Audience: Regulators, supervisors, accredited assessors, implementers, vendors

---

1. Purpose

This document provides a **transparent record of changes** to key IGS-C standards and normative documents:

- **GCR-M – Governance & Cyber-Risk Reference Model**
- **OSPCRM – Pan-African Sovereign Risk Profile & mappings**
- **IGS-C Conformance & Certification Criteria**

It is designed so that:

- Regulators and auditors can see **what changed, when and why**;
- Implementers can judge **backward compatibility**;
- No “silent changes” occur in PDFs between versions.

---

2. Version summary tables

2.1 GCR-M – Governance & Cyber-Risk Reference Model

Version	Date	Change type	Summary	Compatibility impact
1.0	Nov 2025	Initial release	First public version of the GCR-M core standard.	N/A (baseline)

(Future versions of GCR-M will be added to this table as they are released.)

2.2 OSPCRM – Pan-African Sovereign Risk Profile & mappings

Version	Date	Change type	Summary	Compatibility impact

1.0	Nov 2025	Initial release	First official OSPCRM profile and GCR-M mapping.	N/A (baseline)

2.3 IGS-C Conformance & Certification Criteria

Version	Date	Change type	Summary	Compatibility impact
1.0	Nov 2022	Initial release	First publication of conformance levels (L1–L3) and general approach.	N/A
1.1	May 2023	Minor clarification	Clarified evidence expectations for Level 2 vs Level 3.	Backward compatible; no change to existing certifications.
1.2	Nov 2023	Structural update	Introduced capability tiers (T3–T0) and basic ties to ISO/NIST.	Backward compatible; may require mapping updates.
1.3	Nov 2025	Major refinement	Refined tier prerequisites, added AI (T0), tightened independence rules.	Backward compatible; surveillance cycles unaffected.

---

3. Detailed entry – Conformance & Certification Criteria v1.3

Document: IGS-C Conformance & Certification Criteria
New version: 1.3 – Nov 2025
Previous version: 1.2 – Nov 2023
Change type: Major refinement (but backward-compatible)

3.1 Motivation

- Integrate lessons learned from early pilot use of GCR-M/OSPCRM in projects and audits;
- Clarify how tiers T3–T0 build on top of ISO/CREST/TOGAF etc. (not in competition with them);
- Make independence and conflict-of-interest handling more explicit (for regulators and Big-4).

3.2 Key changes

1. Tier prerequisites hardened, but clarified as overlays

- Explicit governance, technical, architecture and AI baselines are now listed.
- Text emphasises that tiers **build on** existing certifications and real-world practice.

2. Defended report / external scrutiny requirement

- For T2+ individuals and higher-tier organisations, at least one engagement must have faced **external challenge** (Big-4, regulator or equivalent).
- This was implicit in v1.2; it is now explicitly normative.

3. Surveillance and revocation clarified

- Section 6 expanded to clarify grounds for suspension/revocation and what appears in the public registry.

4. Criticism-by-design section strengthened

- New subsections address concerns about bureaucracy, regulatory overlap, Global North bias and T0 realism.

3.3 Impact on existing accreditations and certifications

- No immediate invalidation of existing Level 2 / Level 3 certifications or Tier labels.
- During **next renewal**, existing Tiered individuals and accredited organisations are expected to:
    - demonstrate that their prior experience already satisfies the clarified criteria; or
    - present additional evidence (e.g. documented external audit, defended report).

---

4. Change recording rules

To maintain trust:

1. Every normative document must carry a **version and date** on its front page.
2. Every version increment (including minor clarifications) must appear in this **change log** (or a specific change log for that document).
3. For **major changes** (new sections, tightened requirements), IGS-C publishes:
    - a short **“What’s new”** paragraph in the document itself; and
    - an explicit note on **compatibility** (e.g. does it change certification criteria?).
4. Historical versions remain **archived and accessible** for at least 10 years, so that regulators and courts can see which version was in force at a given date.

End of change log text.

Réflexion en cours