ISO/IEC TR 19791:2006-05 (E)

Information technology - Security techniques - Security assessment of operational systems

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Abbreviated terms 4

5 Structure of this Technical Report 4

6 Technical approach 5
6.1 The nature of operational systems 5
6.2 Establishing operational system security 5
6.3 Security in the operational system life cycle 7
6.4 Relationship to other systems 9

7.1 Overview 9
7.2 General philosophy 9
7.3 Operational system assurance 11
7.4 Composite operational systems 13
7.5 Types of security controls 16
7.6 System security functionality 17
7.7 Timing of evaluation 18
7.8 Use of evaluated products 19
7.9 Documentation requirements 20
7.10 Testing activities 20
7.11 Configuration management 21

8 Relationship to existing security standards 22
8.1 Overview 22
8.3 Relationship to non-evaluation standards 24
8.4 Relationship to Common Criteria development 24

9 Evaluation of operational systems 24
9.1 Introduction 24
9.2 Evaluation roles and responsibilities 24
9.3 Risk assessment and determination of unacceptable risks 26
9.4 Security problem definition 27
9.5 Security objectives 27
9.6 Security requirements 27
9.7 The system security target (SST) 29
9.8 Periodic reassessment 31

Annex A (normative) Operational system Protection Profiles and Security Targets 32

A.1 Specification of System Security Targets 32
A.2 Specification of System Protection Profiles 39

Annex B (normative) Operational system functional control requirements 46

B.1 Introduction 46
B.2 Class FOD: Administration 48
B.3 Class FOS: IT systems 56
B.4 Class FOA: User Assets 66
B.5 Class FOB: Business 68
B.6 Class FOP: Facility and Equipment 70
B.7 Class FOT: Third parties 75
B.8 Class FOM: Management 77

Annex C (normative) Operational system assurance requirements 81

C.1 Introduction 81
C.2 Class ASP: System Protection Profile evaluation 88
C.3 Class ASS: System Security Target evaluation 100
C.4 Class AOD: Operational system guidance document 113
C.5 Class ASD: Operational System Architecture, Design and Configuration Documentation 121
C.6 Class AOC: Operational System Configuration Management 128
C.7 Class AOT: Operational System Test 134
C.8 Class AOV: Operational System Vulnerability Analysis 145
C.9 Class AOL: Operational system life cycle support 153
C.10 Class ASI: System security installation and delivery 154
C.11 Class ASO: Records on operational system 158

Annex D (informative) Relationship to Common Criteria development 162

Bibliography 165