ISO/IEC 27013:2012-10 (E)

Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms, abbreviated terms and definitions 1

4.1 Understanding the International Standards 2
4.4 Similarities and differences 2

5 Approaches for integrated implementation 3
5.1 General 3
5.2 Considerations of scope 4
5.3 Pre-implementation scenarios 5
5.3.1 General 5
5.3.2 Neither standard is currently used as the basis for a management system 5
5.3.3 A management system exists which fulfils the requirement of one of the standards 6
5.3.4 Separate management systems exist which fulfil the requirements of each standard 6

6 Integrated implementation considerations 7
6.1 General 7
6.2 Potential challenges 7
6.2.1 The usage and meaning of asset 7
6.2.2 Design and transition of services 8
6.2.3 Risk assessment and management 8
6.2.4 Differences in risk acceptance levels 9
6.2.5 Incident and problem management 9
6.2.6 Change management 11
6.3 Potential gains 12
6.3.1 Use of the Plan-Do-Check-Act cycle 12
6.3.2 Service level management and reporting 12
6.3.3 Management commitment 12
6.3.4 Capacity management 13
6.3.5 Management of third party risk 13
6.3.6 Continuity and availability management 14
6.3.7 Supplier management 14
6.3.8 Configuration management 14
6.3.9 Release and deployment management 15
6.3.10 Budgeting and accounting 15

Bibliography 38

Figures Figure 3: Illustration of relationship between standards for incident management 10