DATA GOVERNANCE & SECURITY CHECKLIST

A practical worksheet for organizations preparing for AI adoption, commercialization, operational optimization, data-intensive growth, or technology implementation.

Organization:		**Prepared by:**	
Project / Initiative:		**Date:**	
Review Period:		**Version:**	

Purpose

Use this checklist to evaluate whether the organization has the data governance and security foundation needed to support responsible AI adoption, operational redesign, commercialization, grant-funded growth, or other major change initiatives. The checklist is intended for leadership, technical teams, operational managers, commercialization advisors, and outside consultants who need a practical view of data readiness and risk.

How to Use This Checklist

- Mark each item as Not Yet, In Progress, or Ready based on current evidence, not assumptions.
- Use the Notes / Evidence column to list policies, system owners, documents, data sources, gaps, or follow-up questions.
- Prioritize issues that could affect privacy, security, compliance, intellectual property, AI outputs, funding milestones, or implementation timelines.
- Revisit the checklist before major technology implementation, AI model deployment, investor review, customer launch, or operational scaling.

1. Data Ownership and Inventory

Before AI, optimization, or commercialization work begins, the organization should know what data exists, who owns it, and how it is used.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
Key datasets used by the organization have been identified and inventoried.	[ ]	[ ]	[ ]	
Each important dataset has a clear business or technical owner.	[ ]	[ ]	[ ]	
The organization understands where critical data is stored and how it moves between systems.	[ ]	[ ]	[ ]	
Sensitive, proprietary, customer, clinical, research, financial, or operational data has been categorized.	[ ]	[ ]	[ ]	
Data retention expectations are defined for important records and project files.	[ ]	[ ]	[ ]	

2. Data Quality, Lineage, and Documentation

Poor data quality can weaken AI outputs, operational analysis, commercialization decisions, and reporting to funders or partners.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
Important data sources are reasonably complete, accurate, and current.	[ ]	[ ]	[ ]	
Known data quality limitations are documented and understood by decision-makers.	[ ]	[ ]	[ ]	

The organization can trace the origin of key data used for analysis or AI-enabled workflows.	[ ]	[ ]	[ ]	
Data dictionaries, field definitions, or user notes exist for important datasets.	[ ]	[ ]	[ ]	
Manual data transformations or spreadsheet-based processes are documented where relevant.	[ ]	[ ]	[ ]	

3. Access, Security, and Privacy Controls

Security controls should be practical, documented, and proportionate to the risk level of the data and systems involved.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
User access to sensitive systems and files is limited to appropriate personnel.	[ ]	[ ]	[ ]	
Access rights are reviewed periodically when roles, consultants, or projects change.	[ ]	[ ]	[ ]	
Multi-factor authentication is used for key systems where available.	[ ]	[ ]	[ ]	
Procedures exist for removing access when employees, vendors, or consultants leave.	[ ]	[ ]	[ ]	
Privacy risks are considered before data is shared with AI tools, vendors, partners, or outside consultants.	[ ]	[ ]	[ ]	

4. AI Use, Intellectual Property, and Confidentiality

AI adoption creates new opportunities but also new obligations around data handling, confidentiality, intellectual property, and review.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
The organization has defined which data may and may not be entered into public AI tools.	[ ]	[ ]	[ ]	
Confidential research, IP, trade secrets, grant materials, customer records, and proprietary data are protected.	[ ]	[ ]	[ ]	
AI-generated outputs are reviewed by qualified humans before being used for important decisions or external materials.	[ ]	[ ]	[ ]	
Ownership, confidentiality, and permitted use of data are considered before sharing data with AI vendors or platforms.	[ ]	[ ]	[ ]	
The team understands that AI tools may introduce errors, unsupported claims, or privacy risks if used without governance.	[ ]	[ ]	[ ]	

5. Vendors, Third-Party Tools, and Data Sharing

Data governance should extend beyond internal systems to the vendors, consultants, and platforms that support the organization.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
Vendors and software platforms that handle important data have been identified.	[ ]	[ ]	[ ]	
The organization understands what data is shared with	[ ]	[ ]	[ ]	

outside platforms or consultants.				
Vendor terms, data use restrictions, confidentiality provisions, and security expectations are reviewed when appropriate.	[ ]	[ ]	[ ]	
Data-sharing practices are documented for partners, subcontractors, university collaborators, or commercialization advisors.	[ ]	[ ]	[ ]	
The organization has a process for evaluating new tools before sensitive data is uploaded or connected.	[ ]	[ ]	[ ]	

6. Compliance, Funding, and Documentation Readiness

Data practices should support the broader business and funding pathway, not operate as an isolated technical concern.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
Grant, contract, regulatory, customer, or partner requirements related to data are identified.	[ ]	[ ]	[ ]	
The organization maintains records needed to support reporting, audit, compliance, or milestone review.	[ ]	[ ]	[ ]	
Data management expectations are considered in SBIR/STTR, federal contract, university, or investor contexts where relevant.	[ ]	[ ]	[ ]	
Security and privacy practices are documented well enough to explain to funders, customers, investors, or partners.	[ ]	[ ]	[ ]	
Data governance responsibilities are aligned with the organization's commercialization, funding, and implementation strategy.	[ ]	[ ]	[ ]	

7. Incident Response and Business Continuity

Even small organizations benefit from having a simple plan for data disruptions, access problems, accidental disclosure, or system failure.

Readiness Item	Not Yet	In Progress	Ready	Notes / Evidence
The organization knows who should be notified if important data is lost, exposed, corrupted, or misused.	[ ]	[ ]	[ ]	
Critical files and systems are backed up or recoverable within a reasonable timeframe.	[ ]	[ ]	[ ]	
There is a basic process for documenting and responding to data incidents.	[ ]	[ ]	[ ]	
The organization has considered how data-related disruptions could affect operations, customers, funders, or partners.	[ ]	[ ]	[ ]	
Security and governance lessons are incorporated into future training, SOPs, and implementation planning.	[ ]	[ ]	[ ]	

Quick Score Summary

Use this section after completing the checklist. Count each item marked Ready as 2 points, In Progress as 1 point, and Not Yet as 0 points. The goal is not a perfect score; it is to identify the areas that should be addressed before data-intensive change, AI adoption, commercialization, or operational redesign moves forward.

Category	Score	Priority Level	Immediate Next Step
Data Ownership & Inventory	____ / ____	Low / Medium / High	
Data Quality & Lineage	____ / ____	Low / Medium / High	
Access, Security & Privacy	____ / ____	Low / Medium / High	
AI Use, IP & Confidentiality	____ / ____	Low / Medium / High	
Vendors & Third-Party Tools	____ / ____	Low / Medium / High	
Compliance & Documentation	____ / ____	Low / Medium / High	
Incident Response & Continuity	____ / ____	Low / Medium / High	

Data Governance and Security Action Plan

List the highest-priority gaps identified in this checklist and assign ownership. Focus first on gaps that could create security exposure, compliance risk, data quality problems, AI implementation risk, or delays in commercialization and operational scaling.

Gap / Risk Identified	Action Needed	Owner	Target Date	Evidence of Completion

Discussion Questions for Leadership and Implementation Teams

- What data-related issue could most disrupt this change initiative if left unresolved?
- Which datasets are most important for AI adoption, optimization engineering, commercialization planning, or customer delivery?
- Do current access controls match the sensitivity of the data being handled?
- Are there any gaps that should be resolved before sharing data with vendors, consultants, AI tools, investors, or partners?
- What policies, SOPs, or training materials should be created before the next phase begins?

Additional Notes and Follow-Up Questions

ScienceDocs Support

ScienceDocs helps startups, research teams, and innovation-focused organizations prepare for AI adoption, commercialization, operational optimization, and grant-funded growth. Our change management, AI strategy, commercialization, and optimization engineering services can help organizations review readiness gaps, clarify governance needs, strengthen documentation, and move forward with greater confidence.

Ready to get started? Contact us HERE.