Executive Summary

Enterprise GenAI & Agentic AI Governance and Evaluation Framework

Key Problem Solved: Bridging the gap between AI innovation and enterprise risk, enabling organizations to move beyond "POC purgatory" into safe, auditable production. Enables faster approvals with auditable controls, without sacrificing safety, sovereignty, or privacy.

Purpose and Scope

This is a practical, enterprise-ready governance framework designed to evaluate, approve, and safely operationalize Generative AI (GenAI) and Agentic AI systems. It is built for regulated and high-impact environments, and for leaders accountable for AI outcomes—not just model performance.

Applies to:

- Enterprise GenAI applications (internal or client-facing)
- Decision-support systems that influence legal/financial/operational outcomes
- Agentic AI systems with bounded or conditional autonomy
- High-impact environments requiring auditability, accountability, and controlled execution

Out of scope by design:

- Research-only prototypes and academic benchmarking
- Open-ended consumer chatbots without enterprise controls
- Vendor-specific "black box" implementations without enforceable governance

Design Posture (European Enterprise Governance)

Aligned with European enterprise governance best practices, the framework emphasizes:

1. **Risk proportionality:** Governance intensity scales with use-case risk, autonomy, and business impact.
2. **Readiness is not permission:** Numerical scores measure readiness; hard governance gates determine permission to deploy.
3. **Role-based oversight (HITL clarity):** Human-in-the-loop is defined by oversight roles (end-user verification, SME review, independent AI auditor) and includes training evidence where required.
4. **Controlled autonomy (agentic safety):** Conditional autonomy is allowed only within pre-authorized, narrow boundaries; out-of-bounds actions require explicit human authorization.
5. **Sovereignty and vendor resilience:** Vendor/model dependency is treated as a first-class risk dimension, including fallback strategies and jurisdictional controls.
6. **Privacy-by-design logging:** Evidence is replayable and audit-defensible, while ensuring PII redaction before immutability to avoid GDPR risk.

Core Components (What's Included)

Week 1 — Foundation: Scope and positioning, governance philosophy, Tier 1–3 risk classification, 8 evaluation dimensions, decision rights

Week 2 — Scoring and Permission Model: Dimension-level scoring anchors, tier-wise weighting matrix, decision thresholds, and hard governance gates (HITL, auditability, security, sovereignty)

Week 3 — Reference Architecture: GenAI and Agentic reference architectures, guardrails/control plane, schema contracts, audit logging + evidence store patterns (privacy-first, replayable)

Week 5 — Templates Pack: Intake form, scorecard template, gates checklist, minimum controls by tier, audit evidence packet, change control and recertification

Repository: github.com/MadhurKh/enterprise-genai-agentic-governance-framework
Status: v1.0 complete (Weeks 1–11) — governance → enforcement → audit-ready operationalization
Generated: 20 Feb 2026
Author: Madhur Khandelwal

Week 6 — Operating Model: RACI and decision rights, governance cadence, exception management and waivers (System of Record), operational assurance plan, governance KPIs

Week 7 — Adoption Kit + Filled Examples: 30/60/90 adoption playbook, filled intake/scorecard/gates examples, exception register example, context drift recertification example

Week 8 — Enforcement Patterns: Policy-as-code blueprint, internal model gateway pattern, circuit breaker + safe fallback patterns, validation test plan (incl. jailbreak attempts)

Week 9 — Executive and Audit Pack: Executive operating standard, governance board pack outline, EU controls crosswalk, audit-ready evidence index, 2-week Quickstart

Week 10 — Reference Implementation Starter Kit: Rego policy samples, model gateway OpenAPI contract, routing table examples, circuit breaker runbook, alerts/SLO examples, JSONL audit event schemas, tiered release readiness checklist

Week 11 — Implementation Packaging + MVI Walkthroughs: Two-repo pattern (policy vs evidence), System of Record mapping, Tier 2 and Tier 3 “minimum viable implementation” walkthroughs, POLICY/EVIDENCE/RUNBOOK starter templates, executive visuals blueprint

Recommended Enterprise Workflow (How to Use)

1. **Classify:** Assign Tier 1 / Tier 2 / Tier 3 based on autonomy and impact.
2. **Score:** Evaluate across 8 dimensions with evidence maturity; compute weighted readiness score.
3. **Gate:** Apply non-negotiable governance gates (permission). Scores do not override gate failures.
4. **Decide:** Approve / Pilot with Controls / Block–Redesign, with named owners and timelines.
5. **Enforce:** Implement policy-as-code, internal model gateway, circuit breaker safe fallback, and audit logging (privacy-first).
6. **Operate:** Monitor governance KPIs, run drills (Tier 3), manage exceptions in a system of record, and recertify on technical changes or context drift.

Leadership Differentiators

- Audit-defensible governance: Clear separation of readiness scoring from permission gates, with traceable evidence.
- Enforceable controls: Policy-as-code + model gateway abstraction + circuit breaker patterns (fail-closed posture for Tier 2/3 where required).
- Sovereignty-first: Explicit vendor and jurisdictional risk evaluation with routing metadata and fallback requirements.
- Privacy-by-design: Redaction before immutability to avoid “right to be forgotten” log exposure.
- Production realism: Templates, operating model, executive pack, and implementation starter kit to move from POC to governed production.

Repository: github.com/MadhurKh/enterprise-genai-agentic-governance-framework
Status: v1.0 complete (Weeks 1–11) — governance → enforcement → audit-ready operationalization
Generated: 20 Feb 2026
Author: Madhur Khandelwal