

ISO/IEC TR 15443-3:2007-12 (E)

Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
1.1	Purpose	1
1.2	Application	1
1.3	Field of Application	1
1.4	Limitations	1
2	Terms and definitions	1
3	Abbreviated terms	4
4	Understanding Assurance	4
4.1	Setting the assurance goal	4
4.2	Applying assurance methods	7
4.3	Assessing assurance results	12
4.4	Example	14
5	Comparing, selecting and composing assurance	14
5.1	Selecting the assurance approach	14
5.2	Composing assurance methods	16
5.3	Comparing assurance methods	17
5.4	Focus on assurance properties	18
6	Guidance	23
6.1	Developmental Assurance (DA)	24
6.2	Integration Assurance (IA)	25
6.3	Operational Assurance (OA)	29
Annex A -- Tabular comparisons		33
A.1	Methods and their target groups	33
A.2	Available Assurance Methods	34
Annex B -- Assurance properties of selected methods		35
B.6	IT Baseline Protection Manual	46
B.7	COBIT	48
B.8	ISO 9000	50
Annex C -- Composition of assurance methods		53
C.5	COBIT + IT Baseline Protection	54
Annex D -- Case Studies		55
D.1	A chip-card manufacturer's assurance composition strategy	55
D.2	A service provider assures the upgrade of business processes	56

Annex E -- Determination of the assurance goal	57
E.1 Risk Assessment	57
E.2 Risk Management	57
E.3 Security Model	58
E.4 Organizational security policy	59
E.5 Applicable Assurance goal	60
E.6 Security Measures	60
Bibliography	62