TECHNICAL CIRCULAR

Ref. DC2026SPM117 **Milan**, 18-09-2026

To all accredited/accreditation-seeking MS - SSI Certification Bodies
To the Associations of Conformity Assessment Bodies
To all Assessors/Experts of the DC Department
Their offices

SUBJECT: Technical Circular DC No. 22/2026 - Provisions and updates regarding UNI CEI EN ISO/IEC 17021-1 accreditation of Certification Bodies against ISO/IEC 27001

These provisions cancel and replace the content set out in Technical Circular DC No. 39/2024.

Foreword

This document provides provisions and guidance following the updates that have taken place in recent years in the field relating to information security standards, and their accreditation and certification. Among the salient elements, it is worth recalling, in particular, the following:

1. The ISMS scheme (formerly SSI) has become an integral part of the scope of the single management systems certificate (ref. ACCREDIA Circular DC No. 1/2023);
2. In February 2024, International Standard ISO/IEC 27001:2022/Amd 1:2024 was published, which amended clauses 4.1 and 4.2 of the standard with reference 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 2015 version as further amended in 2020. This document sets out the operational procedures for the transition in implementation of the IAF MD29 document, "Transition Requirements for ISO/IEC 27006-1:2024”;
4. Several normative guidelines are currently under development and being updated, e.g.: ISO/IEC DIS 27000, ISO/IEC 27017 (in the process of being published), ISO/IEC FDIS 27090.

All provisions expressly set out in the Level 3 standard (UNI CEI EN ISO/IEC 17021-1), the Level 4 standard (ISO/IEC 27006-1), the Level 5 standard (ISO/IEC 27001), and the relevant Accredia Regulations remain unchanged.

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 considered necessary to provide further clarifications regarding the procedures applicable for certification under accreditation.

General requirements

- With reference to req. 6.1.2, 8.2 and A.8.8 of ISO/IEC 27001, et al., the CB must ascertain whether the Organization periodically undergoes vulnerability assessment and/or penetration testing, taking into account the level of risk to which the infrastructure and the Organization as a whole are exposed. This also applies to the assessment of the time frequency with which such evaluations must be repeated. In connection with these activities, the CAB must verify that appropriate records are kept regarding the qualification of the personnel and/or laboratory engaged, and regarding the actions taken to reduce exposure to threats.
- Where applicable, the CB must verify how the client Organization ensures the security of information relating to the infrastructure used for data processing, whether this involves simple proprietary physical servers located at the organization's premises, or Cloud services (private, hybrid, external), or housing or hosting at specific Data Centres operated by external providers. The auditing procedures must also include verification of the maintenance over time of the levels of reliability and effectiveness, with reference to information security and cybersecurity, of the solutions identified.
  It should be noted that the existence of accredited conformity certificates within the EA/MLA framework covering the external infrastructure and services (e.g., Cloud) constitutes a presumption of conformity with the applicable requirements; otherwise, the CB must audit the specific site and maintain the related records.
- With regard to the competence criteria for CB personnel, the requirements of the Level 4 standard (ISO/IEC 27006-1) apply. In any case, it is necessary to remind CBs of the need to assess the ongoing updating of auditors' competences, with special reference to the technical areas in which they are employed (healthcare, automotive, aerospace and defence, medical, food, etc.). In this regard, a useful reference may be represented by the lists set out in the sectors of activity covered by the NIS2 Directive.
- With regard to the criteria for calculating audit durations, the requirements of the Level 4 standard (ISO/IEC 27006-1) apply. Reductions in audit time must be justified in detail and supported by documented evidence. It should further be noted that the existence of certifications for other management systems, even if issued by the same CAB, is not — on its own — sufficient reason to consider the management system "mature", unless there is evidence of outcomes (absence of nonconformities) and positive conclusions from the last third-party audit carried out, demonstrating effective internal audits by the Organization capable of detecting security issues and identifying continuous improvement actions.
  Finally, it should be taken into account that the number of staff to be considered in

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

the man-days calculation must also take into account the services that the organization intends to include within the scope of certification; in this sense, it should be emphasized that the effectiveness of the management system is not the exclusive responsibility of those in charge of managing the ICT infrastructure, but of anyone who, in whatever capacity, handles the information.

In particular, ISO/IEC 27001 applies to information security management systems without limitation; it is a Type A standard that follows ISO's HS structure (the so-called Harmonized Structure). The scope of certification issued by the CB must contain an express reference to the SoA and to its update status, consistent with the processes included within the perimeter of the management system subject to certification. This must be fully reported in the Accredia Database of certifications issued by the CB, in accordance with the already known rules.

Example scope:

"*Design and provision of Housing, hosting, disaster recovery, and business continuity services. Design and provision of cloud computing, IaaS, PaaS, and SaaS services. Provision of application development, management, and maintenance services. Provision of digital identity management and application security services, delivered both as a service and on premise, in accordance with the Statement of Applicability Rev.0 of dd/mm/yyyy.*"

ISO/IEC 27017, 27018 and other Type B Guidelines or standards of the ISO/IEC 27000 series

These are mainly Type B standards, and in other cases guidelines, which are in every respect useful for identifying the operational controls deemed necessary within the ISMS. Such standards are not certifiable.

However, should the applicant Organisation be able to demonstrate the correct application of such standards, the CB must verify the application of the controls.

In such cases, for the purpose of calculating the duration of the scope extension audit, the CB must allow, for each audit and at any stage, an additional time (net of any applicable reductions) of at least 1 man-day per further standard applied.

It remains the responsibility of the CB to demonstrate the competence, and its ongoing maintenance, of the auditors conducting assessment activities against such standards.

The certification scope issued by the CB must contain express reference to the SoA, its update status, and the further standards used as a reference for the controls. In any case, the certificate must clarify that conformity is solely with the Type A standard. Example scope:

"*Design, development, maintenance and support of software, provision of SaaS (software as a service) services in accordance with the Statement of Applicability Rev.0 of dd/mm/yyyy, supplemented by the controls set out in guidelines ISO/IEC 27017:xxxx and ISO/IEC 27018:xxxx.*"

Certifications incorporating ISO/IEC 27017 and ISO/IEC 27018, or other Standards of the same type, remain valid until the certificate's natural expiry or the first relevant amendment (e.g.: extension or modification of scope). They must subsequently be brought into line with the requirements of this document.

Flexible scope management

With the publication of ISO/IEC 27701:2025, this standard takes on the configuration of a standalone standard for the certification of privacy information management systems — Privacy Information Management System, PIMS — and no longer constitutes a mere extension of ISO/IEC 27001 certification. As a result of this regulatory development, within the ISO/IEC 27000 family there are no longer any further Type A management system standards certifiable as schemes dependent on, or directly linked to, ISO/IEC 27001, with the sole exception of ISO/IEC 27001 itself as the reference standard for the certification of information security management systems. It follows that the conditions for maintaining flexible accreditation scopes referring to the ISO/IEC 27000 family of standards no longer apply. Therefore, with effect from 1 July 2026, ACCREDIA will no longer accept new applications for accreditation, or for extension of accreditation, with a flexible scope referring to this family of standards. Bodies already accredited with a flexible scope for the ISO/IEC 27000 family must proceed to renounce the flexible scope and request realignment of the accreditation scope to a fixed scope under the current version of ISO/IEC 27001.

The final deadline for completing the process of renouncing the flexible scope for standards of the ISO/IEC 27000 family is 31 October 2027. From 1 November 2027, all accreditations with a flexible scope for standards of the ISO/IEC 27000 family will be revoked.

ACCREDIA database of certifications issued

As is known, CBs are required to transmit to ACCREDIA-DC, via the SIAC web service, the data relating to parties holding certifications issued by them, in accordance with the procedures defined by ACCREDIA-DC and the related Regulations (RG01 §1.10.7).

Certifications must be recorded in the database with express reference solely to the standards qualifying as Type A ISO standards, namely ISO/IEC 27001 and ISO/IEC 27701. Where other standards in the ISO 27000 series are used, these must be indicated in the description of the certification scope, as exemplified above. These requirements also apply to accreditations granted with a flexible scope.

Accreditation Rules

A	CB already accredited for the ISO/IEC 17021-1:2015 scheme	• Document review of 0.5 man-days; • Assessment at the CB's offices lasting 1 man-day; • 1 (one) witness assessment of a duration adequate to cover the analysis of the salient elements of the audit process conducted by the CAB. A reporting time of 1 man-day applies to each witness assessment where the activities are carried out separately.
B	CB not yet accredited to ISO/IEC 17021-1:2015 but accredited for other accreditation schemes (Level 3)	• Document review of 1 man-day; • Assessment at the CB's offices lasting 2 man-days; • 1 (one) witness assessment of a duration adequate to cover the analysis of the salient elements of the audit process conducted by the CAB. A reporting time of 1 man-day applies to each witness assessment where the activities are carried out separately.

C	Non-accredited CB	• Document review of 1 man-day, to be carried out partly in synchronous remote mode; • Assessment at the CB's offices lasting 4 man-days; • 1 (one) witness assessment of a duration adequate to cover the analysis of the salient elements of the audit process conducted by the CAB. A reporting time of 1 man-day applies to each witness assessment where the activities are carried out separately.

Maintenance of Accreditation

No. of Certificates Issued	No. of Assessments in the Accreditation Cycle
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 accreditation application DA-01, please submit:

a. Checklists, guidelines and instructions prepared by the CB for the Assessment Team;
b. Qualification criteria and CVs of the personnel responsible for contract review, of the auditors and of the decision makers;
c. Template of the Certificate issued by the CB;
d. Procedures applicable to the commercial process for determining audit durations, as well as the procedures for managing the certification file.

Best regards.

Dott.ssa Mariagrazia Lanzanova
Vice Director
Certification and Inspection Department

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 18/09/2026 16:26:59