## Certification Framework

|  |  |
| --- | --- |
| **Qualification title:** | ISO 27001 CIS Lead Implementer |
| **Course identifier:** | CIS LI | **Language:** | EN |
| **Course level:** | Advanced | **CPD/CPE Points:** | 21 |
| **Links to other qualifications:** | Part of the ISO 27001 Pathway | **GLH:** | 1,260 mins |
| **Date of framework review:** | March 2024 | **Date of next review:** | March 2025 |

### Certification description

The Certified ISO 27001 ISMS Lead Implementer certification provides comprehensive and practical coverage of all aspects of implementing ISO 27001 and leads to the IBITGQ ISO 27001 Certified ISMS Lead Implementer (CIS LI) qualification.

### Target audience

This certification is aimed at anyone involved in information security management, writing information security policies or implementing ISO 27001, either as a lead implementer or as part of an implementation team. This includes:

• Business managers;

• IT or information security managers;

• Quality, risk or compliance managers;

• Project managers;

• Lead auditors;

• IT staff; and

• Other relevant staff, such as HR or legal.

### Prerequisites, entry requirements and restrictions

There are no formal entry requirements. However, it is assumed that candidates will have basic knowledge of ISO 27001 gained through practical experience, reading the Standard, or by achieving the ISO 27001 Certified ISMS Foundation (CIS F) qualification.

### Knowledge aim

The aim of this certification is to provide attendees with an understanding of how to implement an ISMS compliant to ISO 27001.

### 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 learning objectives and learning outcomes 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 descriptions

The ISO 27001 Certified ISMS Lead Implementer certification provides comprehensive and practical coverage of all aspects of implementing ISO 27001 for real and leads to the IBITGQ ISO 27001 Lead Implementer Certificate. Specifically, to lead a project to implement a sustainable Information Security Management System capable of achieving accredited certification to ISO 27001.

|  |
| --- |
| **Primary tasks** |
| **T1** | Establish an ISMS project mandate |
| **T2** | Initiate the ISMS project |
| **T3** | Initiate the ISMS |
| **T4** | Establish the management framework |
| **T5** | Determine the baseline security criteria |
| **T6** | Develop and implement an information security risk management methodology |
| **T7** | Implement the ISMS |
| **T8** | Develop and implement arrangements for measurement, monitoring and review of the ISMS |
| **T9** | Prepare for and facilitate ISMS audits |

### Required Knowledge

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

|  |  |  |
| --- | --- | --- |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 1 | Recall and explain the definition of ISO 27001 terms and phrases. | 2 | T2 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 1.1 | Define ISO 27001 terms and phrases. | 1 | T2 |
| 1.2 | Explain the meaning of ISO 27001 terms and phrases. | 2 | T2 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 2 | Understand and apply the fundamental ISO 27001 information/concepts and | 3 | T2 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 2.1 | Understand how the ISO 27001 standard applies to organisations, and be able to implement it. | 3 | T2 |
| 2.2 | Explain and apply the elements of ISMS implementation, and explain how ISO 27001’s requirements map to the PDCA cycle. | 3 | T2 |
| 2.3 | Explain the six ISMS implementation steps involved in planning and how to apply them. | 3 | T2 |
| 2.4 | Explain and understand how to apply likelihood and impact in relation to information security risk management. | 3 | T2 |
| 2.5 | Understand Annex A: Information security controls reference. | 2 | T2 |
| 2.6 | Explain the relationship between ISO 27001 and ISO 27002. | 3 | T2 |
| 2.7 | Understand the importance of change management and document control to preserve data integrity. | 2 | T2 |
| 2.8 | Recognise the ISMS road map – project initiation elements. | 1 | T2 |
| 2.9 | Recognise the ISMS road map – risk management elements. | 1 | T2 |
| 2.10 | Recognise the ISMS road map – implementation and check elements. | 1 | T2 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 3 | Demonstrate what is needed to gain the required level of management commitment. | 3 | T1 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 3.1 | Give examples of why information security is important in today’s business. | 2 | T1 |
| 3.2 | Recognise and understand the growing number of reasons for an ISMS in corporate governance and data protection terms. | 2 | T1 |
| 3.3 | Explain what happens when there is a breach of data protection regulations. | 2 | T1 |
| 3.4 | Explain the reasons ISO 27001 can be the solution, i.e. the benefits of ISO 27001. | 2 | T1 |
| 3.5 | Understand some of the elements to consider when selling information security and ISO 27001 to senior management. | 3 | T1 |
| 3.6 | Explain the importance of gaining implementation support (for a compliance requirement) at the chief executive and/or board level. | 3 | T1 |
| 3.7 | Explain the ways that management can provide evidence of its commitment to the implementation and management of the ISMS programme and apply those methods. | 3 | T1 |
| 3.8 | Recall some of the elements of management commitment. | 1 | T1 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 4 | Remember various attributes of Information Security Standards. | 2 | T2 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 4.1 | Explain other related information security standards. | 2 | T2 |
| 4.2 | Recognise some of the developments that have led to the current ISO 27001 standard. | 1 | T2 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 5 | Analyse how to identify, explain and manage the scope definition for an ISMS. | 4 | T4 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 5.1 | Understand and be able to define the boundaries of an ISMS. | 3 | T4 |
| 5.2 | Apply a unified approach across the scope of the ISMS. | 3 | T4 |
| 5.3 | Analyse how to divide large, complex organisations into manageable ISMS scopes.  | 4 | T4 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 6 | Recall, recognise and apply the various aspects of ISMS policies and documentation. | 3 | T3 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 6.1 | Recall and explain the definitions of terms critical to an ISMS. | 2 | T3 |
| 6.2 | Recognise the documents required by ISO 27001. | 1 | T3 |
| 6.3 | Recall and explain the definitions of ‘procedure’, ‘process’ and ‘record’. | 2 | T3 |
| 6.4 | Understand stakeholders, managers, and auditors in relation to documentation. | 2 | T3 |
| 6.5 | Understand a diagrammatical representation and attributes of a process and be able to apply the process attributes. | 3 | T3 |
| 6.6 | Explain and apply the attributes of proper documentation design. | 3 | T3 |
| 6.7 | Understand the different levels (and associated attributes) of documentation in a management system. | 2 | T3 |
| 6.8 | Explain and apply the requirements of ISO 27001 regarding document management. | 3 | T3 |
| 6.9 | Explain the five stages of document management. | 2 | T3 |
| 6.10 | Understand and apply roles and responsibilities when drafting a management system document (the RACI matrix). | 3 | T3 |
| 6.11 | Recall the major elements when drafting management system documentation. | 1 | T3 |
| 6.12 | Recognise and apply the format of management system documentation. | 3 | T3 |
| 6.13 | Explain and apply information security policy basics. | 3 | T3 |
| 6.14 | Identify and apply corporate information security policy requirements. | 3 | T3 |
| 6.15 | Recognise attributes of information-security-focused policies. | 1 | T3 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 7 | Understand and apply the attributes of ISMS projects, and address concerns | 3 | T1 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 7.1 | Explain and apply the ISMS project road map in relation to PDCA (diagrammatically and otherwise). | 3 | T1 |
| 7.2 | Summarise the requirements and concerns of the ISO 27001/ISMS project plan. | 2 | T1 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 8 | Recall the requirements for ISMS project initiation. | 1 | T2 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 8.1 | Remember the requirements for ISMS project initiation. | 1 | T2 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 9 | Explain and analyse the elements of ISO 27001 risk assessments. | 3 | T5, T6 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 9.1 | Recall and explain risk management terminology. | 2 | T5, T6 |
| 9.2 | Understand the elements of risk analysis and management. | 2 | T5, T6 |
| 9.3 | Apply the preassessment requirements of risk assessment. | 3 | T5, T6 |
| 9.4 | Remember and apply the basic steps of risk assessment. | 3 | T5, T6 |
| 9.5 | Understand and apply regulatory and legislative requirements in an ISMS. | 3 | T5, T6 |
| 9.6 | Explain asset inventory and management concepts. | 2 | T5, T6 |
| 9.7 | Recall and explain asset documentation requirements. | 2 | T5, T6 |
| 9.8 | Recall and implement the different types of asset categories. | 3 | T5, T6 |
| 9.9 | Understand and implement the elements of asset management. | 3 | T5, T6 |
| 9.10 | Explain and communicate the negatives if CIA are compromised. | 4 | T5, T6 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 10 | Recognise and explain the elements of ISO 27001 risk treatment |  | T6 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 10.1 | Explain and apply the risk management process. | 3 | T6 |
| 10.2 | Explain and apply risk treatment. | 3 | T6 |
| 10.3 | Recognise ISO 27001 Annex A: list themes and controls. | 1 | T6 |
| 10.4 | Recall and understand the different types of controls. | 2 | T6 |
| 10.5 | Explain the countermeasures available to the three main business elements (people, processes and technology). | 2 | T6 |
| 10.6 | Recall and apply the process for selecting controls. | 3 | T6 |
| 10.7 | Explain and implement ISMS baseline controls. | 3 | T6 |
| 10.8 | Understand the factors that influence the effectiveness of risk assessment. | 2 | T6 |
| 10.9 | Recognise and explain various risk assessment approaches.  | 2 | T6 |
| 10.10 | Analyse and summarise the advantages/disadvantages of ‘broad brush’ and ‘detailed’ approaches to risk assessment. | 4 | T6 |
| 10.11 | Recognise and explain the advantages of risk assessment software. | 2 | T6 |
| 10.12 | Explain the role of risk assessment tools. | 2 | T6 |
| 10.13 | Understand and create a Statement of Applicability (SoA). | 3 | T6 |
| 10.14 | Recognise and apply SMART attributes to measurement. | 2 | T6 |
| 10.15 | Recognise the considerations when measuring the effectiveness of controls. | 1 | T6 |
| 10.16 | Recall the components of measurements. | 1 | T6 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 11 | Understand and apply support elements within the implementation section. | 3 | T4 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 11.1 | Understand the typical concerns of stakeholders for the implementation of ISMS. | 2 | T4 |
| 11.2 | Explain and analyse key elements of ISMS communication and awareness. | 3 | T4 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 12 | Understand how to implement ISMS controls and understand the relationship between the different control themes and controls. | 3 | T7 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 12.1 | Understand how to implement the organisational controls. | 3 | T7 |
| 12.2 | Understand how to implement the people controls. | 3 | T7 |
| 12.3 | Understand how to implement the physical controls. | 3 | T7 |
| 12.4 | Understand how to implement the technological controls. | 3 | T7 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 13 | Recognise and explain the elements within monitor and review of the ISMS. | 3 | T8 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 13.1 | Recognise and explain the common failings in policy deployment. | 2 | T8 |
| 13.2 | Explain and apply the steps for effective policy deployment. | 3 | T8 |
| 13.3 | Recognise and understand how to test policy understanding and acceptance. | 2 | T8 |
| 13.4 | Recall and summarise the benefits of creating reports on policy deployment. | 3 | T8 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 14 | Understand and apply the elements of an internal audit. | 2 | T8 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 14.1 | Apply the attributes of an internal audit. | 3 | T8 |
| 14.2 | Understand the elements for conducting an internal audit. | 2 | T8 |
| 14.3 | Understand the tasks to perform after the internal audit. | 2 | T8 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 15 | Explain and apply the various aspects of continual improvement. | 3 | T8 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 15.1 | Remember terms relating to continual improvement. | 1 | T8 |
| 15.2 | Explain and apply the elements of corrective action and follow-up. | 3 | T8 |
| 15.3 | Understand and implement the improvement process. | 3 | T8 |
| 15.4 | Explain improvement actions. | 2 | T8 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 16 | Recognise and explain the importance of the certification audit. | 2 | T9 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 16.1 | Explain the accredited certification process. | 2 | T9 |
| 16.2 | Recall the elements of ISO 27001 certification. | 3 | T9 |
| 16.3 | Recognise what is required for certification. | 3 | T9 |
| 16.4 | Explain the benefits of certification. | 2 | T9 |
| 16.5 | Understand the elements of documentation assessment. | 2 | T9 |
| 16.6 | Understand the elements of conformity assessment. | 2 | T9 |
| 16.7 | Recall the objectives of an audit. | 1 | T9 |
| 16.8 | Explain the most common problems at audits. | 2 | T9 |
| **Required Knowledge** | **Cognitive Level** | **Link to job and task** |
| 17 | Recognise and explain the importance of a management review. | 3 | T8 |
| **Knowledge Outcomes** | **Cognitive Level** | **Link to job and task** |
| 17.1 | Recall possible management check activities. | 1 | T8 |
| 17.2 | Understand and apply the critical success factors for information security. | 3 | T8 |
| 17.3 | Explain the common failures of management reviews and apply relevant countermeasures. | 3 | T8 |

## Examination

### Grading System

The following weighting will apply in the examination:

|  |  |  |  |
| --- | --- | --- | --- |
| **Required Knowledge** | **%** | **Cognitive Level** | **Required Knowledge assessed** |
| Recall and explain the definition of ISO 27001 terms and phrases. | 5.0% | 2 | 1 |
| Understand and apply the fundamental ISO 27001 information/concepts and elements. | 5.0% | 3 | 2 |
| Demonstrate what is needed to gain the required level of management commitment. | 7.5% | 3 | 3 |
| Remember various attributes of information security standards. | 2.5% | 2 | 4 |
| Analyse how to identify, explain and manage the scope definition for an ISMS. | 2.5% | 4 | 5 |
| Recall, recognise and apply the various aspects of ISMS policies and documentation. | 7.5% | 3 | 6 |
| Understand and apply the attributes and concerns of ISMS projects. | 5.0% | 3 | 7 |
| Recall the requirements for ISMS project initiation. | 5.0% | 1 | 8 |
| Explain and analyse the elements of ISO 27001 risk assessments.  | 10.0% | 3 | 9 |
| Recognise and explain the elements of ISO 27001 risk treatment. | 5.0% | 3 | 10 |
| Understand and apply support elements within the implementation section. | 10.0% | 3 | 11 |
| Understand how to implement ISMS controls and understand the relationship between the different control themes and controls. | 12.5% | 3 | 12 |
| Recognise and explain key elements of monitoring and reviewing the ISMS. | 2.5% | 3 | 13 |
| Understand and apply the elements of an internal audit. | 5.0% | 2 | 14 |
| Explain and apply the various aspects of continual improvement. | 5.0% | 3 | 15 |
| Recognise and explain the importance of the certification audit. | 5.0% | 2 | 16 |
| Recognise and explain the importance of a management review. | 5.0% | 3 | 17 |
|  | **100%** |  |

### Assessment Method

Candidates must undergo the following assessment to demonstrate meeting the learning objectives:

|  |  |
| --- | --- |
| **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 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% |