ISO/IEC 27001:2022 Foundation

7 – 11 December 2026
Barcelona (Spain)



ISO/IEC 27001:2022 Foundation

Ref: 3255054_199166 **Date:** 7 – 11 December 2026 **Location:** Barcelona (Spain) **Fees:** 5900 GBP

Introduction

In an era where cybersecurity threats are rapidly evolving and growing more sophisticated, information security has become a top strategic priority for organizations across all industries. Both individuals and businesses are exposed to various risks, including data breaches, cyberattacks, and information loss, all of which can seriously damage an organization's reputation and business continuity.

This course provides a comprehensive and practical introduction to the ISO/IEC 27001:2022 standard — the globally recognized framework for establishing, implementing, and maintaining an effective Information Security Management System ISMS. The standard offers organizations a systematic approach to risk assessment, implementation of security controls, and continuous improvement of information security practices.

Throughout this course, participants will explore essential principles of information security governance, gain insight into the structure and clauses of the standard, and learn how to design, implement, and monitor an effective ISMS. Practical topics such as documentation, internal audits, and preparation for certification are emphasized. Ultimately, the course supports organizations in achieving compliance, protecting critical information assets, and building trust with customers and stakeholders.

Course Objectives

By the end of this course, participants will be able to:

- Understand the purpose and benefits of the ISO/IEC 27001:2022 standard.
- Identify the structure and core requirements of the standard.
- Recognize key principles of information security management.
- Apply risk assessment and treatment processes effectively.
- Gain practical knowledge in documentation, internal audits, and certification procedures.

Course Outlines

Day 1: Introduction to Information Security and ISO/IEC 27001:2022

- Overview of information security and the evolving cyber threat landscape.
- Objectives and benefits of ISO/IEC 27001 for organizations.
- Evolution of the standard from 2013 to 2022 update.
- Structure of the ISO/IEC 27001:2022 based on Annex SL.
- Key terminology and definitions in cybersecurity and ISMS.



Day 2: ISMS Concepts and Organizational Context

- Introduction to the Information Security Management System ISMS.
- Clause 4 - Understanding the context of the organization.
- Clause 5 - The role of leadership and commitment in information security.
- Clause 6 - Planning based on risk-based thinking.
- Stakeholder identification and defining the ISMS scope.

Day 3: Risk Management and Operational Planning

- Clause 6.1 - Risk assessment and treatment in ISMS.
- Defining risk criteria and setting risk acceptance levels.
- Clause 7 - Support: resources, competencies, communication, and awareness.
- Clause 8 - Operational control, including outsourcing and third parties.
- Introduction to the Statement of Applicability SoA.

Day 4: Performance Evaluation and Improvement

- Clause 9 - Monitoring, measurement, analysis, and performance evaluation.
- Internal audit processes and planning.
- Conducting management reviews for ISMS effectiveness.
- Clause 10 - Managing nonconformities and corrective actions.
- Ensuring continuous improvement of the ISMS.

Day 5: Annex A Controls and Certification Overview

- Overview of the 93 Annex A controls, categorized into 4 major themes.
- Understanding control objectives, control selection, and implementation.
- Requirements for ISMS documentation and policy development.
- ISO/IEC 27001 certification process: stages, certifying bodies, and readiness assessment.
- Final course recap, Q&A, and assessment if applicable.

Why Attend This Course: Wins & Losses!

- In-depth understanding of the ISO/IEC 27001:2022 standard.
- Practical skills in risk assessment, control implementation, and audit preparation.
- Readiness to support certification processes and external audits.
- Strengthened ability to manage information security governance across an organization.
- Immediate applicability of knowledge in enhancing cyber resilience and regulatory compliance.

Conclusion

By the end of this training, participants will possess a solid, actionable understanding of the ISO/IEC 27001:2022 standard — not only in theory but also through a practical lens that enables them to drive tangible improvements in information security within their organizations.



They will be equipped to assess organizational contexts, identify and mitigate security risks, and develop robust policies and controls in line with global best practices. This course also provides the tools and knowledge necessary to support organizations in certification efforts, strengthening risk management, and ensuring ongoing compliance with international standards.

Ultimately, this course represents a critical step toward building a secure, stable, and resilient business environment in today's complex and ever-changing digital landscape.

