AHEAD

AI Governance and Security

Putting Principles into Practice

AI systems are rapidly transforming how organizations operate, innovate, and compete. But evolving regulations and scrutiny around privacy, fairness, ethics, and transparency make AI compliance increasingly complex. Establishing the processes and tooling needed for continuous oversight of your AI models in production is key to ensuring your organization can scale AI efficiently and with confidence. AHEAD advocates for a flexible, business-aligned approach, drawing from frameworks like ISO/IEC 42001, NIST AI RMF, and the EU AI Act. This whitepaper presents a practical framework for establishing tailored AI governance programs, with room to layer additional frameworks as your program expands.

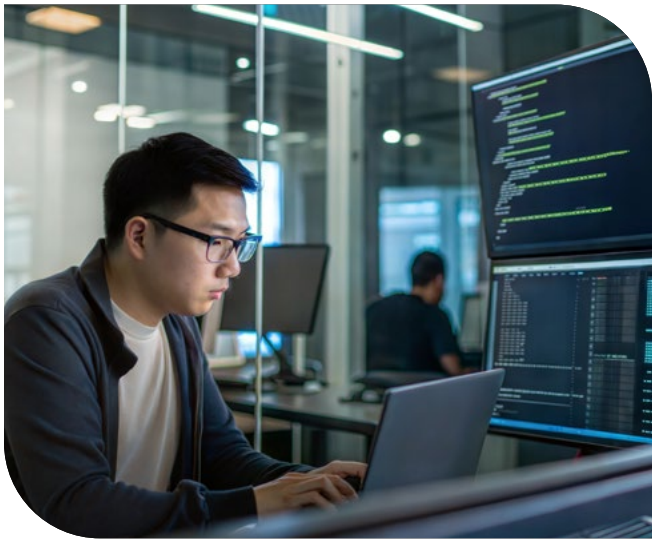
The Case for AI Governance

Traditionally, governance focused on meeting legal requirements and mitigating risks. However, as AI becomes a core driver of digital transformation, governance now holds more strategic significance. AI governance is not just a defensive measure, but a proactive way to create market differentiation. By embedding security, responsibility, ethics, and transparency into AI practices, organizations can foster more substantial stakeholder confidence, unlock new opportunities, and build or further establish themselves as trusted leaders in an AI-driven economy.

But as trust in AI becomes a competitive differentiator, customers and partners are increasingly demanding transparency, security, accountability, and the ethical use of AI. And as each industry has different needs around transparency, security, and ethics, AI governance needs to first and foremost be custom-tailored to an organization's industry and models. How should a healthcare organization protect against model data being exposed externally? How can a finance organization ensure that only the correct internal roles have access to client data even if all roles are utilizing their AI models?

There are tons of questions organizations need to ask themselves to begin constructing an AI governance framework that works for their industry.

As a starting point, though, *all* AI governance frameworks should address:



1. **Bias and fairness issues** that affect decisions related to human beings, such as in hiring, lending, or healthcare.
2. **Privacy concerns** that stem from data collection, inference, and misuse.
3. **Security vulnerabilities** in AI pipelines, models, and supporting infrastructure.
4. **Regulatory uncertainty** that exists due to evolving laws across jurisdictions (global, transnational, national, state and local).

Of course, those four chief concerns are not the end-all, be-all of AI governance. There's an ever-increasing number of emerging AI governance frameworks that organizations can (or must) follow, from the mandatory EU AI Act to the voluntary ISO 42001 standard. Choices around selecting governance frameworks to develop and deploy AI systems securely, responsibly, and ethically keep getting harder.

AHEAD discovered that customers are struggling to implement AI governance effectively because current frameworks lack practical guidance. That's why our AI governance team designed a pragmatic, flexible, and modular AI governance framework to address customers' challenges with implementing AI governance.

A Comparative Overview of AI Governance Frameworks

As a first step, organizations should align their governance practices with relevant frameworks that are tailored to their specific industry, geography, risk tolerance, and maturity level. One framework can serve as the primary core for an AI governance program – it is always possible to interweave elements of others to address secondary AI governance concerns. The chart below describes the strengths and weaknesses of today's most common AI governance frameworks:

FRAMEWORK	DESCRIPTION	STRENGTHS	LIMITATIONS
ISO/IEC 42001	AI Management System Standard	Structured, certifiable, management-focused	New, limited adoption
NIST AI RMF	Voluntary Risk Management Framework	Practical, adaptable, risk-focused	U.S.-centric
OECD AI Principles	High-level policy principles	Broad acceptance, ethical foundation	Not operational
EU AI Act	Risk-tiered regulation for AI systems	Legal force in the EU, sector-specific controls	Rigid, compliance-heavy

A Flexible, Modular Governance Approach by AHEAD

AHEAD's AI Governance framework is grounded in the seven pillars of trustworthy AI: Human Agency and Oversight; Technical Robustness and Safety; Privacy and Data Governance; Transparency; Diversity, Non-Discrimination, and Fairness; Societal and Environmental Well-Being; and Accountability.

Our tailored approach to AI governance begins with three core layers: Strategic, Operational, and Technical. Each layer becomes a fully customizable building block to a complete AI governance program.

Strategic Layer

DEFINING THE AI GOVERNANCE ROADMAP

Every journey begins with a roadmap. AHEAD helps organizations define an AI governance roadmap that covers strategy, mandate, and scope. This involves determining the organization's mandate regarding AI governance, and alignment with the enterprise's values, legal frameworks, and stakeholder expectations. It also establishes clear principles and guidelines for responsible AI and defines the scope of AI governance initiatives, including types of AI systems, applications, and use cases.

ESTABLISHING GOVERNANCE BODIES

AHEAD assists in setting up corporate AI governance bodies and incorporating new policies and procedures. This includes establishing and enhancing AI Centers of Excellence (CoE), which then define roles and responsibilities for responsible AI.

TRAINING AND EDUCATION

AHEAD aids in enabling responsible AI by educating individuals who fund, design, build, and deliver AI solutions on the effects of positive governance of their solutions.

Operational Layer

AI ASSET MANAGEMENT AND RISK ASSESSMENT:

AI Inventory: We facilitate the collection and cataloging of an AI solution inventory across the enterprise. This reduces time-to-implement and time-to-value for subsequent AI projects.

Risk Tiering and Assessment: AHEAD helps implement risk tiering approaches to classify AI use cases based on their risk profiles and conduct comprehensive AI model risk assessments.

Third Party AI Risk Management: We conduct structured reviews of third-party AI models and systems to ensure compliance with ethical standards and frameworks.

Controls and Policy Libraries: We help define controls, policy libraries, and workflows to streamline governance.

PROACTIVE MONITORING AND CONTROLS:

Monitoring: AHEAD operationalizes periodic to continuous monitoring for AI use cases in production environments to identify evolving risks.

Controls: We implement controls to deter data poisoning and ensure data integrity, safeguard user privacy, prevent malicious use, and mitigate "toxicity" in AI outputs.

Procedures: AHEAD implements procedures for data quality, labeling, and model validation.

Methods: We help design methods to monitor model and AI pipeline performance, bias, and model drift.

Technical Layer

AHEAD'S PARTNER PLATFORMS

AHEAD leverages best of breed platforms as components within AI Governance and Compliance Services, creating a connected, end-to-end process for responsible AI. **This includes:**

- Integrating governance and managing associated risks.
- Automating AI discovery and inventory management, risk profiling, and testing, evaluation, validation, and verification.
- Using tools for explainability, robustness testing, and adversarial defense.
- Ensuring data protection and AI-specific security controls.
- Maintaining audit logs and version control.

Key AI Governance Focus Areas

Ethical and Responsible AI

Usage and development is aligned with organizational values and social good

Transparency

Model decisions and limitations should be understandable

Accountability

There is clear ownership and traceability across the AI lifecycle

Privacy and Security

There are safeguards for data protection and preventing model manipulation

Risk Management

The organization performs continuous assessment and mitigation of AI-specific risks

Regulatory Readiness

Ensure preparedness for compliance with ISO 42001, EU AI Act, etc.

AHEAD AI Governance Consulting Services

AHEAD provides a range of services to help organizations operationalize AI governance, **including the following:**

- **AI Governance and Risk Management**
- **Secure AI System Development Lifecycle (SDLC)**
- **Training Data Security and Integrity**
- **Model Security Testing**
- **Governance Compliance and Ethics Alignment**
- **AI Security Training & Awareness**
- **AI Runtime Threat Monitoring**
- **Secure API Endpoints**
- **Model Drift and Shadow AI Detection**
- **Incident Response**
- **Runtime Policy Enforcement**
- **Governance Compliance Auditing and Reporting**

Once your AI governance framework is operational, AHEAD can also help make passing regulatory audits much easier. For organizations with a large compliance footprint, based on the framework(s) your organization aligns to, we can simplify the governance approach so that you can utilize the same data for multiple framework audits. And with our expert capabilities in ServiceNow IRM, we can help simplify the audit required for each framework.

Build Your AI Governance Framework with AHEAD

Organizations deploying AI need more than a check-the-box approach to managing model data and security. They need a governance model that adapts to their business, risk landscape, and innovation goals.

Contact AHEAD **for a free consultation to get started on building your AI governance program that embodies responsibility, security, and ethics.**

AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

Visit us at ahead.com.

National Hubs

CHICAGO
444 W. Lake Street
Suite 3000
Chicago, IL 60606

NEW YORK
500 5th Avenue
Floor 17
New York NY 10010

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583