



AHEAD

Adopting AI Lifecycle
Governance to Deliver
Reliable, Transparent,
and High-Performance
AI Systems

Implementing Comprehensive Governance Throughout the Entire AI System Lifecycle

AI and machine learning adoption continues to grow as computational power increases, large datasets become more available, and machine learning models improve. In fact, nearly half of all businesses now leverage AI compared to just one third in 2019. This has transformed AI from a business experiment into a key aspect of most enterprise strategies.

Despite AI becoming an essential function for enterprises, organizations operationalizing AI still face many challenges related to performance, risk management, and compliance with industry regulations. That's why today's organizations need to implement comprehensive governance throughout the entire lifecycle of AI systems to ensure they're explainable, transparent, and meet performance expectations.

In this whitepaper, we'll discuss the importance of AI governance and the key capabilities required to implement effect governance throughout the entire AI system lifecycle. We'll also cover some of the capabilities AHEAD offers related to AI lifecycle governance.

AI Governance is an Organizational Priority

Evolving Traditional Data Programs to Suit an AI Portfolio



Find

Users across the business and IT can easily identify and catalog AI & ML Models and the underlying code for use and reuse



Understand

AI retention standards, model and analytics purpose (value drivers) and common understanding of the associated risks with improper data use (e.g. model efficacy)



Comply

Ensuring AI fits the organizations ethical and governance guidelines and policies



Trust

Ensuring AI is fit for purpose, of high quality, and certified; models and other solutions fueled by data are developed, tested, used, and monitored appropriately for efficacy and trust



Secure

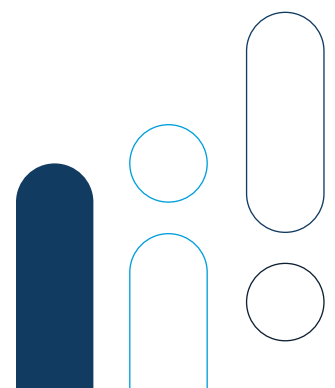
Designing and implementing AI capabilities to manage access and digital threats, address incidents, and maintain privacy

Why Organizations Need AI Governance

AI governance is a process for controlling the implementation and operation of AI systems to meet internal policies and external regulations. AI lifecycle governance takes this a step further by focusing on governance activities across every stage of an AI system — from creation to retirement.

An effective AI governance strategy helps with the following objectives:

- **Achieving adequate AI system performance:** Tracking KPIs related to the development and deployment of AI systems can reduce scope drift, delays in deploying models, and other inefficiencies. Focusing on KPIs related to accuracy, precision, recall, and other performance metrics can also lead to more consistent levels of quality.
- **Meeting internal risk management policies:** Creating risk management policies for designing, developing, and deploying AI systems helps minimize exposure to financial, legal, and ethical issues. A key focus of internal risk management is avoiding the deployment of unexplainable or biased models that could negatively affect customers or the company's reputation.
- **Ensuring compliance with external regulations:** Many organizations — especially those in heavily regulated industries — need to develop AI systems that comply with external privacy and security standards (such as the upcoming European AI Act). This typically requires demonstrating a certain level of transparency for the design, development, and usage of AI models.
- **Quantifying value through qualification:** Organizations should apply their standard risk, cost, and revenue calculators to help measure the value of an AI solution. Using value-based metrics early in the ideation process and comparing to other models in the queue assists with prioritizing resources and driving maximum value.



The AI System Lifecycle

The end-to-end lifecycle of a typical AI system includes the following high-level stages:



1. Ideation

The first stage of the AI system lifecycle is conceptualizing ideas for potential use cases and opportunities to leverage AI. This includes qualifying ideas based on value, validity, and ethical considerations. By defining the objectives and scope of the AI system, it will set the foundation for subsequent development stages.



2. AI Model Creation

The creation of an AI model requires collecting and preparing data, choosing an appropriate algorithm, and iteratively training the model. The model then needs to be tested with new data and validated based on previously defined performance expectations.



3. Deployment & Operation

After an AI model is trained and validated, it is deployed into production. This typically means integrating the AI model into a broader system or application where it can take in new data and make predictions. Once deployed, the AI system needs to be continuously monitored and optimized to ensure it meets performance expectations over time.



4. Retirement

As technology evolves and business requirements change, existing AI models may no longer be useful and should be retired. Switching off an AI system and archiving its inputs, model, and outputs can mitigate the risks associated with outdated models.

Striking the Right Balance in AI Portfolios

Applying the Appropriate Rigor and Control Without Stifling Innovation And Use

Change Factors Driving the Need of AI Governance...



Proliferation
and use of data



Disparate data
landscapes



Spread
of AI use



AI Compliance
and risk



Embedding
trust into AI

Increased Focus on Traditional Data Governance Building Blocks



Scalable operating
model automation



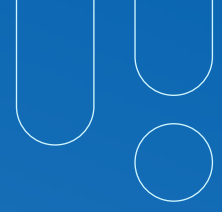
Technology
rationalization



Policies, controls, and risk
management



Change management and
communications



The Key Capabilities of AI Lifecycle Governance

Effectively governing the lifecycle of AI solutions from ideation to retirement requires a number of scalable capabilities:

AI Platform

Selecting, designing, and configuring environments for developing and testing AI solutions. This includes the infrastructure for creating and training AI models, tools for processing data, version control systems, and more.

AI Algorithms & Models

Designing, training and testing AI models to meet performance expectations. This requires tools and expertise for selecting appropriate algorithms for certain use cases, fine-tuning model parameters, and performing other tasks to ensure model efficiency, accuracy, and reliability.

Model Relevance

Ensuring AI models remain relevant, transparent, explainable, and unbiased. This requires measuring and improving the quality of input data for bias, accuracy, and appropriateness. It's also important to test the model for overfitting, concept drift, and model-level bias.

Data Engineering & Operations

Managing the end-to-end data pipeline for AI systems from data collection and preparation to model input. This requires a team of engineers for developing data solutions, automating the data ingestion and curation to feed the AI model, and managing the capacity of the data solution. Data engineering and operations teams are crucial for making adequate high-quality data available to the AI system.

Accountability & Ownership

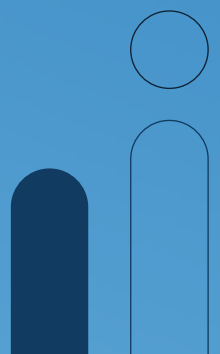
Defining clear roles and responsibilities is important for ensuring accountability and leveraging AI systems effectively. Organizations should assign ownership to cover data governance, model development, model usage, and the overall AI system.

Risk & Compliance

Developing and implementing AI policies is important for minimizing the risks associated with AI systems. This ensures that the AI solution is fully compliant with organizational, regulatory, and legal policies, as well as not creating any risk to the organization or individuals.

Performance Management

Managing AI system performance involves establishing and tracking metrics related to the effectiveness, quality, risk exposure, and performance of AI systems. By continuously monitoring performance metrics, organizations can make sure their AI systems remain effective, safe, and aligned with business requirements over time.



AI Lifecycle Governance

Governing the Lifecycle of AI Solutions, From Ideation to Retirement

AI Lifecycle Stages



Ideation



Stage Gate



AI Model Build



Stage Gate



Operations



Retirement

AI Governance Activities

Gather Ideas

Qualify Ideas
Quantify Value
Prove Ideas

Demonstrate Value

Approve/Reject Ideas
Perform Risk Assessment
Assign Solution Ownership

Ingest and Curate Data

Design and Train AI Model
Test Model and Data Quality
Measure Output Quality and Relevance

Demonstrate Value

Approve/Reject Solution
Perform Risk Assessment

Migrate and Operate AI Solution

Secure Solution
Monitor Performance
Measure Output Quality and Relevance

Test Model Effectiveness and Adoption

Approve/Reject continued use
Retire Solution

Capabilities Required

AI Platform

Environments for Ideation, Engineering, Testing, and Production Operations of AI solutions

AI Algorithms & Models

Ability to design, train and, test AI models

Model Relevance

Ability to ensure the model remains relevant, transparent, explain-able, and unbiased

Data Engineering & Operations

Developing solutions, automating the data ingestion, and curation to feed the AI model, and managing the capacity of the solution

Accountability & Ownership

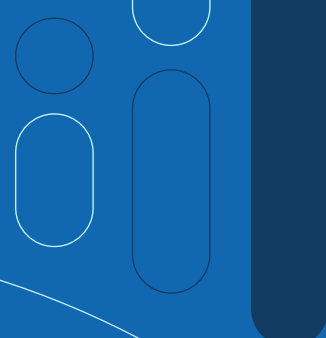
Ensuring clear roles and responsibilities are defined, and assigned to cover data governance, AI model build, data quality assessments, and overarching solution ownership

Risk & Compliance

Ensuring that the AI solution is fully compliant with organization, regulatory, and legal policies, as well as not creating any risk to the organization or individuals

Performance Management

A series of measurements, and metrics to monitor AI solution effectiveness, quality, risk, and performance



Delivering AI Solutions Confidently with AHEAD

Although AI and machine learning can lead to a competitive advantage by transforming data into actionable insights, automating complex business processes, and accelerating innovation, there are still risks associated with new AI solutions. That's why governance across the entire lifecycle of an AI system is crucial for achieving adequate performance while still adhering to internal and external compliance requirements.

AHEAD is a leading provider of enterprise solutions that accelerates the impact of cutting-edge technologies on businesses. This includes services and solutions to streamline the adoption of innovative new capabilities like AI and machine learning. Through workshops, training, strategic guidance, and engineering services, AHEAD helps organizations harness the full potential of AI to improve operational efficiency and stay ahead of the competition without introducing unnecessary risk.

More specifically, AHEAD's approach to designing and developing AI solutions focuses on key areas like AI privacy, security, transparency, risk mitigation, and governance. This includes documenting the potential risks of AI systems, determining where human oversight is needed, assigning accountability for AI model outputs, and defining metrics to gauge acceptable risk. By prioritizing

AI safety, AHEAD allows organizations to adopt AI solutions with confidence while minimizing the risk exposure for the business and its users.

Want to implement AI lifecycle governance to deliver more reliable, transparent, and efficient AI solutions? **Contact AHEAD** to learn about our data science and AI teams can help you navigate your AI journey — from strategy and planning through to customized AI solutions and business integration.

Contributing Author:

Stuart Bonnington, Principal Solutions Architect, Digital Solutions

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.

National Hubs

ATLANTA

1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO

401 Michigan Ave.
#3400
Chicago, IL 60611

SAN FRANCISCO

2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583