THE ESSENTIAL GUIDE TO AI GOVERNANCE

ABSTRACT

AI Governance is no longer a nice-to-have policy. It’s a must-have framework for every organization deploying AI product features or using AI in their everyday business workflows.

PrivacyWise

Table of Contents

An Introduction to AI Governance

Artificial Intelligence (AI) is here to stay, and the overwhelming wave of new and adapted technologies shows great promise in improving our lives and business success. But the law of unintended consequences tells us that, as with any new and powerful tool, the outcomes of AI usage can be positive, negative, and entirely difficult to predict.

That is why AI Governance has become a necessary and urgent new framework for every business deploying or utilizing AI. If you're familiar with other forms of governance, such as Privacy Governance or information security governance, then AI Governance should be familiar. It specifically refers to the laws, policies, frameworks, standards, ethical guidelines, and regulatory mechanisms that manage and oversee the development, deployment, and use of artificial intelligence (AI) technologies.

The goal is to ensure that your AI systems are developed, deployed, and used responsibly, ethically, and in alignment with your organizational values, while at the same time mitigating potential risks such as bias, harm, and misuse. Similar to Privacy and Information Security, it encompasses principles of transparency, accountability, fairness, security, and safety in AI decision-making processes.

Makes sense, right? Yet in late 2024, one survey revealed that only 44% of all companies have established policies around employee and business use of AI.[i] If you haven't yet started to build your AI Governance, then you cannot afford to delay any longer. In this paper, you will learn the importance of AI Governance, the potential downsides of neglecting to consider AI governance, and what to consider when building your framework.

Why Is an AI Governance Plan a Necessity?

AI Governance is chiefly concerned with long-term risk management and readiness for the unexpected. As more companies come to rely on AI, it's critical that they take a beat and put sensible controls in place to anticipate and then avoid negative AI-related outcomes. With so many AI applications, it helps to think of two scenarios: external AI ("AI you sell") and internal AI ("AI you use").

Many, though not all, commercial products now feature AI-based functionality (e.g., smart washing machines, chat tools, medical devices). When building AI into your external offerings, how are you handling the associated risks to your business? These risks span data collection and privacy, customer misuse, model training and development, system and infrastructure integration, legal and regulatory noncompliance, and more.

AI has also been introduced into the productivity tools your employees use every day (e.g., generative AI for research and graphics, mapping software, and coding tools). These solutions can generate a secondary set of potential risks. When your organization purchases and applies third-party AI tools, how do you manage privacy issues, the potential exposure of proprietary information, security concerns, and possible misuse of the tools? Do you have a full understanding of how the AI operates and uses data?

The way to address these potential internal and external risks is a properly crafted and deployed AI Governance policy framework. In addition to improving collaboration and fostering growth and innovation, the safeguards within this framework can deliver many benefits:

Ethical Alignment

Ensures that AI technologies operate in a way that is ethically sound and aligned with human values, respecting privacy, fairness, and individual rights. This is essential for fostering public trust in your AI technologies.

Transparency and Accountability

Fosters transparency in AI systems' decision-making processes, helping to ensure that their actions can be understood, explained, and held accountable, especially in critical sectors like healthcare, finance, and law enforcement. This fosters user and stakeholder trust.

Risk Mitigation & Safety

Helps to identify and mitigate risks related to AI, such as biases in data, potential job displacement, security threats, and unintended harmful consequences. Proactively addressing these risks prevents harm before it occurs. Provides for crisis management.

Legal and Regulatory Compliance

Provides clear governance so that AI systems are more likely to comply with existing laws, such as data protection regulations (e.g., GDPR), and can adapt to future legal requirements. Organizations can avoid legal risks and penalties.

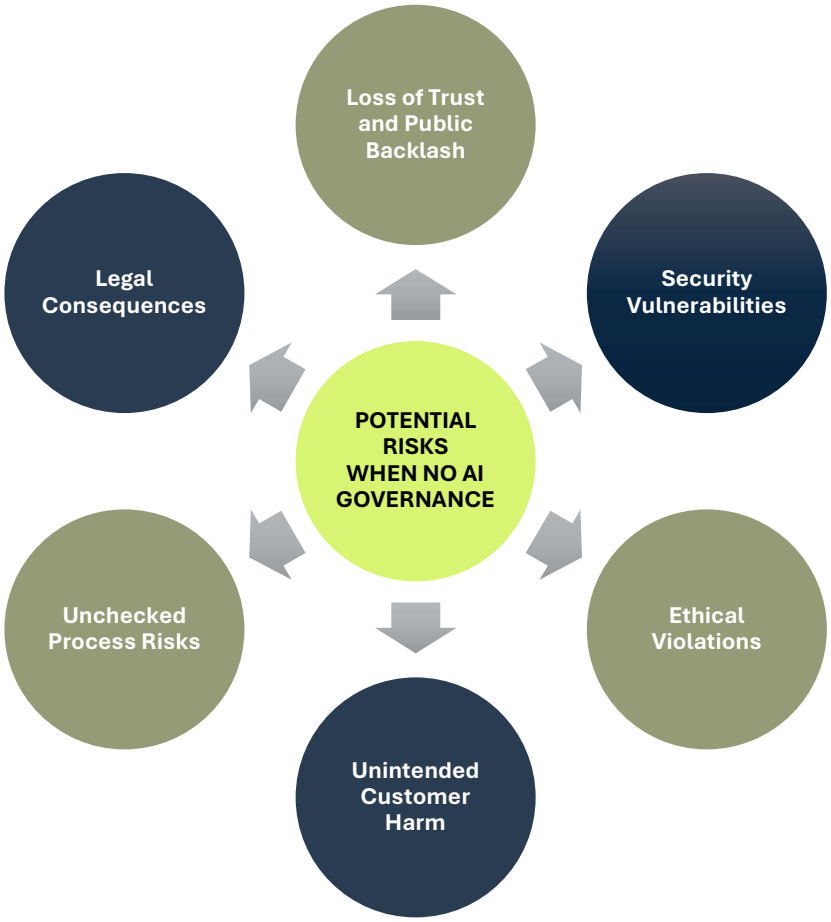
Public Trust and Adoption

Builds public trust and brand loyalty, encouraging wider acceptance and adoption of AI technologies. People are more likely to embrace AI when they feel confident it is being used for the common good.

AI Governance is not meant to deter your innovation and initiatives but rather to ensure those move forward as smoothly and safely as possible. AI Governance allows for company-wide transparency, accountability, and consistency. It's about protecting your company and employees while simultaneously harnessing new technologies as an operational and market advantage.

The Dangers of Not Having a Plan

Potentially nothing, but the odds are not in your favor over the long term. Without a governing framework, the probability of an issue will only increase as you integrate AI deeper into your operations and products. In the last year alone, many of the most recognizable brands and corporations have faced setbacks with and negative press concerning their AI solutions.[ii] This has led to a catalog of undesirable outcomes:



1. **Loss of Trust and Public Backlash**: A lack of governance has led to public skepticism or fear of AI. Scandals or harmful incidents resulting from poorly regulated AI may erode trust in your technology, slowing down acceptance and market innovation.

2. **Security Vulnerabilities**: AI systems, when left unchecked, can be vulnerable to attacks or manipulation. Malicious actors can exploit weaknesses in products and autonomous systems, leading to security breaches, data theft, or even physical harm. This can also occur in third-party AI tools used by your employees.
3. **Ethical Violations**: When AI systems have operated without ethical oversight, they can potentially act in a way that can harm individuals or society—like violating privacy by revealing personally identifiable information (PII), failing to respect human dignity, or making life-impacting decisions with little to no human oversight.
4. **Unintended Customer Harm**: Without governance, AI systems have unintentionally perpetuated biases, leading to unfair or discriminatory outcomes. For example, biased hiring algorithms or AI tools used in criminal justice systems could reinforce existing societal inequalities.
5. **Unchecked Process Risks**: Unforeseen or unmitigated risks can occur when AI is integrated into processes. For example, in industries reliant on AI-driven automation (e.g., autonomous vehicles, healthcare diagnostics), without proper governance, there's a risk of malfunctioning systems or harmful decisions that could result in physical injury or fatality.
6. **Legal Consequences**: Without clear governance, organizations could inadvertently violate laws, such as data privacy regulations, intellectual property rights (copyright infringement), or anti-discrimination laws, leading to legal liabilities and fines.

Are You Tracking the Latest Global AI Regulations?

The United States has not yet passed comprehensive federal legislation for AI regulation. While it appears to be headed towards a more decentralized framework, several laws and regulations do impact AI, including:

- The National Artificial Intelligence Initiative Act of 2020[iii]
- The AI in Government Act[iv]
- The White House Executive Order on AI[v]
- Advancing American AI Act[vi]
- The Equal Credit Opportunity Act[vii]
- Various state legislations (e.g., the Colorado AI Act)

Beyond the United States, most countries have proposed guardrails and released proposed AI regulations. The European Union's (EU) Artificial Intelligence (AI) Act[viii] of 2024 is generating intense interest. It is important to research and understand the status of these initiatives if you intend to do business in or have your products used within these countries.

Building Your AI Governance Framework

With so many potential risks to manage, creating an AI Governance plan from scratch is not easy. While US laws and regulations for AI remain in early development, some companies are studying the emerging international regulatory frameworks mentioned previously as part of their approach to AI policy development. They use these laws to influence how they frame their external and internal policies and determine what documentation and oversight are required.

Other businesses are tapping external expertise or looking to standards organizations like ISO and NIST to ensure they've considered all the relevant facets of AI policy for their specific use cases. No matter whom you involve, you're best off completing your framework well before you may need to use it. To help get you started, this section will cover the who, what, and how of developing and implementing an AI governance plan.

At the Start: Ask the Right Questions

As you decide what to include in the scope of your plan, have your team compile a list of questions that must be answered, such as:

- What AI systems exist today? What's their status?
- Are we developing AI, and do we know every instance?
- What data are we using to train the AI systems we are developing? Where does it come from?
- What third-party AI tools have we procured? Are they deployed? Who has access to these tools?
- If they're not yet deployed, when do we plan to deploy them?
- What Generative AI models are we currently using? Where in our business are these models being used?
- Are employees carefully reviewing the output from AI systems?
- Do we have a definition for personally identifiable information?
- Do employees understand what we consider proprietary information?
- What's our level of understanding for 'formal' versus 'informal' use?
- Do we have a data management policy already established?
- Are there teams already doing the readiness work (duplication of effort)?
- Who must be on our AI Governance team?

Who Should Build Your Plan

Today, most organizations are not mature enough in their AI initiatives to have a dedicated AI Governance team. With technologists in the lead, they often focus first on the feasibility of the intended use case rather than the long-term risk management implications. While it makes sense to prove out the AI functionality, smart companies dedicate resources to exploring the business and ethical impacts of this technology at the outset.

Before creating a new committee, you may already have a resource you haven't considered: the Privacy team.

Privacy professionals, already well-versed in managing data responsibly and security, bring essential skills to AI governance, especially as data regulations grow in complexity and scope. Privacy teams understand the delicate balance between maximizing data utility and safeguarding individual rights, making them ideal stewards to oversee AI initiatives.

From minimizing data risks to ensuring ethical data practices, privacy teams excel at embedding trust and compliance into AI systems. They possess the knowledge to implement robust data protection measures that align with both privacy and AI governance requirements, ensuring data is used transparently, fairly, and ethically.

Another alternative is engaging an outside consultancy with privacy and AI policy expertise. Consulting firms like PrivacyWise can bridge the gap between what your team knows about their technology but does not know about current regulations or certain potential risks. An experienced AI expert will bring ready-made templates and best-practice processes that can speed up the implementation of AI Governance and save on limited resources.

In any case, you must begin by securing internal sponsorship. AI Governance is only successful when supported by an executive sponsor, who may not be intimately involved but can ensure that the creation and rollout is an organizational priority.

No one individual should be responsible for AI policy; this initiative is about collective effort and responsibility. The assembled policy team should be a cross-section of the organization, with invested representatives from product management, legal, software engineering, product marketing, procurement, and anyone who may represent most employee users.

What the Plan Should Include

With AI Governance, there is no one-size-fits-all framework. Not only does each organization have unique AI use cases, but conditions will change with advances in innovation and new and updated regulations. Therefore, it is best to use existing and flexible standards to create your custom framework.

Remember that an AI Governance framework performs multiple, critical functions: risk mitigation for your business, ethical standards for your customers, readiness for unexpected issues, legal and regulatory alignment, and organizational transparency and accountability. Your policies must be based on your organization's values (e.g., respect, customer first, sustainability), a primary reason your team should represent diverse viewpoints beyond those of your technologists.

Corporate AI Policy Coverage (Operational Level)

Your plan should be wide in scope, defining areas of responsibility, communications, definitions, and specifics regarding your internal and external use cases. Plans can include:

The corporate AI strategy	Clear definitions of technical and legal terms
The goals of the policy	Data origin and usage descriptions
Who should use the policy	Which AI systems are approved
When the policy must be applied	Permitted and prohibited uses of AI
How to report concerns	How to properly vet new AI vendors

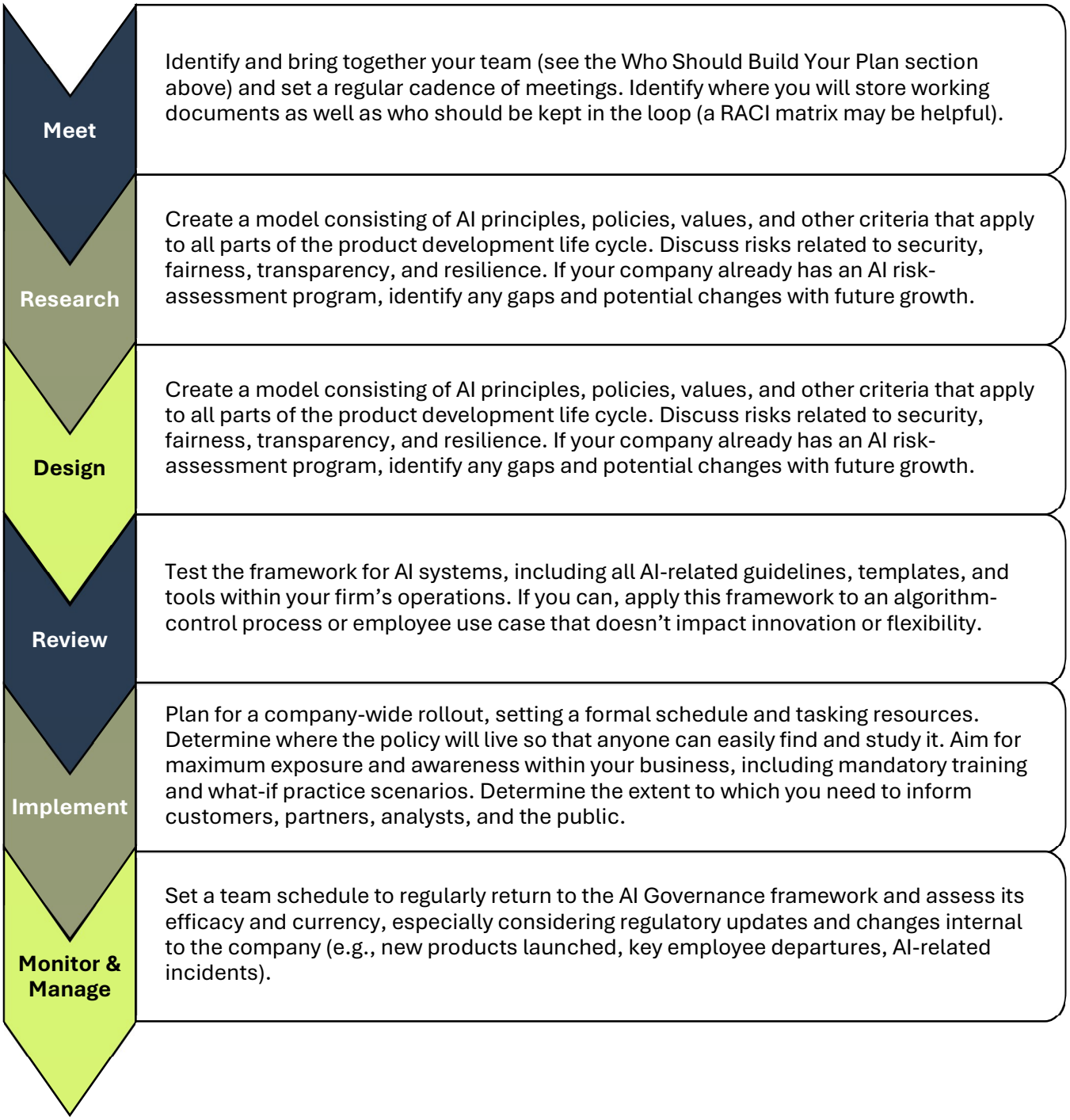
AI Data Management (Product Level)

AI systems rely on vast amounts of data to learn, make decisions, and deliver insights. At the core of every AI system is data—data about individuals, behaviors, trends, and interactions—which powers algorithms to achieve predictive and operational accuracy. Your plan must recognize and address how data is procured, handled, saved, applied, and protected. Privacy and data protection governance practices must be woven into the entire AI life cycle. Data management documentation can include:

The processes for developing and enhancing AI systems	Data quality standards and provenance (is it first party? public? third party?)
The methods and criteria for the acquisition and selection of data in AI systems	Who is responsible for the implementation and enforcement of the policy
The criteria and methods for data preparation for use in AI systems	What disciplinary actions will be used for violations of data management policies

How to Develop Your Plan

When you reach the stage of AI Governance development and implementation, we recommend following these six broad steps.



The Very Real Downside of AI Without Policy

The news is brimming with examples of AI Governance failures. Whether due to a lack of a comprehensive AI policy, an inability to anticipate potential negative consequences, or just plain hubris, the fallout can be very public and a financial and reputational setback for any company. Here are three incidents from 2024.

DeepMind: The Patient Data Controversy	
THE ISSUE	DeepMind, an AI company owned by Alphabet, faced criticism for partnering with UK hospitals to access and analyze patient data without adequate transparency or proper consent measures.
THE IMPACT	The data management controversy sparked major concerns about data privacy, consent, and the ethical use of AI in healthcare. It brought attention to the need for informed consent, proper data anonymization, and robust access controls in AI-powered healthcare projects.
WHAT CHANGED	This raised discussions about the ethical duties of AI developers, data custodians, and regulators in protecting patient privacy and data security. In response, DeepMind improved its transparency and accountability, while stakeholders placed greater emphasis on addressing ethical issues and safeguarding patient rights.

Grindr: The Privacy Breach with AI Analytics	
THE ISSUE	The dating app Grindr came under heavy fire and faced legal challenges for sharing highly sensitive personal information, such as users' HIV status and GPS location, with third-party advertisers through AI-driven analytics.
THE IMPACT	This mishandling of personal data shattered user trust, broke privacy laws, and led to hefty fines and widespread backlash against Grindr.
WHAT CHANGED	Grindr had to change how it shared data, putting more focus on getting consent and being upfront about how user info is handled. The controversy highlighted how crucial it is to use AI ethically and responsibly, especially when dealing with sensitive personal information The incident pushed the tech industry to rethink privacy protections and safeguards.

General Healthcare: AI Diagnostic Tool Misdiagnoses	
THE ISSUE	Multiple incidents with AI-powered diagnostic tools in healthcare revealed the dangers of inaccurate AI evaluations, resulting in misdiagnoses and unsuitable treatment plans.
THE IMPACT	While these tools aimed to assist medical professionals with quicker diagnoses and personalized treatment suggestions, they occasionally produced errors due to biases in training data or issues in algorithm design. This raised serious concerns about relying on AI in critical healthcare decisions, prompting demands for stricter testing, certification, and regulation of AI-driven medical products.
WHAT CHANGED	Healthcare institutions and AI developers were called on to work more closely to ensure AI tools undergo thorough evaluation and ongoing monitoring to maintain patient safety and care quality.

Summing It All Up & Next Steps

AI offers enhanced creativity, faster and greater productivity, valuable data insights, and improved efficiency. Your organization and customers can apply it to content creation, data analysis and prediction, improved communication, and more. But the risks inherent in this new technology dictate that you must be as protected and properly prepared as possible for the unexpected.

As AI technology rapidly advances, so does the field of AI Governance. The lessons learned from AI scandals and missteps continue to inform and expand the fields of policy and data management. That's why now is the time to prioritize your AI Governance roadmap and framework.

Employing a structured AI governance plan will lead to more ethical, transparent, and accountable use of AI technologies. It mitigates risks, ensures compliance with legal standards, builds trust with stakeholders, and supports sustainable innovation. Ultimately, it creates an environment where AI can be developed and deployed responsibly, maximizing its benefits while minimizing potential harm and exposure to your business.

Let Us Help You Build a Robust Plan

Whether you are building an AI Governance plan from scratch, seeking an external plan review, or looking for improvements to your existing framework, PrivacyWise is your go-to AI policy resource. Our experienced team has the knowledge you need to implement robust data protection measures that align with both privacy and AI governance requirements. We can guide you through:

Evaluating AI systems for compliance with current privacy laws, ethical guidelines, and risk mitigation strategies.

Developing and implementing policies that guide ethical AI use, aligning with industry standards and organizational values.

Overseeing data flow, retention, and deletion practices specific to AI, ensuring compliant data use across systems.

Educating staff on AI governance best practices, focusing on ethical considerations, compliance, and operational impacts.

Tracking emerging regulations and guidelines in AI to keep the organization ahead of new requirements.

Curious? We're glad to answer all questions about AI Governance frameworks and your specific needs.

Reach out for a free, 30-minute discovery call today.

Visit www.privacywise.tech to schedule your conversation.

About PrivacyWise

PrivacyWise is a Denver-based consultancy that acts as a translation layer between complex privacy requirements and your business. Our expert consultants apply practical, human-centered solutions that work in tandem with your technology to develop an AI governance or privacy program that works for you.

We know that onerous one-size-fits-all solutions create bottlenecks on the way to your company's policy goals. Through a focus on your specific needs and capabilities, we cooperatively design an effective governance plan for the needs of your organization. At PrivacyWise, we don't start with what you need to do. We start with what you can do.

Learn more at www.privacywise.tech.

Online Resources

- General info on AI governance and Privacy: https://iapp.org/resources/article/the-intersection-of-privacy-and-ai-governance/
- AI Governance in Practice Report: https://iapp.org/media/pdf/resource_center/ai_governance_in_practice_report_2024.pdf
- ISO 42001 information. The International Organization for Standardization (ISO) is the first international, certifiable standard focusing on the governance of AI management systems: https://www.vanta.com/resources/iso-42001
- National Institute of Standards and Technology (NIST) AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework
- Organisation for Economic Co-operation and Development (OECD) AI Principles: https://www.oecd.org/en/topics/ai-principles.html
- UNESCO Recommendation on the Ethics of Artificial Intelligence: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence#
- EU AI Act information: https://iapp.org/news/a/in-scope-or-not-an-eu-ai-act-decision-tree-and-obligations
- Colorado AI Act: https://iapp.org/news/a/the-colorado-ai-act-what-you-need-to-know

Endnotes

[i] News Roundup: Fewer Than Half of Companies Have Policies Governing Employee Use of Generative AI, October 3, 2024, https://www.corporatecomplianceinsights.com/news-roundup-october-3-2024

[ii] Top 50 AI Scandals [2025], https://digitaldefynd.com/IQ/top-ai-scandals/

[iii] H.R.6216 - National Artificial Intelligence Initiative Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/6216

[iv] H.R.2575 - AI in Government Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/2575

[v] IAPP, "White House rolls out comprehensive executive order on AI," https://iapp.org/news/a/white-house-rolls-out-comprehensive-executive-order-on-ai

[vi] S.1353 - Advancing American AI Act, https://www.congress.gov/bill/117th-congress/senate-bill/1353/text

[vii] US Department of Justice, Civil Rights Division, The Equal Credit Opportunity Act, https://www.justice.gov/crt/equal-credit-opportunity-act-3

[viii] The EU Artificial Intelligence Act, https://artificialintelligenceact.eu/