AnovaCloud

FREE PRACTITIONER PACK

AI Governance & Risk Pack

Readiness checklist — 20 checks across 5 categories. Nothing proceeds until every box is honestly ticked.

Pack	AI Governance & Risk Pack
Document	Readiness checklist (20 items)
Use	Gate reviews · phase entry criteria · go/no-go
Date	2026-09

AnovaCloud — Engineering the AI-Native Enterprise. Frisco, Texas. This pack is a working instrument, not a brochure: complete it with your team, score honestly, and bring it to your discovery call.

INVENTORY & TIERING

Inventory & tiering

- [ ] **AI register live**
  All known AI systems inventoried with owner, data, model, and surface; reviewed quarterly.
- [ ] **Risk tiers assigned**
  Every system tiered; high-risk list current and visible to leadership.
- [ ] **Shadow-AI detection**
  Intake/procurement hooks catch new adoption; employee guidance published.
- [ ] **Prohibited uses defined**
  Restricted use cases documented and communicated; exceptions require written approval.

CONTROLS BY TIER

Controls by tier

- [ ] **Tiered control matrix**
  Controls (assessment, testing, approval, monitoring) mapped per tier — proportional, not uniform.
- [ ] **Pre-deployment gates**
  High-risk systems cannot launch without assessment sign-off; gate evidence retained.
- [ ] **Data-rights checks**
  Training/fine-tuning data cleared for rights, consent, and retention before use.
- [ ] **Third-party diligence**
  Vendor AI assessed: DPA, model card, security review, and exit plan on file.

TESTING & MONITORING

Testing & monitoring

- [ ] **Eval thresholds set**
  Per-system metrics and launch thresholds documented for high-risk systems.
- [ ] **Red-team cadence**
  High-risk systems red-teamed before launch and on material change.
- [ ] **Production monitoring**
  Drift, misuse, and incident triggers monitored with alerting.
- [ ] **Human oversight live**
  Approval/override mechanisms in the path for high-stakes decisions.

INCIDENT & RESPONSE

Incident & response

- [ ] **Incident runbook**
  AI incident definition, severity levels, and response steps published and drilled.
- [ ] **Kill-switch verified**
  Rollback/halt path tested per production system.
- [ ] **Rights handling**
  Explanation/appeal/opt-out workflows operational where required.
- [ ] **Breach notification path**
  Regulatory notification responsibilities and timelines documented.

ASSURANCE & REPORTING

Assurance & reporting

- [ ] **Control evidence retained**
  Assessments, test results, and approvals filed per system for audit.
- [ ] **Board reporting cadence**
  AI risk reported to the board/committee on schedule.
- [ ] **Regulatory mapping current**
  EU AI Act / sector obligations mapped to controls; gaps have owners.
- [ ] **Annual program review**
  Governance program effectiveness reviewed; tiering and controls updated.

SIGN-OFF

Checked means done, not planned

Each category owner initials when every item is complete with evidence attached. Items marked N/A need a written reason — 'not applicable' without justification scores as incomplete.

Inventory & tiering	Owner _____	Date _____
Controls by tier	Owner _____	Date _____
Testing & monitoring	Owner _____	Date _____
Incident & response	Owner _____	Date _____
Assurance & reporting	Owner _____	Date _____