The Next Move

Regulatory and policy developments in tech — September 2024

pwc

AI compliance starts with ‘operationalizing’ your risk-assessment capabilities

By Jocelyn Aqua and Rohan Sen

The issue

The regulation of artificial intelligence, while still nascent and evolving, is largely coalescing around a risk-based approach that tailors its requirements to the level of potential harm posed by AI systems.

The EU AI Act, for example, imposes varying obligations depending on which of four risk tiers an AI system falls under — minimal, limited, high and unacceptable. In the United States, regulation at both the federal and state levels is targeting AI systems that typically would fall into the high or unacceptable risk categories under the EU AI Act. In China, the government acknowledges that risk is a factor in the level of obligations imposed by its AI regulations.

The ability to assess an AI system’s risk is therefore important to determining which regulatory provisions apply and, from there, to fulfilling any resulting obligations (documentation, testing, monitoring, impact assessments, conformity assessments, etc.). Equally important, having strong risk-assessment capabilities can help you prioritize your AI governance and compliance implementation efforts according to risk severity.

Organizations should take immediate steps to develop AI risk-assessment capabilities as there’s an increasing risk of exposure from emerging AI regulations as well as from existing requirements for handling personal data.

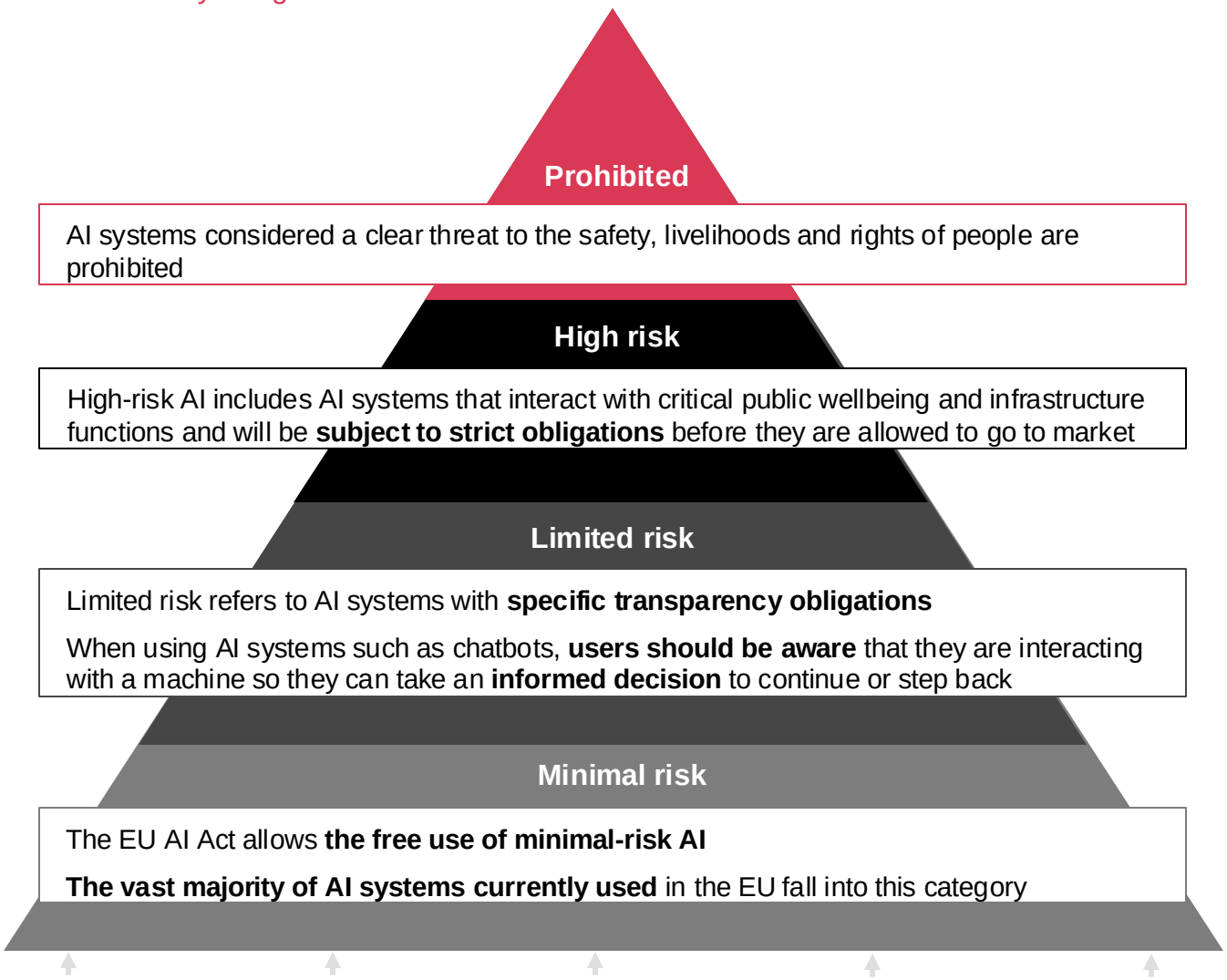
The regulators’ take

The clearest example of risk-based AI regulation is the EU AI Act, which categorizes AI systems based on their potential harm and imposes increasingly strict requirements the higher the risk. General purpose AI (GPAI) and foundation models also face requirements tailored to their risk, with most treated as limited risk — while those that pose systemic risk must undergo model evaluations, risk assessments, adversarial testing and incident reporting.

Risk-based approach: EU AI Act risk hierarchy based on type of AI

AI risk classification is based on the intended purpose of the AI system, in line with the existing EU product safety legislation. Risk classification depends on the function performed by the AI system and on the specific purpose the system is used for.

AI risk hierarchy – Highest risk to lowest risk



General purpose AI models (GPAI)

The EU AI Act provides **distinct requirements** for GPAI and foundation models

GPAI refers to AI systems that have a **wide range of possible uses,** both **intended and unintended** by the developers

Foundation models are AI models that can be **adapted to a wide range of distinctive tasks** and are trained on broad, large-scale datasets designed for generality of output

The AI Act places **additional requirements on high-impact GPAI and foundation models** with systemic risk, including, but not limited to model evaluations, risk assessments, adversarial testing and incident reporting

Generative AI: Individuals **must be informed** when interacting with AI and AI content must be labelled and detectable

Colorado's AI law. Colorado's SB24-205, as noted in our June edition, applies a similar, though less explicit risk-tiered approach to AI regulation. Most of its requirements apply to developers and deployers of "high-risk AI systems," defined as any AI system that, when deployed, makes or is a substantial factor in making "consequential decisions." Consequential decisions, in turn, are those with a material legal or similarly significant effect on the provision or denial to any Colorado resident of, or the cost or terms of:

- Education enrollment or an education opportunity
- Employment or an employment opportunity
- Financial or lending services
- Essential government services
- Healthcare services
- Housing
- Insurance
- Legal services

Exempted from the definition of high-risk AI systems — and from the corresponding obligations — are AI technologies that don't make consequential decisions. These low-risk tools include anti-virus programs, spam filters, calculators, firewalls, networking apps, cybersecurity tools, AI-enabled video games and voice-activated recommendation technology (if subject to terms that prohibit discriminatory or harmful content).

Section 6-1-1704 of the Colorado law also imposes transparency obligations on deployers of AI systems that interact with consumers, requiring disclosure that the consumer is interacting with an AI system. This roughly approximates the EU AI Act's treatment of chatbots, deepfakes and other GenAI content, which fall under that regulation's limited risk category.

Directive to federal agencies. Guidance issued by the White House Office of Management and Budget (OMB) is similarly focused on high-risk AI systems. Although scoped to AI use by federal agencies, the directive signals the federal government's views on AI risk and aligns generally to how other regulators approach the technology. It creates two categories of high-risk AI outputs.

- Rights-impacting AI: AI output that serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material or similarly significant effect on that individual's or entity's:
    - Civil rights, civil liberties and privacy, including freedom of speech, voting, human autonomy, protections from discrimination and unlawful surveillance.
    - Equal opportunities, including fair access to education, housing, insurance, credit, employment and other programs in which civil rights and equal opportunity protections apply.
    - Access to critical government resources or services, including healthcare, financial services, public housing, social services and transportation.

- Safety-impacting AI: AI output that produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of:
    - Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, and mental health.
    - Climate or environment, including irreversible or significant environmental damage.
    - Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21 (or any successor directive) and voting infrastructure.
    - Strategic assets or resources, including high-value property and information marked as sensitive or classified by the federal government.

Your next move

Navigating risk-based AI regulations and the impact of AI risk across your organization will require a holistic AI risk management approach. By taking the following steps, organizations can understand the risks and the risk level of AI models and systems to better manage regulatory requirements and mitigate impacts.

Consider the following actions as your organization addresses AI risk.

1. **Embed risk considerations in your AI inventory and intake process.** Identify and assess AI models, their relevant data and the potential business applications to understand the risk profile of each use case. Your organization's risk tiers and the overall riskiness of each use can be determined by regulatory definitions of high to low risk, as well as broader business and customer impacts specific to your organization. Tiering AI use cases can help your organization to focus time and resources for risk mitigation and management on higher risk use cases. Establishing risk criteria and defined risk tiers can also provide evidentiary support for why a use case doesn't meet regulatory definitions of high-risk and isn't subject to those enhanced requirements.

   Assess risk at the AI system, the AI model or the AI use case level based on the frequency that AI models are reused within your environment. Determining this base unit for evaluation is essential to effective risk analysis and maintaining an AI inventory. Once evaluated during intake, log the AI system, model or use case, as well as the determinative risk criteria, in your organization's centralized inventory. Cloud-based inventory solutions like Model Edge can integrate with other API tools to enable effective model management and risk governance.

A risk- based intake process enables effective governance for AI and beyond

2. **Establish a risk-focused operating model to address risk throughout the AI life cycle.** Management of AI risk requires continual governance throughout the AI life cycle. Create processes and defined roles to meet the specific documentation, testing and monitoring requirements required by an organization for all AI use cases. For high-risk use cases, establish processes aligned with regulatory requirements and more rigorous and frequent testing procedures. For all AI use cases, defining the associated risk will help you calibrate the correct level of governance and controls to mitigate risks for each model and the AI program overall.
3. **Integrate AI risk into enterprise risk management.** Based on the risks defined by regulators and risks particular to your organization or your AI use cases, identify and define AI risks in an enterprise risk taxonomy. These risks should cover AI specific risks like model and use risks, as well as cross-functional risks related to data, infrastructure and regulatory concerns. Determine whether to address AI risk holistically as a new domain or to update existing risk functions like privacy, security, data governance or third party to address risk posed in AI use cases. Integration of AI risk management with existing risk management processes is essential to address the cross-functional impacts of AI risk.

EU democratizes data in connected devices, altering product roadmaps

By Sara Putnam

The issue

Companies that sell connected products or digital services in the European Union will soon face sweeping new rules for data access, sharing and portability. The EU's Data Act — which took effect on January 11, 2024, and becomes largely enforceable in September 2025 — will allow users of connected products to access the data generated by these products and related services, and to share this data with third parties. It will also allow users of cloud and edge services to switch between providers more seamlessly.

As the European Commission explained, "The Data Act will ensure fairness in the digital environment by clarifying who can create value from data and under which conditions. It will also stimulate a competitive and innovative data market by unlocking industrial data, and by providing legal clarity as regards the use of data." The regulation will be enforceable by member states, which will have authority to issue fines of up to 4% of global revenue.

Compliance with the Data Act will likely require significant product, process and contractual changes and the implementation timeline is short for such extensive work. Manufacturers of connected devices and machines sold into the EU market should start now to inventory affected products and assess the impact on product roadmaps. Similarly, cloud service providers will need to remove barriers — technical, contractual and otherwise — that prevent customers from easily switching to other providers.

The regulator's take

The Data Act is a key pillar of the European data strategy and aims to advance the EU policy goal of achieving digital transformation by 2030. It complements the Data Governance Act, which became applicable in September 2023. While the Data Governance Act regulates processes and structures that facilitate voluntary data sharing, the Data Act clarifies who can create value from data and under which conditions. Together, these two measures aim to facilitate reliable and secure access to data, fostering its use in key economic sectors and areas of public interest, while also helping to establish an EU single market for data.

Data access, use and sharing. The Data Act (Chapters I through III) allows users to access the data generated by their use of connected devices and to share this data with third parties of their choice, except designated gatekeepers. Specifically, it gives users the right to access data generated by their use of connected devices, including relevant metadata, requiring further that the data be provided securely, free of charge, in a structured format and in real-time where feasible. Where data is made available in a business-to-business relationship, it must be provided on fair, reasonable and nondiscriminatory terms and in exchange for reasonable compensation.

For example, the owner of a connected car will be able to directly access or request that the manufacturer share certain data generated by the car's use with a repair service of the owner's choice. As the EC explains, "This will give more control to consumers and to other users of connected products and it will boost aftermarket services and innovation. Incentives for manufacturers to invest in data-generating products and services will be preserved, and their trade secrets will remain protected."

The accessibility of data pertaining to the performance of industrial equipment also opens opportunities for enhancing efficiency. Industries such as manufacturing, agriculture and construction can improve operational cycles, production lines and supply chain management, leveraging machine-learning technologies.

Unfair contractual terms. Under Chapter IV, the Data Act protects European businesses from unfair terms in data sharing contracts that one party unilaterally imposes on the other. The goal is to help small and medium-size enterprises (SMEs) participate more actively in the data market.

Data processing service switching. Chapter VI of the regulation aims to increase competition in the European cloud market by allowing customers to switch seamlessly — and eventually free of charge — between different cloud and edge providers. Designed to promote competition and choice on the market while preventing vendor lock-in, this provision requires the removal of technical, contractual and other barriers that hinder users from switching providers. According to the EC, "any European enterprise could combine data services from different cloud providers ('multi-cloud') and benefit from the vast opportunities in the EU cloud market. It will also drastically reduce costs for businesses and administrations when they move their data and applications to a different cloud provider."

Interoperability. Chapter VIII of the Data Act introduces measures to promote the development of interoperability standards for data sharing and for data-processing services, in line with the EU standardization strategy. To facilitate interoperability, companies that offer data or data services to others in the industry must describe the dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty in a machine-readable format to allow the recipient to find, access and use the data. They must also describe data structures, formats, vocabularies, taxonomies and code lists in a publicly available, consistent manner and must provide the technical means for accessing the data.

Implementation and enforcement. Member states are expected to create their own national penalties for infringements, which may include administrative fines of up to four percent of annual turnover. The EC must develop model contractual terms and standard contractual clauses to facilitate data sharing and confirm compliance, which will be published before the date of applicability in September 2025.

Your next move

The Data Act introduces challenges for companies that have historically relied on the exclusive control of data as a competitive edge. These companies should adapt their strategies to maintain their market position in a more open data economy. Affected manufacturers and cloud service providers should consider taking the following steps, where applicable.

1. **Inventory your data assets.** Inventory all data assets collected or generated, processed and stored by connected products and services. Identify where data resides, how it's used and who has access to it. Then categorize data based on relevant dimensions, such as sensitivity, trade secrets, quality and recency. In the context of personal data, the records of processing activities required under GDPR Article 30 may be a helpful starting point.
2. **Review and update data governance program and policies.** If one doesn't already exist, develop and implement an enterprise-wide data governance program or take steps to align your existing program to the Data Act. Establish clear internal policies to help manage data access and sharing, confirming compliance while safeguarding intellectual property and trade secrets. Define roles, such as data owners, data stewards, data custodians and so on, and define role-based responsibilities to manage data as a strategic asset.
3. **Develop a data-sharing framework.** Create a strategy for how your company will manage data sharing. Establish intake, response, escalation and dispute mechanisms. Implement guardrails (e.g., data tagging, access protocols, confidentiality agreements) to safeguard trade secrets and confidential information when sharing data. Establish mechanisms such as noncompete clauses to help prevent use of shared data to develop competing products or services.
4. **Plan for impact on product roadmaps.** Review and adjust your engineering and product development roadmap to ensure that all connected products and related services are designed to comply with Article 3(1) of the Data Act to avoid costly redesigns later. This includes allocating resources to design products and services as needed to meet the requirements for data accessibility, security and interoperability and to help plan for the necessary technical resources to support these changes.

5. **Begin contract remediation efforts.** Define model contract terms and identify your universe of in-scope data-sharing agreements. Begin to establish contract remediation efforts in a playbook to define clear terms, conditions and responsibilities for data access and usage and ensure terms are fair and reasonable in accordance with Article 13 Data Act requirements. Create fallback provisions and escalation plans for counterparties that want to negotiate contractual terms.
6. **Enhance data security and privacy measures.** Evaluate data security protocols, including encryption, access controls and data anonymization techniques, and conduct impact assessment of new requirements against existing measures to identify prioritized enhancements.
7. **Build a data ecosystem.** Develop a strategy for building a data ecosystem that includes active collaboration with key partners, customers, industry consortiums and other stakeholders to facilitate mutual data sharing. By building a robust data ecosystem, your company can leverage shared data to enhance product innovation, improve operational efficiency and create new revenue streams.

Cloud risk in financial services prompts more action from Treasury

By Shawn Lonergan

The issue

As banks and other financial firms become increasingly reliant on cloud services to support internal operations and business line functions, regulators worry that a single incident could have cascading effects on the US economy. In response, the Treasury Department's Cloud Executive Steering Group (CESG) has issued resources to foster secure cloud practices and resilience in financial services.

Although cloud offers many benefits for financial institutions — lower costs, faster deployment times, shorter product development cycles, improved security — it can also introduce unique risks. Under the shared responsibility model, financial entities are ultimately responsible for anything hosted on cloud. This puts sensitive financial data and operations at risk of misconfigurations, outages, cyberattacks and other issues.

Historically, US banking regulators have been generally neutral on the technology that entities use, but recent developments signal more cloud services regulation may be coming. Financial firms and cloud providers that serve them should take steps to improve their security practices to address regulatory concerns.

The regulator's take

On July 17, 2024, the CESG issued a collection of resources to help foster more secure cloud practices and resilience in financial services. This is the latest action since last year's Treasury report describing cloud risks in financial services and outlining a roadmap for next steps. That report, issued February 2023, identifies six specific issues facing the financial sector.

- Lack of transparency needed to monitor risk. Many financial institutions feel the information shared by cloud service providers (CSPs) is insufficient to understand the risks associated with their services. However, to maintain the security of their multi-tenant environments, CSPs often limit physical access and refrain from sharing sensitive information. This can make the type of in-person audit needed to assess third-party risks difficult to accommodate at scale.
- Technical complexity. Security incidents caused by user misconfigurations are increasingly common at financial institutions. In many cases, misconfigurations are a byproduct of highly complex cloud service offerings and/or the lack of appropriate staff expertise.

- Operational incidents. Like any technology used by financial institutions, cloud services are vulnerable to operational risks. This includes operational incidents originating at a CSP. Greater substitutability between CSPs might partially address this challenge, but it can also be impractical.
- Market concentration. The current cloud services market is dominated by a few providers. This means that many financial services firms are relying on the same companies, which could lead to widespread risks if something goes wrong. However, regulators don't have enough data to fully understand this risk's impact on the industry.
- Contract negotiations. While financial institutions of all sizes consider negotiating with CSPs challenging, smaller organizations note a lack of bargaining power. Contract issues include audit rights and termination clauses, the disposition of encryption keys, and custom provisions.
- Fragmented global regulation. Increasing foreign scrutiny of cloud services and CSPs could pose risks to cloud services used by US financial institutions and potentially prevent global firms from deploying cloud services across the entire enterprise.

Cloud steering group. One of Treasury's first moves following its report was to establish the CESG, an advisory body consisting of agency heads and sector CEOs, in May 2023. A broad public-private partnership between the Treasury, the Financial and Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council (FSSCC), and cloud providers, the CESG was created to help make cloud safer and more resilient within and beyond the financial services industry.

Guidance and resources. The CESG's recently issued resources aim to help financial institutions of all sizes with secure cloud adoption and operations. These include:

- A common lexicon for financial institutions and regulators to use in discussions about cloud.
- The Cyber Risk Institute's Cloud Profile 2.0, a tool that provides a framework for secure cloud implementation.
- Cloud outsourcing guidance that outlines key considerations for contracts between financial institutions and CSPs.
- Guidance on cloud security and resilience, which offers leading practices for transparency and architecture and suggests pre-configured cloud setups with built-in security to make deployment easier.

More information on coordinating cyber incident responses and addressing cloud concentration risks will be available soon.

Your next move

Financial institutions should take deliberate steps to make sure cloud strategies are resilient, secure and compliant with forthcoming standards. We recommend several steps your organization can take to prepare for evolving regulatory requirements, mitigate cybersecurity risks and get more value from cloud services.

1. **Improve transparency and monitoring practices**. Better transparency can help you manage third-party risks more effectively and prepare for the possibility of regulations that require more oversight. Start by strengthening due diligence processes while maintaining continuous oversight of cloud environments. This will require a deep understanding of software dependencies, supply chain risks and security practices of CSPs.
2. **Prepare for regulatory coordination**. Work proactively with regulators and align with industry standards to help you stay ahead of policy changes. Start by developing processes to engage with multiple agencies and participate in industry initiatives, like coordinated incident response plans and tabletop exercises.
3. **Manage market concentration risks**. Address market concentration risks now to help you comply with future regulations that will focus on resilience across the sector. Evaluate reliance on CSPs and consider strategies to help reduce these risks, such as using multiple providers or adopting hybrid cloud models.

About | Contact us | Contributors

Why do we publish The Next Move?

Regulators and policymakers — keen to build new guardrails for a digital society — stand on largely unfamiliar ground. They often take different, sometimes contradictory, approaches because they have different missions and visions. At the global level, regulatory divergences reflect profoundly different value systems. Building trust in technology is complex work.

Through PwC's Next Move series, we can provide context to policy and regulatory developments in technology and tell you how you can get ahead of what might come next.

For additional information on our Next Move series, please contact:

Matt Gorham

Cyber & Privacy
Innovation Institute Leader

202 951 0439

matt.gorham@pwc.com

LinkedIn

Chris Pullano

Financial Services
Advisory Partner

917 520 4447

christopher.pullano@pwc.com

LinkedIn

Contributing editors and authors: Ted Trautmann, Julia le Fevre, Sarah Surgeoner, Tony Sebastian