TECHNICAL CIRCULAR

Ref. DC2026LMM009 **Milan**, 05-11-2026

To all accredited/applicant Certification Bodies
To the Associations of Conformity Assessment Bodies
To all Assessors/Experts of the DC Department
Their offices

SUBJECT: Technical circular DC N° 08/2026 - Provisions regarding the ISO/IEC 17021-1 accreditation of Certification Bodies against the standard ISO/IEC 42001

Foreword

This document provides provisions and guidance for the accreditation of Certification bodies (hereinafter CABs) operating in accordance with ISO/IEC 17021-1 for the certification of artificial intelligence management systems against the standard ISO/IEC 42001.

As is well known, in the course of 2024 the European Parliament approved Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, the so-called “AI Act”.

The new Regulation aims to ensure that artificial intelligence systems placed on the European market are safe and respect the fundamental rights and values of EU Citizens and of non-EU Persons present in the European Union in whatever capacity. The AI Act also aims to stimulate investment and innovation in the field of artificial intelligence and to facilitate the development of a single market for lawful, safe and trustworthy artificial intelligence applications, positioning the EU among the leading players worldwide.

In response to the substantial growth in the use of Artificial Intelligence applications, and in consideration of the risks of such applications, the international standardisation bodies ISO and IEC have also taken steps and developed the standard ISO/IEC 42001, published in 2023, whose objective is to support organisations in the reliable and responsible use of AI systems in order to safeguard all the resources involved and create trust in the application of such systems.

ISO/IEC 42001, although not harmonised with the AI Act Regulation, is the only instrument currently certifiable by Management System Certification Bodies accredited against the standard ISO/IEC 17021-1.

To obtain accreditation against the Standard referred to, CABs must meet not only the requirements of the standard ISO/IEC 17021-1, but also those of the standard ISO/IEC 42006:2025, as a Level 4 standard according to document EA 1/06.

The main objective that led to the development of ISO/IEC 42001 is linked to the necessity of satisfying the risk management demands relating to the use of AI systems, with reference to the requirements defined in the various legal domains and to the specificities of the technological domains, also taking into account traditionally known threats. The “governance” that the standard ISO/IEC 42001 requires to be established in organisations adopting AI systems provides for risk governance policies that may affect AI systems throughout their life cycle, from the phase of preparing the data needed for training the algorithms and validating the models obtained, through to the management of unauthorised uses of the solutions made operational.

The harmonised structure of ISO/IEC 42001 allows organisations to integrate the requirements set out with those of another management system already adopted within their own structure (e.g. ISO/IEC 9001, ISO/IEC 27001, ISO/IEC 27701).

Although it is a voluntary standard, it should be noted that the European legislator itself, in the AI Act, in order to mitigate the risks to the health, safety, fundamental rights and freedoms of human beings arising, whether voluntarily or not, from Artificial Intelligence systems classifiable as high-risk, has identified the obligation to implement precisely a Management System, a tool aimed at ensuring the continued reliability, throughout the entire life cycle, of products or services that employ Artificial Intelligence systems.

It is pointed out that the contents of this circular are the result of a number of pilot projects that ACCREDIA-DC conducted prior to the final publication of the standard ISO/IEC 42006.

Characteristics of the conformity assessment service

The purpose of ISO/IEC 42001 is to ensure that systems are developed and used responsibly:

a. by promoting the development and use of AI systems that are reliable, transparent and accountable, in compliance with laws and regulations on data protection or with obligations towards interested parties;
b. by enhancing ethical principles in the use of AI systems, such as fairness, non-discrimination and respect for privacy;
c. by supporting organisations in identifying and managing the risks related to the implementation of AI, ensuring the adoption of appropriate mitigation measures.

The standard, which is also based on the HS structure and the PDCA cycle, provides as its initial step a thorough analysis of the context, in which the needs of the internal and external interested parties that are relevant to its purpose, and that are able to influence the ability of its AI management system to achieve the intended result, must be identified. Once the AI solution or system to be adopted has been defined, it is required that such effects on individuals, groups or society as a whole be the subject of an “impact assessment”, capable of showing how all the phases of the life cycle are such as to guarantee the rights and freedoms of the

Persons who may be affected by it. It follows that, in addition to the typically technological aspect, the need is highlighted for an ethical approach to safeguarding and enhancing the common good, and CABs will be called upon to assess, of course, the technological and business pathways that lead organisations to adopt AI solutions and systems, but above all the governance approach relating to the higher values of protecting the rights and freedoms of Citizens. This vision aims to “reward” conscious and ethically responsible choices with a view to the sustainability of client organisations and of society as a whole. In this perspective, it appears natural that the assessment approach should always be based on a risk-based logic, and the Standard ISO/IEC 42001, by adopting the harmonised ISO structure, is directed precisely in this sense. In fact, once the context and the needs of the interested parties have been defined, the organisation, through its own organisational structure and its management, must equip itself with a policy that defines the objectives of the AI system, identifies the resources involved, the responsibilities associated with them and the training needs, and plans the risk assessment operations and the achievement of objectives, as well as the phases of control and continuous monitoring of the effectiveness of the AI system implemented, up to completing the PDCA cycle.

From a technical point of view, ISO/IEC 42001 also makes direct or indirect reference to other relevant technical standards, some of which are essential in the process of assessing an AIMS:

Standard	**Description**	**Scope of application**
ISO/IEC 22989	Artificial intelligence concepts and terminology.	Definition of the fundamental concepts and roles in the AI ecosystem.
ISO/IEC 23894	Guidance on risk management for AI systems.	Identification, assessment and treatment of AI-related risks.
ISO/IEC TR 24027	Bias in AI systems and in decision making.	Identification and mitigation of bias in AI data and models.
ISO/IEC TR 24368	Overview of the ethical and societal concerns of AI.	Support for assessing the societal impact of AI systems.
ISO/IEC 5338	AI system life cycle processes	Definition of the technical processes of the AI system life cycle (algorithm selection, training, continuous validation); supports the technical implementation of the concept of responsible AI.
Series ISO/IEC 5259	Quality of data used in analytics and machine learning systems	Models, measures, reporting, requirements and guidelines for data quality management.
ISO/IEC 25024	Measurement of data quality.	Assessment of the quality of data used in AI systems.
ISO/IEC 25059	Quality models specific to AI systems.	Definition of a technical model for assessing the quality of AI systems, including characteristics such as explainability, fairness and robustness.

ISO/IEC 42005	AI system impact assessment.	Guidelines on the application of impact assessment methods.
Series ISO/IEC TR 24029	Assessment of the robustness of neural network-based models for AI systems.	Technical tools for assessing the robustness of AI models, applying formal and statistical methods to validate the behaviour of the system.
ISO/IEC TS 4213	Methodologies for the assessment of classification performance in machine learning (ML) models, systems and algorithms.	Assesses the technical performance of ML models; support for model selection and monitoring.
ISO/IEC 23053	Conceptual framework for artificial intelligence (AI) systems based on machine learning (ML).	Conceptual model for describing ML-based AI systems; support for the identification and attestation of the system's components and functions.
ISO/IEC 31000	General guidelines on risk management.	Methodological basis for risk management; helps to structure strategic and operational thinking about risk.
ISO/IEC 38500 and 38507	Governance of IT and implications of the use of AI.	Support for defining policies, roles, responsibilities and IT strategies; promotion of transparency and accountability.
ISO/IEC 27001 and 27701	Information security and privacy management	Framework for information security and privacy to ensure reliable and responsible AI.

In analogy with other management system standards, ISO/IEC 42001 also has a list of controls (Normative Annex A) useful for achieving/measuring objectives in relation to the use of AI and for addressing the threats identified in the risk assessment process relating to the design, development and operation of AI systems.

The text of the standard is then enriched with a series of Annexes useful for forming a guide, albeit not exhaustive, for:

a. implementing the controls (ref. normative Annex B);
b. outlining the potential organisational objectives and the associated risk sources (ref. informative Annex C);
c. using the AI management system across different domains or sectors and its integration with other MSs.

Certification Rules

The requirements of the standard ISO/IEC 17021-1, supplemented by ISO/IEC 42006, apply. In the certification process the CAB must also demonstrate documented knowledge and application of the standards related to ISO/IEC 42001.

Calculation of audit time durations	The applicable requirements of ISO/IEC 17021-1, supplemented by ISO/IEC 42006 with specific reference to Annexes A and B, apply. It is the responsibility of the CAB to apply, using a risk-based approach, Option A or B as outlined in Annex B of the standard itself.
Certificate duration and audit frequencies	The applicable requirements of ISO/IEC 17021-1, supplemented by ISO/IEC 42006, apply.
Competence criteria for the personnel involved in conformity assessment	The applicable requirements of ISO/IEC 17021-1, supplemented by ISO/IEC 42006, apply. In relation to what has been observed in the accreditation processes, it is deemed appropriate to provide the following guidance on the process of selecting and qualifying auditors, starting from what is established in Table 1 of ISO/IEC 42006: 1. Training: knowledge of technical standards must be demonstrated by evidence of training certificates complete with programmes and durations appropriate to the content of the training itself. Alternatively, documented evidence of relevant and related activities in the contexts of teaching, scientific research, development in technical standardisation committees is deemed acceptable. When assessing course attendance certificates, the CAB must demonstrate the adequacy of the syllabuses and the effectiveness of the training itself with adequate tests or audit simulations. In this regard, it is crucial that the CAB has adequate information on the auditors' ability to understand the different roles (e.g. AI producer, AI provider, AI customer/user) and to assess their influence on the certification requirements. 2. Experience: when assessing experience requirements, the CAB must take into account the relevance and currency of the operational experience gained, with reference to current technologies, risks and methodologies in the field of artificial intelligence (for example: machine learning, computer vision, management of training data and bias, ethics and governance of models, etc.). Such experience must have been acquired on a continuous basis in line with modern AI paradigms. The assessment team must be appointed taking into account the customer's business sectors (ref. Table 1 §7.1.2 ISO/IEC 42006), as provided for by the IAF coding in document ID01 for the QMS Accreditation Scope. The CAB must prepare and maintain appropriate documentation providing evidence of the qualification criteria (e.g. qualification records) for personnel qualified as application reviewer, lead auditor and auditor (including any technical experts for the customer's business area) and technical reviewer/decision maker.
Applicable IAF/Globa ACI documents	All IAF/Global ACI documents relating to management systems apply.

ACCREDIA database of issued certifications

As is well known, CABs are required to transmit to ACCREDIA-DC via the web service – SIAC the data related to the entities holding certifications issued by them, according to the procedures defined by ACCREDIA-DC and the related Regulations (RG01 §1.10.7).

Accreditation Rules

A	CAB already accredited against ISO/IEC 17021-1	• Document review of 1 man-day; • Assessment at the CAB's offices with a duration of 2 man-days • 1 witness assessment of appropriate duration.
B	CAB not yet accredited against ISO/IEC 17021-1 but accredited for other accreditation schemes (Level 3)	• Document review of 1 man-day; • Assessment at the CAB's offices with a duration of 3 man-days; • 1 witness assessment of appropriate duration.
C	CAB not accredited	• Document review of 1 man-day to be conducted, where possible, partially in synchronous remote mode; • Assessment at the CAB's offices with a duration of 4 man-days; • 1 witness assessment of appropriate duration.
Maintenance of Accreditation	Please note that ACCREDIA-DC must, in any case, conduct an annual assessment at the offices of the CABs to evaluate their conformity with ISO/IEC 17021-1. ACCREDIA will carry out at least one maintenance assessment per year at the CAB's offices and 1 witness assessment in the accreditation cycle. However, ACCREDIA reserves the possibility, in any case, of modifying the surveillance timing referred to above on the basis of a risk-based approach that takes into account various factors such as, for example, changes made to the certification scheme; changes in the structure of the Body or other similar situations; critical issues related to the scheme (e.g. widespread request in calls for tenders, etc.); a high number of certifications issued; receipt of complaints/reports concerning the work of the CAB and/or certified companies; the CAB's performance in the scheme; specific resolutions of the competent CSA, etc.	

Documentation to be submitted to ACCREDIA-DC for the document review

In addition to what is listed in the application for accreditation DA-01, submission of the following is requested:

a. Checklists, guidelines, instructions prepared by the CAB for the Assessment Team;
b. Qualification criteria and CVs of the personnel responsible for contract review, of the auditors (including any technical experts for the customer's business area) and of the technical reviewers/decision makers, with the related qualification records;
c. Procedures applicable to the commercial process for defining audit times durations, as well as the procedures for managing the certification file.

We take this opportunity to send our kind regards.

Mariagrazia Lanzanova

Vice-Director of

Certification and Inspection Department

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 05/11/2026 11:25:32

