CERTIFICATION REQUIREMENTS OF MANAGEMENT SYSTEM

ANNEX F
ISO/IEC 27001:2022

ADDITIONAL INFORMATION/REQUIREMENTS FOR THE AUDIT

1. General.

During the certification process Q-CERT will verify that the system has been up and running for a sufficient time period and there is able evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective, and will be maintained covering the scope of certification.

2. Access to organizational records

When applying for ISMS certification the applicant shall report to Q-CERT (through the application or by any other means) if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information.

In such case, Q-CERT shall determine whether the ISMS can be adequately audited in the absence of such information.

If through the application review process Q-CERT's designee concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, Q-CERT shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

3. Effective Number of Personnel

In order to be able to correctly estimate the required audit duration when applying and / or when deemed necessary the applicant should provide information regarding the personnel involved in the certification scope such as:

- Total number of personnel within the certification scope (for the main facilities and for each additional site where applicable).
- Number of personnel out of the total that:
  - ✓ have read-only access to information to perform their duties;
  - ✓ have no access to the organization's information processing facilities in scope of the ISMS;
  - ✓ have specific demonstrable restricted access to the company's information processing facilities in scope of the ISMS;
  - ✓ perform activities where strict limitations are implemented to restrict disclosure of information, e.g. measures prohibiting personal belongings and devices into the work area.

4. Fully remote audit due to no physical location

In the case where no activity of the organization within the scope of the certification is undertaken at a defined physical location at all, this must be clearly communicated with Q-CERT through the application form.

In such cases the certification document(s) shall state that all activities of the organization are conducted remotely.

Note: This, together with the certification regulation, form part of the commitments that the customer signs that he accepts through the contract (F-2002) with the Certification Body.

ANNEX F
ISO/IEC 27001:2022

5. Scope of Certification

- Q-CERT during the audit shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.
- The version of the Statement of Applicability shall be included in the certification documents.

NOTE: A change to the Statement of Applicability which does not change the coverage of the controls in the scope of certification does not require an update of the certification documents.

6. Audit Duration and Audit Team for initial certification audit

Audit duration as well as the audit team may change based on the results of Stage I audit.

The process requires that Stage I audit report is presented to the customer and sent to Q-CERT's main office. Q-CERT (a person who has not been involved in the Stage I audit process) will evaluate the findings and will decide whether the audit team designated from the outset meets the requirements of the Organization's activity (covering the applicable points in Annex A of the standard) or should be redefined and if the calculated audit duration continues to be adequate for the purposes of the certification activities.

7. Stage I of the certification audit

For ISO 27001 standard, the results of Stage I as documented in the relevant form are evaluated by QMSCERT (by a person who has not been involved in the Stage I audit process). Based on the results of the review, it will be decided whether the audit team designated from the outset meets the requirements of the Organization's activity (covering the applicable points in Annex A of the standard) or should be redefined

8. Change of scope of certification

When a certified customer requests an extension or a change of the scope that they are certified for, should provide Q-CERT the following information:

a) the type of extension:

b) the activity/ activities of the current certification;

c) the number of locations where the activity/activities take(s) place;

d) the related information security risks related to the activity/activities;

e) the number of controls relevant to the extension;

f) the number of persons doing work under the organization's control of the new scope; and

g) the time required to review the integration of the extended scope into the ISMS.

Note: This, together with the certification regulation, form part of the commitments that the customer signs that he accepts through the contract (F-2002) with the Certification Body.

ANNEX F
ISO/IEC 27001:2022

Audit time shall be added to the calculated duration to review the client's ISMS. This additional time shall be at least:

1) 0,5 d (auditor days) if the extension to scope audit is conducted in conjunction with a surveillance audit or a recertification audit.
2) 1,0 d (auditor days) when the extension to scope audit is conducted as a separate audit.

Note: This, together with the certification regulation, form part of the commitments that the customer signs that he accepts through the contract (F-2002) with the Certification Body.