COGNITIVE VIEW

COGNITIVE VIEW

RESPONSIBLE AI FOR BUSINESS

AI Governance Readiness Checklist

1. AI Discovery
2. Data Governance & Management
3. Model Development & Deployment
4. Governance & Risk Management
5. Regulatory & Compliance Alignment
6. Ethics, Fairness & Transparency
7. Ongoing Improvement & Culture
8. Next Steps

This is a brief version of the AI Governance Readiness Checklist, designed to guide you through key steps in AI discovery, documentation, and governance.

You can adapt the structure and level of detail to fit your regulatory environment, organizational needs, and AI maturity.

For a comprehensive version with tools, templates, and examples, reach out to our team or download the full checklist.

1. AI Discovery

Goal: Ensure you have full visibility into where AI is being used.

- **Application Inventory**
  - Catalog all AI or ML-powered applications in use across the organization — including small proof-of-concepts (POCs), internal tools, and pilot projects.
  - Include third-party or SaaS tools with embedded AI features (e.g., chatbots, recommendation engines, sentiment analysis).
  - Don't overlook widely adopted tools like ChatGPT, Microsoft Copilot, Notion AI, or Google Duet AI — even casual use can pose data security or compliance risks.
  - Engage department heads and IT teams to uncover AI adoption that may not have gone through formal approval processes.

- **Model & Pipeline Identification**
  - Document all ML models (in production, test, or research phases).
  - Record the data sources, preprocessing steps, and any external dependencies (APIs, libraries).

- **Shadow AI Detection**
  - Survey teams for any unapproved or "shadow" AI solutions in use.
  - Review procurement processes to detect purchases or subscriptions of unvetted AI services.

- **Department & Use-Case Mapping**
  - Align each AI application with the department or business function (HR, marketing, operations, etc.) that owns it.
  - Capture the primary business purpose or user benefit (e.g., demand forecasting, anomaly detection).

- **Technology Stack & MLOps**
    - Identify the platforms (AWS Sagemaker, Azure ML, Databricks, internal frameworks) used for training and deployment.
    - Document version control systems, CI/CD pipelines, and containerization strategies (Docker, Kubernetes).

2. Data Governance & Management

Goal: Ensure that data powering AI systems is trustworthy, well-governed, and aligned with privacy, security, and regulatory standards.

- **Data Source Classification**
    - Define metrics for data quality (accuracy, completeness, consistency).
    - Use automated checks or manual reviews to detect anomalies pre-training.
    - Document limitations that could impact model performance or risk.

- **Data Quality & Validation**
    - Define metrics for data quality (accuracy, completeness, consistency)..
    - Use automated checks or manual reviews to detect anomalies pre-training.
    - Document limitations that could impact model performance or risk.
- **Privacy & Consent**
    - Ensure compliance with data privacy laws (e.g., GDPR, CCPA, HIPAA).
    - Validate user consent where required and maintain audit trails.
    - Apply data minimization and consider anonymization or pseudonymization.

- **Data Security Controls**
  - Ensure encryption at rest and in transit for data used to train or run AI models.
  - Restrict data access (RBAC) and maintain audit logs for data usage.

3. Model Development & Deployment

Goal: Ensure robust, ethical, and secure models from development through production.

- **Model Design & Requirements**
  - Define clear business objectives and success metrics (accuracy, F1 score, recall, etc.) for each model.
  - Identify potential ethical and risk implications early (e.g., bias concerns, fairness objectives).

- **Versioning & Change Management**
  - Use a version control system for model code, data subsets, and model artifacts.
  - Maintain a change log detailing modifications in features, hyperparameters, or training data.

- **Testing & Validation**
  - Conduct thorough performance evaluation (train/test/validation splits, cross-validation).
  - Test for adversarial robustness, bias, and reliability under different conditions.

- **Monitoring & Maintenance**
  - Set up monitoring for model performance drift, data drift, and concept drift.
  - Establish processes to retrain, recalibrate, or retire models that degrade or become non-compliant.

- **Security & Access Controls**
  - Restrict deployment environments to authorized personnel and maintain logs of model usage or queries.
  - Scan for vulnerabilities in libraries and container images used in the AI pipeline.

4. Governance & Risk Management

Goal: Align AI practices with organizational policies, regulatory requirements, and risk thresholds.

- **Policies & Frameworks**
  - Adopt or align with relevant AI governance frameworks (NIST AI RMF, ISO/IEC standards, OECD principles).
  - Develop or update internal AI usage policies to reflect organizational values and regulatory obligations.

- **Risk Assessments**
  - Conduct structured risk assessments for each AI model or application, using tools like Data Protection Impact Assessments (DPIAs), Algorithmic Impact Assessments (AIAs), or Domain Risk Assessments (DRAs).
  - Evaluate risks across multiple dimensions—such as privacy, security, bias, explainability, and regulatory exposure.
  - Classify AI systems based on impact and likelihood (e.g., low/medium/high risk), and document risk rationales.

  - Establish thresholds for risk tolerance and link each risk level to specific governance actions (e.g., mandatory audits, human-in-the-loop requirements, deployment constraints).
  - Regularly revisit risk profiles, especially when models are retrained, repurposed, or scaled across new use cases or geographies.

- **Roles & Responsibilities**
  - Clearly define who is accountable for AI risk (e.g., AI Risk Officer, Data Steward, Compliance Manager).
  - Establish cross-functional governance committees to oversee AI initiatives.

- **Vendor & Third-Party Oversight**
  - Incorporate AI vendor solutions into your overall vendor risk management process.
  - Require transparent documentation from external vendors on their models, data sources, and compliance posture.

- **Auditability & Documentation**
  - Maintain a centralized repository for all AI documentation, policies, and logs.
  - Conduct regular internal or external audits to verify adherence to standards.

5. Regulatory & Compliance Alignment

Goal: Understand and meet obligations under applicable laws, standards, and industry regulations.

- **Regulatory Inventory**
  - Identify all relevant regulations (EU AI Act, NIST, GDPR, CCPA, HIPAA if in healthcare, etc.).
  - Track emerging AI-specific legislation and sector-specific guidelines.
- **Compliance Gaps & Action Plans**
  - Conduct gap analyses against applicable standards and frameworks.
  - Develop remediation plans with clear owners, timelines, and milestones.
- **Documentation for Regulators**
  - Maintain explainability and traceability documentation for each AI system.
  - Store compliance evidence (e.g., policies, risk assessments, audits) in an easily retrievable format.
- **Incident & Breach Management**
  - Develop procedures for handling security breaches or compliance incidents involving AI systems.
  - Notify affected parties or authorities within the required timeframe, per regulation.

6. Ethics, Fairness & Transparency

Goal: Minimize unintended bias and ensure AI decisions are fair, explainable, and respectful of user rights.

- **Bias & Fairness Testing**
  - Regularly test for protected group bias (gender, ethnicity, age, etc.) and document findings.
  - Utilize fairness metrics (e.g., disparate impact ratio, equalized odds) to assess model outcomes.
- **Explainable AI (XAI)**
  - Provide end users or impacted individuals with understandable explanations of AI decisions when feasible.
  - Use model-agnostic techniques (e.g., LIME, SHAP) or built-in interpretable models for transparency.
- **Consent & User Rights**
  - Allow users to opt-out of AI-driven decisions (when possible) or request human review.
  - Provide mechanisms for users to appeal AI-driven outcomes (e.g., credit applications, job screenings).

7. Ongoing Improvement & Culture

Goal: Embed AI governance into organizational culture and continuously evolve governance practices.

- **Training & Awareness**
  - Deliver regular training on AI ethics, compliance, and risk to technical and business teams.
  - Encourage a culture of responsibility and open communication about AI risks and challenges.
- **Continuous Feedback Loop**
  - Gather feedback from stakeholders (employees, customers, regulators) to improve AI governance.
  - Use retrospectives, post-mortems, and analytics to refine processes and policies.
- **Innovation vs. Governance Balance**
  - Strike a balance between agile experimentation and necessary guardrails.
  - Pilot new AI applications within a “governed sandbox” environment before wider deployment.

8. Next Steps

Run a Self-Assessment
Quickly gauge your organization's current maturity across AI discovery, risk management, and compliance.

Book a Demo of Our AI Governance Platform
Discover What You're Missing : Uncover hidden AI risks, automate documentation, and streamline oversight with a hands-on look at our AI Governance Platform.

Run a Free AI Auto Discovery Scan
Instantly detect hidden AI tools, risks, and shadow usage across your organization—no setup required.

How to Use This Checklist

- Start with a self-assessment: Review each section to understand your current AI governance maturity.
- Assign ownership: Delegate categories to relevant teams (e.g., Data, Legal, Compliance, Engineering).
- Prioritize high-risk areas: Focus on critical gaps first, then build a phased improvement roadmap.

This brief checklist provides a solid foundation for AI discovery and compliance.

Tailor it to your industry, internal policies, and frameworks like NIST AI RMF, ISO 27001, or SOC 2 to enable scalable, robust governance.