Certification Framework

Scheme Details

Certification Title:	ISO 27001 Certified ISMS Lead Auditor		
Unique Certification Identifier:	CIS LA	**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

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 programme Competence to manage the audit programme Establish the extent of the audit programme Determining 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 auditee Determining feasibility of audit
		T2.2	Preparing audit activities	Performing review of documented information Audit planning Assigning work to audit team Preparing documented information for audit

		T2.3	Conduct audit activities	Assigning roles and responsibilities of guides and observers Conducting opening meeting Communicating during the audit Audit information and availability and access Reviewing documented information while conducting audit Collecting and verifying information Generating audit findings Determining audit conclusions Conducting closing meeting
		T2.4	Preparing and distributing the audit report	Preparing audit report Distributing 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 competence Establishing auditor evaluation criteria Selecting appropriate auditor evaluation methods Conducting auditor evaluation Maintaining and improving auditor competence

Typical applicants

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
- Supply Chain and Procurement 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.

This certification is aimed at people who want to achieve a globally recognised lead auditor qualification to further their careers, and at managers who are responsible for the implementation and maintenance their specific discipline.

Certification Framework

Prerequisites, Entry Requirements & Restrictions

There are no formal entry requirements. This is a Lead Auditor certification, and it assumes that delegates 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.

Scope of Certification

The aim of this certification is to verify the applicants 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.

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
LO01	Explain the purpose and principles of process-orientated auditing.	**2**
LO02	Explain the purpose and relevance to auditing of ISO 19011 and ISO 17021.	**2**
LO03	Explain how management systems standards such as ISO 27001 and ISO 22301 are used as audit criteria.	**3**
LO04	Explain how the audit process is used in 1st, 2nd and 3rd party audits.	**3**
LO05	Explain how to establish and maintain an audit programme.	**3**
LO06	Plan, conduct, report and follow up an audit.	**4**
LO07	Select and lead an audit team.	**3**
LO08	Manage communications with the MS audit client.	**4**
LO09	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**
LO10	Recall ISO Annex SL terms and definitions.	**1**
LO11	Plan, conduct, report and follow-up an audit of an ISO MS for conformance with ISO Annex SL.	**3**
LO12	Identify examples of evidence of conformity/nonconformity with ISO Annex SL	**2**
LO13	Apply observation and active listening skills in the context of a ISO MS ISO Annex SL audit.	**3**
LO14	Write nonconformities of intent, implementation and effectiveness against relevant clauses of ISO Annex SL.	**4**
LO15	Identify inconsistencies in the ISO MS and write them as nonconformities against relevant clauses of ISO Annex SL.	**3**
LO16	Select and lead an ISO Annex SL MS audit team.	**3**
LO17	Understand the audit process used by certification bodies.	**2**
LO18	Understand an overview of the structure and requirements of ISO 27001.	**2**
LO19	Use audits to monitor conformance.	**4**
LO20	Apply continual improvement of the ISMS.	**3**
LO21	Recognise the purpose and benefits of the audit.	**2**
LO22	Recognise the role of auditors and standards in audits.	**2**
LO23	Define common audit terms.	**1**
LO24	Understand and apply the principles of effective ISMS auditing.	**3**
LO25	Use the critical skills required for performing an ISMS audit.	**3**
LO26	Understand the importance of observing and listening in ISMS audits	**2**
LO27	Conduct an ISMS audit follow-up.	**4**
LO28	Understand the competence and evaluation of auditors.	**2**
LO29	Understand and use accredited certification audit specifics.	**3**
LO30	Select and lead an ISMS audit team.	**3**

LO31	Manage communications with the ISMS audit client.	**3**
LO32	Understand and apply how the audit process is used in first-, second- and third-party audits.	**3**
LO33	Establish, maintain and analyse an ISMS audit programme.	**4**
LO34	Plan, conduct, report and follow up on an ISMS audit.	**3**
LO35	Use best-practice audit methodology based on ISO 19011.	**3**
LO36	Understand what the audit criteria are for lead-audit of an ISMS	**4**
LO37	Understand how to audit IS risk assessment.	**3**
LO38	Understand how to audit IS controls.	**3**
LO39	Apply observation skills in auditing an ISMS .	**3**
LO40	Understand how to audit against the clauses of the ISO 27001 standard .	**3**

Examination

Grading System

The following weighting will apply in the examination:

	Learning Objectives	
LO01	Explain the purpose and principles of process-orientated auditing	2,5%
LO02	Explain the purpose and relevance to auditing of ISO 19011 and ISO 17021	2,5%
LO03	Explain how management systems standards such as ISO 27001 and ISO 22301 are used as audit criteria	2,5%
LO04	Explain how the audit process is used in 1st, 2nd and 3rd party audits	2,5%
LO05	Explain how to establish and maintain an audit programme	2,5%
LO06	Plan, conduct, report and follow up an audit	2,5%
LO07	Select and lead an audit team	2,5%
LO08	Manage communications with the MS audit client	2,5%
LO09	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	2,5%
LO10	Recall ISO Annex SL terms and definitions	2,5%
LO11	Plan, conduct, report and follow-up an audit of an ISO MS for conformance with ISO Annex SL	2,5%
LO12	Identify examples of evidence of conformity/nonconformity with ISO Annex SL	2,5%
LO13	Apply observation and active listening skills in the context of a ISO MS ISO Annex SL audit	2,5%
LO14	Write nonconformities of intent, implementation and effectiveness against relevant clauses of ISO Annex SL	2,5%
LO15	Identify inconsistencies in the ISO MS and write them as nonconformities against relevant clauses of ISO Annex SL	2,5%
LO16	Select and lead an ISO Annex SL MS audit team	2,5%
LO17	Understand the audit process used by certification bodies.	2,5%
LO18	Understand an overview of the structure and requirements of ISO 27001.	2,5%
LO19	Use audits to monitor conformance.	2,5%
LO20	Apply continual improvement of the ISMS.	2,5%
LO21	Recognise the purpose and benefits of the audit.	2,5%
LO22	Recognise the role of auditors and standards in audits.	2,5%
LO23	Define common audit terms.	2,5%
LO24	Understand and apply the principles of effective ISMS auditing.	2,5%
LO25	Use the critical skills required for performing an ISMS audit.	2,5%
LO26	Understand the importance of observing and listening in ISMS audits	2,5%
LO27	Conduct an ISMS audit follow-up.	2,5%
LO28	Understand the competence and evaluation of auditors.	2,5%
LO29	Understand and use accredited certification audit specifics.	2,5%

	Learning Objectives	
LO30	**Select and lead an ISMS audit team.**	**2,5%**
LO31	**Manage communications with the ISMS audit client.**	**2,5%**
LO32	**Understand and apply how the audit process is used in first-, second- and third-party audits.**	**2,5%**
LO33	**Establish, maintain and analyse an ISMS audit programme.**	**2,5%**
LO34	**Plan, conduct, report and follow up on an ISMS audit.**	**2,5%**
LO35	**Use best-practice audit methodology based on ISO 19011.**	**2,5%**
LO36	**Understand what the audit criteria are for lead-audit of an ISMS**	**2,5%**
LO37	**Understand how to audit IS risk assessment**	**2,5%**
LO38	**Understand how to audit IS controls**	**2,5%**
LO39	**Apply observation skills in auditing an ISMS**	**2,5%**
LO40	**Understand how to audit against the clauses of the ISO 27001 standard**	**2,5%**

Assessment method

Delegates 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%

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.