

Data Governance Cheat Sheet

AI adoption succeeds when it is safe, transparent, and aligned to business objectives. The Decide & Govern stage ensures organizations make deliberate, responsible choices about tools, data, and policies before deploying AI into workflows.

Without this stage, organizations risk:

Tool sprawl: Chasing “shiny objects” at growing cost and distraction.

Compliance breaches: Including privacy, IP, and regulatory violations.

Trust erosion: Where employees and customers start to doubt safety.

Governance isn't bureaucracy – **it's the enabler of scale**. By codifying rules early, organizations avoid rework later, prove responsibility to stakeholders, and build a system that sustains adoption

A successful Data Governance strategy enables:

1. Define governance principles and policies (acceptable use, data handling, privacy, ethics).
2. Align governance to neutral frameworks (NIST AI RMF, ISO/IEC 42001) for credibility and comparability.
3. Select AI tools/platforms through a consistent evaluation process.
4. Assess data readiness (availability, sensitivity, quality, access).
5. Produce a governance charter and risk register that will guide pilots and scaling.

A successful Data Governance strategy enables:

1. Define governance principles and policies (acceptable use, data handling, privacy, ethics).
2. Align governance to neutral frameworks (NIST AI RMF, ISO/IEC 42001) for credibility and comparability.
3. Select AI tools/platforms through a consistent evaluation process.
4. Assess data readiness (availability, sensitivity, quality, access).
5. Produce a governance charter and risk register that will guide pilots and scaling.

1. Define governance principles and policies.

- Draft a v1 Acceptable Use Policy for AI e.g., “no sensitive PII (personally identifiable information) in public LLMs”. These types of policies help minimize risk across the organization.
- Define data handling rules: These rules typically cover things like encryption policies, retention and disposal, and access levels.
Establish content/prompt policy: clarify ownership, attribution, plagiarism avoidance.
- Outline ethics principles: transparency, fairness, accountability.

2. Align with neutral standards

- Map policies against NIST AI RMF categories (Govern, Map, Measure, Manage).
- Use ISO/IEC 42001 as a checklist for continuous improvement (ethics, accountability, privacy, quality).
- Identify gaps and remediation steps as needed. Consider other expert opinions to help make adjustments.

3. Evaluate and select tools and platforms

Define evaluation criteria:

- Business fit: Does it solve the prioritized use case?
 - Data fit: Does it handle data securely and compliantly?
 - Governance fit: Logging, auditability, bias testing, version control.
 - Vendor viability: Support, roadmaps, exit strategy.
- Use a Tool Evaluation Matrix (weighted scoring).
 - Document decision rationale for auditability.

4. Assess Data Readiness

- Inventory relevant datasets (structured, unstructured, knowledge bases).
- Classify sensitivity (public, internal, confidential, regulated).
- Verify accessibility (APIs, integrations, permissions).
- Document risks (e.g., PII leakage, bias in historical data).

5. Establish governance body and processes

- Empower the AI Steering Committee (named in Stage 0) to review policies, approve tools, and monitor risk.
- Define meeting cadence (e.g., monthly during pilots, quarterly in scale). Set up escalation paths for security, compliance, or ethical incidents.
- Assign an AI Risk Owner for each use case

Common pitfalls to avoid



Ignoring data risks: Even promising pilots can collapse if data is inaccessible, biased, or sensitive



Over-engineering policies: Avoid creating so many rules that pilots stall; focus on v1 policies you can iterate. At this point, policies should be designed to enable safe scaling and not be so restrictive that they hinder the ability to pilot and explore new use cases.



Skipping standards alignment:

Reinventing governance wastes time; standards already exist. Trying to build entire governance models and policies from scratch is both unnecessary and often a waste of time. Focus on adopting what works from experts who have already blazed the trail.



Choosing tools before rules:

Always finalize governance principles before signing vendor contracts.