ISO/IEC 27013:2021-11 (E)

Information security, cybersecurity and privacy protection - 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 Termsanddefinitions 1

4 Overview of ISO/IEC 27001 and ISO/IEC 20000-1 1
4.1 Understanding ISO/IEC 27001 and ISO/IEC 20000-1 1
4.2 ISO/IEC 27001 concepts 2
4.3 ISO/IEC 20000-1 concepts 2
4.4 Similarities and differences 2

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

6 Integrated implementation considerations 6
6.1 General 6
6.2 Potential challenges 7
6.2.1 Requirements and controls 7
6.2.2 Assets and configuration items 7
6.2.3 Service design and transition 8
6.2.4 Risk assessment and management 9
6.2.5 Risk and other parties 10
6.2.6 Incident management 10
6.2.7 Problem management 11
6.2.8 Gathering of evidence 12
6.2.9 Major incident management 12
6.2.10 Classification and escalation of incidents 12
6.2.11 Change management 13
6.3 Potential gains 13
6.3.1 Service level management and reporting 13
6.3.2 Management commitment and continual improvement 13
6.3.3 Capacity management 14
6.3.4 Management of third parties and related risk 14
6.3.5 Continuity and availability management 15
6.3.6 Release and deployment management 15

Annex A (informative) Correspondence between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10 17

Annex B (informative) Correspondence between the controls in ISO/IEC 27001:2013, Annex A, and the requirements in ISO/IEC 20000-1:2018, Clauses 4 to 10 19

Annex C (informative)ComparisonoftermsanddefinitionsbetweenISO/IEC27000:2018 and ISO/IEC 20000-1:2018 22

Bibliography 60