ADDITIONAL INFORMATION / REQUIREMENTS FOR AIMS
ANNEX H
ISO/IEC 42001:2023

1. General

Audit criteria for certification and subsequent audit activities include the requirements of ISO/IEC 42001 standard and any applicable regional and regulatory specificities covered by the AIMS.

Note: applicable regional and regulatory specificities refer to each and every region that the products / services are provided e.g. Europe, USA etc..

2. Organization's Role

The Organization must clearly define its context based on its role relative to the AI system. These roles include:

- ✓ AI producer – design, develop, test and deploy products or services that use one or more AI system
- ✓ AI provider – provide platforms, products or services that uses one or more AI systems
- ✓ AI user – only use AI products or services
- ✓ Any combination of the above

3. Number of personnel & audit duration

One of the factors for calculating audit duration is the effective number of personnel under the organization's control.

Effective No of personnel refers to those that are involved in the AI's life cycle. Depending on the role of the company these persons are:

- ✓ For producers / developers:

  Personnel relevant to the life cycle includes those involved in Inception – Design & Development – Verification & Validation – Deployment – Operation & Monitoring – Continuous Validation – Re-evaluation (e.g. personnel of financial and marketing departments are not taken into account)

- ✓ For providers:

  Personnel relevant to the life cycle includes those involved in installation, monitoring, and support of the services or the products (e.g. personnel of financial and marketing departments are not taken into account)

- ✓ For users:

  Personnel relevant to the life cycle includes only those that use the relevant application (product or service)

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.

4. Statement of Applicability (SOA) & Additional Control

Q-CERT during the audit shall ensure that the Organization's definition of the certification scope includes all significant processes and risks relevant to the AI system and is reflected in the statement of applicability (SoA). The SoA defines the scope of certification

The Statement of Applicability (SoA) must include:

- ✓ the number of AI systems used within the scope of certification,
- ✓ the controls from Annex A of the standard as well as justification for inclusion and exclusion of any of them
- ✓ any additional controls that are necessary beyond those in Annex A in order to implement all risk treatment options (where applicable).

5. Operational Controls

The Organization shall determine all controls that are necessary to implement the AI risk treatment options chosen and compare the controls with those in Annex A of the standard to verify that no necessary controls have been omitted.

Annex A lists reference controls while Annex B provides implementation guidance for them. Both Annexes are normative.

6. Remote activities (as part of the certification process)

In case that remote auditing methods such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the Organization's processes are utilized to interface with the organization, these activities may only be considered as partially contributing to the total "on-site" audit time.

In such cases, the audit report shall include clear indications that remote audit activities have been performed

7. Data Access

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

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.

In such case, Q-CERT shall determine whether the AIMS 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 AIMS without reviewing the identified confidential or sensitive information, Q-CERT shall advise the Organization that the certification audit cannot take place until appropriate access arrangements are granted.

8. Sharing facilities with other entities

During the onsite audit, Q-CERT's auditor(s) shall ensure that interfaces to services or activities that are not entirely within the AIMS scope of applicability are addressed in the AIMS undergoing certification and have been included in the risk assessment of the Organization's artificial intelligence management system. An example of such a situation is the sharing of facilities on which the AI system runs or is interconnected (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations)

9. Stage I audit (for initial certification)

Stage I audit results shall be documented in Q-CERT's relevant report and sent to the head office where the relevant personnel shall review the report before deciding on proceeding with Stage II. Q-CERT shall confirm that the Stage II audit team members have the necessary competence. This may be done by the auditor leading the team that conducted the Stage I audit if deemed competent and appropriate.

10. Additional surveillance audits

In addition to the usual surveillance cycle, Q-CERT, when deemed necessary shall reach an agreement with the Organization to regulate additional surveillance of the Organization's own monitoring activities, if the AIMS manages AI systems classified as high-risk or applied within sensitive purposes (e.g. health; safety critical; affecting personal rights; etc.). This can include additional audits or an agreement on the provision of parameters that can cause extraordinary surveillance measures by Q-CERT.

Parameters shall be set in a way that they indicate changes to certification-relevant criteria of the AI system monitored by the AIMS. In the event of a change indicated by those parameters for which the certified Organization takes measures, Q-CERT shall assess if additional surveillance measures for the AIMS of the Organization are necessary.

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.

11. Scope extensions

When a certified Organization requests an extension or a change of the scope that they are certified for, they should provide Q-CERT with 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 AI system(s) risks related to the activity/activities that are managed within the AIMS;

e) the number of controls relevant to the extension;

f) the number of persons involved in the AI life cycle of the extended scope; and

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

Audit time shall be added to the calculated duration to review the certified Organization's AIMS. 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.