IGS-C Conformance & Certification Criteria

Document type: Normative guidance

Standard: GCR-M – Governance & Cyber-Risk Reference Model
Edition: 1.3 - Nov 2025

(Previous Version: 1.2 / Nov 2023)
Status: Published
Intended audience: Regulators, supervisors, accredited assessors, corporate risk and security leaders, solution vendors, regional standards bodies

---

1. Purpose and scope

This document defines the **conformance and certification criteria** for:

1. Organisations implementing the **GCR-M** model and regional profiles such as **OSPCRM**;
2. **Individuals** (assessors, architects, trainers) applying the model in practice;
3. **Solutions and tools** (e.g. Deep Advisor) that claim compatibility with GCR-M/OSPCRM; and
4. **Accredited organisations** (audit firms, training providers, regional bodies) delivering assessments and training.

Its objectives are to:

- Provide a **clear, auditable framework** for determining conformance;
- Make it possible to differentiate between **levels of maturity** (L1–L3) and **capability tiers** (T3–T0) without creating unnecessary barriers;
- Ensure that IGS-C certifications remain **independent, technically rigorous and vendor-neutral**; and
- Anticipate typical concerns from regulators, auditors and practitioners (e.g. overlap with ISO, risk of vendor capture, practicality in constrained environments).

This document does **not** replace legal or regulatory requirements. Instead, it provides a common technical and governance language that can sit on top of existing frameworks (ISO 27001/27005, ISO 31000, NIST CSF, GDPR, DORA, NIS2, AU/Malabo, etc.).

---

2. Key concepts and relationship to existing frameworks

2.1 Conformance levels (L1–L3)

Conformance levels describe **how far an organisation has gone** in applying GCR-M/OSPCRM:

- **Level 1 – Aligned**
  The organisation uses GCR-M/OSPCRM as a **reference model**. It can show internal mappings to applicable frameworks and regulations, but has not yet undergone an independent assessment.

- **Level 2 – Independently assessed**
  A recognised assessor has reviewed governance, model documentation, metrics and operations. The organisation can demonstrate that GCR-M/OSPCRM is **actually applied**, not only mentioned on slide decks.

- **Level 3 – Certified**
  The organisation or product has passed a formal certification programme, including **on-site or remote evidence review**, interviews and sampling of practice. There is **periodic surveillance** and possible spot checks.

Conformance levels apply primarily to **organisations and solutions**. Individual experts are instead characterised by capability **tiers** (below).

2.2 Capability tiers (T3–T0)

Capability tiers describe **depth and breadth of competence** across governance, technical security, architecture and AI/data science. They are not a replacement for existing certifications; they sit **on top** of them.

- **T3 – Single-path specialist (Governance OR Technical)**
- **T2 – Integrated practitioner (Governance AND Technical)**
- **T1 – Strategic architect (Governance + Technical + Architecture)**
- **T0 – Strategic AI contributor (Governance + Technical + Architecture + AI/Data)**

Tiers apply to individuals, organisations and solutions with role-specific criteria defined below.

2.3 Relationship with ISO, NIST and similar frameworks

IGS-C does not attempt to replace widely adopted frameworks. Instead:

- GCR-M/OSPCRM **re-uses the good parts** of ISO/NIST (terminology, control families, risk management logic) and provides a more precise language for:

    - attack paths and kill-chains;
    - structural vs. incidental risk;
    - measurable risk reduction over time.

- Conformance assessments are designed to be **compatible with existing audits**. An IGS-C assessment is intended to:

    - complement ISO 27001 certification, not duplicate it;
    - provide **extra visibility** on where ISO-compliant programmes still leave exploitable kill-chains;
    - help regulators prioritise **systemic risks** rather than purely control-by-control checklists.

To avoid duplication, this document explicitly states where it expects **evidence that is already commonly produced** for ISO/NIST and where additional artefacts are required.

---

3. Conformance levels for organisations

3.1 Level 1 – Aligned

An organisation is considered **Level 1 (Aligned)** if it meets all of the following:

1. **GCR-M/OSPCRM mapping**

    - There is a documented mapping between GCR-M/OSPCRM components and the organisation's existing frameworks (ISO/NIST/regulatory).
    - This mapping identifies **where the organisation already meets GCR-M expectations** and where gaps remain.

2. **Minimum governance adoption**

    - Senior management has formally endorsed the use of GCR-M/OSPCRM as a **reference model** for digital risk.
    - Risk committees or equivalent governance bodies receive at least one **annual report** structured according to GCR-M concepts (context, pathways, structural controls, metrics).

3. **Initial metrics**

    - The organisation can provide at least a **basic set of metrics** that relate technical events (vulnerabilities, incidents) to governance decisions (risk acceptances, control changes).

Evidence examples:

- Internal mapping document (GCR-M/OSPCRM → ISO/NIST/regulation);
- Board or committee minutes referencing GCR-M/OSPCRM concepts;
- Sample risk or incident reports structured in line with GCR-M.

3.2 Level 2 – Independently assessed

An organisation may claim **Level 2 (Independently assessed)** if, in addition to Level 1 criteria, the following conditions are met:

1. **Assessment by recognised assessor**

    - A Tier-graded assessor or assessment team, recognised by IGS-C or an accredited regional body, has performed a **structured review** of:
        - governance artefacts (policies, decision records, risk reports),
        - technical evidence (logs, vulnerabilities, architectures),
        - metrics and trend reports.

2. **Evidence of application**

    - The assessor's report shows concrete examples where GCR-M has influenced decisions:
        - risk acceptance or rejection based on pathway analysis;
        - structural control changes (e.g. enforcing adaptive auth, consolidating identity flows);
        - prioritisation of systemic mitigations over isolated patching.

3. **Documented remediation logic**

    - For at least one major risk theme, the organisation can demonstrate **how remediation actions were selected and sequenced** using GCR-M logic, and how they changed the attack surface.

4. **Management response**

- Management has formally responded to the assessor's findings and committed to a **follow-up cycle**.

Evidence examples:

- Independent assessment report referencing GCR-M/OSPCRM;
- Clear trail illustrating how GCR-M-based analysis changed at least one significant decision;
- Management letter, action plans, and follow-up commitments.

3.3 Level 3 – Certified

Level 3 (Certified) is reserved for organisations that demonstrate steady, consistent application of GCR-M/OSPCRM in operations and decision-making.

In addition to Levels 1 and 2, the organisation must:

1. **Undergo a full certification assessment**

    - The assessment is conducted by a recognised certification body or consortium of assessors with **appropriate Tier capability** (see Section 4).
    - The assessment includes:
        - document review;
        - interviews with governance, technical and business stakeholders;
        - sampling of real projects/incidents;
        - verification of metrics and how they are used.

2. **Demonstrate longitudinal evidence**

    - There is at least **12 months of traceable evidence** showing:
        - how GCR-M/OSPCRM metrics and analysis are used to steer change;
        - how risk posture evolved across that period;
        - where hypotheses failed and were corrected.

3. **Integrate with existing frameworks**

    - Where the organisation is already ISO 27001/NIST aligned or certified, the assessment confirms that GCR-M/OSPCRM is **not just an added layer of bureaucracy** but a way to:
        - rationalise control sets;
        - justify investment;
        - focus on kill-chain elimination and systemic weaknesses.

4. **Agree to surveillance**

    - The certification is valid for a defined period (normally 3 years) with **annual surveillance**.
    - Surveillance checks focus on **drift**: whether the organisation is still applying GCR-M/OSPCRM as designed.

---

4. Capability tiers for individuals, organisations and solutions

4.1 Baseline prerequisites for individuals

Tiers T3–T0 describe capability, not seniority. Meeting a Tier's criteria is a **baseline**, not an automatic accreditation.

Relationship to existing certifications
Tiers assume that candidates already meet recognised industry baselines and then build on top of them to ensure consistent application of GCR-M/OSPCRM.

- **Governance prerequisites** (depending on role):
  – ISO/IEC 27001 Lead Implementer or Lead Auditor (or equivalent);
  – ISO 27005 / ISO 31000 or recognised risk certification;
  – Sectoral governance/compliance certifications as relevant.

- **Technical prerequisites** (for technical paths):
  – CREST, OSCP, GIAC, CompTIA Security+/PenTest+ or equivalent;
  – or demonstrable, independently validated penetration-testing / security engineering practice.

- **Architecture prerequisites (T1 and above):**
  – TOGAF, SABSA or equivalent; or
  – proven solution/enterprise architecture track record.

- **AI/data prerequisites (T0):**
  – formal training in machine learning/data science;
  – applied work on risk, anomaly detection or attack-path modelling.

Additional IGS-C-specific requirements apply at each Tier (practical exams, defended reports, ethics).

4.2 Tier definitions for individual assessors

- **T3 – Single-path specialist (Governance OR Technical)**
  – Governance path: can perform governance and ISO-style audits, map controls and identify governance gaps.
  – Technical path: can perform security testing, technical reviews and produce technically sound findings.
  – Must work with other Tiers to produce a **full GCR-M/OSPCRM view**.

- **T2 – Integrated practitioner (Governance AND Technical)**
  – Meets governance and technical prerequisites.
  – Can translate technical evidence into risk and remedial plans in GCR-M terms.
  – Leads assessments where **governance and technical realities must be reconciled**.

- **T1 – Strategic architect (Governance + Technical + Architecture)**
  – Meets T2 requirements plus architectural competence.
  – Can design and review architectures that eliminate kill-chains instead of only patching weaknesses.
  – Produces decision matrices and roadmaps aligned with GCR-M/OSPCRM logic.

- **T0 – Strategic AI contributor (Governance + Technical + Architecture + AI/Data)**
  – Meets T1 requirements plus AI/data science competence.
  – Contributes to model design, validation and continuous improvement of risk engines and analytic tools.
  – Helps IGS-C evolve GCR-M/OSPCRM based on empirical evidence.

4.3 Additional cross-cutting requirements for individuals

For all Tiers, the following are required:

1. **Formal training** on GCR-M/OSPCRM and IGS-C principles;
2. **Practical examination** combining case studies and realistic tasks;
3. **Documented real-world experience** applying the model (at least one substantial engagement, more for higher Tiers);
4. **Ethics and independence** obligations, with possible suspension on breach;
5. For T2 and above, a **defended report or short paper** explaining a real or anonymised engagement;
6. For T1 and T0, at least one engagement that has passed **external scrutiny** (e.g. Big Four, recognised audit firm or regulator), showing that their work survives real-world challenge.

These criteria are deliberately rigorous. They aim to ensure that Tier-graded experts have operated in environments where **criticism, cross-examination and constraints are real**, not hypothetical.

4.4 Tiers for organisations and solutions

For organisations and solutions, the Tier corresponds to **the depth of capability they embed**:

- **T3 Organisation/Solution:**
  – Automates or supports either governance or technical aspects of GCR-M/OSPCRM.
  – Uses standardised terminology and basic pathways but does not yet fully integrate all dimensions.

- **T2 Organisation/Solution:**
  – Integrates governance and technical evidence into a **coherent risk story**.
  – Attack paths, vulnerabilities and structural controls are analysed together.
  – Outputs are consumable by both technical and governance audiences.

- **T1 Organisation/Solution:**
  – Architecture-aware: can model systems, trust boundaries and control placements.
  – Can simulate the effect of design decisions on kill-chains.
  – Supports structural redesign, not just incremental fixes.

- **T0 Organisation/Solution:**
  – Embeds AI/data-driven reasoning across governance, technical and architecture dimensions.
  – Learns from incidents, near-misses and control performance.
  – Exposes metrics (e.g. precision, recall, bias indicators) and can be audited.

For organisations, the **highest Tier they may claim** is constrained by the highest Tier of their internal staff and demonstrable engagements at that level.

---

5. Assessment process and evidence

5.1 Principles

IGS-C assessments are guided by five principles:

1. **Evidence-based:** assertions must be supported by artefacts, not slogans;
2. **Context-aware:** the assessment must recognise environmental constraints and regulatory context;

3. **Non-duplication:** existing audits and certifications are leveraged whenever possible;
4. **Transparency:** the reasoning from evidence to conclusions is documented;
5. **Proportionality:** the burden of proof scales with the level and Tier sought.

5.2 Typical assessment stages

1. **Scoping**
   – Define which legal entities, services, profiles (e.g. OSPCRM) and systems are in scope.
   – Identify existing audits (ISO, internal audit, regulator reviews) that can be reused.

2. **Document and evidence review**
   – Governance documents (policies, risk methodologies, committee minutes);
   – Technical artefacts (architectures, logs, vulnerability reports, incident records);
   – Metrics and dashboards used by management.

3. **Interviews and workshops**
   – With governance, risk, security, architecture and operations teams;
   – Where feasible, with business and front-line staff impacted by controls.

4. **Analysis and mapping**
   – Apply GCR-M/OSPCRM to the evidence:
   – identify key pathways and kill-chains;
   – distinguish structural from incidental risk;
   – assess coverage and gaps.

5. **Findings and recommendations**
   – Prioritise systemic issues and explain trade-offs;
   – Show how recommendations relate to frameworks and regulation.

6. **Validation and challenge**
   – Review findings with stakeholders;
   – Confirm factual accuracy;
   – Document disagreements and residual risks.

7. **Certification decision and surveillance plan** (for L3)
   – Independent decision based on assessor report;
   – Defined surveillance frequency and scope.

---

6. Surveillance, renewal and revocation

6.1 Surveillance

For Level 3 certifications and higher Tiers:

- Surveillance is typically **annual**, with the possibility of more frequent reviews in higher-risk contexts.
- Focus is on **drift**: whether the organisation or solution continues to apply GCR-M/OSPCRM as described at certification time.

6.2 Renewal

- Certification is normally valid for **three years**, subject to satisfactory surveillance.
- Renewal requires: – updated evidence of practice;
  – demonstration of how lessons learned (including failures) have been integrated;
  – confirmation that key personnel (for high Tiers) are still active or that successors have equivalent competence.

6.3 Revocation and suspension

Grounds for revocation or suspension may include:

- Misrepresentation of conformance or Tier;
- Systematic ethical breaches or conflict-of-interest violations;
- Persistent refusal to remediate critical structural risks without justified rationale;
- Proven misuse of IGS-C names or marks.

Revocations and suspensions are recorded in the **public registry**, with a short explanation where legally permissible.

---

7. Governance, independence and conflict of interest

7.1 Independence of assessors

To maintain trust:

- Assessors and certification bodies must be **independent** from the organisations and solutions they assess, except where explicitly permitted under transparent rules (e.g. internal audit using IGS-C internally but not awarding public certification).

- Any commercial relationships, shared ownership or other potential conflicts must be **disclosed** and, where necessary, lead to recusal.

7.2 Protection against vendor capture

To avoid capture by any single vendor, region or consortium:

- IGS-C standards and criteria are developed through **multi-stakeholder processes**, with clear voting rules;
- No single vendor or group of vendors may unilaterally approve changes;
- Regional bodies (such as PASC) are recognised as profile editors, not as exclusive gatekeepers;
- All normative documents remain **publicly accessible**.

7.3 Transparency to regulators and the public

- Certification criteria and processes are public, enabling regulators and independent experts to scrutinise them.
- The registry of certified organisations, individuals and solutions is public, with clear Tier and Level indications.
- Where possible, anonymised case studies illustrate how IGS-C assessments have corrected misaligned risk perceptions.

---

8. Anticipated questions and concerns

8.1 “Is this just another layer of bureaucracy on top of ISO?”

Response by design:
GCR-M/OSPCRM conformance is intentionally built on top of existing frameworks. The criteria:

- Re-use existing artefacts whenever possible;
- Focus on **how** decisions are made and justified, not on re-checking every control;
- Add value in areas where ISO/NIST often remain generic (attack paths, structural controls, risk metrics).

8.2 “Are you competing with regulators or replacing their authority?”

Response by design:
No. IGS-C provides a **technical and governance language** regulators can use if they wish. It:

- Does not create new legal obligations;
- Helps regulators interpret technical evidence more consistently;

- Can be referenced in supervisory guidance or expectations without locking regulators into a proprietary model.

8.3 “How do we avoid Global North bias?”

Response by design:
The model is designed so that **regional profiles** (e.g. OSPCRM) are maintained by regional bodies who can encode their own priorities, legal constraints and risk realities. IGS-C’s role is to:

- Provide a backbone language (GCR-M);
- Ensure technical soundness and interoperability;
- Leave room for regional sovereignty and context.

8.4 “Isn’t T0 too ambitious for most organisations?”

Response by design:
Yes – and it is **supposed** to be ambitious. T0 is intended for a small number of organisations and solutions that genuinely operate at the intersection of governance, technical security, architecture and AI/data science. Lower Tiers (T3–T2–T1) are the typical path for most actors.

8.5 “Why link higher Tiers to external audits (Big Four, regulators, etc.)?”

Response by design:
This requirement is not to privilege any particular firm, but to ensure that Tier-graded work has faced **real-world challenge**. External scrutiny provides:

- A reality check on assumptions;
- Evidence that the assessor can defend their reasoning under pressure;
- Additional confidence for regulators and clients.

Appendix A – Example tier prerequisites table (individuals)

Tier	**Focus level**	**Governance baseline (must have)**	**Technical baseline (must have / strong rec.)**	**Architecture baseline (must have / rec.)**	**AI / Data baseline (must have / rec.)**
T3	Single-path specialist (Gov **or** Tech)	**Gov path:** ISO/IEC 27001 LI/LA or equivalent;	**Tech path:** CREST / OSCP / GIAC / CompTIA	Not required	Not required

Tier	Focus level	Governance baseline (must have)	Technical baseline (must have / strong rec.)	Architecture baseline (must have / rec.)	AI / Data baseline (must have / rec.)
		ISO 27005/ISO 31000	Sec+/PenTest+ or equiv.		
T2	Integrated practitioner (Gov + Tech)	ISO/IEC 27001 LI/LA; ISO 27005/ISO 31000 or equivalent	At least one hands-on security cert (CREST, OSCP, GIAC, PenTest+, etc.)	Experience working with real architectures (documented projects)	Basic literacy in data-driven security & risk metrics
T1	Strategic architect (Gov + Tech + Architecture)	Same as T2	Same as T2	TOGAF / SABSA or equivalent, or proven solution/enterprise arch track	Familiarity with AI-assisted security tools & model outputs
T0	Strategic AI contributor	Same as T1	Same as T1	Same as T1	Formal ML / data-science training plus applied work on risk/attack-path models

---

End of document.