

No. 134

CYBERSECURITY

ISO 27001

Building and certifying an information security management system

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 134

ISO 27001

Building and certifying an information security management system

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

ISO 27001

Building and certifying an information security management system

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. ISO and IEC are trademarks of their respective organizations; this book is not affiliated with or endorsed by ISO or IEC. Product names are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What ISO 27001 is 5
2 Why certify 6
3 The family of standards 7
4 The 2022 edition 8
5 The management system idea 9
6 How the standard is structured 10
7 Scope 11
8 Leadership 12
9 ISMS roles 13

PART II · BUILDING THE ISMS

10 Context and interested parties 15
11 Risk assessment 16
12 Risk treatment 17
13 Statement of Applicability 18
14 Tracking implementation 19
15 Objectives 20
16 Support 21
17 Documentation 22
18 Annex A 23
19 The four themes in practice 24
20 New controls in 2022 25

PART III · CHECKING AND IMPROVING

21 Operation 27
22 Monitoring and measurement 28
23 Internal audit 29

FREE SAMPLE · ojayo.com

24 Management review 30
25 Improvement 31
26 Certification audits 32
27 The certification cycle 33
28 Preparing for the audit 34
29 Choosing a certification body 35

PART IV · PRACTICE

30 For small organizations 37
31 Related standards 38
32 Mapping to NIST CSF 2.0 39
33 Tools 40
34 Timelines and costs 41
35 Common mistakes 42
36 A worked example 43
37 Careers 44
38 A learning path 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

ISO/IEC 27001 is the international standard for an **information security management system** (ISMS): a structured way to manage the security of an organization's information through risk assessment, controls, measurement and continual improvement. Organizations can be independently certified against it, and many customers require certification from their suppliers.

This beginner's book explains the 2022 edition of ISO/IEC 27001 in plain language: its clauses, its 93 Annex A controls, risk assessment and treatment, the Statement of Applicability, documentation, internal audit, management review and the certification process. It describes the standard in its own words; buy the official standard from ISO or your national standards body for the exact requirements.

What this book covers

- What an ISMS is and why ISO/IEC 27001 matters.
- Clauses 4 to 10 and the 2024 amendment.
- Risk assessment, treatment and the Statement of Applicability.
- Annex A themes and the controls new in 2022.
- Documentation, audits, management review and certification.
- Links to NIST CSF 2.0, cloud, privacy and AI standards.

Who this book is for

- **Security, IT and compliance staff** building an ISMS.

FREE SAMPLE · ojayo.com

- **Managers** preparing for certification.
- **Students** learning governance, risk and compliance.

How the book is organized

- **Part I — Foundations** (Chapters 1–9): what ISO 27001 is, why certify, the family of standards, the 2022 edition and amendment, the management system idea, structure, scope, leadership and ISMS roles.
- **Part II — Building the ISMS** (Chapters 10–20): context, risk assessment, risk treatment, the Statement of Applicability, objectives, support, documentation, Annex A, its four themes and new controls.
- **Part III — Checking and improving** (Chapters 21–29): operation, monitoring, internal audit, management review, improvement, certification audits, the three-year cycle, audit preparation and choosing a certification body.
- **Part IV — Practice** (Chapters 30–38): small organizations, related standards, mapping to NIST CSF, tools, timelines, mistakes, a worked example, careers and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in real certification projects.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Screens are **simplified illustrations**, not real product screens.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what ISO 27001 is, why organizations adopt it and how the standard is structured.

FREE SAMPLE · ojayo.com

CHAPTER 1

What ISO 27001 is

ISO 27001 defines how to manage information security.

A definition

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS. It is published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Management, not just technology

The standard is about **managing** risk: leadership, roles, risk decisions, controls, measurement and improvement. Technology is one part of that.

KEY IDEA

ISO 27001 is a management system for information security risk, not a list of products.

FREE SAMPLE · ojayo.com

CHAPTER 2

Why certify

Certification builds trust.

- **Customer trust**: many contracts and tenders require certification.
- **Structure**: a proven way to organize security work.
- **Risk focus**: controls chosen for real risks.
- **Continual improvement**: regular audits and reviews.
- **International recognition**: understood worldwide.

FREE SAMPLE · ojayo.com

CHAPTER 3

The family of standards

ISO 27001 has many relatives.

Standard	Purpose
ISO/IEC 27001	ISMS requirements; certifiable
ISO/IEC 27002	guidance on the controls
ISO/IEC 27005	information security risk management
ISO/IEC 27017 and 27018	cloud security and cloud privacy
ISO/IEC 27701	privacy information management
ISO/IEC 42001	AI management system

Figure 3.1 The ISO/IEC 27000 family and relatives

Only 27001 is certifiable

ISO/IEC 27002 gives guidance on implementing controls, but organizations are certified against 27001.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001 (you are reading this)
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

ISO 27001

Enjoyed it? The full book has 53 pages and 38 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.