



ISO/IEC 27001 Information Security Lead Auditor Course (5-day Classroom Training)

This 5-day intensive course enables participants to develop the expertise needed to audit an Information Security Management System (ISMS) and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques.

During this training, the participant will acquire the skills and knowledge needed to proficiently plan and perform audits compliant with the certification process of the ISO/IEC 27001:2013 standard. Based on practical exercises, the participant will develop the abilities (mastering audit techniques) and skills (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary to the efficient conducting of an audit.

Audience

- Auditor wanting to perform and lead an Information Security Management System (ISMS) audit
- Project manager or consultant wanting to master the Information Security Management System audit process
- Person responsible for the Information security or conformity in an organization
- Member of the information security team
- Expert advisor in information technology
- Technical expert wanting to prepare for an Information security audit function

Learning Objectives

At the end of this course, the participant will gain competencies in:

- Acquiring the expertise to perform an ISMS audit as specified by ISO/IEC 27000:2005
- Acquiring the expertise necessary to manage an ISMS audit team
- Understanding the application of the information security management system in the ISO/IEC 27000:2005 context
- Understand the relationship between an Information Security Management System, including risk management and controls and compliance with the requirements of different stakeholders of the organization
- Improve the ability to analyze the internal and external environment of an organization, risk assessment and audit decision-making in the context of an ISMS



Case Study

Scenario driven learning is essential to mastering the content taught during the training. This training includes a real life case study and assignments to:

- Provide applicable situations and cases
- Present a real world connect using situations that can happen in the day to day life of participants
- Perform an audit of an ISMS with a team

Course Logistics

- Whiteboard, flipchart, and projector
- Participants — recommended maximum of 16, no minimum requirement

Prerequisites

- ISO 27001 Foundation Certification or basic knowledge of ISO 27001 is recommended
- Participants are required to purchase a copy of the ISO/IEC 27001:2013 Standard from www.iso.org
- Upon passing the Lead Auditor Exam, the candidate can get registered with PECB to become:
 - A Provisional Auditor – Required: No experience required
 - An Auditor – Required: 2 years of professional experience, 1 year of information security experience, audit activities totaling 200 hours
 - A Lead Auditor - Required: 5 years of professional experience, 2 years of information security experience, audit activities totaling 300 hours

For more information about these requirements, please visit either www.pecb.org or <https://www.pecb.org/en/certifications/iso-27001-and-information-security-certifications/iso-27001-lead-auditor>

Course Student Material

Participants receive:

- A copy of the classroom presentation material
- A study handbook containing information and practical examples



Exam

- The “Certified ISO/IEC 27001 Lead Auditor” exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competence domains:
 - ✓ Domain 1: Fundamental principles and concepts of information security
 - ✓ Domain 2: Information Security Management System (ISMS)
 - ✓ Domain 3: Fundamental audit concepts and principles
 - ✓ Domain 4: Preparation of an ISO 27001 audit
 - ✓ Domain 5: Conducting an ISO 27001 audit
 - ✓ Domain 6: Closing an ISO 27001 audit
 - ✓ Domain 7: Managing an ISO 27001 audit program
- The “Certified ISO/IEC 27001 Lead Auditor” exam is available in different languages (the complete list of languages can be found in the examination application form)
- The paper-based exam consists of 12 essay-type questions
- Open book: Participants may use all PECB provided documentation plus their own course notes, but will not be permitted to use any computer, laptop or any other electronic device.
- A minimum score of 70% is required to pass the exam
- The exam lasts 180 minutes

For more information about the exam, refer to PECB section on [ISO 27001 Lead Auditor Exam](#)

- After successfully completing the exam, participants can apply for the credentials of Certified ISO/IEC 27001 Provisional Auditor, Certified ISO/IEC 27001 Auditor or Certified ISO/IEC 27001 Lead Auditor depending on their level of experience. Those credentials are available for internal and external auditors
- A certificate will be issued to participants who successfully pass the exam and comply with all the other requirements related to the selected credential
- For more information about ISO 27001 certifications and PECB certification process, refer to PECB section on ISO 27001 Lead Auditor



Agenda

Day 1: Introduction to Information Security Management System (ISMS) concepts as required by ISO 27001
Normative, regulatory and legal framework related to information security
Fundamental principles of information security
ISO 27001 certification process
Information Security Management System (ISMS)
Detailed presentation of the clauses 4 to 8 of ISO27001
Day 2: Planning and Initiating an ISO 27001 audit
Fundamental audit concepts and principles
Audit approach based on evidence and on risk
Preparation of an ISO 27001 certification audit
ISMS documentation audit
Conducting an opening meeting
Day 3: Conducting an ISO 27001 audit
Communication during the audit
Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation
Audit test plans
Formulation of audit findings
Documentating nonconformities
Day 4: Concluding and ensuring the follow-up of an ISO 27001 audit
Audit documentation
Quality review
Conducting a closing meeting and conclusion of an ISO 27001 audit
Evaluation of corrective action plans
ISO 27001 Surveillance audit
Internal audit management program
Day 5: Certification Exam