

EKSELENS · SYSTEM OF PROOF

# Model Risk Management Framework

Prepared for Framework v1.0 · 06 Jul 2026

Powered by the ENTERPRISE360 reinvention engine — 12 value streams · 21 sectors · 20 business archetypes.

Organisations lack model **visibility** — which becomes a model-risk problem the moment regulators, customers or boards demand evidence that cannot be produced. This framework treats models as **risk objects, not deliverables**, captures evidence at every lifecycle gate, names human accountability (owner, challenger, sponsor) and is audit-ready by default via the evidence graph. Model risk is a mechanism that corrupts other risks.

## The seven disciplines

---

- Inventory before governance — no model unregistered; every model has a Model Card before build, buy or deploy.
- Risk-tiering before controls — controls scale with risk tier; proportionate effort.
- Independent challenge before deployment — challenger organisationally separate from the developer.
- Evidence continuity through the lifecycle — an unbroken evidence graph from data to decision.
- Human accountability at every material output — named owner, challenger and sponsor.
- Continuous monitoring, not annual review — in-flight, calibrated to model class and tier.
- Decommissioning as a governed event — retirement with rigour; a gate, not a deletion.

## Risk tiering

---

Control effort is proportionate to consequence. A model is scored 1–5 on seven impact dimensions (financial, customer, regulatory, reputational, operational, complexity, data sensitivity); the **highest single dimension sets the tier**.

- Tier 1 Critical — board-visible; regulatory decision / customer detriment; P&L > £50m.
- Tier 2 High — executive-visible; material customer / operational impact; P&L £10–50m.
- Tier 3 Moderate — function-visible; process automation, limited discretion; £1–10m.
- Tier 4 Low — team-visible; analytical support; < £1m.
- Tier 5 Sandbox — development / research only; not in production.

## The governed lifecycle — seven gates

| GATE                             | ACCOUNTABLE  | EVIDENCE                                                |
|----------------------------------|--------------|---------------------------------------------------------|
| <b>G1 Business justification</b> | Sponsor      | Problem statement, intended use, provisional tier       |
| <b>G2 Data suitability</b>       | Owner + Data | Data lineage, quality, lawful basis                     |
| <b>G3 Design review</b>          | Owner        | Design note, assumptions log, limitation register       |
| <b>G4 Independent validation</b> | Challenger   | Validation report, challenger sign-off, dissent log     |
| <b>G5 Deployment approval</b>    | Sponsor      | Complete Model Card, approval record → ERIO risk object |
| <b>G6 In-flight monitoring</b>   | Owner        | Monitoring records, breach/ action log                  |
| <b>G7 Decommission</b>           | Sponsor      | Dependency map, retirement approval, audit tail         |

## The Model Card

The single record of a model and the exchange format into ERIO — complete at G5. A model without a complete Model Card cannot be deployed. Mandatory fields include model ID/version/tier, purpose, named owner/challenger/sponsor, class & technique, data lineage, assumptions & limitations, fairness assessment, performance metrics (dev/current/threshold), monitoring plan, regulatory scope, evidence-graph pointer, ERIO risk-object ID and approval history. Generative models add prompt template/version, guardrail config, retrieval-source tiers and safety-evaluation results.

## Continuous monitoring

- Cadence by tier — Tier 1 daily · Tier 2 weekly · Tier 3 monthly · Tier 4 quarterly.
- Supervised ML — PSI/KS for drift; AUC / calibration for performance.
- Generative — grounding rate, hallucination rate, guardrail triggers, safety evaluation.
- Breaches raise an automatic ERIO event routed to the independent challenger.

## Regulatory alignment

Designed to satisfy the substance of SR 11-7, PRA SS1/23, the EU AI Act (high-risk), ISO/IEC 42001, ISO 31000 and the NIST AI RMF. The mapping is a live control matrix in the evidence graph.

---

An asset of the Ekselens System of Proof. Applied via EKSELENS360 and Enterprise360; operated in steady state via ERIO. Companion diagnostic: the Evidence Graph Maturity Model. Not legal or regulatory advice.

---

Powered by EKSELENS360 · Confidential — for the named client only. Figures are indicative until validated with the client.