Certification Framework

Certification Details

Certification Title:	ISO 27001 Certified ISMS Lead Implementer Certification		
Unique Certification Identifier:	CIS_LI	**Language:**	EN
Certification Level:	ADVANCED		
Links to other qualifications:	Part of the ISO 27001 Pathway		
Date of certification Review:	June 2021	**Planned date of next review:**	June 2022

Job and task description

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 faciltiate ISMS audits
T10	Manage and complete post-certification audit actions

Typical applicants

This certification is suitable for 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 and other staff, including HR, legal and business users.

Prerequisites, Entry Requirements & Restrictions

There are no formal entry requirements. However, it is assumed that delegates will have a basic knowledge of ISO 27001 gained through practical experience, reading the standard, or by achieving the ISO 27001 Certified ISMS Foundation certification.

Framework

Scope of Certification

The aim of this certification is to verify the delegate's understanding of how to implement ISO 27001 and how to prepare for ISO 27001 audit certification within their current environment.

Levels of Knowledge and Assessment

The learning objectives and outcomes in this certification have been designed to develop both low-level and high-level thinking skills. The level of knowledge the candidate must attain to achieve each learning objective is indicated by 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

Learning Objectives and Outcomes

This qualification consists of a number of learning objectives and outcomes, which each delegate needs to be able to do in order to achieve certification.

Learning Objectives		**Cognitive Level**
LO1	***Recall and explain the definition of ISO 27001 terms and phrases.***	***2***
LO1.1	Define ISO 27001 terms and phrases.	1
LO1.2	Explain the meaning of ISO 27001 terms and phrases.	2
LO2	***Understand and apply the fundamental ISO 27001 information/concepts and elements.***	***3***
LO2.1	Understand how the ISO 27001 standard can be applied in organisations and be able to apply it.	3
LO2.2	Explain and apply the elements of ISMS Implementation and apply each element of the Information Security Standards: ISO/IEC 27001 ISMS and explain how its requirements map to the PDCA cycle.	3
LO2.3	Explain and apply the ISMS Implementation 6 steps in planning.	3
LO2.4	Explain and apply Risk Assessment/Management in relation to likelihood and impact.	3
LO2.5	Understand Annex A: Information Security Control Categories and give examples of how controls are structured.	2
LO2.6	Explain and incorporate the relationship between ISO 27001 and ISO 27002.	3
LO2.7	Understand the importance of date integrity in tracking changes in documents.	2
LO2.8	Recognise the ISMS Road Map – Project Initiation elements.	1
LO2.9	Recognise the ISMS Road Map – Risk Management elements.	1
LO2.10	Recognise the ISMS Road Map – Implementation and Check elements.	1

LO3	***Demonstrate what is required to gain the required level of management commitment.***	***3***
LO3.1	Give examples of why information security is important in today's business.	2
LO3.2	Recognise and understand the growing number of reasons for an ISMS in corporate governance and data protection terms.	2
LO3.3	Explain what happens when there is a breach of data protection reputations.	2
LO3.4	Give reasons why ISO 27001 can be the solution i.e. the benefits of ISO 27001 and be able to implement those solutions.	2
LO3.5	Apply some of the elements to consider when selling Information Security and the ISO 27001 standard to senior management.	3
LO3.6	Explain the importance of gaining implementation support (to a compliance requirement) at the Chief Executive and Board level.	3
LO3.7	Explain and apply the ways that management can provide evidence of its commitment to the implementation and management of the ISMS program.	3
LO3.8	Recall some of the elements of management commitment.	1
LO4	***Remember various attributes of Information Security Standards.***	***2***
LO4.1	Explain other related Information Security Standards.	2
LO4.2	Recognise some of the developments which have led to the current ISO 27001 standard.	1
LO4.3	Recognise what future Information Security Standards may be published.	1
LO5	***Analyse how to identify, explain and manage the scope definition for an ISMS.***	***4***
LO5.1	Apply the boundaries of ISMS.	3
LO5.2	Apply a unified approach across the scope involved.	3
LO5.3	Analyse how to divide large, complex organisations into manageable ISMS scopes.	4
LO6	***Recall, recognise and apply the various aspects of ISMS policies and documentation.***	***3***
LO6.1	Recall and explain the definition of ISMS.	2
LO6.2	Recognise the documents required by ISO 27001.	1
LO6.3	Recall and explain the definition of 'procedure, process, record'.	2
LO6.4	Understand stakeholders, managers and auditors in relation to documentation.	2
LO6.5	Understand a diagrammatical representation and attributes of a process and be able to apply the process attributes.	3
LO6.6	Explain and apply the attributes of proper documentation design.	3
LO6.7	Understand the different levels (and associated attributes) of documentation in a management system.	2
LO6.8	Explain and apply the requirements of ISO 27001 regarding document management.	3
LO6.9	Explain the five stages of document management.	2
LO6.10	Understand and apply the guidelines when drafting a management system document (The RACI matrix).	3
LO6.11	Recall the major elements when drafting MS documentation.	1
LO6.12	Recognise and apply the format of management system documentation.	3

LO6.13	Explain and apply information security policy basics.	3
LO6.14	Identify and apply corporate information security policy requirements.	3
LO6.15	Recognise attributes of information security focused policies.	1
LO7	***Understand and apply the attributes and concerns of ISMS projects.***	***3***
LO7.1	Explain and apply the ISMS project road map in relation to PDCA (diagrammatically and otherwise).	3
LO7.2	Summarise the attributes and concerns of the ISO 27001/ISMS project plan.	2
LO8	***Recall the requirements for ISMS project initiation.***	***1***
LO8.1	Remember the requirements for ISMS project initiation.	1
LO9	***Explain and analyse the elements of ISO 27001 risk assessments.***	***3***
LO9.1	Recall and explain risk management terminology.	2
LO9.2	Understand the elements of risk analysis and management.	2
LO9.3	Apply the pre-assessment requirements of risk assessment.	3
LO9.4	Remember and apply the basic steps of risk assessment.	3
LO9.5	Understand and apply the elements of handling regulatory and legislative requirements in an ISMS.	3
LO9.6	Explain asset inventory and management concepts.	2
LO9.6.1	Recall and explain asset documentation requirements.	2
LO9.6.2	Recall and implement the different types of asset categories in the organisation.	3
LO9.6.3	Understand and implement the elements of asset management.	3
LO9.6.4	Explain and communicate the negatives if CIA is compromised.	4
LO10	***Recognise and explain the elements of ISO 27001 risk treatment***	***3***
LO10.1	Explain and apply the risk management process.	3
LO10.2	Explain and apply risk treatment.	3
LO10.3	Recognise ISO 27001 Annex A: list of controls and control objectives.	1
LO10.4	Recall and understand the different types of controls.	2
LO10.5	Explain the countermeasures available to the three main business areas.	2
LO10.6	Recall and apply how controls are selected.	3
LO10.7	Explain and implement ISMS compulsory controls.	3
LO10.8	Understand the factors that influence the effectiveness of risk assessment.	2
LO10.9	Recognise and explain various risk assessment details.	2
LO10.10	Analyse and summarise the advantages/disadvantages of ‘broad brush’ and ‘detailed’ approach to risk assessment.	4
LO10.11	Recognise and explain the attributes of risk assessment software.	2
LO10.12	Explain the role of risk assessment tools.	2
LO10.13	Understand and create a Statement of Applicability (SoA).	3
LO10.14	Recognise and apply the attributes of measurement.	2
LO10.14.1	Recognise the concerns when measuring for effectiveness.	1

LO10.14.2	Recall the construction of measurements.	1
LO11	***Understand and apply support elements within the implementation section.***	***3***
LO11.1	Understand the concerns for the implementation of ISMS.	2
LO11.2	Explain and analyse the elements to consider within ISMS communication and awareness.	3
LO12	***Understand and apply the elements relating to the implementation of ISMS controls as well as understand the inter-relationship between the different control categories and controls***	***3***
LO12.1	***Organisation and Information Security (A6)*** Understand and apply the various elements within the Organisation and Information Security Controls section.	3
LO12.2	***Human Resources Security (A8)*** Understand the various elements within the Human Resources Security Controls section.	2
LO12.3	***Physical and Environmental Security (A9)*** Recognise and understand the various elements within the Physical and Environmental Security Controls section.	2
LO12.4	***Communications and Operations Management (A10)*** Recognise and understand the various elements within the Communications and Operations Management Controls section.	2
LO12.5	***Access Control Security (A11)*** Understand and apply the various elements within the Access Control Controls section.	3
LO12.6	***Information Systems Acquisition, Development and Maintenance (A12)*** Recognise and understand the various elements within the Information Systems Acquisition, Development and Maintenance Controls section.	2
LO12.7	***Information Security Incident Management (A13)*** Understand and apply the various elements within the Information Security Incident Management Controls section.	3
LO12.8	***Business Continuity Management (A14)*** Understand and apply the various elements within the Business Continuity Management Controls section.	3
LO12.9	***Compliance (A15)*** Recognise and understand the various elements within the Compliance Controls section.	2
LO13	***Recognise and explain the elements within monitor and review of the ISMS.***	***3***
LO13.1	Recognise and explain the common failings in policy deployment.	2
LO13.2	Explain and apply the steps for effective policy deployment.	3
LO13.3	Recognise and understand the elements in testing policy understanding and acceptance.	2
LO13.4	Recall and summarise the benefits of creating reports on policy deployment.	3
LO14	***Understand and apply the elements of an internal audit.***	***2***
LO14.1	Apply the attributes of an internal audit.	3

LO14.2	Understand the attributes of conducting an internal audit.	2
LO14.3	Recall the items in an internal audit report.	1
LO14.4	Understand the tasks to perform after the internal audit.	2
LO15	***Explain and apply the various aspects of continual improvement.***	***3***
LO15.1	Remember continual improvements terms.	1
LO15.2	Explain and apply the attributes of corrective action and follow up.	3
LO15.3	Understand and implement the steps in the improvement process.	3
LO15.4	Explain the improvement actions.	2
LO16	***Recognise and explain the importance of the certification audit.***	***2***
LO16.1	Explain the accreditation certification process.	2
LO16.2	Recall and apply the elements of ISO 27001 certification.	3
LO16.3	Recognise and apply what is required for certification.	3
LO16.4	Explain the benefits of certification.	2
LO16.5	Understand the elements of documentation assessment.	2
LO16.6	Understand the elements of conformity assessment.	2
LO16.7	Recall the objectives of an audit.	1
LO16.8	Explain the most common problems at audits.	2
LO17	***Recognise and explain the importance of a management review.***	***3***
LO17.1	Recall possible management check activities.	1
LO17.2	Understand and apply the critical success factors for information security.	3
LO17.3	Explain the common failures of management reviews and apply relevant countermeasures.	3

Examination

Grading System

The following weighting will apply in the examination:

LO1	***Recall and explain the definition of ISO 27001 terms and phrases.***	**5,0%**
LO2	***Understand and apply the fundamental ISO 27001 information/concepts and elements.***	**5,0%**
LO3	***Demonstrate what is required to gain the required level of management commitment.***	**7,5%**
LO4	***Remember various attributes of Information Security Standards.***	**2,5%**
LO5	***Analyse how to identify, explain and manage the scope definition for an ISMS.***	**2,5%**
LO6	***Recall, recognise and apply the various aspects of ISMS policies and documentation.***	**7,5%**
LO7	***Understand and apply the attributes and concerns of ISMS projects.***	**5,0%**
LO8	***Recall the requirements for ISMS project initiation.***	**5,0%**
LO9	***Explain and analyse the elements of ISO 27001 risk assessments.***	**10,0%**
LO10	***Recognise and explain the elements of ISO 27001 risk treatment***	**5,0%**
LO11	***Understand and apply support elements within the implementation section.***	**10,0%**
LO12	***Understand and apply the elements relating to the implementation of ISMS controls as well as understand the inter-relationship between the different control categories and controls***	**12,5%**
LO13	***Recognise and explain the elements within monitor and review of the ISMS.***	**2,5%**
LO14	***Understand and apply the elements of an internal audit.***	**5,0%**
LO15	***Explain and apply the various aspects of continual improvement.***	**5,0%**
LO16	***Recognise and explain the importance of the certification audit.***	**5,0%**
LO17	***Recognise and explain the importance of a management review.***	**5,0%**

Assessment method

Delegates must undergo the following assessment to demonstrate meeting the learning outcomes:

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

Examination Conditions

The candidates must be familiar with and agree to following conditions before starting the exam.

- The examination consists of multiple choice questions.
- The number of correct answers for every question is indicated.
- Each correctly answered question results in 1 point; 40 points can be achieved at maximum.
- A wrong answer is awarded 0 points.
- To pass 75% must be achieved to pass the examination.
- The duration of the examination is 90 minutes.
- Questions during the examination are not permitted and may not be answered.
- It is not allowed to use books, papers, mobile phones or other materials and devices, unless explicitly allowed by the proctor.
- The participants are not allowed to talk to each other during the examination.
- Taking notes is only allowed on the paper provided by the proctor. The notes must be submitted after finishing the exam.
- It is strictly forbidden to take screenshots or pictures of the examination questions.
- Copying or spreading of examination contents and questions is strictly forbidden.
- It is strictly forbidden to disclose any information about the examination questions to any third party.
- After finishing the examination, the result will be displayed automatically.
- Results will be communicated via email within one week of the examination.
- Participants are not permitted to use the toilet during the examination.
- The exam may be submitted before the end of the test.
- Participants must leave the test area after submission of the examination.
- Photo identification for verifying the identity (identity card, passport, driving licence) must be presented.
- Any breach of the exam conditions results in immediate termination of the exam. The exam results will be discarded. The participant will not be able to continue the exam. The exam fee will not be refunded.

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. Certified persons are required to adhere to the IBITGQ Code of Ethics. Any sanctions that are applied shall be reviewed and approved by the IBITGQ Scheme Committee in line with their terms of reference.

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. The recertification exam will be a subset of the original exam and consist of 20 questions with 30 minutes to complete. The exam pass mark will be the same as the original exam unless the scheme requirements have changed in the interim.

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

Should there be a change to regulatory requirements and/or normative documents on which the certification has been based resulting in a new certification scheme being put in place then recertification will not be offered.