ISCB-RQ-17021 | Issue 1 - September 2026

Management System Certification Body Accreditation Requirements

Applies to bodies seeking accreditation to audit and certify organisations against specified management system standards and sector schemes.

Primary standard	**ISO/IEC 17021-1:2015**
Document owner	International Services for Certification Bodies
Review trigger	Standard, scheme, regulatory or ISCB process change

Document status and use

This ISCB applicant guide states the evidence and operating controls normally expected for this programme. It does not reproduce or replace the applicable ISO or ISO/IEC standard. Applicants must hold an authorised current copy and comply with all applicable requirements, legislation, scheme rules and formally issued ISCB criteria.

References to IAF or ILAC publications identify technical criteria that may be relevant. They do not by themselves state or imply that ISCB is an IAF or ILAC arrangement signatory.

01 Applicable framework

The assessment hierarchy begins with the primary standard and includes applicable normative, regulatory, scheme-owner and ISCB documents. ISCB will identify the controlling criterion if requirements conflict.

- ISO/IEC 17021-1:2015 is the primary certification-body standard.
- ISO/IEC 17011:2017 governs ISCB's accreditation process and decisions.
- Current IAF Mandatory Documents and scheme-specific normative documents apply according to the requested accreditation scope.

02 Core organisational requirements

Legal status and responsibility

Be a legally identifiable entity, or a defined part of one, that can be held responsible for conformity-assessment activities, contracts and decisions.

Impartiality and independence

Identify, analyse, treat, monitor and record threats from ownership, finance, relationships, consultancy, commercial pressure and self-review.

Confidentiality and information security

Protect confidential information, personal data, intellectual property and electronic records; control any legally required disclosure.

Organisation and governance

Define authority, responsibilities, reporting lines and safeguards; assign technical work, review and decisions to competent and appropriately independent functions.

Competence and resources

Set role-specific competence criteria; evaluate, authorise, monitor and re-evaluate personnel; control facilities, equipment, software and external resources.

Controlled operations

Accept work only after confirming capability; use controlled methods and records; handle deviations; review outputs; base decisions on sufficient objective evidence.

Management system

Maintain document and record control, risks and opportunities, complaints, appeals, nonconforming work, corrective action, internal audit, management review and improvement.

Accreditation claims

Limit certificates, symbols and claims to the granted scope and amend them immediately after suspension, reduction, withdrawal or expiry.

03 Service-specific technical requirements

1. Define each certification scope using the applicable management-system standard, technical sector classification, geography and certification activity.

2. Operate a documented impartiality process with top-management commitment, threat analysis, stakeholder input and effective safeguards.

3. Establish competence criteria and evaluation processes for application reviewers, auditors, technical experts, reviewers and certification decision-makers by scheme and technical area.

4. Control application review, audit time, multi-site sampling, audit planning, stage 1, stage 2, surveillance, recertification, special audits, transfer and restoration.

5. Ensure independent review and certification decisions, certificate content, public status information and controls over marks and claims.

6. Maintain witnessed-audit readiness and reliable certification data required by applicable schemes and IAF documents.

04 Minimum application and readiness evidence

Submit current, approved documents and representative implementation records. Templates without operational evidence are not sufficient.

01	Legal identity, liability and impartiality committee or equivalent mechanism
02	Scope matrix and scheme approvals sought
03	Competence criteria, technical codes, auditor files and witnessed evaluations
04	Application reviews, audit-time calculations and multi-site rationale
05	Complete initial, surveillance, recertification and transfer files
06	Independent review and decision records
07	Certificate register, mark controls and public-status process
08	Internal audit, management review, complaints, appeals and corrective actions

05 Assessment, decision and continued accreditation

Application and scope review

ISCB reviews legal identity, requested scope, locations, resources, readiness and applicable criteria before quotation and assessment planning. Acceptance of an application is not a promise of accreditation.

Assessment

Assessment may include document review, office or remote assessment, on-site technical assessment, witnessing, interviews, record tracing and evaluation of representative activities. The mix depends on scope and risk.

Nonconformities and decision

The applicant must determine causes, correct the issue, implement proportionate corrective action and provide evidence of effectiveness within the notified period. Accreditation decisions are independent from assessment and limited to demonstrated competence.

Maintenance

Accredited bodies must remain competent, comply with surveillance and reassessment, notify significant changes without delay, cooperate with witnessing and record access, address complaints and nonconformities, and control all accreditation claims.

06 Principal references

- ISO/IEC 17021-1:2015
- Applicable ISO/IEC 17021 series competence documents
- IAF MD 1, MD 2, MD 4:2025, MD 5, MD 11, MD 15, MD 17 and MD 28
- Scheme-specific IAF MDs and normative documents, where applicable

External editions can change. The edition stated in the accreditation agreement, transition notice or other formal ISCB communication controls the assessment. Verify current editions before use.

Prepare	Complete the readiness assessment and organise objective evidence.
Apply	Submit the application and proposed scope for formal review.