ISCB INTERNATIONAL SERVICES FOR CERTIFICATION BODIES

ISCB-RQ-17065 | Issue 1 - September 2026

Product, Process and Service Certification Body Accreditation Requirements

Applies to bodies operating third-party certification schemes for products, processes or services within a defined requested scope.

Primary standard	**ISO/IEC 17065:2012**
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 17065:2012 remains the published primary standard at this issue date; a replacement is under development and transition requirements will be communicated after publication.
- ISO/IEC 17011:2017 governs ISCB's accreditation process and decisions.
- Certification scheme requirements, ISO/IEC 17067 concepts and applicable regulatory rules form part of the assessment criteria.

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. Document each certification scheme, including specified requirements, evaluation activities, surveillance model, decision rules, licensing and control of marks.

2. Protect impartiality through risk analysis and controls over ownership, finance, consultancy, design, manufacture, supply, installation and related bodies.

3. Demonstrate competence for application review, evaluation, testing or inspection, technical review, certification decision and surveillance.

4. Control outsourced evaluation while retaining responsibility, confidentiality, competence evaluation and contractual access to records.

5. Separate review and decision from evaluation as required and control granting, maintaining, extending, reducing, suspending, withdrawing and terminating certification.

6. Maintain accurate public information, certification documentation and enforceable agreements governing claims and marks.

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, finance and impartiality controls
02	Scheme documents and scheme-owner authority
03	Product/process/service scope matrix and normative specifications
04	Evaluator, reviewer and decision-maker competence records
05	Testing, inspection and other evaluation arrangements
06	Representative application, evaluation, review, decision and surveillance files
07	Certificate, licence and mark-control arrangements
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 17065:2012
- ISO/IEC 17011:2017
- ISO/IEC 17067 and ISO/IEC TR 17026, as relevant
- Applicable scheme-owner, regulatory and IAF documents

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.