#  Certification Framework

|  |  |
| --- | --- |
| **Qualification title:** | ISO 27001:2022 Certified ISMS Lead Auditor |
| **Qualification identifier:** | CIS LA | **Language:** | EN |
| **Qualification level:** | Advanced | **CPD/CPE Points:** | 35 |
| **Links to other qualifications:** | Part of the ISO 27001 Pathway | **GLH:** | 2,100 mins |
| **Date of framework review:** | March 2024 | **Date of next review:** | March 2025 |

### Certification description

Lead Auditor certification is designed to equip candidates with the skills to conduct second-party (supplier) and third-party (external and certification) audits. This certification supports candidates in building their Lead Auditor career, leading a team of auditors and achieving compliance.

### Target audience

This Lead Auditor certification is ideal for anyone involved in, or responsible for auditing, such as:

• Business managers

• Compliance managers

• IT managers

• Quality managers

• Project managers

• Risk managers

• Operations managers

• Business Continuity managers

• Emergency Planners

• Information Security managers

• ISO 22301 or ISO 27001 lead auditors

• IT and other staff, including HR, legal and business users.

• Supply Chain and Procurement managers

### Prerequisites, entry requirements and restrictions

There are no formal entry requirements. This is a Lead Auditor certification, and it assumes that candidates have a basic knowledge of the relevant subject specific discipline module they intend to select, gained either through practical experience, reading the standard, or by achieving the ISO 27001 Certified ISMS Foundation or ISO 27001 Certified ISMS Lead Implementer certification. Sufficient Knowledge of the English language is mandatory.

### Knowledge aim

The aim of this certification is to verify the candidates understanding of the audit processes that are used by Certification Bodies to audit a Management System for conformance as well as their skills and knowledge to apply an audit procedure according to an ISO management system standard.

Delegates must be able to understand how to use Audits to monitor conformance of a MS and ISO MS Standard, with relevant laws, regulations and contracts, as well as consistent implementation and effective and continual improvement of the MS.

###

### Levels of knowledge and assessment

The required knowledge and knowledge outcomes detailed in this course have been designed using the cognitive domain of the 2001 revised Bloom’s Taxonomy. This represents knowledge in both low-level and high-level thinking classifications, detailed in the required knowledge table as cognitive levels or k-levels, which are:

Cognitive level 1 (k-level) – **Remember**

Cognitive level 2 (k-level) – **Understand**

Cognitive level 3 (k-level) – **Apply**

Cognitive level 4 (k-level) – **Analyse**

### Job and task description

Lead Auditor certification is designed to equip delegates with the skills to conduct second-party (supplier) and third-party (external and certification) audits. This certification supports applicants in building their Lead Auditor career, leading a team of auditors, and achieving compliance. Specifically, to lead an audit team of one or more people to conduct an audit of an Information Security Management System, either as a one-off activity or as part of an audit programme in accordance with good practice and the principles of auditing. Applicants must be able to understand how to use Audits to monitor conformance of a Management System and ISO MS Standard, with relevant laws, regulations, and contracts, as well as consistent implementation and effective and continual improvement of the Management System.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary task** | **Secondary task** |  | **Primary considerations** |
| **T1** | Managing an audit programme | T1.1 | Establish audit programme objectives | Roles and responsibilities for managing the audit programmeCompetence to manage the audit programmeEstablish the extent of the audit programmeDetermining the audit programme resources |
|  |  | T1.2 | Determine and evaluate audit programme risks and opportunities |
|  |  | T1.3 | Establish the audit programme |
|  |  | T1.4 | Implement that audit programme |
|  |  |  |  |  |
| **T2** | Conducting an audit | T2.1 | Initiating an audit | Establishing contact with auditeeDetermining feasibility of audit |
|  |  | T2.2 | Preparing audit activities | Performing review of documented informationAudit planningAssigning work to audit teamPreparing documented information for audit |
|  |  | T2.3 | Conduct audit activities | Assigning roles and responsibilities of guides and observersConducting opening meetingCommunicating during the auditAudit information and availability and accessReviewing documented information while conducting auditCollecting and verifying informationGenerating audit findingsDetermining audit conclusionsConducting closing meeting |
|  |  | T2.4 | Preparing and distributing the audit report | Preparing audit reportDistributing audit report |
|  |  | T2.5 | Completing the audit |  |
|  |  | T2.6 | Conducting audit follow-up |  |
|  |  |  |  |  |
| **T3** | Competence and evaluation of auditors | T3.1 | Competence and evaluation of auditors | Determining auditor competenceEstablishing auditor evaluation criteriaSelecting appropriate auditor evaluation methodsConducting auditor evaluationMaintaining and improving auditor competence |

### Required Knowledge

Presented with a range of options, candidates will be able to:

|  |  |  |
| --- | --- | --- |
| **Required Knowledge**  | **Cognitive Level** | **Link to job and task** |
| 1 | Explain the purpose and relevance of process-orientated auditing to auditing of ISO 19011 and ISO 17021. | 2 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 1.1 | Explain the purpose and principles of process-orientated auditing. | 2 | T1 |
| 1.2 | Explain the purpose and relevance to auditing of ISO 19011 and ISO 17021. | 2 | T1 |
| **Required Knowledge** | **Cognitive Level** | **Link toT1 job and task** |
| 2 | Explain how management systems standards such as ISO 27001 and ISO 22301 are used as audit criteria. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 2.1 | Explain how management systems standards such as ISO 27001 and ISO 22301 are used as audit criteria. | 3 | T1 |
| 2.2 | Explain how the audit process is used in first, second and third-party audits. | 3 | T1 |
| 2.3 | Explain how to establish and maintain an audit programme. | 3 | T1 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 3 | Plan, conduct, report and follow up an audit. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 3.1 | Plan, conduct, report and follow up an audit. | 4 | T2 |
| 3.2 | Select and lead an audit team. | 3 | T1.4 |
| 3.3 | Manage communications with the MS audit client. | 4 | T2.3 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 4 | Explain the specifics of applying the generic audit process to auditing an ISO MS for conformance with the ISO Annex SL aspects of a requirements standard. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 4.1 | Explain the specifics of applying the generic audit process to auditing an ISO MS for conformance with the ISO Annex SL aspects of a requirements standard. | 3 | T2.3 |
| 4.2 | Recall ISO Annex SL terms and definitions. | 1 | T2 |
| 4.3 | Plan, conduct, report and follow-up an audit of an ISO MS for conformance with ISO Annex SL. | 3 | T2 |
| 4.4 | Identify examples of evidence of conformity/nonconformity with ISO Annex SL | 2 | T2.3 |
| 4.5 | Apply observation and active listening skills in the context of a ISO MS ISO Annex SL audit. | 3 | T2.3 |
| 4.6 | Write nonconformities of intent, implementation and effectiveness against relevant clauses of ISO Annex SL. | 4 | T2.3, T2.4 |
| 4.7 | Identify inconsistencies in the ISO MS and write them as nonconformities against relevant clauses of ISO Annex SL | 3 | T2.3, T2.4 |
| 4.8 | Select and lead an ISO Annex SL MS audit team. | 3 | T1.4 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 5 | Understand and apply the principles of effective ISMS auditing. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 5.1 | Understand the audit process used by certification bodies. | 2 | T1 |
| 5.2 | Understand an overview of the structure and requirements of ISO 27001. | 2 | T1 |
| 5.3 | Use audits to monitor conformance. | 4 | T1 |
| 5.4 | Apply continual improvement of the ISMS. | 3 | T2.6 |
| 5.5 | Recognise the purpose and benefits of the audit. | 2 | T1 |
| 5.6 | Recognise the role of auditors and standards in audits. | 2 | T1 |
| 5.7 | Define common audit terms. | 1 | T2 |
| 5.8 | Understand and apply the principles of effective ISMS auditing. | 3 | T2 |
| 5.9 | Use the critical skills required for performing an ISMS audit. | 3 | T2.3 |
| 5.10 | Understand the importance of observing and listening in ISMS audits | 2 | T2.3 |
| 5.11 | Conduct an ISMS audit follow-up. | 4 | T2.6 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 6 | Establish, maintain and analyse an ISMS audit programme. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 6.1 | Understand the competence and evaluation of auditors. | 2 | T3.1 |
| 6.2 | Understand and use accredited certification audit specifics. | 3 | N/A |
| 6.3 | Select and lead an ISMS audit team. | 3 | T1.4 |
| 6.4 | Manage communications with the ISMS audit client. | 3 | T2.3 |
| 6.5 | Understand and apply how the audit process is used in first-, second- and third-party audits. | 3 | T1, T2 |
| 6.6 | Establish, maintain and analyse an ISMS audit programme. | 4 | T1 |
| 6.7 | Plan, conduct, report and follow up on an ISMS audit. | 3 | T2 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 7 | Use best-practice audit methodology based on ISO 19011. | 3 |  |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 7.1 | Use best-practice audit methodology based on ISO 19011. | 3 | T2 |
| 7.2 | Understand what the audit criteria are for lead-audit of an ISMS | 4 | T1.1 |
| 7.3 | Understand how to audit IS risk assessment. | 3 | T2.3 |
| 7.4 | Understand how to audit IS controls. | 3 | T2.3 |
| 7.5 | Apply observation skills in auditing an ISMS. | 3 | T2.3 |
| 7.6 | Understand how to audit against the clauses of the ISO 27001 standard. | 3 | T2.3 |

## Examination

### Grading System

The following weighting will apply in the examination:

|  |  |  |  |
| --- | --- | --- | --- |
| **Required Knowledge** | **%** | **Cognitive Level** | **Required Knowledge assessed** |
| Explain the purpose and relevance of process-orientated auditing to auditing of ISO 19011 and ISO 17021. | 5% | 2 | 1 |
| Explain how management systems standards such as ISO 27001 and ISO 22301 are used as audit criteria. | 7.5% | 3 | 2 |
| Plan, conduct, report and follow up an audit. | 7.5% | 3 | 3 |
| Explain the specifics of applying the generic audit process to auditing an ISO MS for conformance with the ISO Annex SL aspects of a requirements standard. | 22.5% | 3 | 4 |
| Understand and apply the principles of effective ISMS auditing. | 25% | 3 | 5 |
| Establish, maintain and analyse an ISMS audit programme. | 17.5% | 3 | 6 |
| Use best-practice audit methodology based on ISO 19011. | 15% | 3 | 7 |
|  | **100%** |  |

### Assessment Method

Candidates must undergo the following assessment to demonstrate meeting the required knowldge:

|  |  |
| --- | --- |
| **Assessment method:** | Online |
| **Assessment type:** | Multiple choice |
| **Duration:** | 90 minutes |
| **Pass mark required:** | 30/40 |
| **Pass percentage required:** | 75% |

### Granting of the certification

The certification is granted based on the examination results.

Suspension and withdrawal of certification occurs when the certification has been obtained in an unfair examination procedure using fraudulent examination practices by the participant and/or the proctor.

Reducing or expanding the scope of the certification is not intended.

### Recertification

To retain certification the candidate shall complete a recertification exam every three years. Recertification can currently be done by passing the 27001:2022 Transition exam. This 20-question exam highlights the changes from ISO 27001:2013 to ISO 27001:2022 and can be achieved by scoring a minimum of 75%.

The 60-minute recertification exam will have a minimum pass mark of 75% unless the scheme requirements have changed in the interim. The exam will consist of 20-questions that tests the required knowledge set out in the current certification framework. Recertification exams will be reviewed on a yearly basis meaning that candidates will not attempt the same exam twice over a three-year period.

Candidates can undertake a recertification examination any time from month 35-38. As detailed above, upon successful completion, a new certificate will be issued.

### Assessment Method

Candidates must undergo the following assessment to demonstrate meeting the required knowledge to achieve recertification:

|  |  |
| --- | --- |
| **Assessment method:** | Online |
| **Assessment type:** | Multiple choice |
| **Duration:** | 60 minutes |
| **Pass mark required:** | 15/20 |
| **Pass percentage required:** | 75% |

­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_