# 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.

## Purpose & Scope

A practical, enterprise-ready governance framework designed to evaluate, approve, and safely operationalize **Generative AI** and **Agentic AI** systems. Intended for leaders accountable for AI outcomes in regulated and high-impact environments.

## Design Posture

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

- **Risk Proportionality:** Governance intensity matches the use-case impact.
- **Role-Based Oversight:** Defined layers including end-user verification, SME review, and independent AI auditors.
- **Controlled Autonomy:** Explicit treatment of conditional autonomy (policy-bound and reversible) rather than blanket prohibitions.
- **Vendor & Model Sovereignty:** Built-in evaluation of lock-in risks and tested fallback strategies.

## Framework Components (Current v1)

- **Foundation (Week 1):** Core principles, governance philosophy, Tier 1-3 risk classification, and 8 evaluation dimensions.
- **Scoring & Permission Model (Week 2):** Dimension-level anchors, tier-wise weighting matrix, and Hard Governance Gates that separate technical readiness scores from final permission.
- **Worked Example (Week 4):** Full application to the GenAI Contract Risk Analyzer with Tier 2 classification, weighted scorecard, and a P0/P1/P2 remediation roadmap.

## Recommended Enterprise Workflow

- **Classify:** Assign the use case to Tier 1, 2, or 3 based on risk and autonomy posture.
- **Score:** Evaluate against the 8 dimensions and compute the weighted readiness score.
- **Gate:** Pass the outcome through non-negotiable gates (HITL, auditability, security, sovereignty).
- **Decide:** Issue a decision (Approve / Pilot / Block) and assign owners.
- **Operationalize:** Implement mandatory controls, including quarterly "Red-Button" kill-switch drills for high-risk systems.

## Key Leadership Differentiators

- **Audit-Defensible Governance:** Separates readiness scores from permission gates to ensure transparency and accountability.
- **The "Red-Button" Protocol:** Mandates tested kill-switch and rollback mechanisms for high-risk agentic systems.
- **Sovereignty-First:** Treats vendor dependency and model fallback as first-class evaluation criteria, protecting against API instability.

Repository: github.com/MadhurKh/enterprise-genai-agentic-governance-framework
Status: v1 Complete (Foundation, Scoring, Case Study). Next: Week 3 Reference Architecture - Closing the loop between governance policy and technical enforcement.
Generated: 10 Feb 2026