



QACS International

SC-ISMS

03/06-04-2022

Certification of person Scheme
As per Clause 8 of ISO 17024:2012
For Certification for Auditor/Lead Auditor for ISMS (ISO 27001:2013)

CI		
8.2a	Scope of certificate	Lead Auditor/auditor /provisional Auditor for Information Security MANAGEMENT SYSTEM ISO 27001:2013
8.2b	job and task description	<p>Information Security Management system certification required impartial audit of client organisation. Hence each certification body required trained auditor who have adequate knowledge of standard.</p> <p>Based on their competence within Information Security management systems, the certified ISMS EMS lead Auditors (Team leader) are able to initiate, plan, execute and prepare report of audits within management system in accordance with ISO 19011:2018</p> <p>The auditing may required a mixer of auditors of different experience, the team leader should be competent as lead auditor and other member either lead auditor or only auditor.</p> <p>In case of audit by one auditor, the person should have competency of lead Auditor.</p> <p>ISO 17021-1:2015 and ISO 27006:2015, define the competency required for Lead auditor/ Auditor.</p> <p>The auditor should also have knowledge of ISO 27001:2013 along with competency and knowledge defined in ISO 27006:2015.</p> <p>The objective of QACS is to evaluate knowledge of the properly trained person based on written examination which also include personal attribute test and certify then as per competency.</p> <p>ISMS Lead Auditors have the competence as management systems auditors and in addition are competent to lead an audit team of one or more additional auditors or technical experts.</p> <p>The lead auditors are able to initiate, plan, execute and report first, second and third party audits within Information security management in accordance with ISO 19011:2018 and ISO 17021-1:2015 in the role as sole auditor, member of an audit team or as audit team leader.</p>
8.2c	required competence	<p>For certification to FSMS lead auditor/Auditor will required competency as follows:</p> <ol style="list-style-type: none">1. Education (defined in 8.2e)2. Training : mandatory, Training should be as per IPC SC-11-02 by IPC-member bodies or QACS approved training



		<p>or any training as following:</p> <p>a. 5day 40 hours training for ISO 27001:2013, the training should be divided in two parts (3 days/24 hours for knowledge of standard and 2 days/16 hours for knowledge of auditing as per ISO 19011:2018)</p> <p>b. 3 days/24 hours training for standard if candidate has already taken full lead auditor training of 5 days for any other standard.</p> <p>3. Work experience :(Defined in 8.2e)</p> <p>4. Audit experience (For Auditor/ lead Auditor): defined in 8.2e</p>
8.2d	abilities (when applicable)	Ability to write and read documents in Local language/English.
8.2e	prerequisites (when applicable)	<p>Education: Applicant should have completed at least secondary education (typically all the years full time schooling prior to university entrance) Alternatively applicants may be considered for certification if they can document 10 years full time work experience and satisfy the QACS that they have achieved a satisfactory level of knowledge relevant to Management Systems auditing .</p> <p>Work Experience: Minimum Work experience of 5 Year for applicant having only secondary education. 4 year For applicant having post secondary education. 2 years for applicants completed graduation level. Out of this at least 2 years in the implementation, operation and/or auditing of management systems.</p> <p>Training: Mandatory, Training should be as per IPC SC-11-02 by IPC-member bodies or QACS approved training or any training as following:</p> <p>a. 5day 40 hours training for ISO 27001:2013, the training should be divided in two parts (3 days/24 hours for knowledge of standard and 2 days/16 hours for knowledge of auditing as per ISO 19011:2018)</p> <p>b. 3 days/24 hours training for standard if candidate has already taken full lead auditor training of 5 days for any other standard.</p> <p>Audit experience: (to be acquired in last three years) For provisional Auditor: candidates who fullfill all other prerequisite but do not have minimum audit experience required as auditor will be consider as Provisional Auditor.</p> <p>For Auditor: At least 20 man day audit days(Including onsite audit, preparation and Reporting) of which at least 8 man day should be spend onsite. Further should have attended at least 4 full audit as audit team member.</p>



		For Lead Auditor: At least 3 complete audits in which candidate should be responsible for entire audit process.
8.2f	code of conduct (when applicable)	The Person need to sign the code of conduct agreement with QACS. The code of conduct has been developed based on Clause 7 of ISO 17024:2012 and ISO 19011:2018
8.3 a	criteria for initial certification and recertification	Initial certification would be done based on information (education, training, skill & work experience) provided and after achieving pass marks in examination. The certificate is awarded for three years Surveillance : Yearly evaluation would be done based on the yearly achievement and enhanced work experience. which may result in up gradation from provisional auditor to auditor or auditor to lead auditor if candidate has already passed the required examinations. Recertification would be done between 2.5 years to 3.5 years beyond 3.5 years recertification is not possible. The candidate need to reappear for examination or when there is revision in the standard for which a person has been certified.
8.3 b	assessment methods for initial certification and recertification	Assessment method: Initial certification 1. Application along with documentary proof of basic information. 2. Signing of code of conduct agreement. 3. Review of application form for ability and prerequisite required for certification program. If case candidate do not full fill the ability and prerequisite for certification program the application is declined. 5 For eligible candidates exam is planned. 6. Examination: Examination will be held in two parts Part 1 -Written examination would be held having multiple choice answers. The examination shall have three section. The examination will have following type of Multiple choice question: to judge knowledge of standard, situation judgement, audit text analysis, personal attributes) a. Knowledge of ISO 19011:2018 and ISO 17021-1:2015 b. Knowledge of ISO 27001:2013, Competency as per ISO 27006:2015 c. For Lead auditor (extra examination). Part 2- Oral examination 7. Declaration of results. 8. Award of certificate. Note: Further evaluation of candidate based on technical clusters (EA Code or food subcategories) is not part of



		<p>this certification scheme.</p> <p>Recertification:</p> <ol style="list-style-type: none"> 1. Basic information. 2. Evidence of enhanced work experience. 3. Evidence of training for revised standard. 4. Written examination if there is change in relevant Standard. 5. Signing of code of conduct agreement.
8.3 c	surveillance methods and criteria (if applicable)	<p>Surveillance methods and criteria:</p> <p>Desk top/off line review of following documents and payment of annual fees.</p> <ol style="list-style-type: none"> 1. Basic information. 2. Evidence of enhanced work experience. 3. Signing of code of conduct agreement.
8.3 d	criteria for suspending and withdrawing certification	<p>Criteria for suspension:</p> <ol style="list-style-type: none"> 1. Complaint of serious nature from interested parties, (User of services- Auditing agencies/ client of Audit agencies). 2. Complaint of unethical conduct. <p>QACS will ask for explanation from the person, and failing to give response or improper response will result in suspension.</p> <p>Criteria for withdrawal:</p> <ol style="list-style-type: none"> 1. The QACS will form the investigation committee. 2. The investigation committee will collect the response as well as evidence from complainant and certified person. 3. If investigation committee will find the certified person guilty, will be given notice for withdrawal, and subsequently certificate would be withdrawn. <p>The certified person have right to appeal the decision of investigation committee.</p>
8.3 e	criteria for changing the scope or level of certification (if applicable)	<p>During annual review / renewal of registration of certified person. Enhanced information would be evaluated and based on work experience/complaint the grade would be improved or downgraded.</p> <p>To Improve grade to lead auditor candidate will have to pass</p>
8.4 a	the involvement of appropriate experts	<p>QACS has adequate technical expert of relevant management system having all stages of experience including consultancy and auditing for evaluation of certified person.</p>
8.4 b	the use of an appropriate structure that fairly represents the interests of all parties significantly concerned, without any interest predominating	<p>QACS is having one committee for maintaining impartiality which is represented by all interested parties like QACS, Training providers, Audit agencies and client of audit agencies.</p>
8.4 c	the identification and alignment of prerequisites, if applicable, with the	<p>Most of management system required minimum</p>



	competence requirements	education, training and work experience for allocation of grades to auditors.
8.4 d	the identification and alignment of the assessment mechanisms with the competence requirements	When any competency requirements have been changed. The certification Manager is responsible for preparing proposal for certification mechanism with revised competency requirement of such scheme. Certification manager will maintain a register which is revised with changes in competency requirement due to change in standard or IAF mandatory documents.
8.4 e	a job or practice analysis that is conducted and updated to	
	identify the tasks for successful performance	<ol style="list-style-type: none">1. Application2. Desk top review of submitted documents.3. Result of examination/personnel evaluation.4. Award of certificate.
	identify the required competence for each task	<ol style="list-style-type: none">1. Review of application and desk top review of documents. (reviewer should be lead auditor of relevant standard)2. Evaluation of Examination: Evaluator of examination should be lead auditor and approved to be competent as trainer for Information security Management standard.3. Award of certificate: committee having knowledge of relevant management systems, accreditation standards and IAF Mandatory documents.
	identify prerequisites (if applicable)	The Prerequisites have been defined in 8.2e and reviewed and confirmed in MRM.
	confirm the assessment mechanisms and examination content	Assessment shall be done in two parts: <ol style="list-style-type: none">1. Review of documents.2. Examination: Examination will be held in two parts Part 1-Written examination would be held having multiple choice answers. The examination shall have three sections. The examination will have following type of Multiple choice question: to judge knowledge of standard, situation judgement, audit text analysis, personal attributes)<ol style="list-style-type: none">a. Knowledge of ISO 19011:2018 and ISO 17021-1:2015b. Knowledge of ISO 27001:2013 and Competency as per ISO 27006:2015.c. For Lead auditor (extra examination). Part 2- Oral examination
	identify the recertification requirements and interval	The recertification would be required if and when there is revision in standard/ accreditation standard/ IAF MD for which person has been certified. He may be asked to take up further training and pass the examination.



QACS International

SC-ISMS

03/06-04-2022

8.5	The certification body shall ensure that the certification scheme is reviewed and validated on an on-going, systematic basis.	QACS conduct yearly management review, the chairman of impartiality committee would also be part of management review. One of the agenda point would be to review certification scheme based on revision in relevant standard/ feed back from Interested parties.
8.6	When the certification body is not the scheme owner of a certification scheme it implements, the certification body shall ensure that the requirements contained in this clause (Clause 8) are met	IPC is the owner of certification scheme, QACS is responsible for all requirement of ISO 17024:2012 and specific requirements of AB.

Scheme reviewed and approved in Programme (Scheme) committee meeting held on 06-04-2022

Approved on 06-04-2022