



ISO 27001:2013 Information Security Management System Implementation Guide

with Examples



© deGRANDSON Global (July
2018)



Usage note

The intent of this document is to help you recognize the activities related to establishing an ISMS. This document should not be considered as professional consulting for establishing or implementing an ISMS.

Use of this guide does not guarantee a successful implementation nor an implementation that is ready for certification. If you want to implement an ISMS, consider hiring a professional consultant who specializes in implementing ISO 27001 compliant ISMS.

Contents

Usage note	1
Overview of an ISMS.....	4
1 Purchase a copy of the ISO standards	6
2 Initiating the ISMS Project	7
2.1 Obtain management support (#1)	7
Example of Information Security Policy Statement:.....	7
2.2 Assemble ISMS Project Team (#2).....	9
2.3 Complete Gap Analysis (#3).....	9
2.4 Prepare ISMS Project Plan (#3 cont'd).....	10
3 The Information Security Context of the Organisation	12
3.1 Determine the Information Security Context of the Organisation (#4).....	12
3.2 Identify the applicable legal and regulatory requirements (#5).....	12
EU General Data Protection Regulations 2018 (GDPR)	13
Example of addition of applicable Legislation to Scope of ISMS Statement	13
3.3 Determine other interested parties' needs (#6).....	13
4 Define and establish an Information Security Management System	15
4.1 Define the Scope of the ISMS (#7)	15
Example of Scope of ISMS Statement	16
4.2 Prepare detailed Information Security Policies (#8).....	17
Example of Information Security Policy	18
4.3 Define Key Roles and Responsibilities (#9)	20
5 The Planning Phase	22
5.1 Define a method of Risk Assessment (#10).....	22
Example of CIA Value Table:.....	23
Example of Table of Contents for Risk Assessment Document	25



5.2 Create an inventory of information assets to protect (#11).....	26
Example of an Inventory of Information Assets	26
5.3 Risk Assessment (#12).....	27
5.3.1 Identify risks.....	27
Example of Risk Identification.....	28
5.3.2 Evaluate the risks.....	29
Example of simple Risk Assessment	30
5.4 Identify applicable objectives and controls.....	31
5.4.1 Develop Risk Treatment Plan (#14).....	34
Examples of Risk Treatment Plan:.....	34
Example of Risk Assessment Document with Assessment Information and SOA Included	37
5.4.2 Develop Statement of Applicability (#13)	31
Example of Statement of Applicability	32
5.4.3 Set up policy and procedures to control risks (#15)	38
5.5 Establish ISMS Objectives and plan to achieve them (#16 & 17).....	40
6 Operational Planning and Controls.....	42
6.1 Determine the operational planning and control needs (#15).....	42
6.2 Identify Monitoring and Measurement Needs (incl. Calibration) (#18).....	43
6.3 Establish Operational Controls and Monitoring (#20).....	44
7 Develop the mandatory and other Documentation required (#19)	45
7.1 The specific requirements for documented information... ..	46
7.2 Example listing of ISMS Policies and Procedures	47
7.3 The specific requirements for retained documents... ..	49
8 Determine and secure the required Resources (#21).....	50
9 Pre-launch Activities	51
9.1 Deliver Employee Awareness Training (#22).....	51
9.2 Establish Internal and External Communications (#23).....	52
9.3 Finalise & issue ISMS Documentation (#24).....	53
9.4 Complete Job-specific Training (#25)	54
Example of Employee Training Record incl. competency check:	55
10 Go Live! Implement policies, procedures and Information Security objectives plan (#26)	56
10.1 Deploy Policies	56
10.2 Implement Procedures.....	56
10.3 Control of nonconforming outputs	57
11. Establish IS Incident response processes (#27).....	58
12. Monitor the effectiveness of the ISMS implementation (#26)	59
12.1 Conduct periodic evaluation of performance and effectiveness of ISMS	59
12.2 Conduct periodic evaluation of fulfilment of compliance requirements.....	60



12.3 Periodic re-assessment of Risk Assessments (incl. after major breach or loss of data) (#28)	60
12.4 Periodic re-planning of Risk Treatment Plan and of Improvement Plans	60
12.5 Conduct periodic Internal Audits (#29)	61
12.6 Conduct periodic Management Reviews (#30)	62
13. Implement Continual Improvement (#31)	64
Example: of an Improvement Plan outline	64
14. Prepare for a Certification Audit	66
15 Ask for help	67
Appendix A: The Path to ISO 27001:2013 Certification – the 31 Steps	68
Appendix B Typical Documentation	69
Policies & Procedures	69
Records	69
Appendix C Some Sample Procedures and Records	71
Appendix D: Example of Management Review Record	89