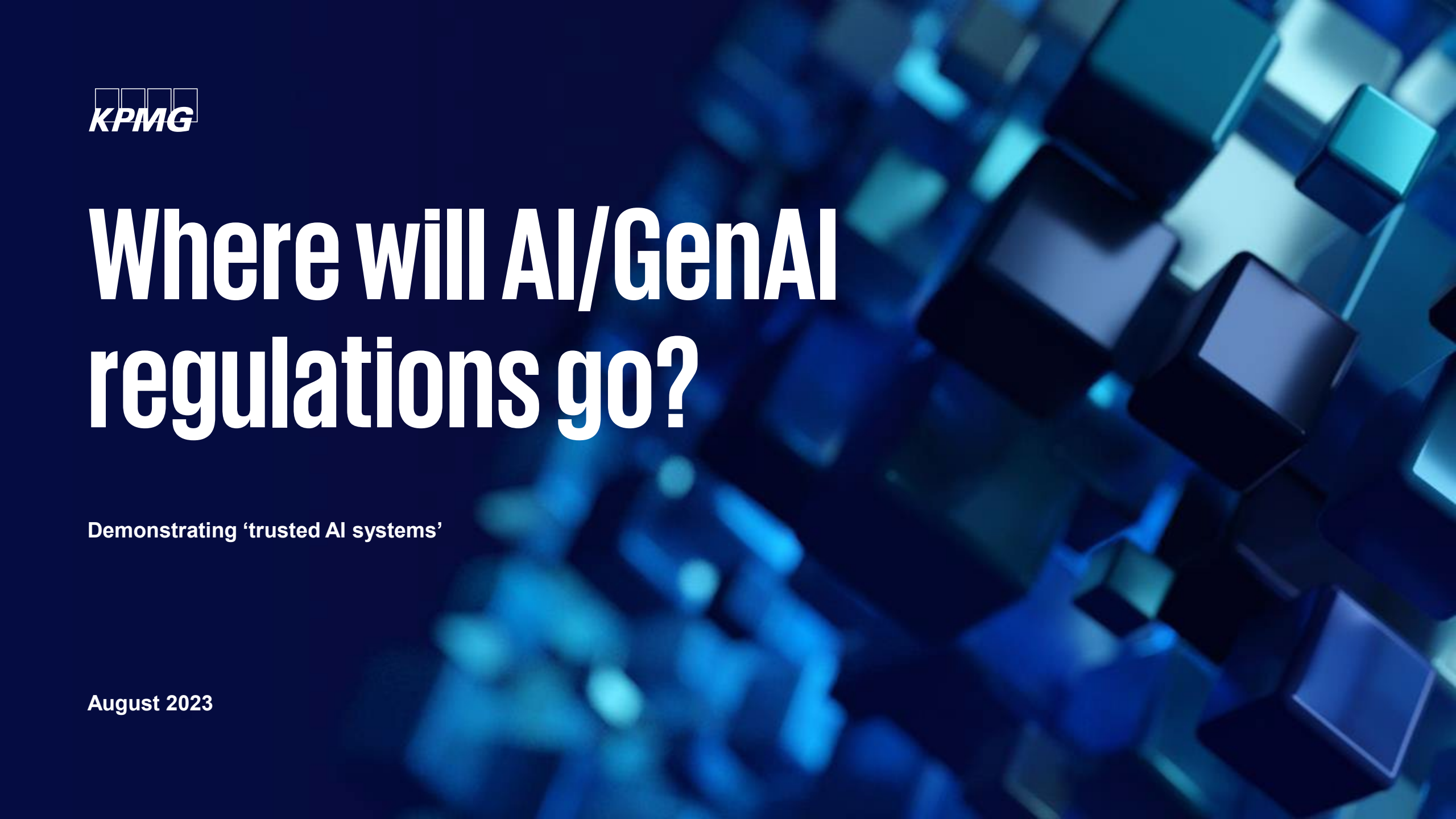


Where will AI/GenAI regulations go?

Demonstrating ‘trusted AI systems’

August 2023

Table of Contents

> *"As AI, including GenAI, is more widely adopted, the role of Risk will be critical to innovating while maintaining trust. In the absence of formal legislation or regulation (and even when such may come), companies must proactively set appropriate risk and compliance guardrails and "speedbumps". Keep in mind, regulators have made clear that existing authorities and regulations apply to "automated systems" , including algorithms, AI, and innovative technologies.*

Amy Matsuo
Principal and National Leader
Compliance Transformation (CT) &
Regulatory Insights
KPMG LLP

> *"Generative AI adoption is quickly moving forward, and organizations are figuring out how to comply with regulation. Executives need to proceed with vigilance as regulation around generative AI is built and implemented."*

Emily Frolick
Partner
US Trusted Imperative Leader
KPMG LLP

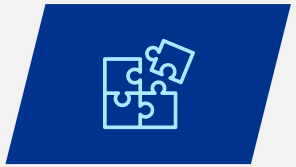
© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Introduction

Businesses are asking key questions on where the regulations are and where they may go. How do we as an organization design our risk governance and risk management so that we take advantage of the automation advances while mitigating the risks?

As artificial intelligence (AI), including Generative AI (GenAI), is more widely adopted, the role of Risk will be critical to innovating while maintaining trust. In the absence of formal legislation or regulation (and even when such may come), companies must proactively set appropriate risk and compliance guardrails and “speedbumps”.

“AI Regulations”: Here Today & More Coming



AI Regulatory Complexity is Not an Excuse

AI Risks Span Silos

Managing it All

How KPMG Can Help:

Speed to modern data, analytics, and AI

AI and Data Ethics Institute

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

"AI Regulations": Here Today & More Coming

Amidst keen public policy and legislative attention to AI, regulators have been clear that existing regulations apply to "automated systems", including AI, and cover the full lifecycle of design, development, deployment, and continuous monitoring.

Key Legislative/Regulatory Activity

Interagency Statement on Enforcement Against Discrimination and Bias in Automated Systems

Existing legal authorities are applicable to "automated systems" (i.e., software and algorithmic processes, including AI) and "innovative new technologies". Legal protections promote civil rights, non-discrimination, fair competition, consumer protections.

White House AI Bill of Rights; NIST Voluntary AI Risk Management Framework

Establishes resources/principles to manage AI risks and promote "trustworthiness" and an independent review and reporting of safety and effectiveness of AI system, including mitigation of bias and conflicts of interest.

SEC Proposed Rule on "Covered Technologies" and Conflicts of Interest

Proposal to address conflicts of interest when firms use "covered technologies" (including AI and predictive analytics) that optimize for, predict, guide, forecast, or direct investors' decisions.

EU AI Act (European Union's Artificial Intelligence Act)

Bill to establish a risk-based framework for AI applications, products, services across design, development, deployment, monitoring with an eye to consumer protections/harms. Establishes requirements/obligations for providers at each risk level including conformity assessments, technical and auditing requirements, and monitoring.

Key Areas to Watch: AI Regulatory Themes

Risk Management

Risk management and governance around the design, use, and deployment of AI, including:

- Safety and effectiveness (e.g., protections against unintended or inappropriate access or use)
- Anti-bias and anti-discrimination (protections against, and ongoing testing)
- Data governance and data privacy
- Transparency (e.g., what/how information is used; potential impacts to business/consumer)
- Accountability and oversight.

Fairness/Consumer Harm Under Existing Regulations

Supervision and enforcement of fairness in applications of AI and other innovative technologies under existing consumer and employee protection laws and regulations

"Whole of government" (multi-agency approach)

Purpose Limitation and Data Minimization (Privacy)

Limitations on access to and use of consumer data for specific, and/or explicit purposes, subject to permission, consent, opt in/out, and/or authorization, as required.

Limitations on data retention (e.g., only for the stated purpose)

Safeguards on data and systems (re: access and use)

KPMG

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AI Regulatory Complexity is Not an Excuse

Expect that regulatory approaches to AI and/or the areas of regulatory and supervisory focus will evolve and may diverge across state, federal, and global jurisdictions increasing the complexity of AI compliance. Similarly, regulatory expectations in other evolving areas that touch on system inputs and outputs as well as customer impact (such as fairness, privacy, and cybersecurity) may overlap with AI expectations, increasing regulatory scrutiny and adding to complexity.

Areas of Complexity

Evolution of AI

AI's wide accessibility and user-friendly interfaces are fostering rapid technological advances and innovations, and drawing state, federal, and global regulatory focus to the existing, new and evolving risks it poses. Companies will need to conduct an enterprise-wide evaluation of these risks, including, but not limited to bias, discrimination, transparency, governance, consistency, and fairness as well as data collection, protection, quality, ownership, storage, and retention.

Enterprise-wide Understanding

Regulatory scrutiny around AI explainability (transparency) and accountability will necessitate appropriate levels of acumen, experience, and training. As companies design and develop AI, enterprise-wide coordination and alignment will be needed. Engage with internal stakeholders throughout the AI lifecycle to Improve enterprise-wide capacity for understanding AI, including benefits, risks, limitations and constraints; Check assumptions about context and use; Enable recognition of malfunctions, misinformation, or misuse.

Known (and Unknown) Risks of AI

As AI technologies, including GenAI, gain ground, it is imperative to prioritize effective risk management to avoid regulatory pitfalls while taking advantage of new opportunities. Look to cultivate and implement an enterprise-wide culture of risk management in the design, development, deployment, and evaluation of AI systems and connect technical aspects of AI systems design and development to organizational values and principles.

Key Areas to Watch: Added Complexity

Continual Evolution

The widening deployment of user-friendly AI products and services is leading to rapid evolution in their applications and capabilities. These advancements add complexity to both how regulators are approaching AI, as well as how companies evaluate compliance.

Overlapping Expectations

The current and rapidly evolving legislative/regulatory focus on fairness, data privacy, cybersecurity, and resiliency will add complexity to the intensifying interagency and cross-jurisdictional focus on AI. Updates to these regulations could overlap with regulatory expectations for the design, development, and deployment of AI, including consumer impact..

Regulatory Divergence

Diverging regulatory approaches or areas of focus to AI supervision would greatly expand the complexity around compliance and necessitate reassessment of current and target state compliance functions and approaches to compliance risk assessments. Consider impact assessments, jurisdictional risks, regulatory awareness, and timing.

KPMG

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AI Risks Span Silos

The benefits and risks of AI will touch areas across the organization, including a variety of aspects related to operations, products and services, and customer protections. Key areas of concern include potential conflicts of interest (between the company and the customer), market concentration (AI base model providers), and macro-prudential policy interventions.

Core Areas of Potential Impact from Regulation

Privacy

Data collection, use, protection, quality, ownership, storage and retention.

Data

Data breaches, malware, fraud, identity theft, or other financial crime.

Security

Security risks of AI use, including adversarial attacks, data poisoning, insider threat, and model reverse engineering, which require swift remediation to manage reputational risks.

Adoption & Integration

Operational risks of AI adoption, including third-party risk management, overreliance on a single provider, limited access to experts, and the need to train the workforce to effectively leverage this technology.

Testing & Evaluation, Verification & Validation (TEVV)

Effective AI design and development requires robust TEVV processes at each stage of the AI lifecycle to ensure alignment with intended use and appropriate calibration, assess user experience, and ensure adherence to relevant requirements and expectations.

Assurance & Attestation

AI trustworthiness is critical to a successful user experience and can be fostered by providing assurances outlining the systems that maintain an AI system's confidentiality, integrity, and availability.

Intellectual Property

AI could raise potential legal considerations around IP rights, including potential for devaluation.

Key Areas to Watch: Impacts

AI "Trustworthiness"

Regulatory focus on AI trustworthiness, particularly around safety, efficacy, fairness, privacy, explainability, and accountability, will necessitate companies to holistically reassess the purpose and application of AI throughout the organization, including data collection, inputs and outputs, use, privacy, and security..

Business Risks

Anticipate current policies and procedures may need reassessment or updating based on emerging public policies and/or regulatory issues and actions around AI and related topics, such as privacy or cybersecurity. Monitor regulatory developments/actions to assess whether they will lead to significant changes to business models, such as business restrictions or limitations.

AI Risk Management

Be attentive to risks associated with incorrect or misused AI and related regulatory scrutiny; Address the potential for such risks through an active AI risk management framework. Regulators will look for:

- Robust AI development, implementation, and use (e.g., Clear statement of purpose; sound design/theory/logic)
- Effective validation conducted independently of the AI design and development
- Sound governance, policies, and controls

KPMG

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Managing it All

Managing risk associated with the design, development, deployment and management of AI solutions will require an understanding of each AI deployment; adapting legacy risk frameworks to embrace and incorporate emerging AI tools and trends; and adapting risk mindset with a focus toward monitoring outcomes, identifying model risk threats, and overall model risk management. To do this, the following are four pillars and representative actions Risk organizations should be focused on today:

Establish Governance

- Establish AI governance framework
- Develop policies that govern the use of AI throughout the organization with clearly defined roles and responsibilities
- Educate stakeholders on the use of AI, emerging risks around AI, and appropriate use policies
- Establish transparency principles and policies
- Incorporate AI into model risk management (MRM) framework including areas such as approved use, ongoing monitoring, and risk ratings
- Establish protocols for AI modeling usage, including business decisions vs experimental (Internal deployments), that align to MRM standards

Compliance and Legal Risk

- Monitor AI regulatory developments
- Ensure appropriate stakeholder groups are implementing requirements and/or controls
- Align AI deployments and governance standards with appropriate regulatory guidelines and requirements
- Validate oversight of enterprise AI use and deployment standards
- Establish consistent contracting and AI deployment requirements for 3rd parties
- Ensure a mechanism has been established to identify, report, and manage AI vulnerabilities
- Assess ethical or societal impacts of planned AI usage
- Monitor legal considerations of external facing deployments

Understand AI Strategy & Roadmap

- Align current vision, strategy, and operating model for AI solutions
- Assess Board level oversight
- Inventory AI landscape within your organization, along with planned use cases, models, and tools.
- Ensure the use cases and vendor landscape for each AI solution are clearly understood
- Monitor 3rd party risks associated with data protection, storage of data, and access to confidential data
- Evaluate software tools that are being acquired to monitor ongoing data and AI pipeline security and privacy concerns (including poison and drift)
- Incorporate AI assessment into annual risk assessment process

Monitor Usage and Deployments

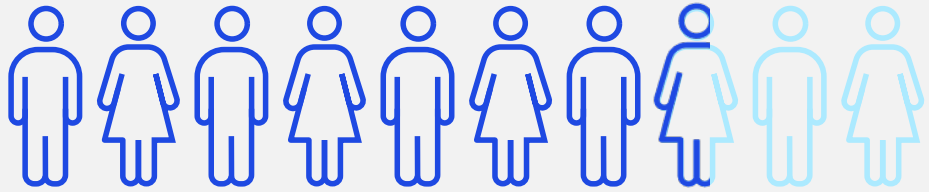
- Perform AI risk assessments around areas such as compliance, governance, security, fairness, bias, accuracy, and explainability
- Assess access, API/interface, data security, privacy and change management controls specific to AI deployments
- Evaluate AI testing, training and deployment standards
- Assess financial reporting impact
- Identify KPIs to monitor AI outcomes, as well as detect anomalies, fraud, data poisoning
- Assess AI solution resiliency and reliability

KPMG

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

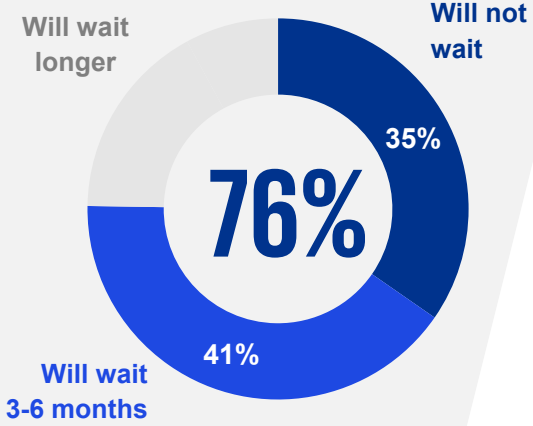
2023 KPMG Generative AI Survey

2023 KPMG Generative AI Survey Report: KPMG surveyed 200 senior U.S. business leaders about GenAI and the transformational impact this emerging technology will have on business. Respondents say that uncertainty about the regulatory environment is the top barrier to implementing generative AI, but most are not slowing down their AI adoption.

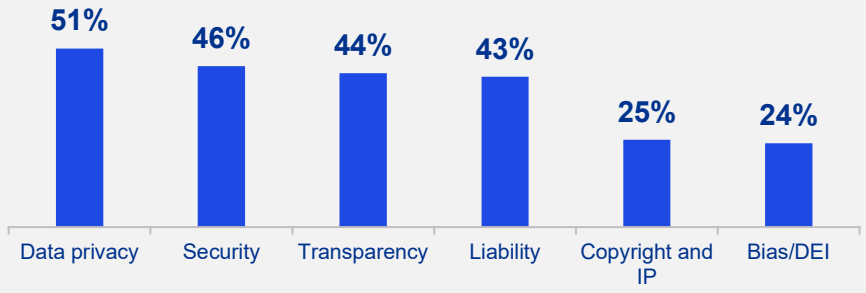


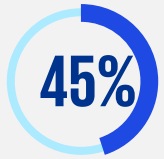
Nearly **8 in 10 business leaders (77%) say that evolving regulations have an impact** on their decision to make additional Generative AI investments.

More than **three quarters of businesses are not waiting or will take a short (3-6 month) pause with AI adoption** to monitor the regulatory landscape—only a quarter say they will wait longer.

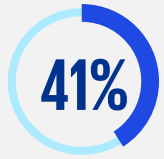


When it comes to GenAI, business leaders **anticipate the most regulatory action around data privacy**—less is anticipated around copyright and bias.





Hiring specialized talent



Creating new roles around regulations

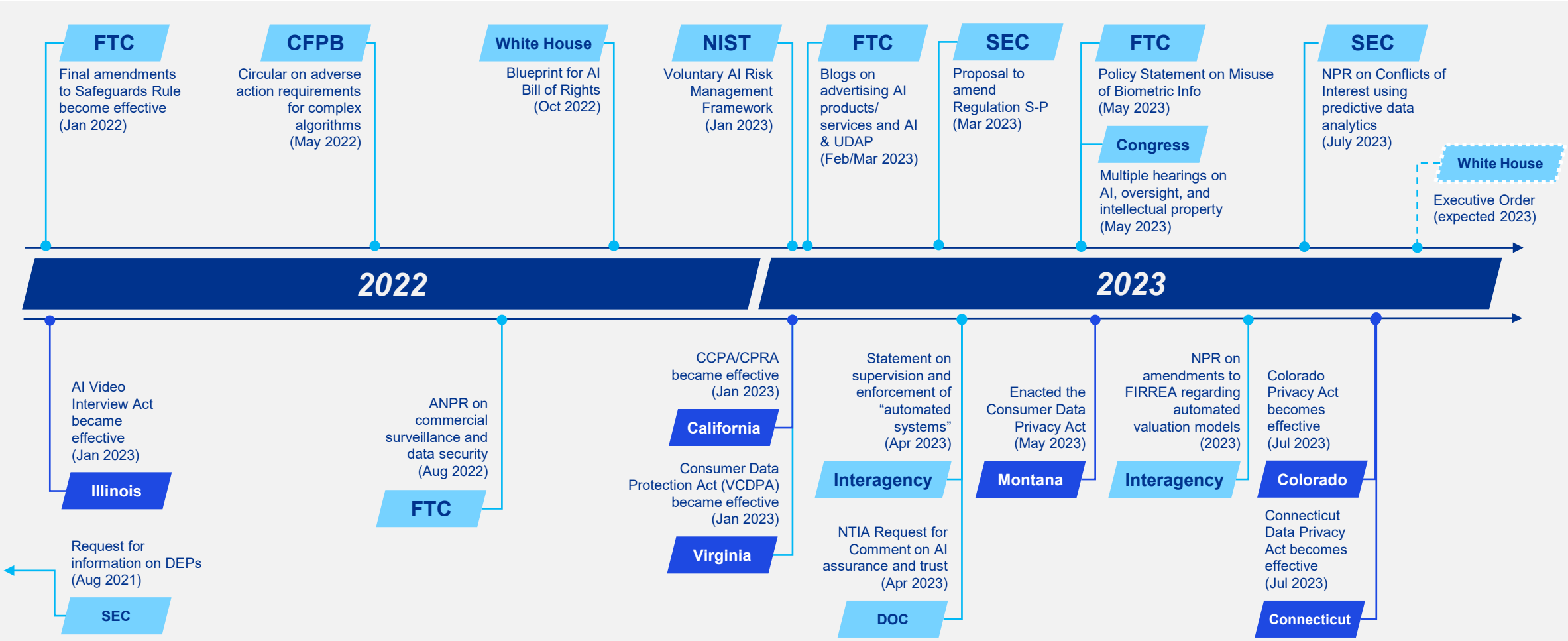
Partnering with third parties

The most common **planning measures** being taken in expectation of changing regulations around Generative AI include **hiring specialized talent, creating new roles around regulations,** and **partnering with third parties**.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AI-related Legislative & Regulatory Actions

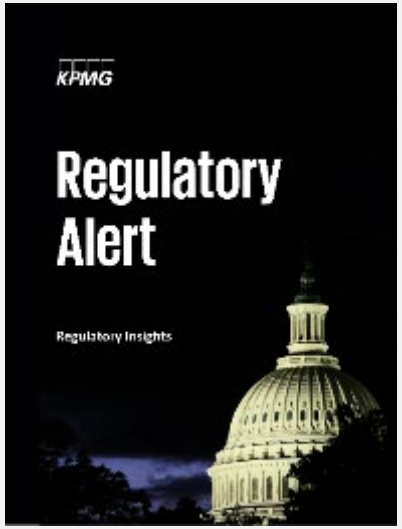
A wide array of actions from legislators and regulators at the state, federal and global levels seek to frame appropriate guardrails on AI technologies on enterprises, consumers, and other stakeholders. The timeline below shows select examples of these actions.



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Relevant Thought Leadership

From KPMG Regulatory Insights



- "Covered Technologies" and Conflicts of Interest: SEC Proposal
- Enforcement/Supervision to "Automated Systems"
- Ensuring Trust in AI: Commerce Department Request for Comment
- Focus on Tech: Cloud, AI, Personal Data

Firmwide

KPMG Speed to Modern Technology: Responsible AI

Download the paper

Download the paper

Download the paper

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contact us

Amy Matsuo
Principal and National Leader
Compliance Transformation (CT) &
Regulatory Insights
KPMG LLP

amatsuo@kpmg.com

Emily Frolick
Partner
US Trusted Imperative Leader
KPMG LLP

efrolick@kpmg.com

Bryan McGowan
Principal
Generative AI Lead, Risk Services
KPMG LLP

bmcgowan@kpmg.com

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP483563-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.