

ISO/IEC 27001:2013 Information Security Management Systems (ISMS) Lead Auditor Training

Course Description Auditing is crucial to the success of any management system. As a result, it carries with it heavy responsibilities, tough challenges and complex problems. This five-day intensive course trains ISMS auditors to lead, plan, manage and implement an Audit Plan. It also empowers them to give practical help and information to those who are working towards certification and also provides the knowledge and skill required to carry out 2nd party auditing (suppliers and subcontractors).

Course Benefits Effective auditing helps to ensure that the measures you put in place to protect your organization and your customers are properly managed and achieve the desired result.

Course Structure A combination of tutorials, syndicate exercises and role play, including the following topics:

Explain the purpose and business benefits of:

- an ISMS;
- of ISMS standards;
- of management system audit;
- of third-party certification.
- Explain the role of an auditor to plan, conduct, report and follow up an Information Security MS audit in accordance with ISO 19011 (and ISO 17021 where appropriate).

Have the skills to:

- Plan;
- Conduct;
- Report;
- And follow up an audit of an ISMS to establish conformity (or otherwise) with ISO/IEC 27001/2, ISO 19011 (and ISO 17021 where appropriate).

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.

- Intended Audience**
- Those wishing to Lead audits of Information Security Management System (ISMS) in accordance with ISO 27001:2013 (either as a 2nd party, or 3rd party auditor)
 - Those wishing to learn about effective audit practices
 - Existing information security auditors who wish to expand their auditing skills
 - Consultants who wish to provide advice on ISO 27001:2013 ISMS Auditing
 - Security and quality professionals

Course Duration 5.0 Days

- Prerequisites** Delegates are expected to have the following prior knowledge:
- Management systems
 - Understand the Plan-Do-Check-Act (PDCA) cycle.
 - Information security management (Knowledge of the following information security management principles and concepts):
 - Awareness of the need for information security;
 - the assignment of responsibility for information security;
 - incorporating management commitment and the interests of stakeholders;
 - enhancing societal values;
 - using the results of risk assessments to determine appropriate controls to reach acceptable levels of risk;
 - incorporating security as an essential element of information networks and systems;
 - the active prevention and detection of information security incidents;
 - ensuring a comprehensive approach to information security management;
 - continual reassessment of information security and making of modifications as appropriate.

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.

ISO/IEC 27001

Knowledge of the requirements of ISO/IEC 27001 (with ISO/IEC 27002) and the commonly used information security management terms and definitions, as given in ISO/IEC 27000.

It is therefore recommended that delegates attend the BSI 'Requirements of ISO/IEC 27001' Training Course, prior to attending this course. It would also be beneficial to have been involved in, or preferably undertaken, ISMS Audits before attending this course.

Agenda

Day 1

Time	Topic
09.00	Course Introduction <ul style="list-style-type: none"> - Housekeeping - Course and learner objectives - Course structure and methods - Delegate assessment
	What is an Information Security Management System? <ul style="list-style-type: none"> - Information security - Management systems - Purpose and benefits of ISO 27001 - Related standards
	Process Approach <ul style="list-style-type: none"> - PDCA model - Process model
	Overview of ISO 27001 contents
	ISO 27001 Mandatory clauses 4 – 8
17:05	End of Day 1
	Homework

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.

Day 2

Time	Topic
09:00	Re-cap and Quiz
	Controls
	Overview of the audit process
	Auditing the SOA
	Audit and Auditors <ul style="list-style-type: none"> - Definitions - 1st, 2nd and 3rd party audits - Roles and responsibilities of auditors and lead auditors - Skills and characteristics of effective auditors
	Audit Planning <ul style="list-style-type: none"> - Information needed to plan the audit, and things to consider - Preliminary visits - Preparation of an audit plan
	Audit communications and meetings <ul style="list-style-type: none"> - Good practice for communication during the audit - Formal meetings - Opening meeting – what to cover and how
	Checklists <ul style="list-style-type: none"> - Benefits and drawbacks - Content – what to include - Developing a checklist for a specific audit
20:10	End of Day 2
20:45	Evening work

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.

Day 3

Time	Topic
09.00	Re-cap and Quiz
	Process Audits
	Case studies
	Conducting the audit <ul style="list-style-type: none"> - interviewing - sampling - note taking - interacting with the auditee - who's involved and general points
	Nonconformities <ul style="list-style-type: none"> - definition of nonconformity - linking to requirements of ISO 27001 - grading nonconformity reports - structure and content of nonconformity reports
17:50	End of Day 3
19:00	Evening Work

Day 4

Time	Topic
09.00	Re-cap and Quiz
	Case studies <ul style="list-style-type: none"> - including interviewing. - developing and following audit trails - identifying non conformities
	Specimen Examination <ul style="list-style-type: none"> - Review of answers - Layout and marking scheme of the papers
	Closing Meeting

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.

	<ul style="list-style-type: none"> - Outcomes - Content - Identifying possible issues and how to prevent or deal with these
	Corrective Actions <ul style="list-style-type: none"> - Corrective action process - Evaluating corrective actions
	Reporting the audit <ul style="list-style-type: none"> - Purpose and content of the written audit report
	Next steps <ul style="list-style-type: none"> - action planning - further development - auditor registration
20:05	End of Day 4

Day 5

Time	Topic
09.00	Course Evaluations Examination Rules
09:30	Written Examination

*IRCA Certified Course (A17287)

This course is certified by the International Register of Certificated Auditors (IRCA) and meets training requirements for those seeking registration as a lead auditor under their ISMS scheme.