Management system standards

ISO/IEC 27001:2022 — Requirements

Two days to understand what ISO/IEC 27001:2022 requires and to prepare the certification of an information security management system. Scope, risk assessment and treatment, statement of applicability, the 93 Annex A controls, incidents and continuity: each topic is applied to your assets, your providers and your procedures. You leave with a first statement of applicability and the list of your priority gaps.

Duration : 2 days

Objectives

1. Explain the structure of ISO/IEC 27001:2022 and the place of Annex A in the approach
2. Define the scope of the system from the context, interested parties and interfaces with providers
3. Apply a method for assessing and treating information security risks
4. Build a justified statement of applicability from the 93 Annex A controls
5. Prepare incident management, continuity, the internal audit and the management review

Programme

Day 1 — morning

• Confidentiality, integrity, availability: what an ISO/IEC 27001 certificate shows your customers

• The ISO/IEC 27000 family: respective roles of 27001, 27002 and 27005

• Context, interested parties, legal and contractual requirements, including Law No. 09-08 on personal data

• Scope: sites, activities, information systems, providers

Day 1 — afternoon

• Leadership, information security policy, roles and responsibilities

• Risk assessment: criteria, identification, analysis, evaluation

• Treatment options, treatment plan and acceptance of residual risks by risk owners

• Exercise: risk assessment of one of your company's processes

Day 2 — morning

• Annex A: 93 controls grouped in four themes: organisational, people, physical and technological

• Statement of applicability: controls selected, justified exclusions, implementation status

• Controls often examined in audits: access rights, backups, suppliers and cloud services, logging

• Security incident management and information security during a disruption

Day 2 — afternoon (workshop)

• Monitoring, measurement, internal audit and management review of the system

• Nonconformities and corrective actions

• Workshop: draft of your statement of applicability and list of priority gaps

• Knowledge test and presentation of the work

Teaching methods

• Guided reading of the requirements and of Annex A
• Exercises on your assets, your data flows and your IT provider contracts
• Guided construction of a statement of applicability
• Case study of a security incident, from detection to corrective action
• Mid-course quiz and final test on the requirements of the system

Assessment and documents

Mid-course quiz and knowledge test at the end of the session, post-course evaluation at D+1. Numbered training certificate, verifiable online, for each participant; training report, draft statement of applicability and list of gaps handed to the company.

Bilingual materials for every participant; each classroom course comes with its digital twin on OmniLearn.

Good to know

To go deeper into the risk assessment method, the course “ISO/IEC 27005:2022 — Information Security Risks” (2 days) complements this one. Personal data protection and Law 09-08 are covered in “ISO/IEC 27701:2025 and Law 09-08”.

Practical information

Duration	2 days
Group size	Groups of 6 to 12 participants, in-company
Format	In-company, face to face on your site
Language	French, Darija or English; bilingual materials
Funding	OFPPT special training contracts (TFP), GIAC, Maroc PME: we prepare the applications with you, at no extra cost.
Programme customisation	Programme adapted to your procedures, your equipment and your audience

Frequently asked questions

Do I need to be an IT specialist to attend?
No. The requirements of the standard concern the organisation first: scope, risks, roles, suppliers, incidents. Technical controls are explained without jargon; having the IT manager or the information security officer present helps tie them to your infrastructure.

Must the statement of applicability select all 93 controls?
No. For each Annex A control it states whether it is selected or excluded, and why. These choices follow from the risk assessment and treatment; the certification auditor checks that they are consistent.

What is the link with Law 09-08?
Law No. 09-08 governs the processing of personal data. ISO/IEC 27001:2022 requires you to identify the applicable legal requirements and take them into account: the law belongs in the context and in risk treatment, but certification does not equal legal compliance.

Can a site already certified to ISO 9001 build on its system?
Yes. The two standards share the harmonised structure: document control, internal audit, management review and corrective actions can be common. The work specific to ISO/IEC 27001 concerns information security risks and the Annex A controls.