

ISO/IEC TR 19791:2010-04 (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	10
7.1	Overview	10
7.2	General philosophy	10
7.3	Operational system assurance	12
7.4	Composite operational systems	14
7.5	Domain Assurance	16
7.6	Types of security controls	18
7.7	System security functionality	20
7.8	Timing of evaluation	21
7.9	Use of evaluated products	22
7.10	Documentation requirements	23
7.11	Testing activities	24
7.12	Configuration management	25
8	Relationship to existing security standards	25
8.1	Overview	25
8.3	Relationship to non-evaluation standards	27
8.4	Relationship to Common Criteria development	28
9	Evaluation of operational systems	28
9.1	Introduction	28
9.2	Evaluation roles and responsibilities	28
9.3	Risk assessment and determination of unacceptable risks	30
9.4	Security problem definition	30
9.5	Security objectives	31
9.6	Security requirements	31
9.7	The System Security Target (SST)	33
9.8	Periodic reassessment	35
Annex A (normative)	Operational system Protection Profiles and Security Targets	36
A.1	Specification of System Security Targets	36

A.2	Specification of System Protection Profiles	42
Annex B (normative) Operational system functional control requirements		49
B.1	Introduction	49
B.2	Class FOD: Administration	51
B.3	Class FOS: IT systems	59
B.4	Class FOA: User Assets	69
B.5	Class FOB: Business	71
B.6	Class FOP: Facility and Equipment	73
B.7	Class FOT: Third parties	78
B.8	Class FOM: Management	80
Annex C (normative) Operational system assurance requirements		84
C.1	Introduction	84
C.2	Class ASP: System Protection Profile evaluation	89
C.3	Class ASS: System Security Target evaluation	101
C.4	Class AOD: Operational system guidance document	115
C.5	Class ASD: Operational System architecture, design and configuration documentation	120
C.6	Class AOC: Operational System configuration management	131
C.7	Class AOT: Operational System test	136
C.8	Class AOV: Operational System vulnerability assessment	146
C.9	Class APR: Preparation for live operation	154
C.10	Class ASO: Records on operational system	157
Annex D (normative) Operational System evaluation methodology		162
D.1	Technical approach	162
D.2	Class ASP: System Protection Profile evaluation	163
D.3	Class ASS: System Security Target evaluation	178
D.4	Class AOD: Operational system guidance document	195
D.5	Class ASD: Operational system architecture, design and configuration documentation	199
D.6	Class AOC: Operational system configuration management	207
D.7	Class AOT: Operational system test	210
D.8	Class AOV: Operational system vulnerability assessment	217
D.9	Class APR: Preparation for live operation	228
D.10	Class ASO: Records on operational system	231
Bibliography		235