



مركز الإمارات العالمي للاعتماد

Emirates International Accreditation Center

متطلبات الاعتماد لجهات منح الشهادات لأنظمة إدارة أمن المعلومات/الأمن السيبراني/الذكاء الاصطناعي (AI)

Accreditation Requirements for Certification Bodies of Information/Cyber Security/Artificial Intelligence (AI) Management Systems

EIAC-RQ-CB-003

Approved by:	EIAC CEO
Prepared by:	Director, Certification Bodies Accreditation Department

Revision history			
Issue no.	Rev. No.	Details	Date
1	00	First Issue for use under EIAC Name	15-11-2018
1	01	Modify Clause no. 3: General requirements regarding the year of issuance the international standards.	20-10-2019
2	00	The document was entirely reviewed and requirements for ADHICS scheme are added. The title of document was also amended.	07-12-2022
2	01	Revised due to the incorporation of the new identity of the Dubai Government.	23-07-2024
2	02	Incorporated the Artificial Intelligence (AI) management systems requirements	06-10-2026

Contents

1	Scope.....	3
2	Definitions.....	3
3	General Requirements	4
4	Requirements for Competence of CB Staff.....	5
5	Witness Audits	6
6	Use of EIAC Accreditation Symbol	6
7	Table 1 and Table 2	8

1 Scope

This document is applicable to certification bodies which are certifying the Information Security Management Systems (ISO 27001:2022), Artificial Intelligence (AI) Management Systems (ISO 42001:2023) and Abu Dhabi-Healthcare Information and Cyber Security Standard-OH/SD/ADHICS/0.9 (ADHICS).

Accreditation criteria for these programs include ISO/IEC 17021-1:2015 and

ISO/IEC 27006-1: 2024 for Information security management systems,

ISO/IEC 42006: 2025 for Artificial intelligence management systems

2 Definitions

The purpose of this section is to define the general and technical terminology that is used throughout this document.

2.1 Certification Body:

For the purpose of this accreditation, a certification body is an independent impartial body, governmental or non-governmental, possessing the necessary competence and reliability and operates in accordance with main standard ISO/IEC 17021-1 and associated technical specifications to perform management system(s) certifications.

2.2 Shall

The term “shall” is used throughout this document to indicate those provisions which, reflecting the requirements of EIAC Criteria is mandatory.

3 General Requirements

- 3.1 The Certification Body (CB) shall be a legally licensed entity and all employees of certification body shall have legally valid contract/permission/work permit to work for the certification body.
- 3.2 The CB shall only certify the legally licensed clients and shall maintain the legal status record of all of its clients.
- 3.3 The Certification Body (CB) applying for accreditation under this program shall have a management system in compliance with ISO/IEC 17021-1:2015 and
ISO/IEC 27006-1: 2024 for Information security management systems,
ISO/IEC 42006: 2025 for Artificial intelligence management systems.
- 3.4 The certification body shall consider ISO/IEC 42005, ISO/IEC 42006, ISO/IEC 23053, ISO/IEC 22989 standards while performing certification activities for artificial intelligence (AI) certifications.
- 3.5 The certification body shall consider all applicable laws related to cyber security, data protection, artificial intelligence and information security.
- 3.6 The certification body shall follow the EIAC Policy on the Responsible Use of Artificial Intelligence (AI) in Conformity Assessment Activities – EIAC-PL-007.
- 3.7 The CB shall employ suitable and qualified technical and administrative staff. As availability of minimum resources, the CB is required to have at least one permanently employed application/contract reviewer, one qualified auditor and one qualified certification decision maker for the certification scheme(s) applied for accreditation/accredited certification scheme.
- 3.8 If auditor/lead auditor does not possess the required auditor's qualification as mentioned in clause 4.1 of this document, then CB can include technical expert(s) in audit team. In this situation auditor/lead shall have educational qualification in any science or engineering discipline.
- 3.9 Before applying for accreditation, the applicant CB must have met the following conditions:
 - a) granted at least one certification for the scheme applied for accreditation or the CB has two applicants for which they have completed at least stage 1 audit for one client.
 - b) conducted at least one internal audit and one management review.
 - c) conducted at least one comprehensive review of risks to impartiality/potential conflict of interests, with consultation/participation of balanced interested parties.

- 3.10 Accredited certification bodies are required to submit accumulated data reports containing certifications and authorized resources' details under EIAC accreditation scheme(s) on prescribed formats on 10 January, 10 April, 10 July and 10 October every year.

4 Requirements for Competence of Certification Body Staff

All relevant requirements of ISO/IEC 27006-1:2024 and/or ISO/IEC 42006:2025 are applicable for relevant certification schemes, in addition to the below mentioned requirements.

4.1 Requirements for auditors

This shall be ensured that auditors shall have met the following requirements:

Successfully completed internationally recognized (such as approved by IRCA or any other internationally recognized training) auditor/lead auditor training on relevant certification standard such as ISO 27001, ISO 42001 standard, and/or Abu Dhabi-Healthcare Information and Cyber Security Standard-OH/SD/ADHICS/0.9 (ADHICS).

- 4.1.1 Completed the typical auditors' approval process of observation, auditor-under- training, auditor & lead auditor stages,
- 4.1.2 Bachelor's degree in computer science, software engineering, software technology, artificial intelligence, data science, machine learning, or other internationally recognized qualifications in these fields. Degree in engineering and other science disciplines is also acceptable if combined with additional qualifications in computers or information technology.
- 4.1.3 At least four years full-time practical workplace experience in information/computer technology/data protection, of which at least one year related to AI systems for AIMS scheme and related to information security/cyber security/software development for ISMS scheme.
- 4.1.4 Thorough knowledge of the latest information security & risk management applications,
- 4.1.5 Familiarity with ISMS family of standards including ISO 27000, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27007, and ISO/IEC 42005, ISO/IEC 42006, ISO/IEC 23053, ISO/IEC 22989 and where relevant ISO 27799.
- 4.1.6 Knowledge of current legal & regulatory requirements relevant to information security, cyber security, artificial intelligence. For ADHICS knowledge of regulations of relevant department of health is essential.
- 4.1.7 Knowledge of ISMS and/or artificial intelligence controls & their implementation,

- 4.1.8 Maintains knowledge and skills in information/cyber security/artificial intelligence up to date through continual professional education (CPE),
- 4.1.9 Fluent in both writing and speaking in the language of audit.
- 4.2 Requirements for technical experts
- 4.2.1 All requirements mentioned in 4.1 above are applicable except point (4.1.1).
- 4.2.2 Technical expert is required to have knowledge of ISO 27001, ISO 42001 and/or ADHICS.
- 4.3 Requirements for certification decision makers
- Certification decision maker(s) shall have Knowledge of audit principles practices and techniques used for information security management system, artificial intelligence management systems, Knowledge of ISO/IEC 27001 standard/ISO/IEC 42001 standard/normative documents and/or ADHICS and Knowledge of information security business sector as applicable.

5 Witness Audits

- 5.1 Minimum one audit shall be witnessed to grant accreditation for any applied standard. For witness audits, stage 2 certification audits (and recertification audits) are preferred; however, extended surveillance audits can also be witnessed.

6 Use of EIAC Accreditation Symbol

The accredited CB is entitled to use EIAC accreditation symbol on the certificates issued under accreditation scope & scheme in line with EIAC-RQ-GEN-002. Before using EIAC accreditation symbol or any reference to EIAC accreditation, the accredited certification bodies are required to take formal approval from EIAC for the use of EIAC accreditation symbol or any reference regarding EIAC accreditation. [Ref: Doc. EIAC-RQ-GEN-002]

Table 1: Scope for ISO/IEC 27001 Information Security Management Systems (ISMS) Certifications

Scope
Low and Medium Complexity
High Complexity

Table 2: Scope for ISO/IEC 42001 Artificial Intelligence Management Systems (AIMS) Certifications

Scope
Artificial Intelligence Management Systems certification ISO/IEC 42001