Standards and Frameworks

ISO/IEC 27001:2013 ISMS Lead Auditor

How to plan, lead, conduct and report an audit of an ISMS for ISO 27001 compliance.

Duration: 5 Days

ISO27001 is the recognised international standard for best practice in information security management systems (ISMS) within any organisation.

This course will prepare you to plan and execute audits of information security management systems in line with the international standard ISO/IEC 27001.

Using the most recent version ISO 27001:2013, this training is based on management system audit guidelines (ISO 19011:2002) as well as international audit best practices: the International Federation of Accountants (IFAC), the American Institute of Certified Public Accountants (AICPA), the Information Systems Audit and Control Association (ISACA) and the Institute of Internal Auditor (IIA).

An audit kit developed by experienced auditors will be distributed to participants.

Who Should Attend

- Internal auditors
- Auditors wanting to perform and lead Information Security Management System (ISMS) certification audits
- Project managers or consultants wanting to master the Information Security Management System audit process
- Persons responsible for the Information security or conformity in an organisation
- Members of an information security team
- Expert advisors in information technology
- Technical experts wanting to prepare for an Information security audit function

Learning Outcomes

- Acquiring the expertise to perform an ISO 27001 internal audit as specified by ISO 19011
- Acquiring the expertise to perform an ISO 27001 certification audit as specified by ISO 19011, ISO 17021 and ISO 27006
- Acquiring the expertise necessary to manage an ISMS audit team
- Understanding the application of the information security management system in the context of ISO 27001
- Understand the relationship between an Information Security Management System, including risk management, controls and compliance with the requirements of different stakeholders of the organisation
- Improve the ability to analyse the internal and external environment of an organisation, risk assessment and audit decision-making in the context of an ISMS

Course Contents

Day 1: Introduction

- Normative and regulatory and legal framework related to information security
- Fundamental principles in Information Security
- ISO 27001 certification process
- Information Security Management System (ISMS)
- Detailed presentation of the clauses 4 to 8 of the ISO 27001 standard

Day 2: Launching an ISO 27001 audit

- Fundamental audit concepts and principles
- Audit approach based on evidence and on risk
- Preparation of an ISO 27001 certification audit
- Documenting of an ISMS 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
  - Drafting test plans
  - Formulation of audit findings
  - Drafting of nonconformity reports

Day 4: Closing an ISO 27001 audit

- Audit documentation
- Quality review
- Review of audit notes
- Conducting a closing meeting and conclusion of an ISO 27001 audit
- Evaluation of corrective action plans
- Surveillance audit
- Audit management program
- Completion of training

Day 5: Course review, exam prep, Certificate exam

alc

Get ahead of the game.
Get certified.

www.alctraining.com.my