ISO/IEC 27003:2010-02 (E)

Information technology - Security techniques - Information security management system implementation guidance

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Structure of this International Standard 2
4.1 General structure of clauses 2
4.2 General structure of a clause 3
4.3 Diagrams 3

5 Obtaining management approval for initiating an ISMS project 5
5.1 Overview of obtaining management approval for initiating an ISMS project 5
5.2 Clarify the organization's priorities to develop an ISMS 7
5.3 Define the preliminary ISMS scope 9
5.4 Create the business case and the project plan for management approval 11

6 Defining ISMS scope, boundaries and ISMS policy 12
6.1 Overview of defining ISMS scope, boundaries and ISMS policy 12
6.2 Define organizational scope and boundaries 15
6.3 Define information communication technology (ICT) scope and boundaries 16
6.4 Define physical scope and boundaries 17
6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries 18
6.6 Develop the ISMS policy and obtain approval from management 19

7 Conducting information security requirements analysis 20
7.1 Overview of conducting information security requirements analysis 20
7.2 Define information security requirements for the ISMS process 22
7.3 Identify assets within the ISMS scope 23
7.4 Conduct an information security assessment 24

8 Conducting risk assessment and planning risk treatment 25
8.1 Overview of conducting risk assessment and planning risk treatment 25
8.2 Conduct risk assessment 27
8.3 Select the control objectives and controls 28
8.4 Obtain management authorization for implementing and operating an ISMS 29

9 Designing the ISMS 30
9.1 Overview of designing the ISMS 30
9.2 Design organizational information security 33
9.3 Design ICT and physical information security 38
9.4 Design ISMS specific information security 40
9.5 Produce the final ISMS project plan 44

Annex A (informative) Checklist description 45

Annex B (informative) Roles and responsibilities for Information Security 51

Annex C (informative) Information about Internal Auditing 55

Annex D (informative) Structure of policies 57

Annex E (informative) Monitoring and measuring 62

Bibliography 68