BATALAS®
EST. 1962

CQI | IRCA
CERTIFIED COURSE

INFORMATION SECURITY

ISO/IEC 27001:2022 Lead Auditor Course ISMS

Delegates will learn the knowledge and skills required to conduct audits of an Information Security Management System (ISMS) against ISO/IEC 27001:2022, including how to plan, lead and report internal, supplier and third-party audits.

🕐 5 days **-** 08.45-18.15 (13.00 finish on last day)

📶 CQI and IRCA training level **-** Professional

▬ CQI and IRCA ref **-** PR373 (ATP number 2554)

Who should attend this course?

- Any new or existing auditors who want to learn how to conduct 1st party (internal), 2nd party (supplier) and 3rd party (external) audits of an information security management system (ISMS) that conforms to ISO/IEC 27001:2022.
- Anyone planning, managing or implementing an ISO/IEC 27001:2022 information security management system.
- Staff/managers who need to identify potential gaps in the effectiveness of an information security management system to help ensure the organisation remains compliant.
- This ISO 27001 Lead Auditor course satisfies the training requirement for anyone wishing to register as an Auditor with IRCA (International Register of Certified Auditors).

Prior knowledge requirements - anyone attending this ISO 27001 Lead Auditor training course must have prior knowledge of ISO/IEC 27001:2022. It is highly recommended that delegates attend our ISO 27001:2022 Foundation course beforehand to gain this knowledge (we offer a £50 discount when booking both courses together).

What will delegates learn on this course?

- The purpose of an Information Security Management System (ISMS)
- The audit process and types of audit
- Audit scope
- Criteria and objectives of an audit
- The role and responsibilities of an ISO 27001 Lead Auditor
- How to audit a risk assessment
- How to plan, prepare and manage an audit
- The opening and closing meetings
- Checklist development and document review
- Conducting and leading audit activities
- Reporting audit findings
- Following up on a previous audit
- Interviewing skills
- Skills for Team Leadership

ISO/IEC 27001:2022 supersedes previous editions ISO 27001:2013 and BS EN ISO/IEC 27001:2017; a summary of the key changes is provided with this course.

ISO/IEC 27001:2022 specifically requires that personnel are competent – this course provides essential skills and knowledge to help delegates become fully competent auditors.

What is the format of this course?

- The tutor combines informative lessons with individual and team-based exercises (approx. 25% theory and 75% practical).
- This interactive course uses a case study to help delegates develop auditing skills.

What is the course assessment?

- Assessment is based on a delegate's overall participation during the course, including their engagement in activities and case studies.
- 100% attendance is required on the course (a CQI and IRCA rule).
- After the course, delegates must complete a 1-hour 45-minute ISO 27001 Lead Auditor exam (an online e-assessment with multiple choice questions). This can be completed on any date or time convenient to each delegate, but it must be within 30 days of the course (a CQI and IRCA requirement). Batalas recommend taking the exam as soon as possible after the course to achieve the best results. A webcam, microphone and speakers are required for the e-assessment.

What certificate is provided?

- A CQI and IRCA certificate

What is included in the course fee?

- Pre-course work to help prepare for training (Training Toolkit)
- Delegate training manual
- Case Study documents
- Post-course notes
- A guide explaining the key changes between ISO 27001:2013 and ISO/IEC 27001:2022.
- CQI and IRCA certificate
- Lunch and refreshments (applicable when training at one of our venues)

This course has the following learning styles available:

In-house team training	Traditional Classroom	Scheduled public course	Live Virtual Classroom

Why choose Batalas?

Founded in 1962, we have over 60 years' experience providing specialist consultancy and training in ISO/AS Management Systems.