ISO/IEC TS 23532-1:2021-11 (E)

Information security, cybersecurity and privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 1: Evaluation for ISO/IEC 15408

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 General requirements 2
4.1 Impartiality 2
4.2 Confidentiality 2

5 Structural requirements 3

6 Resource requirements 4
6.1 General 4
6.2 Personnel 4
6.3 Facilities and environmental conditions 5
6.4 Equipment 6
6.5 Metrological traceability 7
6.6 Externally provided products and services 7

7 Process requirements 8
7.1 Review of requests, tenders and contracts 8
7.2 Selection, verification and validation of methods 8
7.2.1 Selection and verification of methods 8
7.2.2 Validation of methods 9
7.3 Sampling 9
7.4 Handling of test or calibration items 9
7.5 Technical records 10
7.6 Evaluation of measurement uncertainty 10
7.7 Ensuring the validity of results 11
7.8 Reporting of results 11
7.8.1 General 11
7.8.2 Common requirements for reports (test, calibration or sampling) 11
7.8.3 Specific requirements for test reports 11
7.8.4 Specific requirements for calibration certificates 12
7.8.5 Reporting sampling - specific requirements 12
7.8.6 Reporting statements of conformity 12
7.8.7 Reporting opinions and interpretations 12
7.8.8 Amendments to reports 12
7.9 Complaints 13
7.10 Nonconforming work 13
7.11 Control of data and information management 13

8 Management system requirements 14
8.1 Options 14

8.1.1 General 14
8.1.2 Option A 14
8.1.3 Option B 14
8.2 Management system documentation (Option A) 14
8.3 Control of management system documents (Option A) 15
8.4 Records (Option A) 15
8.5 Actions to address risks and opportunities (Option A) 16
8.6 Improvement (Option A) 16
8.7 Corrective actions (Option A) 16
8.8 Internal audits (Option A) 16
8.9 Management reviews (Option A) 16

Annex A (informative) Metrologicaltraceability 17

Annex B (informative) Management system options 18

Annex C (informative) Standards relation in IT security evaluation 19

Bibliography 20