

No. 134

CYBERSECURITY

ISO 27001

Building and certifying an information security management system

oJAYo.com

oJAYo

OJAYO SERIES · NO. 134

ISO 27001

Building and certifying an information security management system

oJAYo
Published by oJAYo.com

FREE SAMPLE · Get the full book at 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 · Get the full book at 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 · Get the full book at 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 · Get the full book at 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 · Get the full book at ojayo.com

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

How the book is organized

- **Part I: Foundations** (Chapters 1 to 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 to 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 to 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 to 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 · Get the full book at ojayo.com

A note on screens

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

FREE SAMPLE · Get the full book at ojayo.com

PART I

Foundations

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

FREE SAMPLE · Get the full book at 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 · Get the full book at 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 · Get the full book at ojayo.com