 Criteria 13
8.5 Maturity of the assurance method 13
8.5.1 Discussion 13
8.5.2 Criteria 13

9 Criteria for the analysis of standards, specifications and SACA documents 13
9.1 The standards development organization 13
9.1.1 Discussion 13
9.1.2 Criteria 13
9.2 The standard or specification 14
9.2.1 Discussion 14
9.2.2 Criteria 14

10 Criteria for the analysis of the SACA results 14
10.1 Documentation produced 14
10.1.1 Discussion 14
10.1.2 Criteria 14
10.2 Identification of the components of the deliverable 15
10.2.1 Discussion 15
10.2.2 Criteria 16
10.3 Scopes and boundaries of the target of the assessment 16
10.3.1 Discussion 16
10.3.2 Criteria 16
10.4 Functionality of the deliverable assessed 16
10.4.1 Discussion 16
10.4.2 Criteria 16
10.5 Supply chain criteria 17
10.5.1 Discussion 17
10.5.2 Criteria 17
10.6 Analysis of the security problem 17
10.6.1 Discussion 17
10.6.2 Criteria 17
10.7 Lifecycle 17
10.7.1 Discussion 17
10.7.2 Criteria 18

10.8 Operational considerations 18
10.8.1 Discussion 18
10.8.2 Criteria 18