ISO/IEC TR 15443-1:2005-02 (E)

Information technology - Security techniques - A framework for IT security assurance - Part 1: Overview and framework

Contents

Page

Foreword iv

Introduction v

1 Scope 1
1.1 Purpose 1
1.2 Approach 1
1.3 Application 1
1.4 Field of Application 1
1.5 Limitations 1

2 Terms and definitions 1

3 Abbreviated terms 6

4 Concepts 7
4.1 Why do we need assurance? 8
4.2 Assurance is distinguishable from confidence 8
4.3 What is a deliverable? 8
4.4 Stakeholders 9
4.5 Assurance requirements 9
4.6 Assurance methods applicability to IT security 10
4.7 Assurance schemes 10
4.8 Quantifying assurance risk and mechanism strength 11
4.9 Assurance reduces security risk 11
4.10 Quantifying assurance 11
4.11 Assurance authority 11

5 Selecting security assurance 12
5.1 Assurance requirements specification 13
5.2 Economical aspects 13
5.3 Organisational aspects 14
5.4 Type of assurance 14
5.5 Technical aspects 15
5.6 Optimisation considerations 15

6 Framework 16
6.1 Assurance approach 16
6.2 Assurance methods 16
6.3 Life cycle aspects 17
6.4 Correctness versus effectiveness assurance 18
6.5 Categorisation of assurance methods 19
6.6 Composite assurance 20
6.7 Assurance rating 20