GCR-M – Governance & Cyber-Risk Reference Model v1.3

Document type: Core standard (normative)
Edition: 1.3 – Nov 2025
Status: Published
Editor: IGS-C Technical Committee

---

1. Introduction

GCR-M is a governance and cyber-risk reference model designed to provide a single, precise language for digital risk across governance, technical and architectural levels. It centres analysis on attack paths and kill-chains, distinguishes structural from incidental risk, and supports measurable risk reduction over time.

GCR-M sits on top of existing frameworks (ISO 27001/27005, ISO 31000, NIST CSF, GDPR, DORA, NIS2, AU/Malabo, etc.) and is technology-agnostic (on-prem, cloud, hybrid, outsourced).

2. Model structure

The model is organised into seven domains:

- **CX** – Context & Scope
- **AS** – Assets & Services
- **TH** – Threats & Actors
- **PW** – Pathways & Kill-Chains
- **CT** – Controls & Design
- **MT** – Metrics & Evidence
- **OP** – Operational Integration

Each element has an identifier (for example, `PW.2` – Critical Attack Path Identification) to support mappings and tooling.

3. CX – Context & Scope

CX.1 – Business & mission context

- CX.1.1 – Define mission and critical outcomes.
- CX.1.2 – Identify core value chains.
- CX.1.3 – State digital risk appetite in concrete terms.

CX.2 – Regulatory and contractual context

- CX.2.1 – List applicable laws and regulations per jurisdiction.
- CX.2.2 – Capture key supervisory expectations.
- CX.2.3 – Identify contractual digital-risk obligations.

CX.3 – Structural environment

- CX.3.1 – High-level enterprise architecture.
- CX.3.2 – Trust boundaries and zones.
- CX.3.3 – Critical dependencies and providers.

4. AS – Assets & Services

AS.1 – Critical services and processes

- Inventory critical business services.
- Map supporting processes and systems.
- Assign impact ratings to each service.

AS.2 – Information and data assets

- Identify key data categories per service.
- Document data residency and sovereignty constraints.
- Map data flows between systems and third parties.

AS.3 – Identity, roles and privileges

- Define identity domains (human, machine, service).
- Map critical roles and privileges.
- Identify toxic combinations enabling kill-chains.

5. TH – Threats & Actors

TH.1 – Threat categories

- External adversaries.
- Malicious insiders.
- Accidental insiders.
- Third-party compromise.

- Environmental / systemic threats.

TH.2 – Motivations and capabilities

Rate motivations, capabilities and likely attack styles for each relevant actor type, to inform pathway feasibility rather than generic lists.

6. PW – Pathways & Kill-Chains

PW.1 – Pathway modelling

- PW.1.1 – Identify entry conditions.
- PW.1.2 – Map steps (privilege escalation, lateral movement, etc.).
- PW.1.3 – Define end conditions (harmful outcomes).

PW.2 – Critical attack paths

- Identify a limited set of critical attack paths to severe outcomes.
- Link each path to threats, services and controls.
- Prioritise kill-chain elimination over generic risk scoring.

PW.3 – Structural vs incidental contributors

- Structural contributors: architectural features, trust assumptions, identity models.
- Incidental contributors: patch levels, misconfigurations, local process failures.

7. CT – Controls & Design

CT.1 – Structural controls

- Identify structural controls per critical path.
- Document how they break or weaken steps in the path.
- Avoid designs that create end-to-end kill-chains even when patch scores look good.

CT.2 – Contextual and operational controls

- Hardening, patching, logs, monitoring, processes, training.
- Explain how these interact with structural controls.

CT.3 – Control patterns and reference architectures

Use patterns (identity, SCIM, remote access, etc.) and justify how they influence pathways.

8. MT – Metrics & Evidence

MT.1 – Structural risk metrics

- Number of critical paths fully broken.
- Dependency on fragile controls.
- Pathway density to key outcomes.

MT.2 – Operational performance metrics

- Detection and response performance.
- Control health indicators.

MT.3 – Evidence quality

Assess data completeness, blind spots, log quality and auditability.

9. OP – Operational Integration

OP.1 – Governance integration

Feed GCR-M outputs into risk committees, internal audit and investment decisions.

OP.2 – ITSM, SOC and DevSecOps integration

Link tickets, changes and incidents to pathways and controls; prioritise changes that close critical paths.

OP.3 – Continuous improvement

Update pathways after incidents, challenge assumptions via red teams, and feed lessons into architecture and investment plans.

10. Criticism and limitations

GCR-M is designed as an overlay, not a replacement for ISO/NIST, and can be applied incrementally. It deliberately forces structural vs incidental distinctions and requires explicit recording of assumptions so that assessments and regulators can challenge them.