Implement and manage an ISO 27001:2013 Project

Seminar of 3 days - 21h
Ref.: ASE - Price 2024: €2 890 (excl. taxes)

EDUCATIONAL OBJECTIVES

At the end of the training, the trainee will be able to:

Explain the components of an information security management system (ISMS) in accordance with ISO 27001.

Explain the content and correlation between ISO 27001 and 27002 as well as with other standards and regulatory frameworks

Adapt the requirements of the ISO 27001 standard to an organization's specific context.

Preparing for ISO 27001 Lead Implementer and Lead Auditor certification.

THE PROGRAMME

last updated: 01/2018

1) » Introduction

- Refreshers ISO 27000 and ISO Guide 73 terminology.
- Definitions: Threat, vulnerability, protection.
- The notion of risk (potential, impact, severity).
- CIAA classification (Confidentiality, Integrity, Availability, Auditability).
- Risk management (prevention, protection, reporting, outsourcing).
- Analyzing events. Trends. Issues.
- SOX, PCI-DSS, and COBIT regulations. For whom? Why? Interaction with the ISO.
- Towards IT governance, links with ITIL® and ISO 20000.
- What ISO adds for regulatory frameworks.
- The alignment of COBIT, ITIL®, and ISO 27002.

2) » ISO 2700x standards

- History of security standards seen by the ISO.
- The BS 7799 standards, what they added to the ISO.
- The current standards (ISO 27001, 27002).
- The complementary standards (ISO 27005, 27004, 27003, etc.).
- Convergence with the 9001 quality and 14001 environment standards.
- What quality experts add to security.

3) » The ISO 27001:2013 standard

- Definition of an Information System Security Management System (ISMS).
- Objectives for your ISMS to achieve.
- The "continual improvement" approach as a founding principle, the PDCA model (Deming cycle).
- The ISO 27001 standard integrated into a QMS quality approach.
- Details of the Plan-Do-Check-Act phases.
- From specifying the ISMS scope to the SoA (Statement of Applicability).
- The recommendations of ISO 27001 for risk management.
- On the importance of risk assessment. Choosing an ISO 27005:2011 method.
- What the EBIOS and MEHARI methods add to your assessment approach.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

- Adopting efficient technical and organizational security measures.
- Mandatory ISMS internal audits. Building a program.
- ISMS improvement. Setting up corrective and preventive actions.
- Corrective and preventive action measures and counter-measures.
- Annex A of the ISO 27002 standard.

4) » Best practices, ISO 27002:2013

- Security goals: Availability, Integrity, and Confidentiality.
- Structure in domains/chapters (level 1), control objectives (level 2), and control (level 3).
- The new ISO 27002:2013 best practices, the measures deleted from ISO 27001:2005. Changes.
- The ISO 27002:2013 standard: The 14 domains and 113 best practices.
- Examples for applying the standard to your company: Key essential security measures.

5) » Implementing security in an ISMS project

- From security specifications to security acceptance.
- How to follow the ISSP and the requirements of the client/project owner?
- From risk analysis to building the Statement of Applicability.
- The ISO 27003 and 15408 standards as an aid to implementation.
- Integrating security measures into specific developments.
- The rules to follow for outsourcing.
- Ensuring that the project is monitored in its implementation and then operation.
- "Security" meetings before acceptance.
- Incorporating the PDCA cycle into the project's life cycle.
- Project acceptance; How to test it: Intrusion test and/or technical audit?
- Preparing the indicators. Continual improvement.
- Putting in place a scorecard. Examples.
- What the ISO 27004 standard adds.
- Vulnerability management in an ISMS: Regular scans, patch management, etc.

6) » ISO 19011:2011 security audits

- Continuous and complete process. Steps, priorities.
- Audit categories: Organizational, technical, etc.
- Internal, external, and third-party auditing, choosing your auditor.
- The ISO process for an audit, the key steps.
- Audit objectives, audit quality.
- Approach for improving an audit.
- Auditor qualities, their assessment.
- Organizational audits: Approach, methods.
- Compared benefits, human involvement.

7) » Legal best practices

- Intellectual property of software, contractual and tort liability.
- Criminal liability, responsibilities of executives, delegation of power, sanctions. The LCEN law.
- ISO compliance and legal compliance: The new domain 18 of the ISO 27002:2013 standard.

8) » ISO certification of IS security - The auditor-audited relationship

- Benefit of this approach, seeking the "label".
- Criteria for choosing the scope. Field of application. Involvement of stakeholders.
- The ISO: Essential supplement to regulatory and standard frameworks (SOX, ITIL®, etc.).
- Expected economic issues.
- Certifying organizations, choices in France and Europe.
- Audit approach, steps, and workloads.
- ISO 27006 standard, obligations for certifiers.

- Recurring and non-recurring costs of certification.

DATES

REMOTE CLASS
2025 : 25 Mar, 03 Jun, 23 Sep, 09 Dec