Management system standards

ISO/IEC 27005:2022 — Information Security Risks

Two days to carry out the information security risk assessment and treatment required by ISO/IEC 27001:2022, following the recommendations of ISO/IEC 27005:2022. Event-based or asset-based approach, scenarios, criteria, treatment plan, acceptance of residual risks: the method is applied to your information systems and your providers, all the way to a usable risk register.

Duration : 2 days

Objectives

1. Explain the role of ISO/IEC 27005:2022 in relation to the requirements of ISO/IEC 27001:2022
2. Define the context, risk acceptance criteria and risk assessment criteria
3. Identify risk scenarios using an event-based or an asset-based approach
4. Analyse and evaluate risks, then build a treatment plan linked to the Annex A controls
5. Organise the monitoring, review and communication of risks over time

Programme

Day 1 — morning

• Why a method: what ISO/IEC 27001:2022 requires on risk assessment and treatment
• Vocabulary: risk source, threat, vulnerability, event, consequence, likelihood
• Context, risk acceptance criteria and assessment criteria
• Risk owners and the role of management

Day 1 — afternoon

• Event-based and asset-based approaches: when to choose one or the other
• Assets, threats and vulnerabilities; building risk scenarios
• Analysis: consequences, likelihood, level of risk
• Exercise: risk scenarios on a scope of your company (email, ERP, customer data)

Day 2 — morning

• Evaluation and prioritisation of risks
• Treatment options: reduce, avoid, share, retain
• Treatment plan linked to the Annex A controls and to the statement of applicability
• Acceptance of residual risks and reporting to management

Day 2 — afternoon (workshop)

• Monitoring and review of risks: indicators, triggers for updating
• Communication and consultation on risks
• Workshop: risk register and treatment plan for your scope
• Knowledge test and presentation of the register

Teaching methods

• Exercises on your information systems, your data flows and your IT subcontracting contracts
• Comparison of the two approaches on the same scope
• Template risk register and treatment plan, adaptable to your tool
• Case study: risk linked to a cloud service provider
• Mid-course quiz and final test on the method

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, risk register and treatment plan from the workshop handed to the company.

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

Good to know

This course assumes knowledge of the requirements of ISO/IEC 27001:2022: the course “ISO/IEC 27001:2022 — Requirements” (2 days) presents them. The general risk management method is covered in “ISO 31000:2018 — Risk Management”.

Practical information

Duration	2 days
Audience	Information security officers, IT managers, risk managers, compliance managers, internal auditors of the information security system
Prerequisites	Basic knowledge of ISO/IEC 27001:2022
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

Can ISO/IEC 27005 be certified?

No. ISO/IEC 27005:2022 provides recommendations. It helps to meet the risk requirements of ISO/IEC 27001:2022, which are the ones audited at certification.

Do we need risk management software?

No. A well-structured spreadsheet is enough to start. The course provides a template; choosing a tool comes later, depending on the size of the scope and the number of risk owners.

How does it differ from ISO 31000:2018?

ISO 31000:2018 gives general risk management guidelines. ISO/IEC 27005:2022 applies them to information security: assets, threats, vulnerabilities, scenarios and the link with the Annex A controls of ISO/IEC 27001:2022.

Who should attend?

The information security officer, the IT manager, risk managers and business process owners. Risk owners must understand the method so that they can accept residual risks knowingly.