AI Governance Operating Model and Launch Checklist

Purpose

Define who may decide, what an AI system may do, which evidence and controls are required, and how outcomes remain accountable and reviewable.

How to use this tool

Govern the use case and its role in work, not the model in isolation. Apply controls in proportion to risk. Name one accountable business owner. Complete the operating model before launch, validate controls in the workflow, and continue only while business value and trust remain acceptable.

1. Use-case classification

Use-case name and purpose: ____

Business outcome and friction addressed: __________________________________

Affected users and stakeholders: ____

AI role: INFORM / GENERATE / RECOMMEND / DECIDE / ACT

Scale, frequency, and operating context: __________________________________

2. Risk tier

Tier	Interpretation	Control expectation
1 - Limited	Low-impact, reversible assistance with no material decision or action.	Basic ownership, approved use, privacy, quality, and monitoring.
2 - Managed	Meaningful internal work or recommendation with bounded impact and human review.	Documented evidence, review, escalation, audit, and operating controls.
3 - Material	Customer, employee, financial, legal, safety, or other consequential influence.	Independent control review, rigorous testing, traceability, incident readiness, and launch authority.
4 - Restricted	Impact or uncertainty exceeds approved authority or risk tolerance.	Do not launch until scope, control, or authority changes.

Selected tier: ______ Rationale: ____

3. Accountability and authority

Role	Named owner	Decision right	Evidence or approval required
Accountable business owner		Own outcome and continued use	
Product or service owner		Own operating performance and change	
Data owner		Authorize data use and quality conditions	
Model or technical owner		Own technical configuration and reliability	
Risk, privacy, security, or legal control owner		Approve applicable controls and exceptions	
Launch authority		Approve, condition, pause, or reject launch	

4. Governance operating model

Dimension	Required decision or control	Owner	Evidence	Review trigger
Data and privacy controls				
Model and prompt governance				
Grounding and evidence				
Action authorization				
Monitoring				
Escalation				
Incident response				
Auditability				
Value and outcome review				

5. Action boundaries

The system may: ____

The system may only with human approval: ___________________________________

The system must never: ____

Override, challenge, or escalation path: ___________________________________

6. Launch checklist

[ ] The use case, decision role, affected stakeholders, and business outcome are documented.

[ ] A risk tier is assigned and supported by evidence.

[ ] One business owner is accountable for every material outcome.

[ ] Data use, privacy, security, retention, and access are approved.

[ ] Approved models, prompts, configurations, versions, and change controls are defined.

[ ] Grounding, sources, confidence, and known limitations are visible where required.

[ ] Action authorization and prohibited actions are explicit and tested.

[ ] Human review, override, escalation, and pause mechanisms work in the operating process.

[ ] Monitoring covers quality, drift, exceptions, control performance, trust, and business outcomes.

[ ] Incident detection, containment, notification, correction, and restart authority are established.

[ ] Material inputs, outputs, decisions, approvals, actions, and exceptions can be reconstructed.

[ ] Continued use depends on acceptable value and risk evidence.

Launch decision

Decision: APPROVE / APPROVE WITH CONDITIONS / PAUSE / REJECT

Conditions and limitations: ____

Launch authority: _____________________ Decision date: ___________________

Review cadence and next review: ____

Stop, correction, or retirement triggers: __________________________________

