

www.degrandson.co.uk

ISO 27001

IMPLEMENTATION HANDBOOK

FOR CERTIFICATION TO THE INFORMATION SECURITY
MANAGEMENT SYSTEM STANDARD



deGRANDSON
Global

Written by

Dr. John FitzGerald, Founder
and CEO of deGRANDSON Global



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	7
2 Initiating the ISMS Project	8
2.1 Obtain management support (#1)	8
Example of Information Security Policy Statement:.....	8
2.2 Assemble ISMS Project Team (#2).....	10
2.3 Complete Gap Analysis (#3)	10
2.4 Prepare ISMS Project Plan (#3 cont'd).....	11
3 The Information Security Context of the Organisation	13
3.1 Determine the Information Security Context of the Organisation (#4).....	13
3.2 Identify the applicable legal and regulatory requirements (#5).....	13
EU General Data Protection Regulations 2021 (GDPR)	14
Example of addition of applicable Legislation to Scope of ISMS Statement	14
3.3 Determine other interested parties' needs (#6).....	14
4 Define and establish an Information Security Management System	16
4.1 Define the Scope of the ISMS (#7)	16
Example of Scope of ISMS Statement	17
4.2 Prepare detailed Information Security Policies (#8).....	18
Example of Information Security Policy	19
4.3 Define Key Roles and Responsibilities (#9)	21
5 The Planning Phase	23
5.1 Define a method of Risk Assessment (#10).....	23
Example of CIA Value Table:.....	24
Example of Table of Contents for Risk Assessment Document	26
5.2 Create an inventory of Information Assets to protect (#11).....	27
Example of an Inventory of Information Assets	27



5.3 Conduct Risk Assessment (#12).....	28
5.3.1 Identify risks.....	28
Example of Risk Identification.....	29
5.3.2 Evaluate the risks.....	30
Example of simple Risk Assessment	31
5.4 Identify applicable objectives and controls.....	32
5.4.1 Develop Statement of Applicability (#13).....	32
Example of Statement of Applicability	33
5.4.2 Develop a Risk Treatment Plan (#14)	35
Examples of Risk Treatment Plan:.....	35
Example of Risk Assessment Document with Assessment Information and SOA Included.....	38
5.4.3 Set up policy and procedures to control risks (#15)	39
5.5 Establish ISMS Objectives and plan to achieve them (#16 & 20).....	41
6 Operational Planning and Controls.....	43
6.1 Determine the operational planning and control needs (#20).....	43
6.2 Identify Monitoring and Measurement Needs (incl. Calibration) (#21)	44
6.3 Establish Operational Controls and Monitoring (#20 cont'd)	45
7 Develop the mandatory and other Documentation required (#19).....	46
7.1 The specific requirements for documented information.....	47
7.2 Example listing of ISMS Policies and Procedures	48
7.3 The specific requirements for retained documents... ..	50
8 Determine and secure the required Resources (#21).....	51
9 Pre-launch Activities	52
9.1 Deliver Employee Awareness Training (#22).....	52
9.2 Establish Internal and External Communications (#23).....	53
9.3 Finalise & issue ISMS Documentation (#24).....	54
9.4 Complete Job-specific Training (#25)	55
Example of Employee Training Record incl. competency check:.....	56
10 Go Live! Implement policies, procedures and Information Security objectives plan (#26)	57
10.1 Deploy Policies	57
10.2 Implement the Risk Treatment Plan and other Procedures (#27).....	57
10.3 Control of nonconforming outputs.....	58
11. Establish IS Incident response processes	59
12. Monitor the effectiveness of the ISMS implementation (#28)	60
12.1 Conduct periodic evaluation of performance and effectiveness of ISMS	60
12.2 Conduct periodic evaluation of fulfilment of compliance requirements.....	61
12.3 Periodic re-assessment of Risk Assessments (incl. after major breach or loss of data).....	61
12.4 Periodic re-planning of Risk Treatment Plan and of Improvement Plans	61
12.5 Conduct periodic Internal Audits (#29)	62



12.6 Conduct periodic Management Reviews (#30)	63
13. Implement Continual Improvement (#31).....	65
Example: of an Improvement Plan outline	65
14. Prepare for a Certification Audit.....	67
15 Ask for help	68
Appendix A: The Path to ISO 27001:2022 Certification – the 31 Steps.....	69
Appendix B: Typical Documentation.....	70
Policies & Procedures	70
Records.....	70
Appendix C: Some Sample Procedures, Records and Tools.....	72
Appendix D: Example of Management Review Record	90