AI Governance Masterclass: A 201 Session for Professionals

November 12, 2025

relyanceai

Panelists

Leila Golchehreh
Co-Founder &
Chief Strategy Officer
Relyance AI

Entrepreneur, Attorney, and expert in AI Governance and Data Protection. Her background includes international legal work at firms like Allen & Overy and organizations such as the US Mission to the EU, the International Court of Arbitration, and the OECD. She has built multiple law practices and served as a CPO/DPO and Legal Lead for companies like Workday, Adaptive Insights, and General Motors Cruise, developing global data protection programs across various sectors. Leila has founded 2 global tech companies and is passionate about the intersection of technology, law, and foreign policy.

relyanceai

Leah Perry
Vice President, Legal, Chief Privacy Officer & Global Head of Public Policy
Box

Leah is an experienced international and comparative law attorney with 20 years of demonstrated success and expertise in AI, SaaS and the financial services industries, as well as regulatory, product, congressional oversight and investigations experience. Currently, Leah leads Box, Inc's Global AI Governance Program, Privacy Program and Public Policy Functions. In addition, she was appointed by Governor Wes Moore of Maryland as Chair of the State's Consumer Protection Commission. Leah also serves as Vice Chair of the Board of Directors for the AI Trust Foundation. Lastly, she is founder and Chair of the National Bar Association's Privacy, Cybersecurity & Technology Law Section.

Anil Gupta
Senior Solution Engineer
Relyance AI

Anil is a Senior Solutions Engineer at Relyance AI, working with prospects and customers in industries such as Technology, Healthcare, Manufacturing, and Recruiting. Prior to his role at Relyance AI, Anil spent over 20 years in the Business Intelligence and Database spaces.

What is AI governance?

Governance

An organization's approach to using laws, policies, technology, frameworks, practices, and processes to help stakeholders implement and oversee the use of AI.

It helps ensure the safe, ethical development and deployment of AI tools and systems and helps to manage risk.

relyanceai

What are some of the key AI governance frameworks and principles?

Coming into Focus: OECD Principles

Values-based principles

Inclusive growth, sustainable development and well-being

Human rights and democratic values, including fairness and privacy

Transparency and explainability

Robustness, security and safety

Accountability

Recommendations for policy makers

Investing in AI research and development

Fostering an inclusive AI-enabling ecosystem

Shaping an enabling interoperable governance and policy environment for AI

Building human capacity and preparing for labour market transition

International co-operation for trustworthy AI

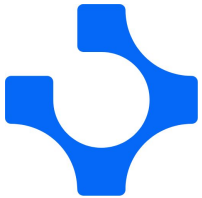
relyanceai

Commonly Known:

AI Governance Frameworks & Regulations

01	OECD AI Principles	A set of international standards and recommendations for the responsible development and deployment of AI, emphasizing human-centric values and fairness.
02	NIST AI Risk Management Framework (AI RMF)	A voluntary framework from the U.S. National Institute of Standards and Technology to help organizations manage risks associated with AI systems and promote trustworthiness.
03	EU AI Act	A comprehensive legal framework in the European Union that categorizes AI systems based on risk and establishes rules for various risk-levels.
04	ISO/IEC 42001	An international standard specifying requirements for an AI management system, helping organizations establish, implement, maintain, and continually improve their AI governance.
05	Industry Specific Frameworks	Certain regulated industries including the public sector, e.g., the UK Financial Conduct Authority, International Banking Guidance, etc.

Where do we start with respect to the development of AI Governance programs?



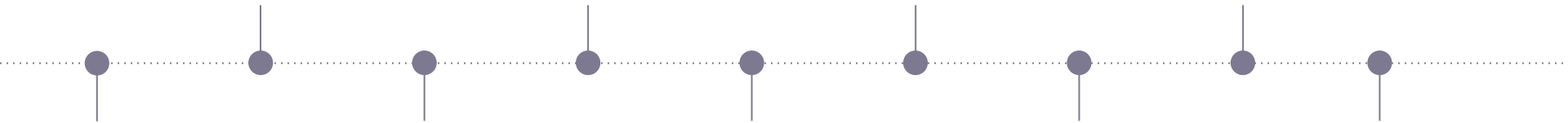
12 Month Roadmap for Programmatic Success: AI Governance

Q1
Map AI Initiatives
Inventory current and planned AI uses across the company to gain a clear overview of all AI projects.

Q2
Engage Stakeholders + Establish Responsibilities & Oversight
Collaborate with relevant departments, such as Legal, IT, and HR, to discuss governance needs and gather input.

Q3
Prioritize Higher-Risk AI
Identify and focus initial governance efforts on the most critical and high-risk AI applications.

Q4
Comm. & Training
Set up communication channels for reporting and provide ongoing employee education on AI governance.



Q1
Learn & Inform
Understand AI basics and educate internal teams on its importance through workshops and training sessions.

Q2
Assess Governance
Review current policies, legal obligations, standards, and procedures for gaps related to AI and identify areas for improvement.

Q3
Policies, Principles, Paper & Technology
Establish ethical guidelines and principles to shape AI development and usage within the company. Implement technology to assist. We cannot only push paper and expect progress.

Q4
AI Gov. by Design
Implement AI governance in stages, allowing for feedback, iteration, and continuous improvement. Embed into workflows

Q4
Continuous Monitoring
Continuously monitor AI systems through ongoing evaluation of the AI environment using AI tooling

relyanceai

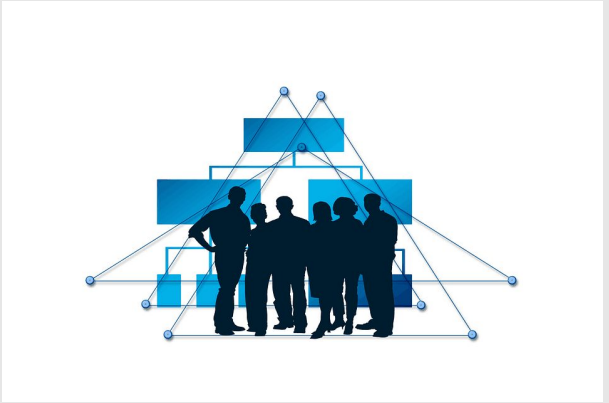
Who is responsible for AI governance? Examples of successful collaboration?

Collaboration is key to effective AI governance.

Effective AI governance requires collaboration among legal, compliance, and technology teams is essential. Legal teams ensure adherence to data protection laws and ethical standards. Compliance teams establish policies to mitigate AI risks. Technology teams design AI systems with privacy and fairness. Cross-functional collaboration identifies biases, enhances transparency, and fosters shared responsibility, maintaining public trust and regulatory compliance.

Governance

AI Governance Reporting Structure



Key Considerations

- Role clarity ensures that each member within the AI governance function is aware of their responsibilities, promoting accountability and effective oversight.
- Choosing between reporting to the General Counsel, Chief Data Officer, Chief Technology Officer, or Chief Information Security Officer can impact both the focus of the AI governance program.
- Cost evaluation should include potential expenses for resource allocation and personnel training under different reporting lines.
- Benefits vary based on reporting: legal compliance is enhanced through the GC, technical expertise through the CDO/CTO, and security oversight through the CISO.
- Cross-functional collaboration is vital to strengthen governance and align it with the organization's strategic objectives.

What are the key considerations when building & implementing AI governance and risk management policies?

Governance

AI governance programs require clear objectives, continuous monitoring, flexibility, and embedded programs.

Clear objectives: Define the goals of the governance framework to guide policy development.

Stakeholder engagement: Involve relevant stakeholders from legal, compliance, technology, and business units to ensure comprehensive input.

Regulatory compliance: Stay updated on relevant laws and regulations to ensure policies meet legal requirements.

Regular risk assessments: Identify and evaluate risks associated with AI technologies to inform policy decisions.

Flexibility and adaptability: Create policies that can evolve with technological advancements and regulatory changes.

Training and education: Provide ongoing training to staff on governance policies and risk management practices.

Monitoring and evaluation: Establish mechanisms for regularly reviewing and updating policies based on performance and emerging risks.

What interesting use cases in AI are you seeing, and what are some practical strategies for addressing those use cases?

Some Key AI Use Cases & Governance Strategies

AI Chatbots for Customer Support

- Data privacy (GDPR, CCPA)
- Transparency (AI vs. human interaction)
- Bias detection and fairness

AI for Software Development & Coding

- Intellectual property protection
- Security (data used in code suggestions)
- Regular auditing for bias in code

Text Generation for Content Creation

- Avoid plagiarism (cite sources, originality)
- Ethical use (prevent harmful or biased content)
- Transparency (disclose AI involvement)

Predictive Analytics for Business Insights

- Data privacy and security (GDPR, CCPA)
- Transparency in data usage
- Regular model audits for accuracy

AI in Personalization (Marketing & Recommendations)

- Data privacy (GDPR, CCPA)
- Transparency and consent for data collection
- Avoiding discriminatory algorithms

AI for Fraud Detection

- Adherence to financial regulations (AML, KYC)
- Data protection (GDPR, CCPA)
- Ensuring fairness and accuracy in predictions

What are some of the major ethical AI and governance issues?

Key Ethical AI Issues

- Lawfulness
- Safety for people and the planet
- Protection from unfair bias
- AI use is transparent and explainable
- Individuals have appropriate choices about the use of their personal information to develop AI
- Individuals can choose to have human intervention in key AI-driven decisions that impact their legal rights or well being
- Organizations must be accountable for ensuring AI they develop and use is secure

AI Governance

Governing AI Agents

Autonomy & Control

Define agent independence with clear intervention methods.

Safety & Reliability

Implement protocols for safe autonomous operation.

Accountability

Establish who's responsible for agent actions.

Data Governance

Manage data use and privacy in agent interactions.

Transparency

Ensure agent reasoning can be understood and audited.

Ethical Alignment

Embed values for ethical autonomous decisions.

AI Safety

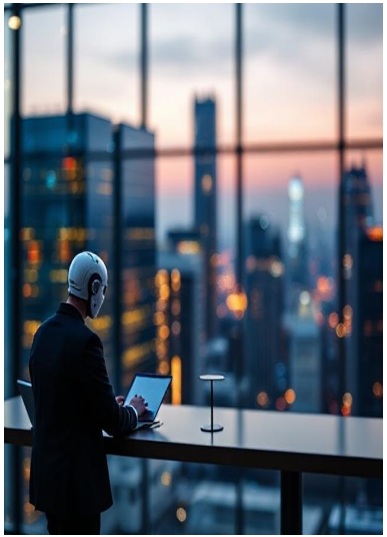
Defining Safety in an AI Context:

Assurance that systems operate as intended, preventing unintended negative consequences (physical, economic, privacy, discrimination, etc.).

Robustness	Reliable performance on novel data.
Robustness & Intended Behavior	Reliable performance on novel data. Prevents unprogrammed actions.
Value Alignment	Goals align with human ethics. Understanding decisions in safety-critical areas.
Explainability	Ability to understand and articulate the reasons behind an AI system's decisions or predictions in a way that humans can comprehend.
Privacy & Security	Protects personal data and against malicious attacks. Safeguards sensitive information.
Fail-Safes & Continuous Monitoring	Graceful error handling, fallback modes, ongoing performance checks, and rigorous testing for safety requirements.

How do we address AI Governance issues in our commercial agreements and privacy statements?

Key Legal Considerations in B2B Agreements



Intellectual Property & Data Governance

Clearly define ownership of IP derived from or generated by AI, rights to input data (especially training data), and responsibilities for privacy/security compliance (e.g., GDPR, CCPA). Specify permitted uses and restrictions.

Data Protection + AI Governance Assessment required as well.

Incidents, Liability, Indemnification

Establish incident response notification obligations, and clear lines of responsibility for damages or losses from AI's performance, including inaccurate outputs, biases, or security breaches. Define indemnification obligations for each party.

Performance Standards & Service Levels

Outline expected performance metrics for the AI solution, including accuracy, reliability, uptime, and response times. Incorporate SLAs with remedies for non-performance.

Transparency & Explainability

Include provisions for transparency regarding the AI's decision-making processes. Strive for a level of explainability appropriate to the context and risk.

Auditability & Compliance

Include clauses allowing some type of audit to ensure compliance with terms, data protection, and regulations. Define the scope and process for such audits.

Continuous Monitoring & Updates

Address ongoing maintenance and updates of the AI system. Clarify responsibilities for updates, addressing vulnerabilities, and ensuring fitness for purpose.

AI Governance

Key Legal Considerations in Consumer Facing Statements

Clear Identification of AI Use

Explicitly state when and how AI is being used in the product or service. Avoid vague language and clearly explain the AI's role in the user experience.

Data Collection and Use Practices

Clearly and concisely explain what data is being collected, how it's being used by the AI (including for training or personalization), and the purposes of this data processing. Provide easy-to-understand information about data privacy and security measures.

Explanation of AI Capabilities and Limitations

Set realistic expectations by outlining what the AI can and cannot do. Highlight potential limitations, biases, or areas where the AI might not be perfectly accurate or reliable.

User Rights and Choices

Inform users about their rights regarding their data, such as access, correction, or deletion. Explain any choices users have regarding the AI's functionality or data usage, including opt-out options where applicable.

Contact Information and Support

Provide clear contact information for users to seek assistance, report issues, or ask questions about the AI system and its use of their data.

Regular Updates and Notifications

Inform users about any significant changes to the AI system, its data handling practices, or the terms of service. Provide clear and timely notifications of such updates.

AI Assessments: Key Considerations

Key Considerations for Advanced AI Assessments

A comprehensive AI assessment must address data integrity, model robustness, algorithmic fairness, explainability, benchmarking, privacy, ongoing monitoring, and security to ensure responsible and effective deployment.

Critical factors to evaluate in advanced AI Assessments:

- **Risk**
- **Audit Committee**
- **UK ICO Risk Assessment**
- **Building into the DPIA process**

- Data Provenance and Integrity: Rigorously evaluate the lineage, quality, and integrity of training and operational datasets using techniques like data lineage tracking, anomaly detection, and statistical validation.
- Model Robustness and Adversarial Resilience: Assess the AI model's stability under various input perturbations and its resistance to adversarial attacks using methods like adversarial training and sensitivity analysis.
- Algorithmic Bias Detection and Mitigation: Use statistical and causal inference methods to identify and quantify biases; implement and evaluate bias mitigation techniques (pre-, in-, post-processing).
- Explainable AI (XAI) and Interpretability: For critical applications, utilize XAI frameworks (e.g., SHAP, LIME) to provide insights into model decision-making processes and assess the interpretability of model features.
- Performance Benchmarking and Scalability: Conduct rigorous benchmarking against state-of-the-art models and evaluate the AI system's scalability and resource utilization under varying loads.
- Privacy-Preserving AI Techniques: For sensitive data, assess the implementation and effectiveness of privacy-preserving techniques like federated learning, differential privacy, or homomorphic encryption.
- Model Drift and Continuous Monitoring: Establish robust monitoring systems to detect and quantify model performance degradation (drift) over time due to changes in input data distributions.
- Security Vulnerability Analysis: Conduct thorough security assessments, including penetration testing and vulnerability scanning, specifically targeting AI/ML components and their dependencies.

Connect with us!

Leila Golchehreh
Co-Founder &
Chief Strategy Officer
Relyance AI

leila@relyance.ai

https://www.linkedin.com/in/leilagolchehreh/

Leah Perry
Vice President, Legal, Chief
Privacy Officer & Global Head
of Public Policy
Box

lperry@box.com

https://www.linkedin.com/in/leah-p-9686206/

Anil Gupta
Senior Solution Engineer
Relyance AI

anil.gupta@@relyance.ai

https://www.linkedin.com/in/anil-gupta-a9a139/