IGS‑C Assessor & Trainer Accreditation Programme v1.3

Document type: Normative / procedural guidance
Standard family: GCR‑M – Governance & Cyber‑Risk Reference Model
Edition: 1.3 – Nov 2025
Status: Published
Audience: Individual assessors, architects, trainers, accredited organisations, regulators, regional partners

1. Purpose and scope

This document defines how **individual experts** become and remain accredited under the IGS‑C framework, in particular:

- Assessors and architects who perform GCR‑M/OSPCRM‑based reviews;
- Trainers who teach GCR‑M/OSPCRM and prepare candidates for Tier accreditation;
- The relationship between individual Tiers (T3–T0), existing certifications (ISO, CREST, OSCP, etc.) and organisational accreditation.

The design goal is to make the programme **credible but attainable**:

- demanding enough that regulators and large institutions can trust Tier labels;
- realistic enough that practitioners in emerging markets and public sectors can participate;
- explicitly built **on top of** existing, widely recognised certifications rather than attempting to replace them.

2. Roles and tiers

2.1 Role types

IGS‑C recognises three primary individual roles:

1. **Assessor / Architect** – applies GCR‑M/OSPCRM to real organisations, systems and solutions;

2. **Trainer** – delivers structured training programmes and prepares candidates for Tier accreditation;

3. **Contributor** – participates in the evolution of the standard (e.g. T0 experts feeding empirical data and models).

The same person may hold more than one role, but **conflicts of interest must be managed** (e.g. an assessor who is also a vendor architect must disclose this fact when assessing related solutions).

2.2 Capability tiers (T3–T0)

Tiers describe capability, not job title. They apply to **assessors and trainers**; contributors at T0 are a subset of T0 assessors.

- **T3 – Single‑path specialist (Governance OR Technical)**
  – Governance path: ISO‑style and regulatory audits, policy and control reviews.
  – Technical path: security testing, code/config review, exploit paths.
  – Requires collaboration with other Tiers for full GCR‑M/OSPCRM coverage.

- **T2 – Integrated practitioner (Governance AND Technical)**
  – Bridges governance and technical perspectives.
  – Leads end‑to‑end assessments where risk must be explained to both boards and engineers.

- **T1 – Strategic architect (Governance + Technical + Architecture)**
  – Designs and evaluates architectures that remove kill‑chains rather than merely patching vulnerabilities.
  – Uses decision matrices and roadmaps aligned with GCR‑M/OSPCRM.

- **T0 – Strategic AI contributor (Gov + Tech + Arch + AI/Data)**
  – Adds AI/data‑science competence.
  – Co‑designs and critiques models used in governance and risk tools.
  – Contributes to the evolution of GCR‑M/OSPCRM based on empirical evidence.

Trainers are graded by the **highest Tier they are authorised to train for**:

- A **T3 Trainer** can prepare candidates for T3;

- A **T2 Trainer** can train for T2 and below;
- A **T1 Trainer** can train for T1 and below;
- A **T0 Trainer** can train for all Tiers, including AI/data-oriented curricula.

3. Baseline prerequisites

3.1 Relationship to existing certifications

Tiers are **overlays**, not substitutes. IGS-C expects candidates to already have solid foundations:

- **Governance** – ISO/IEC 27001 LI/LA or equivalent; ISO 27005/ISO 31000; sector-specific compliance where relevant;
- **Technical security** – CREST, OSCP, GIAC, CompTIA Security+/PenTest+ or equivalent hands-on certification;
- **Architecture (T1/T0)** – TOGAF, SABSA or equivalent, or a demonstrable track record in solution/enterprise architecture;
- **AI/Data (T0)** – formal training in machine learning or data science plus applied work on risk, detection or attack-path modelling.

Where candidates do not hold formal certifications but can demonstrate equivalent competence (e.g. long-standing Big-4 audit practice, regulator role, well-documented open-source contributions), IGS-C may recognise **equivalence** through a documented Recognition of Prior Learning (RPL) process.

3.2 Cross-cutting accreditation requirements

For any Tier, accreditation requires at minimum:

1. **IGS-C approved training** on GCR-M/OSPCRM and related profiles;
2. **Practical and theoretical examination**, including case-based questions;
3. **Documented real-world case** where the candidate applied the model (more cases expected for higher Tiers);

4. **Ethics and independence** commitment, with binding code of conduct;
5. Agreement to **periodic renewal** including continuing professional development (CPD).

For T2 and above, the candidate must also produce a **defended case report**. For T1/T0, at least one engagement must have undergone **external scrutiny** (e.g. Big-4 review, recognised audit firm or regulator assessment) to demonstrate that the candidate's reasoning withstands challenge.

---

4. Tier-specific criteria (assessors)

4.1 T3 – Single-path specialist

Scope: Governance-only or technical-only.

Prerequisites:

- Meets baseline governance or technical certification requirements in Section 3;
- Completed IGS-C foundational training (GCR-M/OSPCRM fundamentals);
- At least one year of post-certification practice in their chosen path.

Assessment:

- Written exam focused on their chosen path (governance or technical), with GCR-M/OSPCRM terminology;
- One documented case showing how they:
  – mapped their existing methods to GCR-M concepts; and
  – produced outputs that can be consumed by the complementary path (e.g. governance-ready reporting for a technical specialist);
- Ethics questionnaire and interview.

Limitations:

- May not lead full GCR-M/OSPCRM assessments alone;
- Must work under or alongside at least a T2 assessor for integrated engagements.

4.2 T2 – Integrated practitioner

Scope: End-to-end assessments where governance, technical and operational perspectives must be reconciled.

Prerequisites:

- Meets both governance and technical baselines;
- At least three years of combined governance/technical practice;
- Evidence of working on at least one project where they mediated between technical and non-technical stakeholders.

Assessment:

- Scenario-based written exam requiring translation between technical findings and risk narratives;
- Two documented cases showing:
  – integrated analysis (pathways, controls, governance decisions);
  – prioritisation of structural mitigations over isolated fixes;
- Defended report (live or recorded) in front of an IGS-C panel;
- Ethics and independence review.

Authorisation:

- May lead most GCR-M/OSPCRM assessments;
- May be designated as lead assessor on Level 2 (Independently assessed) conformance engagements.

4.3 T1 – Strategic architect

Scope: Complex architectures, structural change programmes, design of target states.

Prerequisites:

- Meets T2 criteria;
- Architecture baseline (TOGAF/SABSA or equivalent track record) validated;

- Experience leading at least one architecture review or design project that addressed systemic security risks.

Assessment:

- Architecture-focused exam, including:
  – trust boundaries;
  – authentication/authorisation patterns;
  – identity flows, SCIM/SSO patterns;
  – cloud/on-prem and hybrid patterns;

- Defended architecture case: candidate must present how their design removed or reduced key kill-chains;

- Evidence that at least one such engagement stood up to external challenge (e.g. regulator or external audit).

Authorisation:

- May lead Level 3 certification engagements for organisations with significant architectural complexity;

- May chair technical design reviews and decision boards related to GCR-M/OSPCRM.

4.4 T0 – Strategic AI contributor

Scope: AI-augmented governance and risk, model design and validation, data-driven improvement of the standard.

Prerequisites:

- Meets T1 criteria;

- Formal training in data science/ML;

- Demonstrated work on models related to security, risk, detection or attack-path analysis.

Assessment:

- Technical exam on AI/data topics relevant to GCR-M/OSPCRM;

- Defended model or analytic pipeline used in practice (e.g. scoring model, detection algorithm, advisory engine);
- Evidence of collaboration with other roles (governance, architecture, operations) to ensure that AI outputs remain auditable and accountable.

Authorisation:

- May advise IGS‑C committees on AI‑related aspects of the standard;
- May participate in evaluation and Tiering of T0 solutions;
- May co‑author methodological updates based on empirical data.

5. Trainer accreditation

5.1 General requirements

Trainer accreditation ensures that training programmes prepare candidates **realistically** for their intended roles and Tiers.

All Trainers must:

- Be accredited at **at least the Tier they intend to train for**;
- Demonstrate basic pedagogical skills (prior teaching experience, formal trainer certification, or equivalent);
- Use IGS‑C approved or recognised training materials, or have their bespoke materials reviewed;
- Commit to fair assessment practices and transparent marking criteria.

5.2 Tier‑specific trainer expectations

- **T3 Trainer:**
  – May deliver foundational GCR‑M/OSPCRM training and T3‑level courses;
  – Focuses on helping candidates anchor GCR‑M concepts in their existing governance or technical practice.
- **T2 Trainer:**
  – May deliver T2 and below;

– Must be able to illustrate integrated cases where governance and technical evidence collide;
– Encourages cross-disciplinary thinking and communication.

- **T1 Trainer:**
 – May deliver architecture-focused curricula (T1 and below);
 – Teaches decision matrices, design trade-offs and patterns aligned with the standard;
 – Uses real or realistic architecture examples from multiple sectors.

- **T0 Trainer:**
 – May deliver AI/data-oriented curricula;
 – Must be able to explain model assumptions, validation, bias and governance in non-technical terms;
 – Works closely with governance and legal experts when teaching AI-driven decision support.

5.3 Monitoring trainers

- Trainer accreditation is reviewed at renewal;

- Feedback from candidates and accredited organisations may be considered;

- Repeatedly poor outcomes (e.g. systemic exam failures, misaligned expectations) may trigger a review of trainer accreditation.

---

6. Renewal, CPD and suspension

6.1 Renewal

- Individual accreditation is normally valid for **three years**;

- Renewal requires evidence of **continuing professional development (CPD)** and **recent practice**;

- For higher Tiers, at least one relevant engagement within the last two years is expected.

6.2 CPD expectations

Examples of CPD activities:

- Participation in relevant conferences, workshops, or IGS-C working groups;
- Publication of case studies, papers or guidance notes;
- Delivery of internal training or mentoring (for higher Tiers, particularly T1/T0);
- Participation in external audits or regulatory reviews related to GCR-M/OSPCRM.

6.3 Suspension and revocation

Accreditation may be suspended or revoked in cases of:

- Proven ethical breaches or misrepresentation of Tier;
- Systemic conflicts of interest not disclosed;
- Gross negligence in assessment work leading to material harm;
- Criminal convictions or regulatory findings incompatible with the role.

Suspensions and revocations are noted in the **public registry**, with a short explanation where legally possible.

IGS-C Membership & Organisational Accreditation Guide v1.0

Document type: Governance and membership guidance
Edition: 1.0 – Nov 2025
Status: Draft for consultation
Audience: Regional councils, regulators, public authorities, corporates, audit firms, training providers, civil society, academia

---

1. Purpose and scope

This guide explains:

- The **membership categories** within IGS-C;

- How organisations can become **accredited members** and what that implies;
- How organisational capability tiers (T3–T0) and conformance levels (L1–L3) interact;
- How governance, voting and independence are protected from vendor or geopolitical capture.

The aim is to make membership and accreditation **transparent and predictable** for external observers, including regulators and the public.

---

2. Membership categories

IGS‑C distinguishes between **membership** (participation in governance and development) and **accreditation** (ability to deliver training, assessments or certified solutions).

2.1 Regional / founding members

Regional or continental standard bodies (e.g. Pan‑African Standards Council – PASC) may be recognised as **Regional / Founding Members**.

They typically:

- Maintain regional or sectoral profiles (e.g. OSPCRM);
- Represent local regulatory and industry priorities;
- Participate in Steering and Technical Committees;
- Nominate experts to working groups.

2.2 Regulators and public authorities

Central banks, financial and sector regulators, data protection authorities and supervisory bodies may join as **Regulator / Public Authority Members**.

They typically:

- Provide supervisory and legal perspectives;
- Help align GCR‑M/OSPCRM with regulatory expectations;
- May act as observers or active voting members, according to internal rules;

- Do **not** lose any statutory authority by being members; IGS‑C remains a technical coordination space.

2.3 Corporate members

Financial institutions, critical‑infrastructure operators and large enterprises may join as **Corporate Members**.

They typically:

- Adopt GCR‑M/OSPCRM;
- Provide feedback from real‑world implementation;
- May seek conformance or certification for their organisations and solutions;
- May nominate experts to technical working groups.

2.4 Auditors and certification bodies

Independent assurance firms, security assessment companies and certification bodies may join as **Assurance / Certification Members**.

They typically:

- Seek accreditation to deliver IGS‑C assessments and certifications;
- Commit to independence and conflict‑of‑interest rules;
- Participate in refining assessment methods and criteria.

2.5 Academic and civil‑society members

Universities, research centres, NGOs and advocacy groups may join as **Academic / Civil‑Society Members**.

They typically:

- Contribute research, empirical data and critical perspectives;
- Provide user‑centric and societal viewpoints;
- Help monitor the impact of standards on equity, inclusion and rights.

3. Organisational accreditation and tiers

3.1 Organisational capability tiers

Organisations may be accredited at **capability tiers** that mirror the individual Tier logic:

- **T3 Organisation:** able to deliver governance‑only or technical‑only work aligned with GCR‑M/OSPCRM;
- **T2 Organisation:** able to deliver integrated governance+technical work;
- **T1 Organisation:** additionally able to design and review architectures;
- **T0 Organisation:** additionally able to design AI/data‑driven models and solutions.

An organisation’s Tier is constrained by:

1. The **highest Tier of its internal staff** (or permanent associates) in relevant roles; and
2. The **real‑world engagements** it can prove at that Tier.

3.2 Relationship with conformance levels

- An organisation may be **Level 1 (Aligned)** without being an accredited member;
- An accredited T2 organisation may deliver Level 2 assessments for others, provided conflict‑of‑interest rules are respected;
- Only appropriately Tiered and accredited organisations may participate in **Level 3 certification** decisions.

This separation reduces conflicts and makes it clear whether a statement relates to **internal alignment** (L1–L3) or **external capability** (T3–T0).

3.3 Accredited trainers and assessors

Organisations that wish to run official training or certification programmes must:

- Employ or formally mandate sufficient numbers of Tiered assessors and trainers;

- Demonstrate internal quality assurance for training and exams;
- Accept periodic IGS‑C review and, where relevant, shadowing of assessments.

4. Governance, voting and independence

4.1 Governance bodies

Key governance bodies include:

- **General Assembly** – all members; approves major policies and standards;
- **Steering Committee** – provides strategic oversight and resolves conflicts;
- **Technical Committees** – develop and maintain GCR‑M and profiles;
- **Advisory Council** – composed of regulators, academics and civil society.

4.2 Voting rules and safeguards

To prevent capture:

- No single vendor, region or interest group may hold a blocking minority in key votes;
- Regional members have structured representation but cannot unilaterally impose changes on others;
- Regulators may opt for observer status if statutory constraints limit voting, but their input is still formally recorded.

4.3 Conflict of interest and transparency

- Members must disclose potential conflicts (e.g. ownership in vendors, significant commercial dependencies);
- When assessing or certifying members, independence rules apply as for any assessment;
- Minutes of key decisions, including dissenting views, are recorded and summarised publicly.

5. Fees, sustainability and fairness

5.1 Fee principles

Membership and accreditation fees are designed to:

- Cover operational costs (secretariat, infrastructure, coordination);
- Avoid creating pay-to-play dynamics;
- Allow participation from low-income or resource-constrained institutions.

5.2 Reduced fees and waivers

- Regulators and public authorities may benefit from reduced or waived fees;
- Academic and civil-society members may have lower fees or in-kind contribution options;
- Emerging-market institutions may be offered staggered or capped fees to avoid excluding those most impacted by digital risk.

5.3 Transparency

- Fee structures and any changes are published;
- Financial statements are available to members;
- Sponsorship policies ensure that contributions do not translate into undue influence.

6. Anticipated questions and concerns

6.1 "Is membership required to use GCR-M/OSPCRM?"

No. The standard is **openly available**. Membership is about **governance and collaboration**, not access.

6.2 "Does membership guarantee certification?"

No. Conformance and certification are based on evidence and independent assessment. Being a member **does not exempt** an organisation from scrutiny.

6.3 "Can large vendors dominate decisions?"

By design, voting rules, transparency, and multi-stakeholder representation limit the influence of any single actor or group. Critiques and minority positions are formally documented.

IGS‑C Compatibility & Conformance Claims Policy v1.0

Document type: Legal / policy guidance
Edition: 1.0 – Nov 2025
Status: Draft for consultation
Audience: Vendors, integrators, marketing teams, accredited assessors, legal and compliance teams

---

1. Purpose

This policy defines **how organisations and solutions may describe their relationship to IGS‑C standards**, including GCR‑M and regional profiles such as OSPCRM.

It aims to:

- Protect users, regulators and buyers from misleading claims;
- Allow fair and accurate descriptive use of IGS‑C terminology;
- Clarify when the use of phrases such as "implements", "compatible", "conformant" or "certified" is appropriate.

---

2. Definitions

For the purposes of this policy:

- **"Implements GCR-M"** – the product or process uses GCR-M concepts internally (e.g. for modelling risk or structuring reports) but has not been formally evaluated by IGS-C.
- **"Compatible with GCR-M" / "GCR-M compatible"** – the product or process demonstrably aligns with GCR-M concepts and interfaces, and this has been verified by an independent Tiered assessor.
- **"Conformant with GCR-M"** – the organisation or solution has undergone a structured assessment against GCR-M/OSPCRM criteria with satisfactory outcome.
- **"Certified"** – the organisation or solution has achieved **Level 3** certification under the IGS-C Conformance & Certification Criteria and is listed as such in the public registry.

These terms are not mere marketing language; they imply different levels of evidence.

---

3. Permitted descriptive uses

3.1 Referring to GCR-M and OSPCRM

Any party may **descriptively** refer to IGS-C standards, for example:

- "Our internal risk methodology is inspired by GCR-M."
- "We map our ISO 27001 controls to OSPCRM for African operations."
- "This report uses the context/pathway/structural control structure of GCR-M."

These statements are acceptable as long as they are **true and not misleading**, and do not imply formal endorsement or certification.

3.2 Claiming "implements GCR-M"

An organisation or solution may state that it **implements GCR-M** if:

- It can provide internal documentation showing how GCR-M concepts are used;
- It does not claim formal evaluation or approval by IGS-C;
- It is willing to share such documentation under NDA with regulators or prospective clients if requested.

4. Controlled claims: "compatible", "conformant", "certified"

4.1 "Compatible with GCR‑M" / "GCR‑M compatible"

These claims are **controlled**. They may only be used when:

- A Tiered assessor (T2 or above) has performed a limited compatibility review;
- A short written statement exists, describing:
  – the aspects of GCR‑M/OSPCRM that were evaluated;
  – any limitations or excluded areas;
- The assessor and scope are recorded in the IGS‑C registry.

Compatibility is **not** equivalent to full conformance or certification.

4.2 "Conformant with GCR‑M" / "Conformant with OSPCRM"

These claims require a broader assessment:

- The organisation or solution has undergone a structured assessment against relevant GCR‑M/OSPCRM criteria;
- Gaps have been identified and either remediated or clearly documented as accepted risks;
- A formal report exists and can be made available to regulators or clients under appropriate confidentiality;
- The result and scope are recorded in the IGS‑C registry.

Conformance may map to **Level 2 (Independently assessed)** or **Level 3 (Certified)** depending on the depth of the review.

4.3 "Certified by IGS‑C" / "IGS‑C Level 3 certified"

These claims are reserved for:

- Organisations and solutions that have achieved **Level 3** certification;

- Assessments carried out by accredited organisations and Tiered assessors;
- Entities explicitly listed as "Certified" in the public registry.

Any use of the word "certified" in connection with IGS-C, GCR-M or OSPCRM **must** correspond to a specific registry entry.

5. Examples

5.1 Acceptable claims

- "Deep Advisor implements the GCR-M risk language to generate contextual remediation plans."
- "Deep InfoSec has been assessed as a T0 organisation under IGS-C criteria."
- "Our African operations are OSPCRM-conformant (Level 2), as independently assessed by a T2 assessor."
- "This training uses GCR-M structure but is not an official IGS-C accreditation course."

5.2 Unacceptable or misleading claims

- "IGS-C certified" when no Level 3 certification exists in the registry;
- "Official IGS-C architecture" stated by a vendor for proprietary reference architectures without formal review;
- "Compliant with all IGS-C requirements" without specifying scope or profile;
- Using IGS-C logos to imply endorsement of a non-assessed product.

In cases of doubt, organisations should err on the side of **more precise wording** and consult the secretariat.

6. Enforcement and revocation

6.1 Monitoring

IGS-C may:

- Periodically review public claims by vendors and organisations;
- Act on reports from regulators, clients or competitors about potential misuse.

6.2 Responses to misuse

Possible responses include:

- Private clarification request;
- Public clarification where necessary to avoid user confusion;
- Suspension or revocation of accreditation or certification;
- Legal action in cases of repeated, intentional misuse of names or marks.

6.3 Cooperation with regulators

Where misleading claims may impact regulated sectors (e.g. financial services, healthcare, critical infrastructure), IGS-C may inform relevant authorities so they can take appropriate supervisory action.

End of document.