

The rapid deployment of Artificial Intelligence (AI) across multiple industries is capturing the interest of regulators, who aim to promote AI technologies while ensuring their responsible use. Recent regulatory developments in the European Union (EU), United States (US) and United Kingdom (UK) illustrate how such regulatory interest can take various forms, with some common themes.

Below, we provide a comparison of key points among the regulatory approaches to AI in the EU (on the basis of the [EU AI Act](#)), US (based on the Biden Administration's [Executive Order on AI](#)) and UK (based on the UK Government's [response to its AI consultation](#) [[the UK Response](#)]).

Comparative Table on Approaches to AI Regulation in the EU, US and UK

	EU - EU AI Act	US - Executive Order on AI	UK - UK Response
Horizontal vs sectoral regulatory approach	This is horizontal legislation, meaning that it lays down rules to regulate AI in a harmonized way across the EU, without differentiation by sector.	This adopts a sectoral approach, requiring executive departments and agencies across various sectors to formulate a consensus on industry standards, guidelines, practices, and regulations for the development and use of AI.	This adopts a primary “context-based” approach to AI regulation – i.e. regulation that fits various sectoral contexts, on a technology-neutral basis subject to five cross-sectoral principles: <ul style="list-style-type: none"> • Safety, security and robustness; • Appropriate transparency and explainability; • Fairness; • Accountability and governance; • Contestability and redress.
Definition of AI	This defines an AI system as <i>“a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives,</i>	This defines AI as <i>“a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to</i>	There is no formal, general definition of AI. Instead, the UK’s context-based approach is intended to guide interpretation(s) of the concept of AI by sectoral regulators, some of which have adopted their own definitions for AI or particular types of AI.

	<p><i>how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”</i></p>	<p><i>perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.”</i></p>	
<p>Focus on risk</p>	<p>This envisages a risk-based approach. It classifies AI systems based on their level of risk and provides subsequent obligations depending on this classification. Namely:</p> <ul style="list-style-type: none"> • Some AI systems are considered as presenting an unacceptable level of risk and are completely prohibited in the EU (prohibited AI systems); • Some AI systems are considered as presenting a high level of risk and are subject to stringent regulatory obligations (high-risk AI systems); • Some AI systems are subject to specific transparency obligations. 	<p>This generally uses a risk-based approach that balances AI’s upsides with potential downsides. Higher-risk applications are likely to receive greater scrutiny.</p>	<p>The UK Government intends to establish a central government coordinating function “to monitor and assess risks across the whole economy and support regulator coordination and clarity.”</p> <p>A key focus of this central coordinating function is risk. In 2024, the UK Government plans to launch a consultation on a “cross-economy AI risk register.”</p> <p>As a starting point, the UK Response identifies three broad categories of AI risk:</p> <ul style="list-style-type: none"> • Societal harms: This includes workforce issues, intellectual property protection, bias and discrimination, privacy, safe and trusted content, competitive markets, and best practice in the public sector; • Misuse risks: This encompasses risks like electoral interference, cyberattacks and criminality, and AI-based weapons; and • Autonomy risks: This primarily involves advanced AI systems that could evade human control.

<p>Rules on General Purpose or Generative AI/ Foundation models</p>	<p>This provides statutory obligations for General Purpose AI models (GPAI models), i.e. AI models that display significant generality and are capable to competently performing a wide range of distinct tasks, such as Large Language Models (LLMs). At the same time, it imposes additional and more stringent regulatory obligations on GPAI models with systemic risks (GPAI models with high-impact capabilities).</p>	<p>This directs the enactment of guidelines and best practices for the secure development of generative AI and so-called “dual-use” foundation models (referring to AI models that are broadly trained on billions of inputs and parameters and could pose risks to national security, the economy, or public health). In addition, guidelines will be adopted relating to assessing and managing the safety, security, and trustworthiness of such dual-use foundation models.</p>	<p>This explores affirmative regulation for “highly capable” GPAI systems, noting that the UK’s primary context-based approach may not be appropriate for GPAI systems that are useful across sectors.</p> <p>It then explores voluntary and non-regulatory steps that the UK Government is already taking, including cooperating with the US Government to convince leading AI companies to publish their safety policies, a report on processes for frontier AI safety, and to have their advanced AI models tested by the newly-established UK AI Safety Institute. However, the UK Response ultimately suggests that mandatory regulation will likely be necessary <i>“to ensure risks are adequately addressed.”</i></p>
<p>Testing and monitoring throughout the AI’s lifecycle</p>	<p>This requires providers of certain AI systems to comply with a set of obligations on requirements, including testing for market access as well as post-market monitoring.</p>	<p>This stresses the importance of testing and evaluations, including post-deployment performance monitoring, with the aim of ensuring that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed, and secure. For example, it provides for pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.</p>	<p>The UK AI Safety Institute is heavily involved in the testing and monitoring of AI, with numerous activities underway. Leading AI companies developing highly capable AI systems have pledged to collaborate with the UK AI Safety Institute to test their AI systems pre- and post-deployment.</p> <p>Moreover, at the first AI Safety Summit which took place in November 2023, leading AI developers set out the steps they are already taking to</p>

		Further, the March 28 Office of Management and Budget (OMB) Policy Statement <u>requires</u> federal agencies to have a plan to develop continuous-monitoring infrastructure to build, test, and maintain AI used by agencies.	make their AI models safe and committed to sharing the most powerful AI models with governments for testing to ensure safety and prepare for the risks of tomorrow.
Open source AI	This excludes AI systems released under free and open source Licenses as long as they are not prohibited, high-risk or AI systems that are subject to transparency obligations.	This does not include any provisions targeted specifically on open source AI. However, in late February, the Department of Commerce’s National Telecommunications and Information Administration published a Request for Comment (RFC) on open weight AI models. The RFC follows from the Executive Order on AI’s focus on dual-use foundation models and seeks to balance the risks and benefits from widely available access to AI model weights.	In its discussion of GPAI systems, this addresses the issue of whether there should be restrictions on open source release of AI systems. It observes that open release of AI has been beneficial for innovation, but suggests that there is “an emerging consensus on the need to explore pre-deployment capability testing and risk assessment” for powerful GPAI systems, especially those that are open source. The UK Government plans to engage further with experts on this issue in 2024.
Measures to support innovation	This seeks to promote the establishment of “regulatory sandboxes” and real-world-testing, by EU Member States’ authorities. Regulatory sandboxes are controlled environments, where stakeholders can develop and train innovative AI systems with the support of regulatory authorities before placing them on the market.	This envisions the establishment of “testbeds”, i.e. facilities or mechanisms equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI, to help evaluate their functionality, usability, and performance, as well as assess the near-term capabilities of AI systems.	The main focus of the UK Response is to support innovation.

		<p>Likewise, the March 28 OMB Policy Statement requires that government agencies innovate in their use of AI, including by sharing data and developing the continuous-monitoring infrastructure referenced above to build, test, and maintain AI systems.</p>	
<p>Role of sectoral regulators</p>	<p>This provides that certain aspects of internal risk management processes for high-risk AI systems may be part of, or combined with the risk management processes established in certain sector-specific EU laws. Moreover, it establishes that any amendments, delegated or implementing acts of the EU AI Act must take into account the regulatory specificities of each sector. The same applies to existing governance, conformity assessment, and enforcement mechanisms and authorities on the basis of certain sector-specific EU laws. However, no discretion is awarded to sectoral regulators in terms of the regulatory obligations of the EU AI Act.</p>	<p>This establishes a framework for US Executive departments and agencies that develop industry standards, guidelines, practices, and regulations for the development and use of AI, tailored to their respective sectors.</p>	<p>The UK’s non-statutory approach gives significant discretion to sectoral regulators, with possible central government coordination. For example, although the UK Response does not announce any affirmative AI regulatory measures by the Department for Science, Innovation and Technology (DSIT) or other central government departments, it does speak with approval of actions by sectoral regulators, including a review of foundation models by the Competition and Markets Authority (CMA) and guidance on data protection and AI by the Information Commissioner’s Office (ICO). In addition, the UK has established a Digital Regulation Cooperation Forum, comprising the CMA, ICO, the Financial Conduct Authority, and communications regulator Ofcom.</p>

<p>Type of regulatory intervention and enforceability</p>	<p>This will be the world’s first comprehensive AI law establishing statutory obligations for all actors across the AI value chain. As an EU Regulation, it will be directly applicable in all EU Member States, and it will have a direct impact on organizations that fall within its scope.</p> <p>It establishes a shared supervision and enforcement regime between the EU Member States and the European Commission. The EU AI Office, established within the European Commission, will have exclusive powers over GPAI models. EU Member States’ authorities will oversee other AI systems.</p> <p>Moreover, failure to comply with the obligations enshrined in the EU AI Act could be sanctioned by fines up to € 40 million or 7% of worldwide annual turnover.</p>	<p>This does not have the direct force of a law passed by Congress and signed by the President. Instead, it is a series of directives to federal departments and suggestions to agencies on various aspects of AI. It can be revoked or modified by the current or any future President. While the Executive Order on AI does not provide any new causes for enforcement, it does stress the applicability of existing US law to AI, especially IP law, consumer protection, law related to fraud, etc. For example, Deputy Attorney General Lisa Monaco has noted that the US Department of Justice’s “Disruptive Technology Strike Force” would put AI enforcement at the top of its priority list. Further, the US Securities and Exchange Commission (SEC) has brought three enforcement actions related to AI in Q1 of 2024 under allegations of fraud or making false and misleading statements. Other agencies have also instituted rulemakings or guidance on AI: the Federal Trade Commission (FTC) proposed rulemaking to ban AI impersonation fraud; and the Consumer Financial Protection Bureau (CFPB) issued guidance on the use of AI in credit denials.</p>	<p>The UK Government will approach AI regulation on a non-statutory basis for the time being, including the high-level “context-based” approach described above. The UK has not established any AI-specific enforcement or supervisory regime. Since the UK Response, there have been proposals in Parliament for AI legislation, which have not yet advanced significantly.</p>
--	---	---	--

Issues Emerging from the Different Regulatory Approaches to AI and Action Points

The differing approaches of the three jurisdictions will have significant impact on businesses that use AI systems. For example, the definition of AI Systems under the EU AI Act includes the generation of outputs for both for explicit and implicit objectives, while the Executive Order on AI only mentions only the requirement that predictions, recommendations, or decisions pertain to human-defined objectives, without specifying whether these include situations of both implicit and explicit such objectives. As the EU AI Act, the Executive Order on AI, and the UK Response progress on separate regulatory timeframes and added divergent approaches emerge, it is wise for companies to adopt a proactive compliance approach sooner rather than later and begin mapping their upcoming obligations in each jurisdiction. Getting an early start in revising company policies and procedures will allow businesses to mitigate potential liabilities and ensure compliance in a timely and appropriate manner.

With the formal adoption of the EU AI Act just around the corner and with US federal agencies having undertaken a series of actions in response to the Executive Order on AI, businesses must be proactive and agile. When it comes to the UK, much remains in play for its approach to AI regulation, and organizations who are interested in the development of this regulation would do well to begin to engage with it this year. Overall, the ongoing and divergent approaches to AI regulation in the EU, US and UK, will make it challenging for companies to navigate in the global AI regulatory landscape.