TECHNICAL CIRCULAR

Ref. DC2024SPM218 **Milan, 13/12/2024**

To all MS - ISMS Accredited/Accrediting Certification Bodies
To the Associations of Conformity Assessment Bodies
To all Assessors/Experts of the CI Department

Their offices

SUBJECT: Technical circular DC N° 39/2024 – Provisions and Updates Regarding the ISO/IEC 17021-1 Accreditation of Certification Bodies for ISO/IEC 27001 and ISO/IEC 27701

These provisions cancel and replace the content of the following documents:

- Technical Circular No. 02/2018;
- Informative Circular No. 01/2019;
- Technical Circular No. 10/2019;
- Informative Circular No. 02/2021.

Foreword

This document sets out provisions and guidance following updates in recent years in the field of information security standards, as well as their accreditation and certification processes. Among the key elements, we particularly highlight:

1. The ISMS scheme has become an integral part of the scope of the unified certificate for management systems (ref. ACCREDIA DC Circular No. 1/2023)
2. In February 2024, the International Standard ISO/IEC 27001:2022/Amd 1:2024 was published, which has updated clauses 4.1 and 4.2 with regard to the so called “Climate action changes” (ref. IAF/ISO Joint Communication of 22.02.2024)
3. In March 2024, the new level 4 Standard ISO/IEC 27006-1:2024, *Information security, cybersecurity and privacy protection, Requirements for bodies providing audit and certification of information security management systems, Part 1: General* was published, replacing the previous version from 2015, which had been further amended in 2020. This document outlines the operational procedures for the transition to the adoption of IAF MD29 “Transition Requirements for ISO/IEC 27006-1:2024”

4. Several standards or guidelines are currently under development and update, e.g.: ISO/IEC DIS 27701, ISO/IEC FDIS 27706, ISO/IEC CD 27017, ISO/IEC DIS 27018, ISO/IEC 27011, ISO/WD 27799. Others have already been published: ISO/IEC 27019:2017, ISO/IEC 27035-1:2023, ISO/IEC 27032:2023.

All provisions expressly outlined in the level 3 standard (ISO/IEC 17021-1), level 4 standard (ISO/IEC 27006-1, subject to transition, and ISO/IEC TS 27006-2), level 5 standards (ISO/IEC 27001 and ISO/IEC 27701), and the relevant ACCREDIA Regulations remain unchanged.

Transition ISO/IEC 27006-1:2024

On 20 March 2024, the international Standard ISO/IEC 27006-1:2024 was published, replacing the previous ISO/IEC 27006:2015 and incorporating Amendment 1:2020. The main changes contained in ISO/IEC 27006-1:2024 are:

1. A clearer specification regarding the requirements for remote audits (see sections 9.1.3 and 9.4.3.2).
2. Update to the Audit Time Calculation Requirement (see Annex C).
3. Update to annex D of the 2015 version, which has been aligned with the information security controls listed in annex A of ISO/IEC 27001:2022 and relocated as Annex E in the 2024 version.
4. Clarification regarding the reference to other standards in ISMS certification documents (see par. 8.2.3).
5. Removal of redundancies with the Level 3 Standard ISO/IEC 17021-1:2015. See, for example, points 5.2, 7.1.3, 9.3.2.2, and 9.4 of ISO/IEC 27006-1:2024.
6. Elimination of the minimum requirement regarding years of work experience and training for ISMS auditors, for example, four years of full-time practical workplace experience.

For further details on the changes, explicit reference is made to the IAF MD 29 document, which also provides the following provisions regarding the transitional period:

Accreditation transition	• 01.12.2024: Start of assessment activities against the new standard by ACCREDIA-DC. • 30.03.2025: Deadline for managing accreditation activities or accreditation extension in accordance with ISO/IEC 27006:2015+Amd1:2020 • 31.03.2026: Deadline for the completion of accreditation transition. From 01.04.2026, accreditations that have not yet been updated will be withdrawn.
Certification transition	• Once accredited against the new standard, the Certification Body may only use the outdated version of the standard for surveillance activities. • 31.03.2026: Deadline for the completion of certification transition.

In accordance with the IAF MD29 document, ACCREDIA-DC will verify the alignment of the certification process with the new standard (transition verification) through a one man-day off-site document review. The documents required by paragraph 4.2 of the IAF MD29 document will be requested and evaluated for the document review. Additionally, refer to the “Self-Assessment Transition Plan Annex”.

Finally, it is noted that the new ISO 27006-1 once again reaffirms the recommendation (req. 10.1.2) for the Certification Body to implement an information security management system in accordance with ISO/IEC 27001. Given the current historical context, Certification Bodies are encouraged to carefully consider this aspect.

Certification Rules

The ISO/IEC 27000 series is now populated with standards of various types, some of type A and others of type B, in relation to the ISO classification[1]. In light of this, it is deemed necessary to provide further clarifications regarding the applicable procedures for certification under accreditation.

General requirements	• With reference to req. 6.1.2, 8.2, and A.8.8 of ISO/IEC 27001, the Certification Body must verify whether the organization undergoes periodic vulnerability assessments and/or penetration tests, considering the level of risk to which the infrastructure and the entire organization are exposed. This also applies to the assessment of the frequency with which such evaluations must be repeated. In relation to these activities, the CAB must verify that appropriate records are maintained regarding the qualifications of the personnel and/or laboratory assigned, as well as the actions taken to reduce exposure to threats. • Where applicable, the Certification Body must verify how the client organization ensures the security of information related to the infrastructures used for data processing, whether they are simple proprietary physical servers located at the organization’s premises, cloud services (private, hybrid, external), or housing or hosting at specific external service provider Data Centres. The auditing procedures must also include the verification of the ongoing maintenance of the reliability and effectiveness levels, with reference to information security and cybersecurity, of the solutions identified. It is noted that the existence of accredited conformity certificates within the EA/MLA framework covering external infrastructures and services (e.g., Cloud) is presumed to indicate compliance with the applicable requirements. Otherwise, the Certification Body must audit the specific site and maintain the related records.

.....
[1] https://www.iso.org/management-system-standards-list.html#TypeAB

	• Regarding the competence criteria for Certification Body personnel, the provisions of the level 4 standards (ISO/IEC 27006-1 and ISO/IEC 27006-2) apply. In any case, it is necessary to remind the certification bodies regarding the assessment of the continuous updating of auditors' competencies, with special reference to the technical areas in which they are employed (e.g., healthcare, automotive, aerospace and defence, medical, food, etc). In this regard, a useful reference may be the lists provided in the sectors referred to by the NIS2 Directive. • Regarding the criteria for calculating audit durations, the provisions of the level 4 standards (ISO/IEC 27006-1 and ISO/IEC 27006-2) apply. Reductions in audit time must be justified in detail and supported by documented evidence. It is also noted that the existence of certifications for other management systems, even if issued by the same CAB, is not, on its own, sufficient to consider the management system "mature," unless there is evidence of results (absence of non-conformities) and positive conclusions from the most recent third-party audit, which demonstrate effective internal audits by the organization capable of identifying security issues and continuous improvement actions. Finally, it should be considered that the number of personnel to be included in the man-day calculation must also account for the services the organization intends to include within the application scope of certification. In this regard, it is emphasized that the effectiveness of the management system is not the sole responsibility of those responsible for managing the ICT infrastructure, but of anyone who manages, in any capacity, the information.
ISO/IEC 27001	It applies to information security management systems without limitations. It is a Type A standard that follows the ISO HS (Harmonized Structure). This standard is certifiable according to the well-established rules in accordance with accreditation regulations. The certification scope issued by the Certification Body must explicitly reference the SoA and its status of updates, in line with the processes included within the scope of the management system subject to certification. It must be fully recorded in the ACCREDIA database of certifications issued by the Certification Body, according to the established rules. Example of scope:

	"Design and provision of housing, hosting, disaster recovery, and business continuity services. Design and provision of cloud computing services, IaaS, PaaS, and SaaS. Provision of services for the development, management, and maintenance of applications. Provision of identity management and application security services delivered both as a service and on-premises, in accordance with the Statement of Applicability Rev.0 dated dd/mm/yyyy."
ISO/IEC 27701	It applies to information security management systems designed to allow the addition of specific requirements for personal data management. It is a Type A standard, which, however, does not follow the HS structure. This standard is certifiable as an extension of ISO/IEC 27001, and standalone certifications are not permitted. Therefore, the ISO/IEC 27701 conformity certificate must be explicitly referable to the ISO/IEC 27001 certificate, of which it is an extension. Example of scope: *"Personal data management system, in the role of Data Controller and Data Processor, in relation to the following processes".* • *Design and provision of ICT infrastructure services for Data Centres, such as Housing, Networking, and Disaster Recovery.* • *Design and provision of inbound and outbound call centre services in IaaS (Infrastructure as a Service), SaaS (Software as a Service), and PaaS (Platform as a Service) modes.* • *Design, development, and maintenance of online banking services, tools, and services supporting application design and development, as well as the management of systems and networks located in the Server Farm* *According to the specific Statement of Applicability outlined in certificate no. xxxxx* [where "xxxxx" refers to the number of the linked ISO 27001 certificate]
ISO/IEC 27017, 27018 and other Type B guidelines or standards from the ISO/IEC 27000 series	In some cases, these are Type B standards, and in others, guidelines that are useful for identifying the operational controls considered necessary within the ISMS. These standards are not certifiable. However, if the requesting organization is able to demonstrate the correct application of such standards, the Certification Body must verify the implementation of the controls.

In such cases, for the calculation of the audit duration for the scope extension, the Certification Body must consider an additional time (net of applicable reductions) of at least 1 man-day for each additional standard applied, for each verification and at any stage.

It is the responsibility of the Certification Body to demonstrate the competence, and its maintenance, of the auditors conducting evaluation activities against these standards.

The certification scope issued by the Certification Body must explicitly reference the SoA, its update status, and the additional standards referenced for the controls. The certificate must, in any case, clarify conformity solely to the Type A standard.

Example of scope:

"*Design, development, maintenance, and support of software, provision of SaaS (Software as a Service) services according to the Statement of Applicability Rev.0 dated dd/mm/yyyy, integrated with the controls specified in the ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines.*"

Regarding the management of flexible scopes, while adhering to the provisions of Regulation RT-37, the only standards that can fall under this category are those of Type A, namely ISO/IEC 27001 and ISO/IEC 27701 as of today.

The following criteria apply for adjustments to accreditations and certifications issued:

- accreditations issued against ISO/IEC 27017, ISO/IEC 27018, or other guidelines will be withdrawn as of 01.03.2025.
- certifications that include ISO/IEC 27017, ISO/IEC 27018, or other Standards of the same type, remain valid until the natural expiration of the certificate or until the first applicable modification (e.g., scope extension or modification). Subsequently, they must be aligned with the provisions of this document.
- all provisions set out in this document are fully effective as of 01.01.2025.

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).

Certifications must be recorded in the database with an explicit reference to the standards classified as Type A ISO standards, namely ISO/IEC 27001 and ISO/IEC 27701. If other standards from the ISO 27000 series are used, these must be listed in the certification scope description, as previously exemplified. These provisions also apply to accreditations granted with a flexible scope.

Accreditation Rules

A	Certification Body already accredited for the ISO/IEC 17021-1:2015 and ISO/IEC 27001 schemes	• Document review of 0.5 man-days to be conducted partially in synchronous remote mode. • 1 witness assessment with a duration appropriate for the ISO/IEC 27701 extension
B	Certification Body already accredited for the ISO/IEC 17021-1:2015 scheme	• Document review of 0.5 man-days. • Office assessment with a duration of 1 man-day. • 1 (one) witness assessment with an appropriate duration to cover the analysis of the key elements of the audit process conducted by the CAB for each requested scheme (e.g., ISO/IEC 27001 and ISO/IEC 27701). A reporting time of 1 man-day applies to each witness assessment if the activities are carried out separately.
C	Certification Body not yet accredited for ISO/IEC 17021-1:2015 but accredited for other accreditation schemes (Level 3)	• Document review of 1 man-day. • Office assessment with a duration of with a duration of 2 man-days. • 1 (one) witness assessment with an appropriate duration to cover the analysis of the key elements of the audit process conducted by the CAB for each requested scheme (e.g., ISO/IEC 27001 and ISO/IEC 27701). A reporting time of 1 man-day applies to each witness assessment if the activities are carried out separately.
D	Certification Body not accredited	• Document review of 1 man-day to be conducted partially in synchronous remote mode. • Office assessment with a duration of with a duration of 4 man-days. • 1 (one) witness assessment with an appropriate duration to cover the analysis of the key elements of the audit process conducted by the CAB for each requested scheme (e.g., ISO/IEC 27001 and ISO/IEC 27701). A reporting time of 1 man-day applies to each witness assessment if the activities are carried out separately.

Maintenance of Accreditation	Number of certificates issued	Number of assessments in the accreditation program
	0÷50	4 Office assessments 1 Witness assessment
	51÷150	4 Office assessments 2 Witness assessments
	>150	4 Office assessments 4 Witness assessments

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

In addition to what is listed in the application for accreditation DA-01, applicant shall submit:

a. Checklists, guidelines, and instructions prepared by the Certification Body for the Assessment Team.

b. Qualification criteria and CVs of the personnel responsible for contract review, auditors, and decision-makers.

c. Certificate template issued by the Certification Body.

d. Procedures applicable to the commercial process for defining audit times, as well as procedures for managing the certification process.

We take this opportunity to send our kind regards.

Dott.ssa Mariagrazia Lanzanova

Deputy Director

Certification and Inspection Department

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 13/12/2024 12:45:54