

CoTrust

Enterprise AI Governance Handbook

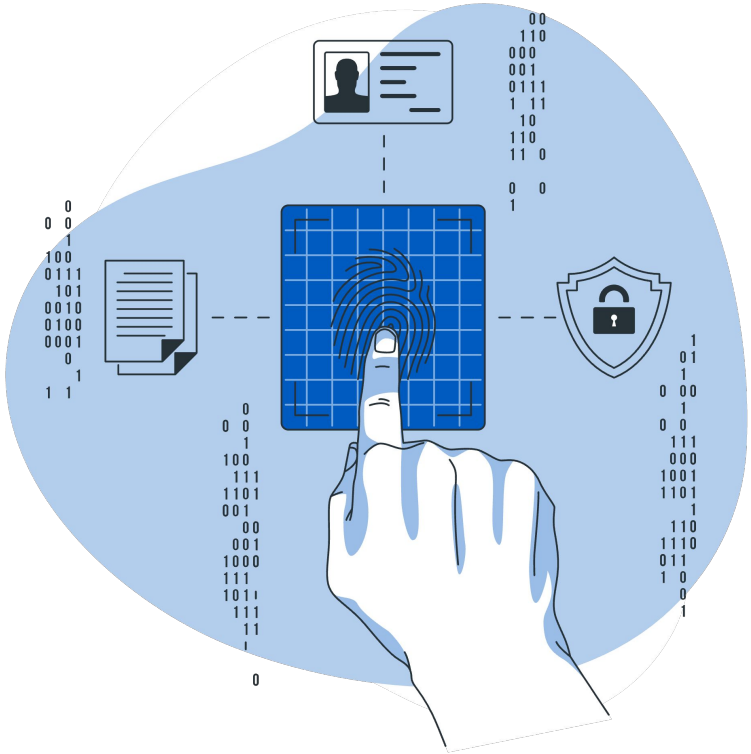
Consented Data for Confident Growth

Powered by

digio

Artificial Intelligence (AI) has the potential to revolutionize business by automating complex tasks, uncovering data-driven insights, and creating new revenue streams. However, without proper controls, AI systems can introduce significant risks, including unintended bias, privacy violations, and regulatory non-compliance. This document aims to:

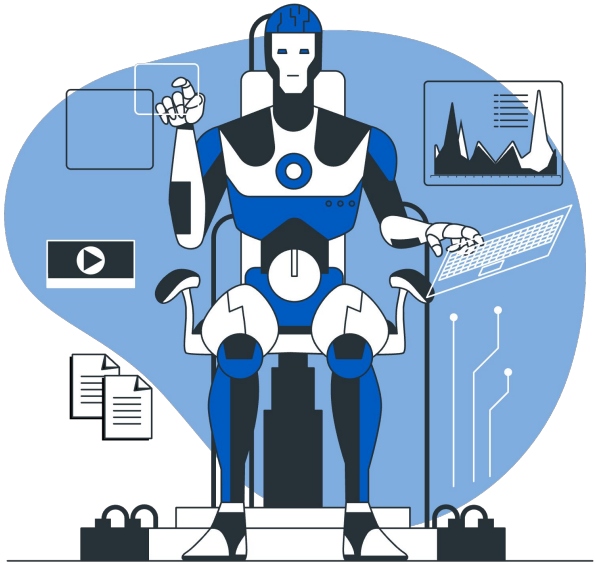
- Define the essential components of an AI governance framework.
- Compare relevant global and national regulations that shape AI oversight.
- Provide a structured approach for embedding governance at every stage, from system design to retirement.



Scope of Responsible AI Governance

Responsible AI Governance encompasses the policies, roles, and procedures that guide AI system development, deployment, monitoring, and decommissioning. Its scope includes:

1. **Policy Framework:** Establishing clear standards and guidelines, along with decision authorities responsible for approving AI use cases and changes.
2. **Process Controls:** Implementing risk assessments, fairness and robustness tests, explainability reviews, and audit trails to ensure ongoing compliance.
3. **Organizational Roles:** Defining responsibilities for data stewards, model developers, compliance officers, and business sponsors to ensure accountability and effective collaboration.



By delineating these dimensions, organizations can systematically manage AI risks while maximizing value creation.

Global Regulatory Landscape

OECD AI Principles have been adopted by 42 member countries to emphasize safeguarding human rights, promoting fairness, and ensuring transparency in AI systems.

The **NIST AI Risk Management Framework (2023)** organizes risk mitigation into four core functions:

- **Govern**: Establish governance structures and policies.
- **Map**: Inventory AI assets and stakeholder roles.
- **Measure**: Quantify risks through metrics and tests.
- **Manage**: Implement safeguards and monitor system performance.

The **EU Artificial Intelligence Act (2024)** introduces a risk-based approach, classifying AI applications into unacceptable, high, limited, and minimal risk categories. High-risk systems must undergo conformity assessments and continuous post-market monitoring.

In the United States, **Executive Order 14028** focuses on AI safety and security, while state-level regulations such as the **Colorado AI Act** require organizations to perform impact assessments for high-risk AI implementations.



India’s Legal & Policy Framework

Information Technology Act, 2000: Establishes the legal basis for addressing cyber offenses, including malicious AI-generated content and identity theft. Organizations must report significant security incidents within six hours.

Digital Personal Data Protection Act, 2023: Mandates privacy-by-design practices and requires **Data Protection Impact Assessments (DPIAs)** before deploying automated decision-making systems that process personal data.

Sectoral Guidelines:

- **Reserve Bank of India (RBI):** Requires banks and their technology providers to adhere to robust cybersecurity standards, including controls for AI service providers.
- **Securities and Exchange Board of India (SEBI)** & **Insurance Regulatory and Development Authority of India (IRDAI):** Enforce data protection measures and vulnerability assessments for AI-driven trading and underwriting models.

Criminal Liability under IPC: The Indian Penal Code now explicitly penalizes data theft, identity fraud, and defamatory AI-generated content.

Emerging Efforts: MeitY’s advisory working groups are drafting India-specific AI governance guidelines, while the IndiaAI Mission promotes research and ethical standards.



digio

Enterprise AI Governance

Core Governance

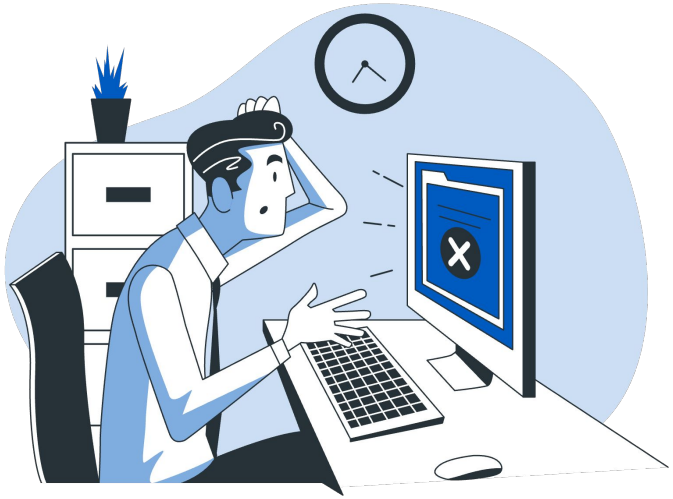
1. **Transparency:** Publish model cards detailing AI system purpose, data sources, performance metrics, and known limitations.
2. **Accountability:** Assign ownership for each AI asset, with clear incident escalation paths and documented decision logs.
3. **Safety & Robustness:** Conduct adversarial testing and define fail-safe mechanisms to ensure reliable performance under unexpected conditions.
4. **Privacy & Security:** Enforce data encryption, access controls, and periodic penetration testing to safeguard sensitive information.
5. **Fairness & Non-Discrimination:** Use statistical fairness tests and representative datasets to detect and correct systemic bias.
6. **Human Oversight:** Maintain human-in-the-loop checkpoints for AI recommendations in high-impact domains, such as credit scoring and medical diagnosis.
7. **Sustainability & Inclusion:** Assess and minimize the environmental impact of AI training processes, and ensure accessibility for diverse user groups.
8. **Digital-By-Design:** Integrate automated policy enforcement tools into development pipelines to ensure continuous compliance.

Model Lifecycle Governance

1. **Design Phase:** Conduct ethical risk screening and data quality assessments before model development begins.
2. **Development Phase:** Perform peer code reviews, run bias detection algorithms, and generate documentation artifacts such as datasheets.
3. **Deployment Phase:** Monitor model performance in production using dashboards that track accuracy, drift, and fairness metrics, while capturing user feedback.
4. **Operation Phase:** Schedule continuous audits and retraining based on monitored anomalies; conduct regular security and privacy assessments.
5. **Retirement Phase:** Archive model artifacts, purge or anonymize data according to retention policies, and transfer knowledge to stakeholders for future reference.

Risk Assessment & Gap Analysis

1. **Use Case Identification:** Catalog all AI initiatives, categorizing them by domain (e.g., financial risk scoring, customer service chatbots).
2. **Risk Taxonomy Application:** Evaluate each use case based on ethical, legal, operational, and reputational impact, assigning quantitative scores.
3. **Gap Analysis:** Compare current governance practices against: global standards (OECD, NIST), national laws (IT Act, DPDP Act), and industry-specific guidelines.
4. **Risk Register Creation:** Compile a centralized register listing high-risk AI systems, their risk scores, current controls, and remediation plans.

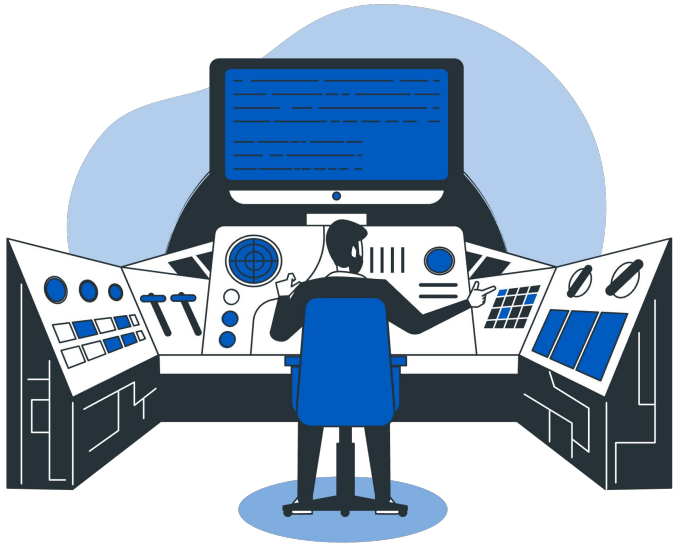


This structured assessment reveals compliance gaps and prioritizes risk mitigation efforts.

Metrics & Continuous Monitoring

To ensure ongoing compliance and performance, organizations should track:

- **Accuracy Drift Rate:** Monitor shifts in model accuracy, targeting a maximum drift of 2% per quarter.
- **Fairness Metrics:** Measure demographic parity and equalized odds, aiming for disparities under 5% across sensitive groups.
- **Incident Counts:** Track the number of critical compliance breaches, striving for zero critical incidents annually.



Implement real-time monitoring dashboards that visualize performance, data drift, and security alerts. Establish a governance audit cadence with quarterly internal reviews and annual third-party assessments. Define incident response SLAs to ensure timely detection, investigation, and remediation of governance issues.



CoTrust

Powered by

digio

Data compliance for Legal teams,

Data Access for Business teams,

Data Privacy for Customers.

Schedule a demo today, Get in touch with us at

Email : bd@digio.in

Ph: 080-69489510