Rules Governing Management System Certification		
Document No: IGC-P-RGMSC		**Revision No: 03**
ISO GLOBAL CERTIFICATION **Drafted By:** Managing Director **Date of Review:** 2026-11-02	**Purpose**	To define clear, enforceable certification rules covering application, auditing, independent decisions, continuing certification and client obligations.
	Scope	IGC management-system certification services and all applicant/certified clients, schemes, sites and personnel within authorised scope.
	Reference	ISO/IEC 17021-1:2015; IGC-P-CBMS; applicable current IAF mandatory documents and applicable accreditation-body conditions only within IGC's verified authorisation and scope. Clauses 8 and 9; IAF MD 1:2023, MD 2:2023, MD 4:2025, MD 5:2023, MD 11:2023 and MD 22:2023 as applicable.
	Responsibility	Top Management and the designated competent personnel specified in this procedure.

1. Purpose

To define clear, enforceable certification rules covering application, auditing, independent decisions, continuing certification and client obligations.

2. Scope

IGC management-system certification services and all applicant/certified clients, schemes, sites and personnel within authorised scope.

3. References and scheme applicability

ISO/IEC 17021-1:2015; IGC-P-CBMS; applicable current IAF mandatory documents and applicable accreditation-body conditions only within IGC's verified authorisation and scope. Clauses 8 and 9; IAF MD 1:2023, MD 2:2023, MD 4:2025, MD 5:2023, MD 11:2023 and MD 22:2023 as applicable.

ISO/IEC 27001:2022 including Amendment 1:2024 defines client ISMS requirements; ISO/IEC 27006-1:2024 supplements ISO/IEC 17021-1 for ISMS certification bodies. IGC's ISO/IEC 27001 certification is not accredited and carries no accreditation mark.

4. Responsibilities and publicly accessible information

Top Management controls and communicates certification rules and the legally enforceable client agreement. Competent reviewers, auditors and decision-makers apply scheme-specific requirements. Clients maintain effective systems, provide access and accurate information, and comply with certification and mark conditions.

Make information about the certification process, rights/duties, complaints/appeals and suspension/withdrawal publicly accessible. IGC confirms the certification status of a client on request, subject to confidentiality. ISO itself does not certify organisations.

5. Application, agreement and audit programme

Use IGC-F-CA applications, IGC-F-APPR application review and IGC-F-AGQ agreement/quotation, including review of scope, sites, personnel, risks, legal requirements, competence, impartiality and audit time. An applicant becomes a client once an IGC client number is allocated. Applications not progressed within 30 days are archived, with a reminder sent on day 25.

Establish the initial two-stage audit and subsequent programme using IGC-F-AP. Stage 1 assesses readiness, scope, documentation and preparation; Stage 2 evaluates implementation and effectiveness. Stage 2 is normally scheduled about one month after Stage 1, adjusted to the client's readiness and any changes.

Apply IGC-P-MDCP and IGC-P-MSSP. ICT use requires suitability, security, agreement and achievement of audit objectives under IAF MD 4:2025. Apply OH&S controls under MD 22 and the relevant audit-time requirements.

6. Audit evidence, findings and independent decision

Provide auditors access to relevant sites, personnel, records and outsourced activities within scope; arrange observers where required. Auditors record objective evidence and findings, not assumed conformity. Use the existing audit reports, evidence uploads, NCRs and technical-review records.

IGC shall not grant initial certification until major nonconformities are corrected and corrective actions verified. For minor nonconformities, review and accept the correction/corrective-action plan as required before the decision. When corrections/corrective actions for major findings cannot be verified within six months after the last day of Stage 2, conduct another Stage 2 before recommending certification.

Technical review and certification decisions shall be performed by competent authorised personnel independent of the audit. Use IGC-F-TRCO and IGC-F-CERTD. An audit is put forward for a certification decision only after it has taken place and its technical review has been accepted; transfer audits also require a completed pre-transfer review.

Nonconformities are normally due for closure within 80 calendar days after the last audit day, and audit reports are due within seven days after the audit. These timeframes never allow a certificate to be issued before sufficient evidence is available.

7. Certificates, surveillance and recertification

IGC-F-CERT shall identify the certified legal entity, applicable standard/edition, scope, relevant sites, decision/issue and expiry information, and the certification body. Management-system certification does not certify products, services or processes. Accreditation wording/symbols are limited to verified authorisation and scope.

First surveillance shall occur within 12 months of the initial certification decision. Surveillance shall occur at least once per calendar year except in recertification years; address performance, changes, complaints, corrective action, internal audit, management review and certification claims.

Plan recertification before certificate expiry and evaluate the full cycle and current effectiveness. Significant changes may require Stage 1. Where recertification is not completed in time, apply ISO/IEC 17021-1 expiry/restoration rules; restoration within six months is conditional on completion of outstanding recertification activities, otherwise at least Stage 2 is required. Certification validity is never backdated.

8. Changes, scope reduction, suspension and withdrawal

Clients shall promptly notify IGC of legal/ownership/management, address/site, process, scope and significant system changes affecting conformity. Use IGC-F-CCN and IGC-F-SCR; assess additional audit or amended programme/certificate needs.

Suspend for persistent or serious failure, failure to permit required audits or voluntary suspension as applicable. Certification is temporarily invalid while suspended; require cessation of misleading promotion and define conditions for restoration. Suspension does not exceed six months.

Failure to resolve suspension conditions leads to withdrawal or scope reduction as appropriate. Scope reduction shall exclude persistently nonconforming parts consistently with scheme requirements. On withdrawal, cease certification/mark use and update status; records of the certification are retained.

9. Transfers, mark use and appeals

Apply IAF MD 2:2023 only for eligible accredited certification, with competent pre-transfer review; suspended certification is not eligible for transfer. Review accreditation/MLA scope, certificate status, reports, findings, complaints and outstanding obligations; this forms part of the application review. Other applications require the appropriate initial certification route.

Use IGC-P-UOCL for logo artwork, authorised claims, prohibited uses, monitoring and enforcement.

Use IGC-P-ACHP for independent complaints/appeals and IGC-F-CF, IGC-F-AF and IGC-R-CAR for cases. No discrimination is permitted.

10. ISMS-specific application

For ISO/IEC 27001, review ISMS scope, organisational interfaces, outsourced processes, risk assessment/treatment, Statement of Applicability and justified Annex A exclusions. Plan sufficient competent audit coverage of the ISMS and applicable controls using ISO/IEC 27006-1:2024; protect sensitive evidence and consider secure ICT and on-site feasibility.

An ISO/IEC 27001 certificate does not certify every product or guarantee absence of security incidents. Certificates are issued against the current edition of the standard, following applicable transition requirements.

11. Document control and records

Maintain this governing procedure in IGC-R-DOC, the Document Register. Certification records are kept in IGC’s digital forms and registers and retained in line with IGC-P-RORP. Keep access controlled and changes traceable.

Top Management reviews adequacy and authorises release through the controlled-document process.