AIFS0074

Written evidence submitted by UK Finance

About UK Finance

UK Finance represents over 300 firms within the financial services sector. Our objectives are to support industry to drive innovation and economic growth, assist vulnerable customers, combat economic crime, and facilitate the transition to net zero.

Introductory comments

AI offers the potential for a range of benefits, including improved personalisation of products, increased efficiency, more effective risk management and compliance and more effective prevention of fraud and other crime.

The financial services sector has a long history of digital innovation and has been gradually adopting AI for many years. Our members are in the process of adopting AI carefully and responsibly as they build on their risk management frameworks, within the context of a robust and comprehensive regulatory environment.

We support the UK's innovation-focused approach to AI regulation, based around guidance and outcomes, and led by existing authorities. We look forward to continuing to work with them as the technology evolves to ensure that the opportunities offered by AI can be taken advantage of, and the related risks effectively managed.

We explore these themes in more detail in our responses to the Committee's questions, below.

How is AI currently used in different sectors of financial services and how is this likely to change over the next ten years?

1. *Are there areas of financial services that are adopting AI more quickly and at higher rates of penetration than others? Are Fintech firms better suited to adopting AI?*

- We do not have data on hand to answer this question directly. However, Bank of England research indicates that international banks and insurance are the areas within financial services that have adopted AI the most widely so far (see **Chart 2**). Other parts of the sector, including UK banks, also have high rates of adoption.
- We also highlight that the use of AI is not new to financial services, and some financial institutions have been exploring and adopting the use of AI and machine learning (ML) applications for more than a decade. Common use cases are explored later in our response.
- The adoption of AI varies significantly across financial services – as highlighted in the Bank of England research (see **Chart 3**) and a recent independent third-party survey (**Jaywing**). Both studies highlight that there is a sliding scale of adoption with most institutions in the exploratory phase, with smaller numbers on the extremes of no adoption to advanced adoption. The rate of adoption will be dictated by firms' board appetite, having skilled individuals to deliver AI solutions in line with business needs and the infrastructure to be able to operationalise use cases.

2. *What percentage of trading is driven by algorithms/artificial intelligence?*

- We do not have data to answer this question. However, we can make a number of observations.

Use of algorithms and AI in trading

- Algorithmic trading and AI-driven trading should not be conflated. The use of algorithms in trading has been standard for many years and it is incorrect to say that all algorithmic trading is AI-driven.
- There are traditional statistical techniques used in trading, which are not considered AI. These include methods such as time series analysis and regression analysis. These have long been used in financial markets and are typically well understood.
- Simple ML techniques have also been employed for many years in trading. More complex ML techniques such as deep learning and reinforcement learning have been explored more recently and are applied based on the suitability of the technique to improve human decision making.
- Generally speaking, financial institutions are not currently using generative AI for developing trading strategies and are proceeding cautiously with the use of generative AI.
- As financial institutions operate within an extensive regulatory framework, the appropriate regulatory controls are applied to trading activity regardless of the technology being used.

Regulation of trading activities

- Algorithmic trading is well regulated by the FCA. A suite of rules set out the governance, oversight and control expected to be in place by firms to mitigate any conduct and operational risks that might arise from the use of algorithmic trading.
- Regulated financial service providers design control functions like compliance and risk management to match the scale and complexity of their automated trading. Steps are set

out within governance frameworks including ongoing monitoring, human oversight, annual validation, pre-trade checks, kill switches, user training, and change control for model updates.

3. *Are financial services adopting AI at a faster rate than other sectors in the economy?*

- As noted above, the use of AI is not new to financial services, and some financial institutions have been exploring and adopting the use of AI for more than a decade. Widespread use cases are outlined under question four.
- A World Economic Forum **report** from 2025 states that – globally – financial services firms are adopting AI at a faster rate than most other sectors in the economy. This is based on AI spend data – see figure 2 on page 8.
- Similarly, a 2024 **report** by Databricks notes that financial services are ahead of other sectors in generative AI adoption in some areas, such as acquisition of graphics processing units (pages 26-33).
- In relation to the UK specifically, research by the FCA and Bank of England from late 2024 reveals that 75% of firms have already adopted AI, with an additional 10% planning to implement it within the next three years (**see 2.1**). In contrast, June 2023 **data from the ONS** showed that only 16% of UK businesses were using at least one AI technology. Although overall adoption among UK businesses likely increased during 2024, these figures indicate that the financial services sector is embracing AI at a significantly faster rate than the broader UK economy.

To what extent can AI improve productivity in financial services?

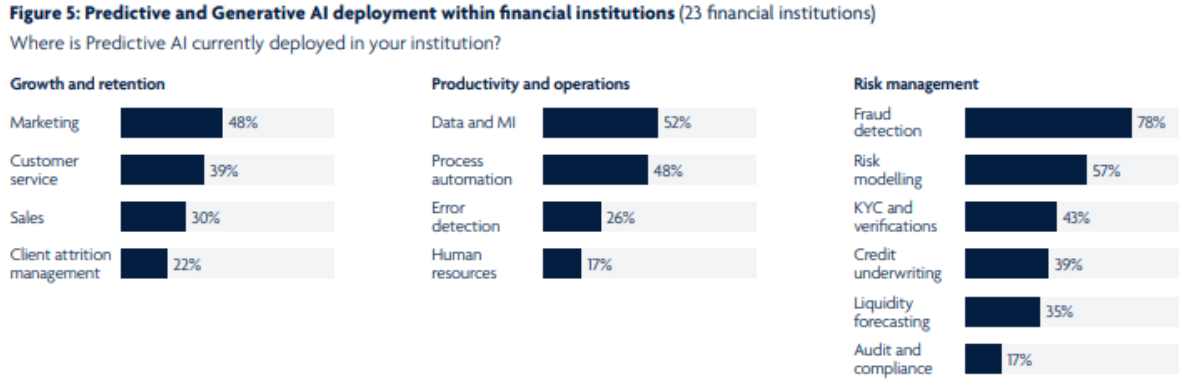
4. *Where are the best use cases for AI?*

- As AI technology is evolving rapidly, it is challenging to answer this question with confidence. Nonetheless, we can provide some observations based on the insights we have from members.
- Of the use cases currently deployed, we see particular promise in those related to risk management, fraud detection and cybersecurity.
- We can also illustrate more generally where the technology is being utilised currently and areas where generative AI, in particular, might be poised to play a widespread role.
- Current important use cases of AI in financial services include the following, though some are still in early stages of development:
  - **Fraud detection**: ML models to detect fraud, for instance on outbound payments and inbound deposits. ML models are more capable than traditional models and controls to pick up 'niche' complex fraudulent activity. This enables more operationally efficient targeting of fraud, and better risk targeting.
  - **Anti-money laundering / transaction monitoring and sanctions screening**: AI tools for high volume businesses (like payments) to screen transactions and detect anomalies. ML models can enable the more sophisticated targeting of outlier/anomalous behaviour using Gaussian Mixture Models to support more traditional models of the Standard Deviation type. AI models may also be used to reduce false positives and improve operational efficiency.
  - **Trading**: Reinforcement learning techniques can be used to improve pricing and hedging accuracy.
  - **Credit decisioning**: Traditional ML models based on decision trees are used to facilitate credit decisions about credit approvals, detecting overlimit account transactions, pricing and loan amounts for customers. The application of ML models to credit decisioning more broadly is also now being explored, for example to

underwrite risk scores. ML models can enhance risk identification, and improve inclusion, over and above traditional credit scores (see for example this paper).

- **Marketing and customer support**: Using AI tools to engage and retain existing customers by using historical customer data to identify next best products and target rewards offers. Natural language processing (NLP) – ML technology that gives computers the ability to interpret, manipulate and process human language – has also been used to help direct and resolve customer queries.
- **Cybersecurity**: Firms are starting to use AI to detect and respond to potential cyberattacks more efficiently. For instance, AI can be used by security analysts to help classify suspicious emails.
- **Back-office functions**: In addition to the above, firms are also exploring traditional AI in back-office functions, including financial reporting, knowledge management and employee productivity enhancements. Productivity enhancements can be diverse but include utilising generative AI to increase the efficiency of routine internal processes, creating space for more creative activities (e.g. Microsoft365 Copilot). Other examples include using optical character recognition – the process that converts an image of text into a machine-readable text format – and NLP. –.
- **Payments, clearing and settlement**: AI tools used to provide real-time settlement insights, detecting anomalies and identifying settlement risks that enable firms to take action to mitigate the risk of settlement failure or delay.
- **Treasury and cash management**: AI models to enhance liquidity forecasting capabilities, helping treasurers to plan and pre-position effectively for potential market volatility.
- **Investment and wealth management**: Using generative AI to summarise client calls, extract key facts and capture actions, freeing up relationship managers to concentrate on the customer rather than administration activity. Firms also use traditional AI for market analysis.
- **Customer communications**: Use of generative AI to prepare correspondence, such as to draft complaint response letters. (See also below for our recent report on generative AI).
- **Code generation and conversion**: Utilising generative AI tools to provide coding assistance to software developers, automate code testing and pull request reviews, and translate legacy code.
- **Contact centre**: Streamlining and improving contact centre processes, using sentiment analysis to better understand customer demands or complaints with the aim to improve customer outcomes.
- **Risk management**: Using AI to help with key risk management operations, such as regulatory compliance.

- Our 2023 research with Oliver Wyman identifies the rate of AI use across a number of use case areas, in particular on page 8 (though this snapshot from mid-2023 may be going out of date):



- Our more recent **research** with Accenture from January 2025 identifies emerging use case areas for generative AI, specifically.
  - It indicates in section two that a wide range of generative AI use cases are emerging. These can be put into various buckets: customer engagement and personalised marketing, knowledge management and information retrieval, software development and data management, intelligent workflow and email processing, fraud and financial crime, legal, contractual and compliance text analysis, and desktop productivity.
  - It also takes a deeper look at three potentially impactful generative AI use cases: a complaint handling tool, a Know Your Customer (KYC) documentation tool, and use to accelerate the software development process.
- The 2024 Bank of England **survey** (Chart 6), indicates that the range of use cases is quite varied from firm to firm. Although around 75% of survey respondents were currently using AI, even the most common use case class – optimisation of internal processes – had uptake of only 41%.
- Appropriate controls are of course necessary and will vary for each use case. Having a 'human in the loop' and other types of controls are explored further in other parts of this response.

5. *Which transactions may benefit from AI?*

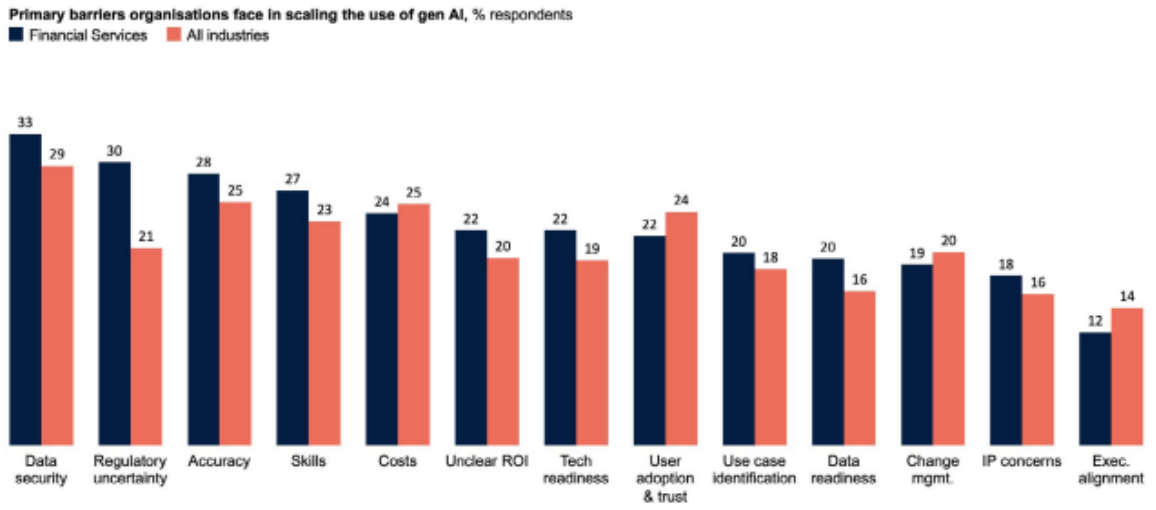
- We are not entirely sure what is intended by this question, though our comments above should be relevant. We can also add that international transactions might be able to derive particular benefits from AI. There is potential to improve speed and reduce costs using AI, for example to automate currency conversion, checks for anti-money laundering and KYC, and by routing transactions through chains of intermediaries more quickly.

6. *What are the key barriers to adoption of AI in financial services?*

Research on constraints in the round

- In relation to generative AI specifically, our recent paper with Accenture identifies a range of constraints (page 21):

Figure three: Perceived barriers to scaling generative AI



Source: Accenture

- The 2024 Bank of England survey (see 4.4 and 4.5) also examines this issue in relation to AI more generally and identified:
  - Key regulatory constraints are, in particular, data protection, and resilience, cybersecurity and third-party rules. The FCA Consumer Duty and Conduct Rules, intellectual property (IP) rights, and wider financial services requirements are also noted. Regulatory burden was the dominant constraint in relation to data protection, while the other regulation types were more varied, including for example lack of clarity. Suggestions on how best to address some of these key constraints can be found under question nine.
  - Diverse non-regulatory constraints were also identified. Those identified by over half of respondents were: safety, security and robustness concerns, insufficient talent or skills access, and achieving appropriate transparency and explainability.

Specific constraints identified by our members

- Our members identify a range of more specific constraints, though the significance of each varies according to the institution. Some of these constraints are challenges that are inherent to the technology, while others are due to wider factors:
  - For on-premises use cases a major barrier is the cost of high-performance compute.
  - **Technology changes at a very fast rate**: As a regulated industry with predefined controls, checks and risk mitigations, adoption within financial firms requires more time than in less regulated institutions.
  - **Deployment and implementation**: Legacy data and systems can mean it is not possible to implement sophisticated AI solutions. Broader system changes might be required for some firms before certain AI applications are feasible.

- **Data entitlement and accessibility**: IT infrastructure and controls over user access to specific data within larger data sets can cause complexity for firms in the development of models. All data used by firms has to be used in accordance with any usage restrictions imposed by the data owners. In many cases, these are sensible restrictions. However, in some cases – particularly usage restrictions imposed by regulators such as the FCA and Bank of England, for example – these are an impediment to use cases that can improve firms' compliance with the regulators' rulebooks. We would note, for example, a **restriction** imposed by the FCA preventing firms from reproducing more than 20,000 words from the FCA Handbook, without applying for a licence.
- **Skills and culture**: AI requires specialists across multiple areas, including data science, data engineering, risk management and operations. It can be challenging to recruit as required, due to competition in the marketplace and the relative scarcity of some skillsets. It can also be challenging to develop skills internally, due to the niche expertise that can be required for specialist roles. Furthermore, upskilling is required for the wider workforce to ensure successful and safe adoption of tools to support more generalist roles.
- **Governance, compliance and validation**: It is critical to ensure that AI is adopted safely. This requires thorough due diligence to capture niche, new ways that risks may present themselves, amplification of existing risks, and ensuring that adoption of AI is in line with risk appetite across a variety of risk areas. Financial institutions have sophisticated risk management frameworks in place to manage the risks across the whole lifecycle, starting from adoption.
- **Customer trust and digital education**: Some firms identify customer nervousness around the use of AI, particularly given high-profile cases of AI incidents within the media. This may reduce the speed of adoption among firms. As best practice risk management frameworks emerge, digital education and awareness develops, and more consumers have positive experiences with AI, this sentiment may recede. This issue is of course much wider than financial services.
- **Transparency and explainability**: Model complexity means it can take time for firms' senior management to familiarise themselves with the implications and necessary risk management tools for AI adoption. Similarly, model complexity can necessitate careful consideration of each use case to ensure that monitoring can be effective and that customers can be provided with key information about decisions, when needed.

Potential future constraints

- A potential emerging constraint might be inconsistency in international regulation. Most jurisdictions do not have an AI-specific regulatory or legal framework, but this may change. (The key exception is the EU AI Act, which we do not support reproducing in the UK – see also our response to question 19). If highly divergent regimes are developed globally, this will add significant additional complexity to global businesses, including not just financial institutions but also technology companies that wish to make AI products available to them. For global organisations, this will also require ongoing interaction with a large number of authorities regarding the application of AI.
- It is therefore important that there is a level of international cooperation. Any best practices or internationally accepted standards for AI should be developed through voluntary, industry-driven, multi-stakeholder collaboration in existing fora to promote interoperability across borders. Emerging best practice should be outcomes-focused rather than prescriptive. This is particularly important given differences between jurisdictions' legal and regulatory systems; a focus on outcomes allows firms to apply rules more readily across their group operations.

- Uncertain regulatory and legislative changes – the UK Government and regulators have a pro-innovation approach to regulation, which we support (see also our response to question 19). Nonetheless, the UK is still in an information gathering phase and there is a possibility of additional regulation or legislation in due course. Depending on the details of any rule changes, new regulation could create barriers.

7. *Are there areas where the financial services should be adopting Gen AI with little or no risk?*

Generative AI adoption and risk

- The ability of generative AI technology and large language models (LLMs) to process and generate natural language and to unlock informational value from unstructured data has huge value potential for firms. These emerging techniques can help firms to transform data and analytics for faster, better-informed decision-making, improve operational efficiencies and better manage risk, regulations and economic crime.
- Nonetheless, generative AI models have inherent limitations and give rise to certain challenges and risks. These include susceptibility to 'hallucinations', limited explainability of the AI model, firms' reliance on a limited (though growing) number of third-party LLM vendors, and data privacy risks.
- Financial institutions are mindful of these risks and as such are proceeding cautiously with their adoption of generative AI, starting out with lower risk in-house applications and maintaining human involvement. For example, internally facing applications used to augment capabilities of employees such as content creation, software production, analysis of public documents, tools to help navigate internal documents and document summarisation. Understanding of generative AI and effective risk mitigation is continually improving and, as it improves, further use cases become more feasible. We refer to other emerging use cases, being developed within strong risk management and governance practices, in other sections of this response.

Risk management

- The financial services industry is supportive of using generative AI within a strong risk management and governance framework. As mentioned, UK Finance recently published a **report** with Accenture, which specifically examines generative AI use cases in financial services and how risks are being managed. It includes case studies on 1) a customer complaints agent tool, 2) KYC documentation, 3) software development.
- Where necessary, financial institutions are readily adapting their existing risk management frameworks to account for the risks presented by generative AI, and third-party providers of AI solutions are proactively benchmarking themselves against established and developing AI governance frameworks.
- The controls on such activities should be proportionate to the application and use case, as well as the broader potential risks to the UK regulators' objectives – including financial stability, consumer protection, innovation, competition and competitiveness. A proportionate approach could look to streamline governance frameworks for lower-risk applications to avoid introducing unnecessary barriers to adoption of AI.
- Additionally, a number of bodies across the world have already developed recommended industry standards and guidance for AI usage, including the National Institute of Standards and Technology's (NIST) AI Risk Management Framework.

AI as risk mitigation

- It is also important to note that, though AI adoption can involve certain risks, there are also AI use cases that can reduce or better mitigate existing risks. These include improved compliance practices and improved management of counterparty risk.

8. Are there likely to be job losses arising from AI in financial services and if so, where?

- While there is potential for jobs within financial services to be replaced by AI, others may adapt and evolve alongside emerging technologies, particularly in areas which continue to require meaningful human judgement and emotional intelligence. The integration of AI also brings potential opportunities for employees across all business areas, not just those in technology-facing roles, to reskill or upskill in response to changes within their organisations. Many firms are already training employees to use AI appropriately in accordance with their risk management frameworks.
- Members are currently focused on deploying AI solutions that will enhance employees' day-to-day activities, rather than replace them. Some tasks may become automated, but new opportunities are also being created, allowing employees to spend time on more meaningful work. By embracing AI, employees can work smarter and more efficiently, leading to a more dynamic and fulfilling work environment.
- We observe that it is possible AI may create jobs overall, noting the recent World Economic Forum's **Future of Jobs Report 2025** which anticipates that by 2030, AI and other information processing technologies will transform 86% of businesses, sparking the creation of 170 million new roles worldwide while making 92 million existing jobs redundant.
- We do, however, also recognise the potential for disruption and the significant shifts in the job market. As AI becomes more integrated it may result in less need for humans in certain roles, for example in back office administrative support functions. Some low-skill jobs might be replaced by higher skill jobs, necessitating effective upskilling to enable a transition into these new roles. How this will play out in practice will depend on the pace of adoption and how firms choose to implement and manage the integration of AI.
- As noted earlier in our response, there are also concerns around AI skills shortages, which could have an impact on slowing the adoption of AI as firms struggle to find and recruit the required talent. With increased demand for particular skills, competition could also lead to higher salaries for certain specialised roles, resulting in increased expense for both public and private sector organisations to acquire and retain appropriately skilled individuals.
- The issues around potential skills shortages and upskilling are cross-sectoral so any initiatives should be considered at that level.

9. Is the UK's financial sector well-placed to take advantage of AI in financial services compared to other countries?

- The UK is well placed to take advantage of the adoption of AI in financial services, thanks to well-developed expertise in technology, financial and professional services.
- The UK has promise as an attractive jurisdiction for AI adoption with its currently flexible regulatory framework.
- Regulation sometimes struggles to keep pace with innovation. There is the potential for this to lead to unnecessary hurdles to technology adoption, over time. This can arise in particular for firms that are less technically sophisticated.
- For international comparison, the Monetary Authority of Singapore as early as 2018 launched the **Veritas Initiative** and Project MindForge in 2023, bringing together a number of financial sector participants and technology firms. Veritas aims to enable financial institutions to evaluate their AI-driven solutions against the principles of fairness, ethics, accountability and transparency (FEAT) to strengthen internal governance around the application of AI and the management and use of data. At the most recent AI Action

Summit in France, Singapore also **announced new AI Safety initiatives**, including a pilot for best practices around testing generative AI applications. The Trump administration in the USA has also recently published an **Executive Order** to remove barriers to American leadership in AI (although the details of the Trump administration's new approach to AI are yet to be published).

- In this context, the UK's regulators should consider ways for industry and regulators to collaborate to explore possible barriers to AI adoption in existing regulation and consider how they can be addressed. It would also be worth exploring the potential for such a public-private partnership approach to identify areas where there might be a need for greater clarity as to compliance best practice. The Singaporean approach above and the UK's Cross Market Operational Resilience Group (CMORG) provide potential models to explore.
- We note that the Bank of England and FCA are in the process of convening an '**AI Consortium**', which might contribute to, or consider the merits of, such a process.

What are the risks to financial stability arising from AI and how can they be mitigated?

10. Does AI increase the risks relating to cybersecurity?

- The relationship between AI and cybersecurity risks in financial services is multifaceted and requires careful consideration of both defensive and offensive capabilities. AI technologies can simultaneously strengthen security postures and introduce new vulnerabilities.

AI as a cybersecurity risk

- Cybersecurity is one of the most significant risks relating to the use of AI in the financial sector – see for example 4.2 in the recent Bank of England **report** on AI in the sector. There are two key elements, here:
  - First, the accessibility of AI tools (e.g. publicly available LLMs) can make it easier for malicious actors to engage in cyber activities and leverage AI to enhance their offensive capabilities. Opportunities for bad actors include using AI tools to develop more sophisticated phishing attacks, automate vulnerability discovery, generate malware, carry out social engineering, and conduct disinformation campaigns (for example, through the use of deepfakes).
  - Second, the increasing complexity of AI models used in financial services can bring risks. For example, growing use of complex AI systems can make it more challenging to audit security measures and identify potential weaknesses.
- The integration of AI also expands the attack surface and introduces vulnerabilities for firms. AI systems themselves can become targets, with threat actors potentially exploiting training data or launching attacks that manipulate AI decision-making processes. New threats such as prompt injection and jailbreaking could lead to bad actors manipulating AI models to behave differently or unexpectedly, or to leak data and bypass security systems.
- Nevertheless, cybersecurity is not a new challenge for the financial services industry. Many of the risks presented by AI applications are not novel or specific to the use of AI and are risks that financial services firms are already well equipped to manage through their existing governance and risk management frameworks.
- In addition, firms are already required to comply with existing legislation pertaining to cybersecurity, including UK GDPR and, where relevant, the Networks and Information Systems Regulations and Directors Duties.

AI as a tool to enhance cybersecurity

- From a defensive capability perspective, AI can also be used by firms as a tool to support with combatting emerging cybersecurity threats, for instance by improving threat detection and response times, which could help to improve risk management in this space. As noted in the US Treasury **report** on AI-specific cybersecurity risks in the financial services sector, types of cybersecurity AI tools used by firms may include anomaly detection and behaviour analysis methods, intrusion detection/prevention, data-loss prevention, and firewall tools.
- AI systems enhance threat detection by identifying patterns and anomalies in network traffic that would be impossible for human analysts to process in real-time. ML algorithms can adapt to evolving threats, providing dynamic protection against sophisticated attacks, and reducing response times to potential breaches. These systems are particularly valuable in detecting fraud patterns and protecting against automated attacks that traditional rule-based systems might miss.
- Overall, these technological advances require financial institutions to continuously evolve their security frameworks, ensuring robust governance around AI deployment while maintaining the flexibility to respond to emerging threats. Firms need to manage risk not by avoiding AI adoption, but by implementing it thoughtfully with comprehensive security controls and ongoing risk assessment processes.

11. What are the risks around third-party dependencies, model complexity, and embedded or 'hidden' models?

Third-party AI challenges

- AI does not introduce completely novel risks, per se, but does introduce challenges in third-party risk management (TPRM) that extend beyond traditional vendor risk frameworks, including model complexity, supply chain transparency, explainability and the presence of embedded models within third party products.
- However, while these factors may create new due diligence challenges that may require existing TPRM practices and processes to be adapted, they do not require a fundamentally different approach to third-party oversight or translate to unmanageable regulatory risk. Financial institutions' existing TPRM frameworks are evolving to address these risks and firms are continuing to leverage contractual, model risk and data governance frameworks to ensure they continue to meet their regulatory obligations.
- There are a number of operational challenges in this area that firms are adapting their risk management frameworks for. In particular:
  - Model complexity can make due diligence more operationally challenging for organisations, for example in relation to their financial services regulatory obligations and their UK GDPR obligations ensuring transparency for customers, etc. Complexity also makes such requirements as auditability and accountability more challenging.
  - Supply chains can be complex, with a model trained by one developer, supplied to another provider that fine tunes it before it is deployed by yet another actor further down the chain. Challenges include:
    - It can be more difficult to determine which firms hold the 'data controller' responsibilities at different points within the ecosystem.
    - There is outstanding uncertainty around liability for incidents caused by third-party models, though financial services firms will remain responsible for ultimate outcomes.
    - Problems with a model may manifest and become visible during deployment but can be due to bias or other issues at the level of one of the developers further up the chain. Complete information on the design

training of a model might not be available to all entities in the chain. (See also our comments under question 13, below).
    - Best practice is yet to emerge on the information AI providers should make available to clients to assist with their due diligence activities. Where a firm does not consider that it has received sufficient information about a model and its design, due diligence and assurance processes become more challenging. (We understand that the forthcoming AI Bill will focus on the providers of advanced models which might assist with firms' due diligence requirements).
    - It is possible that a supplier could have a model included in a product that is not fully disclosed. This raises the chance of issues like 'model drift' going undetected. (We presume that this is what the Committee intends by its reference to 'hidden models').

- Although these are indeed challenges, they are not novel or insurmountable. Similar issues arise with other types of external providers and firms address them through contractual arrangements, due diligence processes, monitoring and ongoing updates to risk management practices. Firms need to work through the relevant challenges for each use case, including taking steps to identify AI usage in the supply chain.
- Given these challenges, firms are cognisant of the need to be able to identify AI usage in the supply chain.

Existing and emerging safeguards

- As noted above, despite the operational challenges presented by AI, financial services organisations are already subject to a range of relevant regulatory requirements. Firms are required to demonstrate compliance with existing regulatory requirements, such as the 'good customer outcomes' requirements of the Consumer Duty. These outcomes-based requirements will apply whether a service is delivered using AI or not.
- Furthermore, TPRM rules require that firms have third-party oversight (TPO) programmes, policies and processes that establish an overarching and technology-neutral TPRM framework. These must be designed to be able to adapt to changes in technology and business models.
- Additional technical safeguards are also emerging. These include:
    - Testing and control techniques to help manage risks associated with LLMs, including fact-checking systems, automated citation tools, retrieval augmented generation (RAG) and fine-tuning of models with well-understood in-house data. See for example chapter 4 of our recent **report** on generative AI with Accenture for further detail.
    - Some firms are also utilising 'explainability' techniques, such as 'LIME' and Shapley values, which help illuminate the data inputs that are most influential on the outputs of an AI system in general, or which are most influential in relation to a specific decision. See also 2.7 of the 2024 Bank of England **survey**.
- There are also relevant regulatory changes either in train or being considered:
    - The Bank of England has **highlighted** that, depending on how the AI provider market evolves, this could require changes to the Critical Third Parties regime. (Although we also note that it is possible that a wider group of providers of high-performance models might emerge, as perhaps suggested by the appearance of DeepSeek).
    - We also note that some members with an international footprint are beginning to use the mechanisms of the EU AI Act in their AI risk management. Although much of the AI Act is yet to come into force, firms are beginning to use such components as the AI Act definitions in order to ensure a common approach across group compliance. (The Organisation for Economic Co-operation and Development's definition of AI is also used in the AI Act, which makes it relevant beyond the EU).

12. How significant are the risks of Gen AI hallucination and herding behaviour?

- In our view, hallucination and herding behaviour should be considered and treated separately and should not be grouped together.

Hallucination

- Risk relating to generative AI hallucination can be challenging, as 'creativity' is a core part of LLMs, but incorrect, false or misleading information as a result of generative AI hallucination could have a significant impact when it comes to financial services. Nevertheless, there are known techniques emerging, as explored in chapter 4 of our recent generative AI **report**, e.g. RAG, confidence scoring and model fine tuning.
- Over-reliance on AI or inadequate user knowledge could result in hallucinations impacting stakeholders. These impacts can manifest in reputational damage, loss of trust, legal issues, and ethical concerns, which pose significant risks to a firm's business operations.
- At present this risk means that financial services firms are being careful to limit the applications of LLMs to lower risk areas, where a 'human in the loop' makes sense to identify potential misinformation or errors in outputs. As mentioned above, where such mitigations improve, further use cases will become more feasible.

Herding

- There are concerns that the use of the same or similar models by market participants might result in the risk of herding whereby algorithmic outputs lead to uniformity in behaviour and potentially exacerbate flash crashes. However, this is an overly simplistic view of how AI might be used in trading.
- For example, foundation models are not currently directly suitable for developing trading strategies. Furthermore, there are existing mechanisms in place to address the risk of crowding or market volatility following previous flash crashes and algorithmic trading incidents.
- As mentioned in our response to question two, algorithmic trading is well regulated by the FCA under a suite of rules that set out the governance, oversight and control expected to be in place by firms to mitigate any conduct and operational risks that might arise from the use of algorithmic trading. Regulated financial service providers design control functions like compliance and risk management to match the scale and complexity of their automated trading. Steps are set out within governance frameworks including ongoing monitoring, human oversight, annual validation, pre-trade checks, kill switches, user training, and change control for model updates.
- There are also concerns regarding the risk of herding behaviour if third-party models are adopted at scale across financial service institutions without fine-tuning. For example, if third party fraud models were commonly adopted across multiple institutions without adjusting, it would mean that fraudsters could game the model to evade fraud defences. To mitigate this, third-party models should be integrated into broader rules suites leveraging other alerting triggers and models.

13. *Are there risks of having AI tools used in the financial sector concentrated in the hands of a few large tech companies? To what extent do the AI financial market tools rely on social media outlets? E.g. trading algorithms using social media posts?*

Concentration of the AI provider market

- AI is one of the few technologies driven by open-source libraries. The current landscape offers industries the ability to run, subject to resource capacity, fully on-premises solutions without reliance on tech company 'hyperscalers' thanks to open-source models.
- That said, concentration risk is a well-established concept in the financial services sector across a number of activities, including but not restricted to technology adoption. As such, we do see the merits of a diversified set of providers, while also recognising the benefits of scale and expertise that exist among the current set of leading firms developing AI.

Concentration, systemic risk and existing regulation

- It is true that the concentration of AI capabilities among a small number of large technology providers presents several important considerations for operational resilience and market dynamics. When financial institutions rely heavily on a concentrated pool of AI providers, this can create shared vulnerabilities across the sector that may amplify systemic risks. For instance, if multiple institutions depend on similar AI models or infrastructure from the same providers, any technical failures or security breaches could have widespread impacts across the financial system. This technological interdependence also raises questions about the sector's ability to maintain operational resilience and business continuity in scenarios where key AI service providers face disruptions.
- However, it's important to also recognise that large technology companies often possess the substantial resources, expertise, and infrastructure necessary to develop and maintain sophisticated AI systems at scale. These organisations can invest significantly in security and compliance measures that may be challenging for smaller providers.
- Furthermore, financial institutions can address the challenges through robust vendor management practices, maintaining internal AI capabilities where strategically appropriate, and ensuring contractual arrangements preserve their operational autonomy. This approach allows the sector to benefit from advanced AI capabilities while managing concentration risks through careful oversight and diversification of technology partnerships.
- While these providers offer robust, sophisticated AI solutions backed by significant resources and expertise, the sector must carefully manage potential concentration risks. The recent development of a critical third-party **regulatory regime** represents a significant step forward in addressing these challenges, providing potential additional oversight for technology providers deemed systemically important to the sector's stability. This regulatory evolution helps create a more balanced ecosystem where financial institutions can continue benefiting from advanced AI capabilities while maintaining appropriate operational resilience.

Additional potential complications stemming from concentration

- In order to carry out supplier due diligence, financial services firms need information about model design, training, etc. However, model developers can be reluctant to provide all the information that firms would ideally wish to have. We note, of course, that AI providers have legitimate concerns about protecting their IP.

- It is possible that a market with few model developers will lead to less competitive pressure for them to provide high quality information to clients. Ultimately, commonly agreed best practice for 'model cards' and other information to be provided to deployers of AI needs to emerge.
- Similarly, in the context of high concentration in the AI provider market, it might be more difficult in practice for firms deploying AI systems as 'data controllers' under UK GDPR to enforce controls on AI providers that are in theory acting as 'data processors' under the controller's instruction. For example, it is possible – though unlikely – that an AI provider could require financial services clients to allow the use of their data to enrich the developer's product. (At present, enterprise solutions from LLM providers do not typically include this as a condition of service).
- We also note that recent developments – notably the appearance of DeepSeek – might mean that markets will become more dispersed than previously anticipated. This could help to reduce the risk of third-party dependency and concentration in the model provider market.

Use of social media data

- Regarding reliance on social media outlets, our understanding is that AI financial market tools do not currently rely on social media. AI *might* be used to *gather information* to support human traders and support their individual judgment, but there is not an explicit *dependency* on this data source.

What are the benefits and risks to consumers arising from AI, particularly for vulnerable consumers?

14. What benefits to consumers might arise from using AI in financial services? For example, could AI be used to identify and provide greater assistance to vulnerable consumers?

Potential benefits from AI

- AI can potentially offer multiple benefits to consumers, by making banking more efficient and secure while also providing targeted support to those who may need it:
  - **Personalised financial advice and planning:** AI can offer tailored financial guidance and help with financial planning by analysing individual data, aiding consumers in making informed decisions on saving, investing, and spending.
  - **Fraud detection and prevention:** AI could enhance fraud protection by monitoring transactions in real-time to identify unusual patterns, potentially safeguarding consumers from financial fraud and identity theft.
  - **Improved customer service:** AI might improve customer service by offering greater self-service options and potentially quicker, more accurate resolutions.
  - **Credit scoring and lending:** AI has the potential to refine credit scoring by efficiently analysing diverse data points, possibly helping consumers with limited credit histories to access loans and credit products.
  - **Cost reduction:** AI could reduce operational costs for financial institutions by automating routine tasks, potentially leading to lower fees and better rates for consumers.
  - **Assistance to vulnerable customers:** AI might identify vulnerable consumers through financial behaviour analysis, enabling firms to provide targeted assistance and tailored financial products.

Complexities and points of caution

- In principle, AI could in time enable better identification of vulnerable customers through large-scale pattern recognition capabilities that can help identify vulnerable customers in a more objective or reliable way. Firms have obligations to identify and assist vulnerable customers under the Consumer Duty but the use of AI to do so would need careful consideration to ensure that there is no undue intrusion into customers' affairs.
- Care would also be needed to avoid tensions with UK GDPR requirements. For example:
  - To ensure that processing is within the 'reasonable expectations' of individuals.
  - To ensure that special category data is not inappropriately inferred. Schedule 2 of the UK Data Protection Act 2018 outlines exemptions which can in some cases be relied upon by firms for the processing of sensitive personal data (such as health data) to meet vulnerable customer obligations. It is unclear, however, to what extent these exemptions could be applied to bulk AI analysis across a firm's customer base, for example.
  - To ensure compliance with the automated decision-making (ADM) provisions of the UK GDPR. Although we welcome the simplification of requirements relating to ADM proposed by the Data (Use and Access) Bill, AI continues to raise challenges, such as providing meaningful information about the logic involved, effecting human review, or identifying the lawful basis for processing using ADM. This is particularly the case in scenarios where AI involves a 'black box', has a significant effect on the individual, or where AI is providing real-time or large volume decisioning. These challenges are only likely to increase as more extensive adoption of AI leads to a decrease in a meaningful 'human in the loop' as part of its deployment.
- Furthermore, where AI data monitoring is used to feed inclusive design, processes and operational practices it must be able to clearly demonstrate the evidence that drives change and improvement. Appropriate safeguards are required to mitigate the potential for poor, unfair, or potentially harmful outcomes based on inaccuracies or assumptions. For example, where identifying vulnerabilities via data such as call recordings or in app message content where context or tone may be missing.
- There are also certain products or offerings, such as Open Banking, which might be more difficult to use for certain customer groups, such as customers who struggle with English. AI interpretation could mask the real reasons why a customer might be struggling with a product, and this could lead to firms failing to understand what a customer is really vulnerable to.

15. What is the risk of AI increasing embedded bias? Is AI likely to be more biased than humans?

- AI has the potential to amplify or reduce bias, potentially becoming more or less biased than humans depending on numerous factors, such as the data and techniques used to train AI models and bias mitigation measures employed during the development and deployment processes. Humans are prone to implicit biases - unconscious preferences or prejudices - and these biases can be introduced into AI systems. The sources of bias in AI primarily come from three areas:
  - **Algorithmic bias**: Prejudiced hypotheses made during the design of AI foundational models.
  - **Training and data bias**: Bias introduced through the way the model is trained and the datasets used.
  - **Human bias**: Bias that comes through feedback from real-world users (developers, testers, business users) interacting with AI models.

- How AI models are used can also influence bias. If models are used to make automated decisions and bias is present, then they could reproduce biases. The risk is greater for generative AI models as they are 'black box' in nature, with their inner workings largely unexplainable, and are trained on vast datasets. This increases the risk that they may learn and reinforce biases which might go undetected.
- With careful design, automated systems have the potential to offer more objective and consistent decision-making. This includes ensuring that training datasets are representative of the population segment relevant to the AI system. It further requires careful review of data inputs to ensure that they do not act as proxies for protected characteristics, and that they are objectively justified for the use case.
- In relation to generative AI we note that bias is more complicated to identify, as it can manifest in subtle ways. Techniques are emerging to manage these risks, including careful consideration of permitted data inputs, filtering of outputs, giving the model access to authoritative data sources, and human review of outputs during both design and production. See chapter 4 of our **recent report**.

16. What data sharing would be needed to make AI more effective in financial services, and will there be a need for legislative change to achieve that?

Sharing between financial institutions

- Currently the trend is for organisations to leverage in isolation their own data in two ways: 1) forming internal knowledge bases that the AI model would look into without storing any of this data, and 2) by training a smaller scale AI model using its internal data and hosted internally. Therefore, at this point there is no specific need to share the data.
- However, data sharing, especially across borders, plays a critical role in the effective use of AI in financial services. This is particularly the case for sharing of data for the purpose of detecting and preventing fraud and financial crime.
- In February 2024, the ICO published a **summary** of financial institutions' participation in the ICO's Regulatory Sandbox with a focus on financial crime data sharing, facilitated by the Home Office and UK Finance.
- Examples of possible use cases where it would make sense to share data include possible applications to Authorised Push Payment (APP) fraud and anti-money laundering (AML). A common database from all financial institutions including all the AML patterns could be used to train a ML model to increase pattern identification capability. This might require legislative change, with important questions to consider about data lineage and ownership.
- International collaboration to ensure that data privacy and protection regulatory frameworks enable trusted, secure cross-border data flows can help support continued development and use of AI technologies to combat fraud and other crime.

Sharing with model developers

- There will also be a need for firms to share data with model developers to develop models with greater specificity for financial services use cases.

17. Are there any current or future concerns around data protection and AI in financial services?

Data protection and AI

- As mentioned in the government's recent **International AI Safety Report**, in many cases the principles underlying existing data protection regulations already apply to the ways in which AI interacts with and uses personal or sensitive data. These include:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability
  - ADM governance
- Many of the risks related to data protection and AI are also not new to financial services and firms are well practiced in assessing their data protection risks, with additional requirements under UK GDPR to carry out data protection impact assessments for high-risk processing of personal data. However, existing risks and concerns may be compounded or exacerbated when it comes to AI due to the increased capacity for information processing, increased scale of training, and the complexity of models / the overall AI ecosystem.
- AI systems often require large datasets, raising issues related to data categorisation, classification, lineage, entitlement and therefore privacy and security. There is also the risk of AI decision-making tools producing biased or discriminatory outcomes if trained on flawed or dummy data, as discussed above. Regulatory scrutiny is increasing to address these concerns, with a focus on consumer protection, data bias, and AI governance.
- As previously mentioned, controllership is also a concern in terms of defining and allocating appropriate roles and responsibilities across the generative AI supply chain, and the degree of shared liability between developers and deployers.
- The International AI Safety Report references examples of some specific concerns relating to data protection and AI, for example:
  - Bad actors using AI to violate the privacy of individuals (e.g. gaining access to personal information through prompt injection, or deepfakes / voice cloning).
  - Challenges regarding data subjects' information rights (e.g. the ability for firms to stop/restrict data processing, to erase, or to rectify inaccurate information).
- Often, issues arising from the use of AI can also be difficult to identify since they are usually unintentional or occur without the knowledge of affected individuals.
- Data protection and privacy is central to financial services and the Bank of England **survey** on Artificial intelligence in UK financial services recently identified privacy and data protection as the top 'data-related risk' (4.2). However, the survey also indicates that data protection compliance is a material cost and constraint (4.3 and 4.4).

Generative AI and data protection

- Further to the above, and as outlined in the responses to earlier questions, there are uncertainties around UK GDPR compliance in relation to *generative* AI, in particular. Examples include:
  - Potential for larger scale personal data breaches involving increased volumes of personal data, which could impact larger numbers of individuals (and in turn lead to increased sanctions and monetary penalties).
  - Transparency issues around ascertaining how AI models make decisions affecting data subjects – complicating the establishment of UK GDPR 'lawfulness of processing' and other regulatory requirements.
  - Potential for inaccurate data to be held about an individual due to hallucinations or bias, which could lead to unfair outcomes. (See question 18).
  - Risk of the 'human in the loop' becoming complacent or failing to notice errors in outputs, meaning the firm does not achieve the "meaningful human involvement" that

will in some cases be required under UK GDPR Article 22 (noting that this is likely to be reformed by the Data (Use and Access) Bill this year).

- This is a new technology, so it is not surprising that some time is required to fully account for it in firms' and regulators' approaches.
- We note that the **ICO** consulted on some of these areas in 2024 and plans to issue draft guidance later in 2025. A key area of uncertainty is how precise model developers need to be when training a model and setting its intended / permitted uses (processing purposes).

18. What sort of safeguards need to be in place to protect customer data and prevent bias?

- See also our comments above under 15 and 17.
- Please also see sections 3 and 4 of our recent generative AI **report**, which looks in particular at practical privacy risk mitigations, including as applied in specific customer complaint processing and KYC tool case studies.
- Implementing robust data quality controls, encrypting customer information, using multi-factor authentication for sensitive access, and regularly auditing AI systems are all required. Additionally, maintaining human oversight of AI systems, documenting AI decision-making processes, and ensuring compliance with privacy regulations are crucial. These practices are widespread within financial services at present.
- As AI has the potential to introduce bias depending on the training data used, controls and processes are needed to mitigate the risk of bias. For example, data used to train and run models should be evaluated regularly and asymmetric distributions corrected. This is something many firms do already.
- An important risk to be cognisant of is that as AI becomes more prevalent in the everyday lives of consumers, the extent to which users rely on AI systems and trust them without feeling the need to validate the results will likely increase. Emphasis should be placed on the continued importance of review of AI responses, including where bias may be embedded.
- The ICO has already issued extensive guidance on **AI and data protection**, as well as AI **explainability**. As noted above, there are outstanding areas of uncertainty in relation to generative AI and data protection but the ICO has announced **plans to consult** on updates to AI guidance later in 2025, including specifically in relation to generative AI. We also note that the government committed to tasking the ICO with preparing a statutory code of practice in relation to AI and ADM, once the Data (Use and Access) Bill has passed (see **comments** by Lord Vallance of Balham on 21 January 2025).

How can Government and financial regulators strike the right balance between seizing the opportunities of AI but at the same time protecting consumers and mitigating against any threats to financial stability?

19. Are new regulations needed or do existing regulations need to be modified because of AI?

Overarching approach to regulation

- Overall, we consider that the UK's pro-innovation sectoral approach to AI regulation is correct. Proportionate, tech-neutral rules should be relied on as far as possible, with existing regulators issuing guidance in their domains to resolve any emerging uncertainties if and when these become apparent.

- We do not believe there needs to be a cross-economy regulatory or legislative framework for AI at present, while use cases are still emerging and risks being better understood.
- We also do not believe there is a requirement at this time for any additional regulation for financial services specifically and would like to underline that financial institutions have been working with AI for several years and managing risks via the established three-lines-of-defence operating model.
- In addition, existing sectoral regulation and supervision (see paragraph below) ensure consumer and investor protection and risk management when it comes to using technology, including AI. Any consideration of new initiatives must take stock of existing rules at a sectoral and horizontal level.
- There are a number of existing powers and rules the UK regulators already possess and use – such as those relating to operational risk, model risk and the Consumer Duty – that can be applied to firms' use of AI. Through their supervisory role, the FCA and PRA also engage regularly on firms' use of AI – including through the third AI/ML survey, published in 2024 (**referenced** several times in our response).
- We also note that the Data (Use and Access) Bill will amend the ADM rules, adding flexibility while maintaining effective safeguards, including a right to request human review of significant automated decisions. As previously mentioned, we understand that this will be supported by a statutory code from the ICO.

Future evolution of regulation

- While the uses and risks of AI continue to emerge, we recommend that regulators continue to monitor usage of AI to ensure that (a) any risks specific to AI are appropriately mitigated, (b) any unwarranted barriers to AI usage in existing regulation are – where appropriate – removed or eased. There may also emerge a need for some harmonisation of definitions and wider review of the overlaps of existing regulation, so that the complex network of existing regulation does not hinder AI adoption.
- We also note that the Bank of England has highlighted several areas where additional guidance *might* be necessary, notably:
  - Model risk management, given generative AI explainability limitations
  - Training data quality
  - Expectations on senior managers
  - 'Human in the loop' expectations and governance
  - Third-party risks
- We look forward to supporting the Bank of England as it considers these issues.
- Acknowledging the risks identified by the Bank of England, alongside various other comments in this response, we note that the dynamics between AI providers and AI deployers may need further consideration from regulators. Development of commonly understood best practice, or a light-touch code of practice, might help set or standardise technical disclosures that would provide firms with greater confidence in their AI deployment. The merits of such options could be considered collaboratively by industry and regulators in a public-private partnership arrangement. This is an issue we continue to discuss with members.
- (A source of complexity in relation to this issue is that, under the EU AI Act, financial services firms could be legally treated as AI providers, if they buy in a model to which they then make 'substantial modifications').
- We note that the Bank of England's AI Consortium could explore the potential challenges the financial service industry might face in collaboration with firms, depending on how it is implemented. Similarly, industry and regulators could collaborate to identify any gaps in sectoral regulation and guidance that might emerge over time. See also our comments in relation to public-private partnership under question nine.

- To enable ongoing international collaboration on trustworthy AI innovation and global economic efficiency/growth, multistakeholder collaboration to promote interoperability across global AI governance/policy frameworks will be important.

20. Will Government and regulators need additional information, resources or expertise to help monitor, support and regulate AI implementation in financial services?

- AI is not a new feature of financial services; it has been used and regulated successfully for many years. The ongoing adoption of AI should not be seen as a standalone trend, but as part of a broader shift towards the digitisation of financial services and the economy more broadly. As with technology generally, as tools become more accessible and more powerful it will be key for regulators to be given the resources and access to expertise required to ensure that guidance and any further regulation is practical and of relevance to the entities they regulate.
- At this stage, firms are focusing on low risk use case deployment with monitoring of the benefits and risks effectively covered by existing supervisory regimes.
- Enhancing collaboration between regulatory bodies and investing in AI expertise is also essential. Initiatives such as the UK's AI Sector Champion and the Digital Regulation Cooperation Forum are good examples of this work (although the detail of the AI Sector Champion proposal still needs to be developed by government).
- Additionally, government may wish to understand and monitor the extent to which AI is used relative to the human workforce in different sectors, and for which types of processes. This will help identify where AI risks may crystallise, or any risk of over-reliance on AI in a given discipline or industry.
- UK Finance have long supported collaboration between industry and authorities to ensure that AI risks and novelties are managed effectively, and uncertainties resolved.
- See also our comments about industry-regulator collaboration under question nine.

April 2025