FSB FINANCIAL STABILITY BOARD

The Financial Stability Implications of Artificial Intelligence

14 November 2024

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on X/Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Copyright © 2024 Financial Stability Board. Please refer to the terms and conditions

Table of Contents

Executive summary

The financial sector has long used artificial intelligence (AI) tools, but adoption has become more widespread and use cases have become more diverse in recent years – most notably with the development of generative AI (GenAI) and large language models (LLMs). This was largely driven by developments in deep learning, big data and computational power, coupled with significant software and hardware improvements. The collection of large amounts of unstructured data, advances in cloud computing, and the wider deployment of pre-trained AI models have also contributed to AI adoption.

The lack of comprehensive data on AI adoption by financial services firms complicates an in-depth assessment of use cases. However, available evidence suggests a notable acceleration in the adoption of AI in financial services in recent years. Most use cases in finance focus on enhancing internal operations and improving regulatory compliance; use cases generating new revenue streams are not widely observed at present.

LLMs and GenAI have also given rise to new use cases, such as document summarisation, information retrieval, and code generation. Financial institutions (FIs) are becoming more aware of AI risks. While many appear to be taking a cautious approach to using GenAI, interest remains high, and the technology's accessibility could facilitate more rapid integration in financial services.

Financial authorities have also adopted AI to meet their supervisory responsibilities more efficiently and this may increase in the future to keep up with FIs. However, the fast pace of innovation and AI integration in financial services, along with limited data on AI usage, poses challenges for monitoring vulnerabilities and potential financial stability implications.

While AI offers benefits like improved operational efficiency, regulatory compliance, personalised financial products, and advanced data analytics, it may also potentially amplify certain financial sector vulnerabilities and thereby pose risks to financial stability. Several AI-related vulnerabilities stand out for their potential to increase systemic risk, including:

- Third-party dependencies and service provider concentration – The reliance on specialised hardware, cloud services, and pre-trained models has increased the potential for AI-related third-party dependencies. The market for these products and services is also highly concentrated, which could expose FIs to operational vulnerabilities and systemic risk from disruptions affecting key service providers.

- Market correlations – The widespread use of common AI models and data sources could lead to increased correlations in trading, lending, and pricing. This could amplify market stress, exacerbate liquidity crunches, and increase asset price vulnerabilities. AI-driven market correlations could be exacerbated by increasing automation in financial markets.

- Cyber – AI uptake by malicious actors could increase the frequency and impact of cyber attacks. Intense data usage, novel modes of interacting with AI services and greater usage of specialised service providers increase the number of cyber attack opportunities.

- Model risk, data quality and governance – The complexity and limited explainability of some AI methods and the difficulty of assessing data quality for widely used AI models

could increase model risk for FIs that lack robust AI governance. The use of opaque training data sources for these models also complicates data quality assessments. Understanding the quality and accuracy of model outputs is complicated by new inaccuracies, such as hallucinations.

In addition to the above vulnerabilities, GenAI could increase financial fraud and the ability of malicious actors to generate and spread disinformation in financial markets. Misaligned AI systems that are not calibrated to operate within legal, regulatory, and ethical boundaries can also engage in behaviour that harms financial stability. And from a longer-term perspective, AI uptake could drive changes in market structure, macroeconomic conditions, and energy use that, under certain circumstances, could have implications for financial markets and institutions.

While existing financial policy frameworks address many of the vulnerabilities associated with use of AI by FIs, more work may be needed to ensure that these frameworks are sufficiently comprehensive. To this end, the FSB, standard setting bodies (SSBs) and national authorities may wish to:

- Consider ways to address data and information gaps in monitoring developments in AI use in the financial system and assessing their financial stability implications.
- Assess whether current regulatory and supervisory frameworks adequately address the vulnerabilities identified in this report, both domestically and internationally.
- Consider ways to enhance regulatory and supervisory capabilities for overseeing policy frameworks related to the application of AI in finance, for instance, through international and cross-sectoral cooperation and sharing of information and good practices.

1. Introduction

This report provides a high-level overview of recent developments in AI, along with an assessment of their potential financial stability implications.[1] It revisits the 2017 FSB report on AI in financial services[2] (henceforth the "2017 FSB report") and takes stock of the latest advancements, exploring current use cases in the financial sector and drivers of adoption, as well as new potential benefits and AI-related financial sector vulnerabilities. To this end, the FSB assessed the experience and initiatives from member jurisdictions, reviewed the existing literature and conducted multiple bilateral and multilateral outreach meetings, including an OECD-FSB joint AI roundtable.[3]

The financial services industry has long used AI tools, but adoption has become more widespread and use cases have become more diverse in recent years. The 2017 FSB report identified key use cases in the financial system, including customer-focused applications (e.g. assessing credit quality and automating client interactions), operations-focused applications (e.g. capital optimisation and model risk management), as well as applications for trading, portfolio management, regulatory technology (RegTech), and supervisory technology (SupTech). Since then, many of these use cases have made further inroads, and AI has continued to advance – most notably with the development of GenAI. FIs and their service providers are exploring business uses of GenAI such as customer support, fraud detection, market analysis, document processing, information retrieval, and software development. These AI use cases could have considerable benefits for FIs, their customers, and financial markets more broadly. However, AI usage by FIs and malicious actors also has the potential to increase important sources of financial sector vulnerabilities.

The rest of the report is structured as follows. Section 2 reviews developments since the 2017 FSB report, providing context to the technological advancements and taking into consideration supply and demand-side drivers. Section 3 discusses selected AI use cases by industry participants and official sector authorities. Section 4 discusses implications for financial stability, focusing on how AI could amplify specific types of financial sector vulnerabilities. Section 5 concludes by discussing policy implications. Annex 1 discusses the LLM supply chain.

2. Developments in AI since 2017

The field of AI has seen significant advancements since the 2017 FSB report.[4] The most salient developments include advancements in deep learning, big data, computational power (also referred to as "compute"), and GenAI. Interest in AI has increased – particularly following the

---

1 This Report adopts the OECD definition of an AI system, which is 'a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.' See OECD (2024), *OECD AI Principles*, May.

2 FSB (2017), *Artificial intelligence and machine learning in financial services*, November.

3 OECD and FSB (2024), *OECD - FSB Roundtable on Artificial Intelligence (AI) in Finance*, September.

4 The field of AI is vast and complex. This overview is not meant to be comprehensive but aims to equip readers with a conceptual understanding of key developments before delving into use cases.

launch of ChatGPT in November 2022 – alongside a steady rise in the number of professionals employed in, and patent applications filed related to, AI.[5]

The 2017 FSB report examined supply and demand factors that could spur AI in financial services. Advancements in technology suggest supply factors may be playing a bigger role today. Supply-side drivers include technological developments and financial sector factors, while demand-side drivers include profitability, competition, and regulation. The following subsections review the main changes in these drivers, with a particular focus on the supply-side. Demand-side drivers remain (and are likely to remain) significant drivers of current and future AI adoption but have not materially changed since 2017 and are hence reviewed succinctly.

2.1. Supply-side factors

Supply-side factors have been the major driver of changes in AI adoption by FIs since 2017. They include technological, data-related, and business model developments.[6]

2.1.1. Technological developments

The advent of GenAI, coupled with significant software and hardware advancements, have increased the appeal of AI. Three developments stand out, two arising from software and one from hardware improvements. First, the continued enhancements of deep learning models improve the ability to handle unstructured data through so-called embeddings. Second, the development of the transformer architecture has revolutionised natural language processing (NLP) and laid the foundation for the development of GenAI and LLMs. Part of the appeal of LLMs is that they qualitatively transform the way people interact with computers, away from code and programming interfaces to ordinary text and speech – making the technology much more accessible.[7] Third, in terms of hardware, the wider integration of Graphics Processing Units (GPUs) with increased compute capabilities particularly for mass calculations, has facilitated the processing of larger datasets and the use of more complex models at reduced cost[8] (see Box 1 for further details). The IMF estimates that by 2027 investment in software, hardware, and services for AI systems in the financial services sector could reach $400 billion, up from $166 billion in 2023.[9]

---

5 See Leitner et al (2024), *The rise of artificial intelligence: benefits and risks for financial stability*, May.

6 In the 2017 report, financial sector factors encompassed the availability of infrastructure and data to apply new techniques within financial services. This included the proliferation of electronic trading platforms, the computerisation of markets, proliferation of retail scoring systems, and the growing availability of data. The Covid-19 pandemic further increased the digitisation of the financial services sector as lockdowns forced many firms to shift their activities online, with knock-on effects for firms' willingness to use AI. See IMF (2021), *Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance*, October; Bholat et al. (2021), *How has the COVID-19 crisis impacted the use of machine learning and data science in UK banking?*, European Economy; and McKinsey (2021), Building the AI bank of the future, May.

7 See BIS (2024), *Artificial intelligence and the economy: implications for central banks, Annual Economic Report*, Chapter III, June.

8 See Papenbrock and Schwendner (2021), *Accelerated Data Science, AI, and GenAI for Sustainable Finance in Central Banking and Supervision*, International Conference on "Statistics for Sustainable Finance", 14-15 September.

9 IMF (2023), *Financial institutions are forecast to double their spending on AI by 2027*, December.

Box 1. Key technological developments in AI

Early uses of AI. AI and ML have been used in the financial sector long before the advent of LLMs and GenAI. These earlier technologies were primarily used for automating routine tasks, detecting fraud, and making predictions based on historical data. ML, a subset of AI, employs algorithms to learn from data and make decisions or predictions. Neural networks, a technology used in a specific type of ML and inspired by the human brain, are particularly effective at recognising patterns and complex relationships in large datasets. Deep learning, a further subset of ML, uses multi-layered neural networks to learn and extract complex patterns from large data sets, thereby significantly enhancing the accuracy of predictions. These foundational technologies paved the way for more advanced applications like LLMs and GenAI.

Advent of LLMs and GenAI. The launch of consumer-facing advanced AI systems like LLM chatbots in November 2022 demonstrates how rapidly the field of AI can experience significant technological change. LLM chatbots are a specialised application of generative AI with focus on language, whereas GenAI models are able to generate new content, such as images, text or video, based on user prompts.

Role of NLP. LLMs are an advanced application in the broader field of natural language processing (NLP), which is concerned with enabling machines to recognise, process, and understand the content and meaning of language. NLP has been used by firms, including those in financial services, for many years for customer interaction, regulatory compliance monitoring, automated advice, and sentiment analysis on customer feedback. Prior to LLMs, the most advanced forms of NLP operated by transforming words into "tokens" or individual units and then translating tokens into numerical representations (vectors) that attempt to capture the meaning of words, a process known as "word embedding". However, there are limitations to this approach: words can have multiple meanings (e.g. "interest" can refer to "attentiveness" or "interest rates") and the context of an entire text can provide more nuance around the meaning of a word compared to focusing on surrounding words.

Features of the Transformer. The Transformer, a deep learning architecture and one of the foundational technologies of LLMs, addresses the aforementioned limitation of word embeddings by incorporating an attention mechanism, which focuses the neural network on specific parts of the text. For example, it can differentiate the meaning of the word "bark" depending on whether it is used in a sentence about dogs (e.g. "the dog has a loud bark") or trees (e.g. "the tree's bark is brown"). Positional encoding is used to understand the order of words in a sentence. LLMs also have other features such as the feed-forward mechanism, which helps to predict the next word based on previous words, and a system that identifies the most likely next word occurring in a sentence. Altogether, these components, particularly the attention mechanism and positional encoding, enable LLMs to process and generate text more efficiently. The Transformer also processes data in parallel, rather than sequentially, which contributes to further efficiency gains compared to older models.[10]

Limitations and future prospects. While LLMs and GenAI are able to mimic human language and creativity, the currently available models do not truly understand the content they generate. This is because their outputs are the result of a stochastic process rather than a deep understanding of the underlying text.[11] The field of AI is dynamic and future advancements, potentially emerging from other AI sub-fields, could reshape the landscape and impact the financial system in ways that are not fully predictable at present. These future developments could introduce new vulnerabilities and challenges for financial stability, underscoring the importance of continued monitoring, research, and policy consideration by financial authorities.

---

[10] The attention mechanism in LLMs is more accurately described as "multi-head" attention mechanism. This allows multiple neural networks to run in parallel, thereby capturing different meanings for the same word.

[11] See Perez-Cruz and Shin (2024), *Testing the cognitive limits of large language models*, BIS Bulletin, No 83, BIS, January.

There may be a growing demand for workers capable of addressing model and data risk issues, such as in compliance or risk management within firms. However, while technology has driven adoption, human capital has not kept pace with these developments, meaning that uptake of AI by financial firms may be constrained going forward by staffing limitations. Workers with specialised skills to develop AI models are already scarce and costly – and will be even more so for GenAI.

2.1.2. Data-related developments

The increasing digital engagement of customers with FIs and the collection of large amounts of unstructured data from various channels are key drivers for AI adoption.[12] The availability, size, and use of datasets have increased since 2017. Building on the technological developments just discussed, large unstructured data (e.g. from videos, satellites, images) can be used alongside more traditional quantitative datasets. Concurrently, the growing complexity of many ML models, particularly GenAI models with their billions of parameters, allow for the parsing of such data, while also requiring large volumes of data for their own training.[13]

The data-hungry nature of the recent crop of AI models raises the prospect that high-quality real data might be exhausted. Available estimates suggest such a limit might be reached as early as 2026.[14] The use of synthetic data, including that produced by LLMs themselves, emerges as a way to address this challenge, as well as challenges arising from privacy and intellectual property considerations.[15] But this comes with its own risks and limitations, including the quality of the model used and the dataset produced, as well as the fact that its generation relies on known data generating processes and continued reliance on it diminishes the information coming from the tails of the distribution.[16]

2.1.3. Business model developments

Two recent business model developments stand out, namely the wider reliance on cloud computing and the increasing development and usage of pre-trained AI models.

Cloud computing has enabled the flexible delivery of services, such as computing power, information storage, and software usage via virtual data and processing capabilities.[17] FIs have become more willing to use cloud computing services over the last few years, including for business-critical areas, which may be shaping their readiness to use third-party providers for related services, such as AI.[18] Many firms are also relying on cloud providers for AI models –

---

12 World Bank (2022), *COVID-19 Boosted the Adoption of Digital Financial Services*, July; BIS (2023), *Fintech and the digital transformation of financial services: Implications for market structure and public policy*, July.

13 See IBM (2024), *Bigger isn't always better: How hybrid AI pattern enables smaller language models*, April.

14 Villalobos et al. (2024), *Will we run out of data? Limits of LLM scaling based on human-generated data*.

15 According to IBM, synthetic data is computer-generated data that is based on real data. In some cases, the real data may be too sensitive to share. Hugging Face and IBM are two such examples of providers offering synthetic data generation capabilities for LLMs. See IBM (2023), What is synthetic data?, February.

16 Gartner (2022), *Is Synthetic Data the Future of AI?*, June; Shumailov et al. (2024): *AI models collapse when trained on recursively generated data*, Nature 631, pp 755-759.

17 Bank of England (BoE) (2020), *How reliant are banks and insurers on cloud outsourcing?*, January.

18 In 2019, a survey conducted by Information Age suggested that 70% of financial services firms were only at the initial trial or testing stage for cloud adoption, which was included in an FSB report on cloud computing. A second survey in 2021 conducted by Google and the Harris Poll suggested that 83% of 1,300 financial services firms globally had adopted some form of public or

particularly GenAI models – due to the increased cost of both the infrastructure (e.g. computing power) and training required to develop and deliver these models.

Wider dissemination and usage of pre-trained AI models, particularly LLMs, is another important business model development. While pre-trained models were available for certain AI use cases prior to LLMs, and parallels have existed for many years with respect to vendor-provided AI services, the extent of pre-trained model availability and usage has accelerated considerably. Wider usage of pre-trained models stands in contrast to the traditional in-house AI model development approach. While the shift could drive AI adoption, as FIs can leverage pre-existing models without needing extensive AI expertise or resources, it could also hinder adoption due to explainability and accountability concerns.

There appears to be a growing trend towards open-sourced models. Pre-trained LLMs vary in size, are calibrated for different modelling tasks, with two broad modes of accessibility: closed-source and open-source.[19] Closed models have traditionally outperformed open-source models on various benchmarks. However, open-source model performance has significantly improved, with some leading open-source LLMs now on par with the top closed models for many tasks.[20] Developers typically access closed models through the provider's Application Programming Interface (API) or through a cloud-based channel, often limited to specific cloud platforms. Open-source models are generally free, highly accessible, and customisable to a firm's needs, reducing financial investment in developing LLM-based applications. In 2023, 66% of newly released foundation models were open source, up from 33% in 2021. The number of open-source AI-related projects on GitHub, one of the major online software development platforms, increased from 845 in 2011 to 1.8 million in 2023.[21]

2.2. Demand-side factors

The 2017 report identified three demand-side factors driving increased adoption of AI in FIs: profitability, competition, and regulation. These factors remain (and are likely to remain) significant drivers of current and future AI adoption but have not materially changed since 2017 and are hence reviewed succinctly.

2.2.1. Profitability

Opportunities to improve firms' profitability through revenue generation, cost reduction, risk management, and productivity gains still drive AI adoption by FIs. Firms highlight that revenue generation opportunities stem from better targeting of customers with tailored products and

hybrid cloud. Another report by the Cloud Security Alliance (CSA) suggested that the share of cloud adoption in business-critical areas rose from around 17% in 2020 to around 32% in 2023, although they did not define "business critical". See FSB (2019), *Third-party dependencies in cloud services: Considerations on financial stability implications*, December; and Yang Koh and Prenio (2023), *Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector*, FSI Insights No. 53, November.

19 There is some debate over the extent to which AI models, particularly LLMs, are open source. Many providers claim to be open source, yet users have limited access to the code and training data powering these models. See Gibney (2024), Not all 'open source' AI models are actually open: here's a ranking, Nature, June; Center for Research on Foundation Models (2024), *The Foundation Model Transparency Index*, May; Kapoor et al. (2024), *On the Societal Impact of Open Foundation Models*, arXiv preprint arXiv:2403.07918, February.

20 See Lynch (2024), *AI Index: State of AI in 13 Charts*, Stanford University Human-Centred Artificial Intelligence, April.

21 Stanford University Human-Centred Artificial Intelligence (2024), *Artificial Intelligence Index Report 2024*, April.

services, better onboarding of customers, and reduced churn rates. Cost reduction benefits are generated through efficiency savings from automating manual tasks that can instead be performed by AI. Similarly, risk management-related applications of ML include predicting expected cash flows, delinquencies, and excess losses, to name a few.[22] GenAI has the potential to improve workers' productivity across a range of tasks including report writing, email drafting, information retrieval, and code generation. Multiple studies have found that access to GenAI tools increases worker productivity, although some suggest the benefits are concentrated among novice or low-skilled workers.[23] Efficiency gains could enable firms to allocate more time and resources to focus on revenue-generating activities that may be harder to automate.[24]

2.2.2. Competition

Perhaps the most influential factor on the demand side is firms' concern of keeping up vis-à-vis their competitors. FIs are increasingly concerned with being left behind their peers if they fail to adopt AI, particularly GenAI. These fears have supported cautious experimentation. Competitive pressures are likely to intensify as firms begin to deploy these models, particularly in customer-facing applications. In the medium to long term, such pressures could foster greater innovation, business dynamism and the reduction in the price of goods and services (hence increasing real wages). However, increased competition may also cause harm, if firms deploy AI technologies without adequate testing or safeguards in place. Additionally, increased competition may have a detrimental impact on incumbent firms, as well as their workers, that are left behind.

2.2.3. Regulatory compliance

The drive to improve regulatory compliance and meet requirements more efficiently is another demand-side factor increasing the adoption of AI in finance. For example, in 2022, UK FIs cited compliance, anti-money laundering/counter-terrorist financing (AML/CFT) and Know-Your-Customer (KYC) rules as the most critical areas for ML applications within their business.[25] More broadly, the increasing regulatory requirements over the last seven years across multiple jurisdictions, for example, requirements on data protection, the growing use of principles to guide AI development and adoption, and the growing body of international standards, including in specific sectors such as financial services, have led financial firms to increasingly leverage AI to enhance their compliance capabilities.[26]

---

22 BoE and Financial Conduct Authority (FCA) (2022), *Machine learning in UK financial services*, October.

23 Noy and Zhang (2023): *Experimental evidence on the productivity effects of generative artificial intelligence*, Science, pp 187-192; Gambacorta et al. (2024), *Generative AI and labour productivity: A field experiment on code programming*, BIS Working Paper No. 1208, September; Brynjolfsson et al (2023): *Generative AI at work*, NBER Working Paper no 31161, November; and Microsoft (2023), *Early LLM-based tools for Enterprise information Workers Likely Provide Meaningful Boosts to Productivity*.

24 See Morgan Stanley and Oliver Wyman (2023), *The AI Tipping Point*; and UK Finance and Oliver Wyman (2023), *The Impact of AI in financial services*.

25 BoE (2022), *ML in UK financial services*, October.

26 Deloitte (2023), *AI regulation in the financial sector: How to ensure financial institutions' accountability*, September.

3. Selected use cases

The lack of comprehensive data on AI adoption by financial services firms complicates an in-depth assessment of use cases.[27] Some survey evidence suggests firms are willing and able to switch from experimentation with AI to deployment quickly,[28] though available data presents a mixed picture. Many sources that suggest high levels of adoption are voluntary surveys focused on larger firms. In contrast, indications from economy-wide measures suggest that adoption is low, at least for customer-facing activities.[29] The gap between the perceived and actual use of AI could be due to competitive pressures to be seen to pilot or adopt AI, as evidenced by firms' marketing initiatives.

This report adopts an activity-based framework to categorise existing and emerging use cases, divided into industry use cases and regulatory/official sector use cases. Table 1 provides a non-exhaustive overview based on the classification of AI systems developed by the OECD and tailored to financial services.[30] Different AI models can be applied to the same use cases, and developers will typically test multiple models depending on the task at hand and the limitations of any given model. Annex 2 includes further definitions.

Table 1: Overview of tasks and example use cases in finance

Task	Type of learning/reasoning	Example use cases
Recognition	• Supervised classification of text, images, voice, etc.	• Facial recognition
Event detection	• Non-machine and machine learning techniques (e.g. unsupervised and reinforcement learning) used to detect patterns or outliers in data	• Fraud and risk detection • Intelligent monitoring
Forecasting	• Supervised learning using past/existing behaviours to predict future outcomes	• Stock price prediction • Risk modelling • Economic forecasting
Personalisation	• Supervised or reinforcement learning used to develop a profile of an individual	• Personal finance recommendations • Provision of tailored/on-demand financial services

27 The BoE's engagement with regulated financial firms in the UK suggests that firms are cautiously experimenting with LLMs, focusing primarily on low-risk use cases. See BoE (2023), *Financial Policy Summary and Record of the Financial Policy Committee meeting on 21 November*, December.

28 For example, the BoE and the FCA joint surveys on ML in UK financial services suggest that the share of respondents adopting ML rose from 67% to 72% between 2019 and 2022. Responding to this survey was voluntary and it should be noted that the non-response rate was 63% and 58% respectively in these years. The final sample was skewed towards larger firms and therefore should not be seen as representative of the entire UK financial services industry. It highlights that deployed applications among respondents rose from 56% to 79% between 2019 and 2022.

29 An economy-wide survey in the US suggests that, as of a recent reading in June 2024, 4.7% of firms had adopted at least one of five AI-related technologies, including machine learning, natural language processing, and voice recognition, in the production of goods and services. The financial sector had higher adoption rates below 6.7%. See US Census Bureau, *Business Trends and Outlook Survey*.

30 OECD (2022), *OECD Framework for the Classification of AI systems*, February.

Task	Type of learning/reasoning	Example use cases
Interaction support	• Semi-supervised or reinforcement learning used to power interactions between humans/machines	• Chatbots • Voice assistants
Goal-driven optimisation	• Range of AI techniques used to determine the optimal solution to a problem	• Bidding • Scenario simulation
Knowledge-Based Reasoning	• AI techniques, beyond machine learning, are used to infer new outcomes using models and simulations	• Recruitment systems • Expert systems

3.1. Industry use cases

Discussions with industry and authorities strongly suggest that the adoption of AI has increased considerably since the 2017 FSB report. There have been material developments in the main categories included in the 2017 report (e.g. customer-facing, operations-focused, and trading and portfolio applications), as well as new use cases (e.g. summarisation, code generation), enabled by GenAI. At the same time, increased regulatory scrutiny in some jurisdictions, alongside greater awareness of risks (both within firms and externally), have led to a cautious approach to implementation. For example, industry engagement reveals that many firms prefer to use less complex, easily interpretable AI models and so-called "co-pilot" applications, which support rather than replace human decision-making.

3.1.1. Customer-focused use cases

The use of AI models in credit underwriting, insurance pricing, client-facing chatbots and marketing has grown since 2017. Increased data availability through initiatives such as open banking has enabled financial services firms to build AI models assessing customers' creditworthiness. This may particularly benefit customers with 'thin' credit files or no credit record at all, while also enabling firms to better predict default risk.[31] Survey evidence suggests that firms are increasingly relying on ML to supplement traditional credit scoring approaches, by processing unstructured or large volumes of data during the pre-approval process.[32] A UK survey highlighted that some firms are starting to move away from traditional credit scoring by introducing ML-based decisioning for personal loans, such as auto finance.[33]

Several AI applications have been implemented in the marketing sector to customise products and improve customer retention. One use case identified in the 2017 report was the use of ML to analyse user behaviour to tailor specific marketing campaigns, thereby improving click-through and conversion rates. These approaches have become more widespread. For example,

---

31 OECD (2021), *Artificial Intelligence and Machine Learning in Financial Services*, October.

32 See BoE (2022), *Machine learning in UK financial services*, October; and Bonaccorsi di Patti et al. (2022), *Artificial Intelligence in Credit Scoring. An Analysis of Some Experiences in the Italian Financial System*, Bank of Italy Occasional Paper 721, October.

33 BoE and FCA (2022).

AI is now being leveraged to intelligently assign financial advisors who can potentially offer appropriate products at the right time. The advent of GenAI may increase the efficiency and scalability of digital marketing campaigns by enabling the creation of text and visual content that is customised to specific market segments.[34]

Firms are also using ML models to improve pricing and risk management of insurance policies. This includes upgrading previous approaches (e.g. generalised linear models) to ML models that predict the risk of specific policies or estimate individuals' behaviour (e.g. in automotive insurance).[35] Other applications include automated insurance claims handling, but these often incorporate human oversight in decision making.

Finally, the advent of GenAI has moved the types of chatbots deployed away from rules-based chatbots towards LLM-based approaches offering more complex interactions. Since the 2017 report, NLP-based chatbots went from experimentation stage to wider deployment. LLM-based chatbots in turn are a key area of ongoing experimentation, likely to reach wider deployment across a range of use cases, including robo-advisory.

3.1.2. Operations-focused use cases

Firms have demonstrated greater willingness to pilot, test, and deploy AI models in operations-focused use cases. This includes capital optimisation, model risk management, market impact analysis, and code generation. Although customer-facing use cases tend to get more attention, these back-office use cases may be of even greater importance in terms of potential impact on firms' bottom line and the wider financial system.

Some firms are using AI to better manage volatility and liquidity risk. For example, anticipating larger- or smaller-than-expected stock market moves has been a long-standing challenge for traders. Some financial firms have built ML models to better assess their stock options book in the event of higher or lower volatility than predicted by traditional models.

Some firms are also exploring AI to manage riskier use cases, such as optimising their regulatory capital requirements. According to a consultation response by the European Banking Authority (EBA), some firms use – or intend to use – ML techniques in areas such as default probability modelling, although issues such as explainability remain a barrier to full-scale adoption.[36]

GenAI has enabled a range of new operations-focused use cases. These include improving information search and retrieval, content generation (e.g. automated text, image, and video generation), voice transcriptions (e.g. voice-to-text and text-to-summary service requests), and code generation or legacy code streamlining. Moreover, GenAI's code generation capabilities could expand the use cases identified in 2017 to more firms. Historically, a significant barrier for many smaller firms has been access to engineering staff with the appropriate coding skills. Many

---

[34] See Soni (2023), *Adopting Generative AI in Digital Marketing Campaigns: An Empirical study of Drivers and Barriers*, Sage Science Review of Applied Machine Learning, August. Recent research suggests that GenAI-generated advertisements outperform traditional advertisements; see Heitmann (2024), *Generative AI for Marketing Content Creation: New Rules for an Old Game*, NIM Marketing Intelligence Review, May.

[35] BoE and FCA (2022).

[36] EBA (2023), *Machine Learning for IRB Models: Follow-up report from the consultation on the discussion paper on machine learning for IRB models*, August.

of these code generation tools are quite advanced, enabling firms to accelerate the deployment of more traditional use cases such as fraud detection or credit underwriting. As a result, GenAI could stimulate a wider adoption of traditional AI models.

3.1.3. Trading and portfolio management

Quantitative approaches have long been used in trading and portfolio management, and these approaches are now expanding beyond traditional AI towards GenAI applications.[37] For example, some firms are using GenAI to assess market sentiment from text data, such as earnings calls or regulatory disclosures, or to implement reinforcement learning for trade execution. Although NLP and other machine learning techniques have been used to achieve similar outcomes, LLMs may enable trading algorithms to better understand subtle relationships between words, rather than relying on frequency counts to infer the general discussion topic or sentiment.[38] Portfolio management, similarly, may benefit from increased automation of insights through GenAI tools, alongside existing quantitative tools.[39]

3.1.4. Regulatory compliance

FIs' use of AI to comply with regulatory requirements (e.g. RegTech) has seen significant uptake.[40] For example, AI tools are being deployed across a greater number and wider variety of fraud and AML/CFT use cases. Although the use of AI models to comply with AML/CFT requirements and to perform fraud detection were already identified in the 2017 report, they have been more widely deployed since then to facilitate investigations into sanctions evasion, to identify misuse of legal persons and legal arrangements, to uncover trade fraud and trade-based money laundering, and to detect tax evasion, fraud/scams, and money mules.[41] Furthermore, while traditional AI may perform better on specific tasks, such as identifying potentially fraudulent transactions, GenAI can potentially automate the generation of financial crime reports, incorporating a range of different sources and supporting investigators.[42] These are likely to remain critical use cases as regulatory requirements for firms increase and financial fraud – itself partly driven by technology use – rises.[43]

---

37 ESMA (2023), *Artificial intelligence in EU securities markets*, February.

38 See Goldman Sachs (2023), *How generative AI tools are changing systematic investing*, September.

39 EY (2023), *The transformation imperative: generative AI in wealth and asset management*, October.

40 See Hernandez de Cos (2024), *Managing AI in banking: are we ready to cooperate?*, keynote speech delivered at the Institute of International Finance Global Outlook Forum, Washington DC, 17 April 2024.

41 The Association of Banks in Singapore (2024), *Industry Perspectives on Best Practices - Leveraging on Data Analytics and Machine Learning Methods for AML/CFT*, March.

42 See SymphonyAI's Sensa Copilot here.

43 WEF (2024), *'Pig-butchering' scams on the rise as technology amplifies financial fraud, INTERPOL warns*, April. The global RegTech market is forecasted to reach $19.5 billion by 2026, as regulatory demands on firms increase; see Deloitte (2022), *Open Innovation in RegTech: Methodology and use cases of successful startup – corporate collaboration in a highly regulated environment*.

3.2. Regulatory and supervisory use cases

Financial sector authorities are also engaging with AI through a variety of use cases, including the use of technology by supervisors (e.g. SupTech).[44] Supervisory authorities' use of SupTech has increased, with 59% of authorities surveyed using various applications in 2023, a 5-percentage point increase from 2022.[45] AI can also assist central banks in key tasks such as enhancing oversight of payment systems and information collection and statistical compilation supporting real-time analysis of economic activity.[46]

Many central banks and regulators are adopting AI to meet their supervisory responsibilities more efficiently.[47] This includes exploring how AI can deliver 'faster indicators' for real-time economic analysis, exploring using alternative data for supervisory assessments,[48] and, more recently, experimenting with LLMs for research, analysis, and drafting. For example, some regulators have been exploring and using NLP and GenAI to analyse textual data sources, such as earnings call transcripts and management, discussion and analysis sections of public filings.[49] Another area where NLP and GenAI are being tested and applied is for inspections: these methods can extract relevant paragraphs from large volumes of inspection documents and summarise and draft inspection reports for supervisors.[50] LLMs could be used to augment data quality assessments and customise regulatory reporting error messages for specific circumstances and jurisdictions. Proposed use cases also include employing GenAI to model social media interactions within the context of bank runs or in stress testing, both in conceptually designing stress testing scenarios and in operationalising stress testing models in code.[51] The use of AI in SupTech may increase in the future, partly driven by regulatory authorities' need to keep up with and understand the rapid uptake in the use of AI by FIs.

4. Financial stability implications of AI

While the responsible and productive use of AI could have significant benefits for FIs and their customers as discussed in Section 3, rapid AI uptake by FIs without commensurate risk management and controls, inadequate monitoring by financial authorities and novel usage by malicious actors could harm financial stability. The remainder of this section examines the potential financial stability implications of AI. While these vulnerabilities are not unique to AI, greater AI adoption by FIs could increase their relevance for financial stability.

---

44 See BIS (2024), *Artificial intelligence and the economy: implications for central banks*, *Annual Economic Report*, Chapter III, June; Araujo et al (2024), Artificial intelligence in central banking, *BIS Bulletin* 84; Aldasoro et al (2024), *Intelligent financial system: how AI is transforming finance*, *BIS Working Paper*, no 1194.

45 Cambridge Centre for Alternative Finance (2023), *Cambridge SupTech Lab: State of SupTech Report 2023*.

46 See BIS (2024), *Artificial intelligence and the economy: implications for central banks, Annual Economic Report*, Chapter III, June.

47 See BIS (2019), *The SupTech generations*, October.

48 Ibid.; BoE (2021), *Forecasting UK GDP growth with large survey panels,* May; BoE (2019), *Predicting bank distress in the UK with machine learning*, October; BoE (2020), *Credit growth, the yield curve, and financial crisis prediction: Evidence from a machine learning approach*, January; BoE (2020), *Making text count: Economic forecasting using newspaper text*, May.

49 Federal Reserve Bank of Cleveland (2024), *Regional economic sentiment: Constructing quantitative estimates from the Beige Book and testing their ability to forecast recessions*, April.

50 Araujo et al (2024).

51 Kazinnik (2023), *Bank Run, Interrupted: Modelling deposit withdrawals and Generative AI*, October.

4.1. Key developments and monitoring challenges

Recent developments in AI, summarized in Table 2, have the potential to amplify certain financial sector vulnerabilities and thereby affect financial stability.[52] These vulnerabilities, discussed further in section 4.2, relate to the interaction of third-party dependencies and service provider concentration, market correlations, cybersecurity and cyber fraud, model and data risk and other emerging vulnerabilities, such as AI-driven disinformation.

Table 2: Key AI-related developments that could have financial stability implications

Key development	Relevance of the development in financial markets
Wider integration of AI in financial services	• Recent years have seen wider uptake of powerful and complex AI methods in finance. • FIs use AI for core business lines and operations, but the centrality of AI in these use cases remains unclear.
Technological breakthroughs in LLMs and GenAI	• While many FIs appear to be taking a prudent, risk-based approach to incorporating GenAI in business activities, the technology's accessibility and competitive pressures could facilitate more rapid deployment. • LLMs and GenAI will likely enable FIs to develop and deploy more traditional AI applications in the coming years. • The increased automaticity, speed, and ubiquity of GenAI relative to previous generations of AI could amplify several AI-related vulnerabilities in financial markets.[53]
Greater importance of specialised hardware and infrastructure services	• AI application development by FIs and their AI service providers increasingly relies on a highly concentrated market for accelerated computing chips. • Cloud services, which FIs already use for a range of other computing services, have become tightly integrated in various aspects of AI development.
Increasing usage of unstructured and/or opaque training data sources	• Diverse, unstructured data sources that FIs may not be accustomed to evaluating, such as text files, social media activity, and images, are now widely used in training AI models.[54] • Training data sources are often opaque or unavailable for pre-trained models. FIs seeking to use these models face challenges in applying traditional data quality assessment methods.

Financial authorities face two key challenges in evaluating the financial stability implications of AI: significant uncertainty amid rapid innovation and limited data on AI uptake. The remarkable

[52] A vulnerability is "a property of the financial system that: (i) reflects the accumulation of imbalances, (ii) may increase the likelihood of a shock, and (iii) when acted upon by a shock, may lead to a system disruption"; see FSB (2021), *FSB Financial Stability Surveillance Framework*. Financial stability is the "capacity of the global financial system to withstand shocks, containing the risk of disruptions in the financial intermediation process and other financial system functions that are severe enough to adversely impact the real economy"; see FSB (2021), *FSB Financial Stability Surveillance Framework*, September.

[53] Aldasoro et al (2024), p. 15.

[54] Several data-as-a-service providers have emerged that help firms process unstructured data.

rate of change in this space creates uncertainty about the landscape of available AI technologies and services and their uses. Vulnerabilities could evolve considerably with the pace of innovation and the degree of AI integration in financial services. Furthermore, while some national authorities have data about AI model usage at regulated entities, the data tend to be irregular snapshots and focused on narrow sets of institutions. The scarcity of consistent, representative data on AI usage poses significant challenges for conducting vulnerabilities surveillance in this rapidly evolving area. Financial authorities have an even more limited view of AI usage at FIs that are less subject to financial regulations or outside the regulatory perimeter.

Supervisory effectiveness could suffer if financial regulators' AI-related skills and knowledge do not keep pace with developments in this space. In addition to the financial sector vulnerabilities discussed throughout this section, it is important to acknowledge that inadequate investment by financial authorities in skills and resources that are necessary to critically assess AI developments and FIs' use of AI could also pose risks to the financial system. In a recent survey of SupTech approaches at 64 financial regulators globally, most respondents reported organisational skills deficiencies in data science and essential IT capabilities.[55] In another survey, central bank cyber experts express similar concerns about skills and IT capital.[56]

4.2. Financial sector vulnerabilities

Four types of AI-related vulnerabilities stand out for their potential to increase systemic risk in financial markets. First, the interaction of AI-related third-party dependencies and market concentration among technology and AI service providers could increase domestic and international interconnections, as major service providers are only located in a few jurisdictions, exposing FIs to losses arising from operational impairments and supply chain disruptions affecting key vendors. Second, widespread use of AI models with similar behaviour or training data sources could increase correlations in financial markets, which can expand interconnections, amplify market stress, and increase asset price vulnerabilities. Third, AI uptake by malicious actors could increase cyber vulnerabilities, due to the potential for AI to improve threat actors' capabilities and from the increasing number of attack opportunities from expanding AI usage. Finally, the limited explainability of some AI methods and the difficulty of assessing data quality underlying more widely used AI models could increase model risk for FIs that do not have robust AI governance in place. Table 3 summarises how the key AI developments identified in Table 2 may affect the nature and magnitude of these vulnerabilities.

Table 3: How AI-related developments affect key financial sector vulnerabilities

Vulnerability	Effects of AI developments
Third-party dependencies and service provider concentration	• Wider AI uptake in finance, increasing importance of specialised hardware and cloud services for AI development, and greater usage of pre-trained models have created more AI-related third-party dependencies. • Complexity in AI supply chains, highly concentrated markets for inputs to AI development, and market consolidation in the financial data

55 Cambridge SupTech Lab (2023), *State of SupTech Report 2023*.

56 Aldasoro et al. (2024).

Vulnerability	Effects of AI developments
	aggregation market could increase service provider concentration vulnerabilities. • Depending on the trajectory of AI penetration in finance, greater reliance on and market concentration among AI service providers can increase systemic third-party dependencies in the financial sector.
Market correlations	• Broader usage of AI in financial markets could lead to common modelling approaches and training data sources across FIs. • Greater uptake of pre-trained AI models could increase market correlations. • AI-driven correlation vulnerabilities could interact negatively with increasing levels of automation in financial markets, as well as greater speed and accessibility enabled by financial market infrastructures.
Cyber	• LLMs and GenAI could enhance cyber threat actors' capabilities and increase the frequency and impact of cyber attacks. • Intense data usage and novel modes of interacting with AI services increase the number of cyber attack opportunities. • Greater usage of specialised service providers exposes FIs to operational risk from cyber events affecting these vendors.
Model risk, data quality, and governance	• Wider uptake of complex AI approaches could increase model risk for FIs that are unable to effectively validate, monitor and, when necessary, correct AI models. • The increasing importance of massive, unstructured training datasets in AI development and lack of transparency in training data sources of leading LLMs pose challenges for performing data quality assessments. • The accessibility of modern AI tools may incentivise rapid adoption without the development of commensurate governance and controls.

4.2.1. Third-party dependencies and service provider concentration

Recent trends in AI usage and development approaches have given rise to more third-party dependencies, which can create operational vulnerabilities for FIs that use AI. Third-party service providers in the AI supply chain help FIs develop and deploy effective AI applications within acceptable time and budget constraints. However, such relationships also expose FIs to operational vulnerabilities. In recent years, wider uptake of AI in finance, the increasing importance of specialised hardware and infrastructure services for AI development, and the prohibitive cost and complexity of training LLMs for non-specialist firms have increased the potential for AI-related third-party dependencies in finance. Table 4 summarises three important sources of dependencies related to hardware, cloud services, and models that have increased in recent years, provided by BigTech companies.

Table 4: Increasing sources of AI-related third-party dependencies for FIs

Source	Relevance for FIs
Hardware	• FIs that develop AI models, customise pre-trained models, and deploy AI in applications increasingly rely on accelerated computing chips, such as GPUs and application-specific integrated circuits (ASICs), which they acquire directly from chip suppliers or rent from cloud service providers (CSPs).
Cloud services	• CSPs, which offer flexible computing power arrangements, easy access to cutting edge AI toolsets and increasingly convenient LLM access channels, have become tightly integrated in AI development. Major CSPs also train and disseminate LLMs. FIs have indicated that one of the primary drivers of cloud adoption involves AI capabilities.[57] FIs also increasingly assume indirect cloud exposure through specialised AI service providers, which often use cloud services.[58]
Models	• At present, the cost and complexity of training LLMs from scratch are generally prohibitive for non-specialist firms. FIs seeking to customise and deploy LLMs in domain-specific applications generally use pre-trained, third-party models. More broadly, FIs have long used vendor-provided models for targeted applications, such as fraud and cyber anomaly detection. The scale and scope of AI model usage in vendor-provided risk management services is increasing.

Highly concentrated service provider markets exist across important aspects of the AI supply chain, including in hardware, infrastructure, and data aggregation. Service provider concentration vulnerabilities increase when many FIs rely on a limited set of providers for specific services or when FIs rely on the same service provider for multiple services. The markets for accelerated computing chips and cloud services are dominated by a limited number of entities. Moreover, vertical integration exists across aspects of the AI supply chain, as certain entities are keys providers of various combinations of hardware, software, cloud services and models.[59] Additionally, the financial data aggregation market has become increasingly consolidated in recent years, as major data providers have acquired smaller competitors.[60] Data from these providers are often key inputs to predictive models in financial markets. Fundamentally, AI services and related infrastructures tend to be increasing returns to scale businesses. Some level of market concentration is thus difficult to avoid.

Service provider concentration in the market for LLMs and GenAI is a significant and growing concern from an operational vulnerability perspective. Table 5 summarises key factors that could increase or reduce concentration in the market for LLMs and GenAI. High costs, complexity, persistent supply chain bottlenecks, investments and acquisitions, vertical integration, and the demand for multimodal models [61] could potentially increase LLM market concentration. Conversely, competitive open-source models, architectural innovations, hardware market

57 US Treasury (2023), *The Financial Services Sector's Adoption of Cloud Services*.

58 *Ibid.*

59 Financial institutions use a wide range of important computing services offered by CSPs beyond those relevant for AI.

60 Danielsson and Uthemann (2024), *Artificial intelligence and financial crises*, p. 14.

61 Multimodal models can process multiple forms of data and information such as texts, images, audio and videos.

competition and task- and domain-specific models could help support a competitive LLM market.[62] Annex 1 expands on several of these dynamics.

Table 5: Factors that could influence LLMs and GenAI market concentration

Directional effect	Key factors
Increase	• **Cost and complexity:** Barriers to entry driven by the high cost and complexity of training LLMs. Training LLMs from scratch requires considerable monetary and human capital resources. Additionally, where end-users' systems are designed around specific models, it may be costly to pivot to alternative model providers.
	• **Supply chain constraints**: Persistent scarcity of accelerated computing chips, particularly GPUs. A key driver of cost, supply constraints may confer a competitive advantage on GPU-rich firms.
	• **Investment behaviour**: Significant or controlling investments by incumbent firms in frontier AI labs. Major technology firms are already important benefactors of leading AI labs. Funding and infrastructure support have enabled startup AI labs to compete but have also created strong ties between labs and incumbent technology firms.
	• **Vertical integration**: Consolidation of multiple AI supply chain activities in a limited number of firms. Certain firms are important providers of various combinations of hardware, software, models and infrastructure services.
	• **Multimodality**: Development of and demand for models that perform many or most GenAI tasks better than task- or domain-specific models. Such model training is more likely to be dominated by a limited number of AI firms.
Decrease	• **Open-source models**: Continued performance improvements in and availability of open-source LLMs.[63]
	• **Architectural breakthroughs**: Innovations in ML architectures that improve the efficiency and scalability of LLM training relative to the currently dominant transformer architecture.[64]
	• **GPU market competition**: More competition in the hardware market that increases the supply of and reduces prices for GPUs.
	• **Model specificity**: Development of and market demand for task- and domain-specific models. Model specificity could support market competition.

62 Kapoor and others describe publicly available foundation models as "open" rather than "open source" because often, only the model weights are released. See Kapoor et al. (2024), *On the Societal Impact of Open Foundation Models*, arXiv preprint arXiv:2403.07918, February.

63 Although competitive open models could decrease concentration vulnerabilities, they could increase certain cyber-related risks.

64 Gu and Dao, for example, recently introduced a language modelling architecture for which computing power needs scale linearly with input sequence length, as opposed to quadratically as in the Transformer. See Gu and Dao (2023), *Mamba: Linear-time sequence modelling with selective state spaces*, arXiv preprint arXiv:2312.00752, December.

The systemic relevance of third-party dependencies and service provider concentration will depend on technological penetration and the criticality and substitutability of AI services.[65] If AI emerges as a critical service in financial markets, the interaction of third-party dependencies and service provider concentration may reduce FIs' ability to mitigate losses arising from operational impairments, including cyber events, supply chain disruptions, and other shocks affecting third- and nth-party service providers.[66] Such losses can stem from disruptions to important services FIs provide, breakdowns in risk management products that institutions use, and failures in cyber event detection systems, among other sources. Importantly, however, synergies with a given service provider may, in certain cases, promote risk management efficiency and effectiveness, and overall resilience.

Some FIs may already use AI for core business lines and critical operations, but the criticality of AI in these use cases is unclear. As discussed in Section 3, lending institutions, insurance companies and asset managers already deploy AI in areas that are central to their core business offerings, including credit decisioning, claims processing and portfolio management. Some firms also use AI for risk management. Adequate risk management in areas such as credit, liquidity, and market risk is essential for the viability of FIs. The lack of representative data about AI usage makes it challenging to ascertain the extent to which AI plays a central or complementary role in helping FIs carry out these functions and, conditional on the level of centrality, how integral service providers are in enabling these activities.

Although most FIs appear to be taking a risk-based approach to GenAI adoption, interest is high, and the technology's accessibility could facilitate more rapid deployment. The intense focus of major technology firms on developing, deploying, and commercialising GenAI could soon increase the viability of integrating the technology in critical operations. Several of the largest, most systemically relevant FIs have publicly unveiled LLM-based applications to help with price discovery and investment advisory services. As more firms experiment with and vet GenAI's information security, risk management, and customer protection implications, it could be deployed for important regulatory compliance and risk management tasks and leveraged for customer-facing services, such as recommending specific payment, credit, insurance and investment products. As discussed above, one of the most compelling GenAI use cases in the financial sector is in coding assistance.[67] Coding is intimately connected to AI development and to software engineering more broadly. Code generation tools could soon support engineers in developing and maintaining software that drives important services in the financial sector, such as core banking, payment execution, claims processing, and loan servicing platforms. Operational vulnerabilities could increase in financial markets if FIs widely adopt and come to rely on the same core set of code generation tools.

Third-party risk management frameworks establish expectations for mitigating risks associated with AI service providers. Micro-prudential authorities in many jurisdictions maintain third-party

---

65 The FSB's third-party risk management toolkit defines a critical service as a "service provided to a financial institution whose failure or disruption could significantly impair a financial institution's viability, critical operations, or its ability to meet key legal and regulatory obligations." Critical services are institution-specific and can change over time. See FSB (2023a), *Final Report on Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities*, December.

66 An nth-party service provider is "part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more financial institutions". See FSB (2023a).

67 Chui et al. (2023), *The economic potential of generative AI: The next productivity frontier,* McKinsey, June.

risk management standards that apply to AI service providers. These standards typically include expectations for FIs in conducting due diligence and ongoing monitoring, including maintaining active vendor inventories and carrying out periodic risk assessments.[68] The FSB's third-party risk management toolkit complements these prudential standards by presenting strategies for assessing the criticality of services, monitoring supply chain risks and identifying systemic third-party dependencies.[69]

4.2.2. Market correlations

AI uptake by FIs could be associated with widespread use of similar data sources and models, giving rise to greater correlations in financial markets.[70,71] The use of common data and models could be driven by several factors, including:

- Herding behaviour: Market participants imitate data and model choices of others.[72]
- Network externalities: The performance of models trained by third parties may improve from interactions with a wider range of end-users and thus incentivise multiple agents to use specific third-party models.
- Limited choice: Few data sources and models meet acceptable performance levels. Limited choice could be driven by service provider concentration (see Section 4.2.1).
- Lack of transparency: Model providers may not disclose their training data sources. End-users could thus unknowingly rely on the same data sources as other financial market participants.

Correlation vulnerabilities could have implications for AI usage in trading, lending, and insurance pricing. Correlated AI approaches in portfolio management and trading execution,[73] including identifying price signals, developing investment strategies, forecasting clients' trading patterns, and conducting market impact analysis, can amplify volatility, exacerbate liquidity crunches during downturns, and increase the probability of flash crashes.[74] More broadly, when models are trained on similar data sources, they are more likely to make correlated predictions,[75] which can lead to unexpected interconnections among FIs. This has relevance for applications beyond

---

68 See, for example, Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (2023), *Interagency Guidance on Third-Party Relationships: Risk Management*, Federal Register, vol. 88, no. 111 (June 9), pp. 37920-37937.

69 FSB (2023a).

70 Gensler and Bailey (2020), *Deep learning and financial stability*, Available at SSRN, November.

71 There are existing regulatory frameworks that aim to mitigate the negative effects of market correlations to ensure market integrity and efficiency; IOSCO (2011), *Regulatory issues raised by the impact of technological changes on market integrity and efficiency*, October; IOSCO (2018), *Mechanisms used by trading venues to manage extreme volatility and preserve orderly trading*.

72 For definitions of herding behaviour in financial markets, see Abhijit V (1992), *A simple model of herd behaviour*, The quarterly journal of economics, 107(3): 797-817, August; and Scharfstein and Stein (1990), *Herd behaviour and investment*, The American economic review, 80(3): 465-479, June.

73 Even though there is limited information about the actual strategies of hedge funds, a few of claim their strategies are solely based on AI (e.g. Aidyia Holdings, Cerebellum Capital, Taaffeite Capital).

74 Gensler and Bailey (2020); Shabsigh and Boukherouaa (2023), *Generative Artificial Intelligence in Finance: Risk Considerations*, IMF Fintech Notes No 2023/006, August; OECD (2021), *Artificial Intelligence, Machine Learning and Big Data in Finance*, August.

75 Gensler and Bailey (2020).

trading, such as credit decisioning and insurance pricing. Shocks that act upon a segment of the financial sector using the same models and data could affect the segment as if it were a single institution.[76] Moreover, the use of models that are calibrated to similar risk management standards can give rise to homogeneity in risk assessments and exacerbate pro-cyclicality in markets.[77] Many of these issues can be amplified by poor governance around model risk and lack of explainability (see Section 4.2.4).

FIs may derive correlated outputs from LLM and GenAI usage, and this could become a concern in specific use cases.[78] FIs seeking to use LLMs for domain-specific applications generally rely on models that have already been trained by a technology firm. Even if a firm customises a model with domain-specific data, the core model is typically pre-trained. Most LLMs are trained using the same underlying architecture and many are trained, at least in part, on common sources of web crawl data.[79] The homogenisation in training data and model architecture can lead to correlated outputs, which could amplify market stress and exacerbate liquidity crunches.

Data-related correlations could increase if the volume of GenAI outputs on the internet grows and is recycled into future training. The impact of LLM and GenAI usage on market correlations will depend on how FIs integrate these technologies in their business models. If they are widely used to develop investment strategies, inform risk management approaches and create new AI applications, their usage could significantly increase correlation-related vulnerabilities. However, if FIs primarily use LLMs for internal efficiencies, such as document drafting, employee education and information retrieval, the impact on market correlations is likely to be minimal.

AI-driven market correlations could be exacerbated by increasing automation in financial markets. Highly automated trading execution is a growing feature of important trading markets. Corporations also increasingly have access to semi-automated services for treasury management. Additionally, many financial market infrastructures and payment systems are working to offer high-speed, around-the-clock methods of moving money. AI-driven market correlations can be amplified by automated optimisation behaviour and speed. For example, semi-automated corporate depositor behaviour that reacts in real-time to news and data about FIs, as well as yields offered by specific products, could have implications for funding and liquidity vulnerabilities.[80] Moreover, coordinated reactions to extreme market conditions—for example, the synchronous pulling of "kill switches" on automated systems—could deepen stress events.

AI could also help reduce market correlations if it facilitates building customised trading and investment strategies and increases diversity in financial markets. If AI enables investment firms and advisors to develop and recommend truly customised trading and portfolio management approaches, this could reduce correlations in financial markets. Notably, asset and wealth

---

76 FSB (2017).

77 Shabsigh and Boukherouaa (2023); Danielsson et al. (2022), *Artificial intelligence and systemic risk*, Journal of Banking & Finance, 140: 106290, July.

78 Examples of LLM/GenAI uses, as part of a wider trading strategy could include sentiment analysis news articles/social media posts, financial report analysis and predictive analysis of historical data. For instance, see Kirtac & Germano (2024), *Sentiment trading with large language models*, Finance Research letters (62), April.

79 Although transparency about training data is limited, it is widely believed that many foundation models are trained on the Common Crawl dataset.

80 FSB (2024), *Depositor Behaviour and Interest Rate and Liquidity Risks in the Financial System: Lessons from the March 2023 banking turmoil*, October.

management firms have been early adopters of customised LLM and GenAI tools to support their investment professionals. Furthermore, if AI-powered customer engagement helps lower barriers to entry in financial markets, this could diversify capital market bases.

Transparency requirements and volatility control mechanisms could help mitigate AI-driven correlation vulnerabilities. Regulatory authorities have implemented enhanced transparency requirements and market exchanges have adopted circuit breaker mechanisms in the past to mitigate risks from the use of new technologies, greater automation and extreme volatility.[81] These measures could also help reduce vulnerabilities associated with AI-driven market correlations. However, better data and surveillance mechanisms would be important complements to these tools. Market correlations play out across firms. Consistent monitoring can help authorities and market intermediaries take pre-emptive action to address the accumulation of correlation-related imbalances.

4.2.3. Cyber

AI could increase cyber-related operational vulnerabilities in the global financial system by expanding threat actors' capabilities and increasing cyber attack opportunities.[82] GenAI tools could increase the quantity, novelty and success of cyber attacks. In this regard, GenAI could lower barriers to entry for potential threat actors, speed up cyber attack prototyping and aid in social engineering, business email compromise, malware development, impersonation and synthetic identity creation.[83] In addition to augmenting threat actors' capabilities, research has shown that leading LLMs can autonomously carry out successful cyber attacks.[84] Moreover, the intense data usage and unique ways of interacting with modern AI systems increase the number of cyber attack opportunities. Important types of cyber attacks that occur in training and interacting with AI models include data and model poisoning (where attackers manipulate training data or model weights) as well as prompt injection (where attackers manipulate GenAI tools or LLMs to extract confidential information).[85]

These vulnerabilities could increase the likelihood and impact of cyber attacks on the financial sector, which stands among the most attacked industries.[86] Cyber attacks can harm financial stability if they target financial market infrastructures, central banks, systemically important firms, critical service providers or, more generally, critical financial services that are not easily substitutable.[87] Service disruptions or loss of confidence resulting from cyber incidents can

---

81 IOSCO (2011), *Regulatory issues raised by the impact of technological changes on market integrity and efficiency*; IOSCO (2018), *Mechanisms used by trading venues to manage extreme volatility and preserve orderly trading*.

82 US Treasury (2024), *Managing artificial intelligence-specific cybersecurity risks in the financial services sector*, March; Shabsigh and Boukherouaa (2023). For definitions of key cyber terms used in this report, see FSB (2023b), Cyber Lexicon: Updated in 2023, April.

83 Financial Services Sector Coordinating Council (FSSCC) (2024), Artificial intelligence in the financial sector: cybersecurity and fraud use cases and risks;, March; Shabsigh and Boukherouaa (2023); OECD (2023) Generative Artificial Intelligence in Finance, *OECD Artificial Intelligence Papers*, No. 9, OECD Publishing, Paris, December.

84 Fang et al. (2024), *LLM agents can autonomously hack websites,* arXiv preprint arXiv:2402.06664.

85 Aldasoro et al. (2024); FSSCC (2024); Shabsigh and Boukherouaa (2023); US Treasury (2024); for definitions of important types of AI-related attacks. See also Vassilev et al. (2024), *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations*, Gaithersburg, MD: National Institute of Standards and Technology, January.

86 Aldasoro et al. (2022), *The drivers of cyber risk*, *Journal of Financial Stability*, volume 60, 100989, June.

87 IMF (2024), *Cyber risk: a growing concern for macrofinancial stability*, Global Financial Stability Report, Chapter 3, April; Adelmann et al. (2020), *Cyber risk and financial stability: it's a small world after all*, December; OFR (2017), *Cybersecurity and financial stability: risks and resilience*, Department of the Treasury, OFR Viewpoint, February; Kosse & Lu (2023), *Transmission of cyber risk through the Canadia wholesale payment system*, Journal of financial market infrastructures, September.

amplify volatility and increase funding and liquidity vulnerabilities in financial markets. Cyber vulnerabilities could have micro-financial implications as well. Banks and other FIs have seen increasing operational losses from a growing number of cyber incidents in recent years.[88]

AI advancements could help reduce cyber vulnerabilities, but in the near term, malicious actors may benefit more than legitimate actors from GenAI breakthroughs. FIs and public authorities already use AI for cyber anomaly detection and see value in GenAI tools for enhancing cyber defences.[89] In a recent survey of the Global Cyber Resilience Group, a body of cybersecurity experts from central banks, a majority of respondents saw GenAI as bringing more cybersecurity benefits than risks.[90] LLMs and GenAI can be deployed to help improve cyber event detection systems, speed up incident response times, and automate routine tasks to free up resources for investigative work.[91] GenAI can also be used to diagnose potentially malicious code and to help educate employees about important cybersecurity standards and techniques.[92] Despite potential benefits, available evidence suggests that FIs and regulators are taking a cautious, risk-based approach to adopting GenAI.[93] In the short-run, asymmetric uptake between legitimate and malicious actors, who likely do not observe the same guardrails, could increase cyber vulnerabilities.[94]

International and jurisdiction-specific cyber resources can help FIs, and authorities monitor and mitigate AI-related cyber vulnerabilities. The FSB, SSBs and national authorities have published a wide range of standards, guidance and toolkits to support cybersecurity risk management and incident responses.[95] Recently, the US Treasury highlighted a range of practices shared by FIs for managing AI-related cybersecurity risks, many of which were derived from existing risk management standards.[96] These include developing an AI risk management framework, integrating AI risk management in existing enterprise risk management frameworks (whether those are based on the three lines of defence recommended by the Basel Committee on Banking Supervision (BCBS) or a different principles-based approach), and integrating AI-specific questions in vendor due diligence, among others.

---

88 Aldasoro et al. (2023), *Operational and cyber risks in the financial sector*, *International Journal of Central Banking*, vol 19, no 5, December; IMF (2024), *Cyber risk: a growing concern for macrofinancial stability*, *Global Financial Stability Report*, Chapter 3, April.

89 US Treasury (2024); FSCC (2024); Araujo et al. (2024).

90 Aldasoro et al. (2024).

91 Aldasoro et al. (2024); US Treasury (2024); Shabsigh and Boukherouaa (2023).

92 FSSCC (2024); U.S. Treasury (2024).

93 US Treasury (2024); and FSSCC (2024); BCBS (2024), *Digitalisation of finance*, May.

94 US Treasury (2024).

95 For example, see BCBS (2021), *Revisions to the Principles for the Sound Management of Operational Risks*, June; FSB (2020), *Effective Practices for Cyber Incident Response and Recovery*, October; IAIS (2023), *Issues paper on insurance sector operational resilience*, May; National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, April; UK National Cyber Security Centre and others (2023), *Guidelines for secure AI system development*; Committee on Payments and Markets Infrastructures (CPMI) and IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, June.

96 US Treasury (2024).

4.2.4. Model risk, data, and governance

Wider AI uptake could increase model risk in the financial system to the extent that such models are more difficult to validate, monitor, and correct, especially during crises.[97] The limited explainability of some AI approaches can impede the evaluation of a model's suitability and soundness.[98] Excessive complexity and lack of transparency can also make it difficult to find independent and knowledgeable model validators, who can effectively challenge model development approaches. Moreover, explainability issues can complicate an end user's ability to diagnose and a quickly address significant model inaccuracies, which may be more likely during extreme volatility or crisis periods. Further, AI systems may suffer from accountability issues[99] throughout their lifecycle, making it difficult to assess their adequacy, safety, and trustworthiness for use.

Understanding the quality and accuracy of LLM outputs is inherently challenging. Outcomes analysis generally involves evaluating the accuracy of model outputs. LLM outputs are typically unstructured text. This can make it more challenging, though not impossible, to generate error rates and conduct effective outcomes analysis. GenAI has also given rise to a new type of model inaccuracy, the hallucination, where a model provides a seemingly confident but inaccurate response to user inputs. Hallucinations can be difficult to detect and evaluate.

More widespread use of massive, unstructured data sources in AI development and lack of transparency in training data for pre-trained models make it more difficult to assess data quality. Assessing data quality is a key aspect of model risk management.[100] Data quality issues may be more pronounced with AI usage due to the relative importance of data in driving model specifications and outcomes.[101] However, assessing data quality is often difficult as training data sources may be opaque or completely unavailable. This is often the case for pre-trained models. Furthermore, modern AI model training may consume a wide variety of data types and sources that FIs are not accustomed to evaluating. These factors can pose challenges for performing data quality assessments.[102]

Model risk and data quality are difficult to manage if firms do not have robust governance structures in place for vetting and monitoring AI usage and underlying data sources. Policymakers have expressed concern that the accessibility and utility of modern AI tools can incentivise rapid adoption without the development of commensurate controls.[103] At the same time, the increasing complexity of AI approaches and the size and lack of transparency of some

---

[97] Financial regulators have highlighted several challenges AI usage can pose for effective model risk management. See, for example: Financial Stability Oversight Council (FSOC) (2023), *Annual Report, 2023*; FRB, Bureau of Consumer Financial Protection, FDIC, National Credit Union Administration, and OCC (2021), Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, *Federal Register*, vol. 86, no. 60, pp. 16837-16842, March.

[98] Explainability generally refers to "how and AI approach uses inputs to produce outputs". See FRB, Bureau of Consumer Financial Protection, FDIC, National Credit Union Administration, and OCC (2021.

[99] In the context of AI, accountability refers to the ability to audit, explain, justify, and take responsibility for the decisions and actions of AI, as well as the potential consequences of these actions. See European Commission (2019), *Ethics Guidelines for trustworthy AI*, April.

[100] FRB and OCC (2011), *Supervisory Guidance on Model Risk Management*, *Supervision and Regulation Letter* SR 11-7, April.

[101] FSSCC (2024).

[102] Explainability and data governance issues can also expose financial institutions to a variety of legal, reputational, and consumer compliance risks.

[103] Hsu (2024), *AI Tools, Weapons, and Accountability: A Financial Stability Perspective*, speech delivered at the 2024 Conference on Artificial Intelligence and Financial Stability, June.

training data sources can pose challenges for effective governance mechanisms, especially if FIs lack the skills and expertise necessary to evaluate AI adoption.

Regulated FIs under the purview of model risk management regimes are responsible for addressing AI-related model risk and data quality challenges.[104] Model risk management standards typically lay out expectations for model validation, ongoing monitoring, performing outcomes analysis, and assessing data quality. The use of AI will not absolve FIs from applicable risk management expectations. Model risk management standards may recommend risk mitigation techniques for challenging circumstances, such as when data are limited or unavailable.

4.2.5. Other vulnerabilities

AI could be used to perpetuate fraud and disinformation in the financial system, while poorly aligned AI systems could introduce novel vulnerabilities for financial markets.[105] Table 6 and this section analyse how recent AI developments could increase financial fraud and the propensity for disinformation in financial markets, as well as lead to concerns about AI systems that are not calibrated to operate within legal, regulatory and ethical boundaries.

Table 6. AI developments and other financial sector vulnerabilities

Vulnerability	Effects of key AI developments
Fraud	• GenAI is being used to perpetuate financial fraud, which was already on the rise in many jurisdictions globally. Differing rates of GenAI adoption between malicious and legitimate actors and challenges in detecting fake content could worsen fraud in the short run.
Disinformation	• GenAI could enable malicious actors to generate and spread disinformation that causes acute crises, such as flash crashes and bank runs.
Misalignment	• Misaligned AI systems—those that do not work as intended or in line with legal and regulatory standards—can engage in behaviour that harms financial stability.

Fraud

Financial fraud is on the rise in many jurisdictions, and AI has played a role in facilitating fraud schemes.[106] As a result, the cost of both tackling and rectifying fraud is increasing for many FIs. GenAI's capabilities in voice and video-based generation could pose considerable problems for financial services firms if malicious actors use them to generate fake IDs or profiles, including voices or video images (known as deepfakes), to bypass security checks or defraud

[104] For examples of standards addressing model risk, see FRB and OCC (2011); PRA (2023), *Model Risk Management Principles for Banks*, Supervisory Statement SS1/23, May; HKMA (2019), *High-Level Principles on Artificial Intelligence*, November; IAIS (2023), *Regulation and supervision of AI and ML in insurance: a thematic review*, December.

[105] Alignment generally refers to AI systems that work as intended and in line with legal and regulatory standards.

[106] WEF (2024), *'Pig-butchering' scams on the rise as technology amplifies financial fraud, INTERPOL warns*, April; BDO (2024), *Reported fraud doubles in 2023, BDO report finds*, February.

customers.[107] There is also a risk that GenAI could be used to defraud FIs through, for example, submitting false insurance claims or through business email compromise schemes.[108]

AI can help FIs and authorities fight fraud, but GenAI may benefit malicious actors more than legitimate actors in the short run. As in cybersecurity, AI can help bolster fraud detection and prevention. Indeed, these are consistently cited as key AI use cases in the financial sector.[109] However, asymmetries along two dimensions could benefit malicious actors in perpetrating fraud in financial systems, at least in the short run. First, as discussed in connection with cyber vulnerabilities, there may be differing rates of AI usage by malicious actors and financial services providers, with the latter proceeding more cautiously.[110] Second, although synthetic content detection methods are being developed, they are still nascent and can be challenging to implement.[111] Thus, in the near term, it will likely be easier to generate fraudulent content using GenAI than to detect it. AI-driven fraud could have non-trivial effects on certain aspects of financial systems. In addition to the efforts by FIs to fight fraud, improving financial and AI literacy of consumers and investors would also help mitigate the risks of fraud.

Disinformation

GenAI could enable more sophisticated disinformation campaigns that have financial stability implications if they cause acute crises, such as flash crashes or bank runs.[112] While disinformation via technology is not new and is discussed frequently with respect to social media, GenAI could enable more convincing disinformation at scale, which could adversely affect investors, particularly during times of stress. Financial markets are susceptible to a wide range of information shocks. Malicious actors need not target financial markets directly to have an adverse impact. In May 2023, a fake image of an explosion at the U.S. Pentagon, which was likely AI-generated, appeared to have affected equities markets, albeit briefly.[113] Recent research by OpenAI found that threat actors use GenAI tools to conduct influence operations, though it is unclear to what extent such campaigns may have influenced public opinion in a meaningful way.[114] Nevertheless, as the technology and threat actors' competence with it improves, disinformation could increase in financial markets. Such vulnerabilities could be exacerbated by the role of social media in information dissemination, lack of financial and AI literacy among investors and consumers, and the increasing ease of transferring funds between FIs, as discussed above with respect to correlation-related vulnerabilities (see Section 4.2.2).

---

[107] See Washington Post (2023), They thought loved ones were calling for help. It was an AI scam, March; and Marchetti (2022), Rolling in the deep (fakes), *Bank of Italy Occasional Paper* 668, February.

[108] See Zurich (2024), *Insurance must prepare for a rise in deepfake AI fraud*, January; and CNBC (2024), *Generative AI financial scammers are getting very good at duping work email*, February.

[109] FRB and OCC (2011); FSB (2017); OECD (2021).

[110] FSSCC (2024) and U.S. Treasury (2024).

[111] NIST (2024), *Reducing risks posed by synthetic content: An overview of technical approaches to digital content transparency*, April.

[112] OECD (2023). Examples of disinformation that could precipitate acute crises include fake images of depositor withdrawal lines or so-called deep fakes of finance executives and public authorities expressing negative information about institutions or markets.

[113] Marcello (2023), *Fact focus: Fake image of Pentagon explosion briefly sends jitters through stock market*, Associated Press, May.

[114] OpenAI (2024), *AI and covert influence operations: Latest trends,* May.

Misalignment

In optimising profit maximisation objectives, poorly aligned AI systems could autonomously spread disinformation or engage in other behaviour that negatively affects financial markets. Alignment refers to AI systems that work as intended and in line with legal and regulatory standards.[115] Since AI systems seek to optimise pre-defined objectives, it can be difficult to specify all relevant objectives that meet regulatory and ethical expectations up front, with potentially adverse consequences for financial stability.[116] For example, an AI system could implement a profit maximisation strategy that involves spreading disinformation about a bank with the goal of catalysing a bank run while simultaneously shorting the firm's stock.[117] As a more current example, there is growing evidence that AI systems may strategically coordinate and collude.[118] Research has shown that AI-powered algorithms consistently learn to charge higher prices through collusive strategies, even without direct communication among them.[119] Strategic coordination and algorithmic autonomy could be facilitated by research breakthroughs in reinforcement learning that have enabled autonomous AI systems to beat humans in highly complex strategy games.[120]

Longer-term considerations

In addition to the vulnerabilities identified above, AI uptake could drive broader changes in the structure of the financial system, macroeconomic conditions, and energy use that, under certain circumstances, could have implications for financial markets and institutions (see Box 2). The potential effects of these changes are longer-term in nature and not well-understood as of now.

Box 2. Longer-term considerations of AI uptake

Competitive landscape: The 2017 FSB report projected that the effect of AI uptake on financial market consolidation was ambiguous and scenario-dependent, and no clear evidence has emerged since then. While it is still not clear how financial firms will use AI in the longer-term, the development and deployment of AI currently requires significant amounts of data and computing resources. At this time, financial firms that are larger and have more resources appear to be more engaged in evaluating how AI could be used to create internal efficiencies. The effects over the longer-term may depend on where LLMs and GenAI drive value in financial services. If building customised AI-based applications unlock significant value, then larger FIs with considerable resources could be in the best position to take advantage of recent technological breakthroughs. Alternatively, if the most value lies in using accessible

---

115 Iason (2020), *Artificial intelligence, values, and alignment*, Minds and machines, 30(3): 411-437, October; Kenton et al. (2021), *Alignment of language agents*, arXiv preprint, March.

116 Liang (2024), *Remarks on Artificial Intelligence in Finance*, speech delivered to the FSB Roundtable on Artificial Intelligence in Finance, May.

117 Hsu (2024).

118 See, for example, Assad et al. (2024), *Algorithmic pricing and competition: Empirical evidence from the German retail gasoline market*, *Journal of Political Economy*, 132(3): 723-1063, March; and Calvano et al. (2020), *Artificial intelligence, algorithmic pricing, and collusion*, *American Economic Review*, 110 (10): 3267-97, October.

119 Calvano et al. (2020; Dou et al. (2024), AI-Powered Trading, Algorithmic Collusion, and Price Efficiency, *Jacobs Levy Equity Management Center for Quantitative Financial Research Paper*, The Wharton School Research Paper.

120 Reinforcement learning is a branch of machine learning in which simulated agents "learn for themselves to achieve successful strategies that lead to the greatest long-term rewards" through "trial-and-error, solely from rewards and punishments". See Silver (2016), *Deep reinforcement learning*, Google DeepMind, Blogs, June. For recent breakthroughs in reinforcement learning, see Silver et al. (2017), *Mastering the game of go without human knowledge*, Nature, 550(7676): 354–359, October; Brown and Sandholm (2019), *Superhuman AI for multiplayer poker*, Science, 365(6456): 885-890, July; and Meta Fundamental AI Research Diplomacy Team (2022), *Human-level play in the game of Diplomacy by combining language models with strategic reasoning*, Science, 378(6624): 1067-1074, November.

GenAI products as productivity-enhancing tools, this could help smaller FIs compete more effectively, including by developing and deploying traditional AI use cases more easily. Uneven regulatory and supervisory treatment both within the financial sector and with respect to new entrants may lead to regulatory arbitrage between sectors.

Macroeconomic conditions: AI could drive long-term changes in the economy such as shifts in labour markets, inflation, and interest rates. GenAI presents novel considerations for the economy, although the magnitude, timing and distribution of these effects remains uncertain.[121] GenAI could lead to productivity gains and affect output, wages, and other important macroeconomic variables.[122] The technology's facility with cognitive tasks poses risks for some high-skilled workers, whereas most historical waves of innovation have tended to automate routine tasks.[123] AI-driven labour market dislocations could increase vulnerabilities in the financial sector through asset-quality and leverage channels by increasing delinquencies and debt-to-income ratios in unexpected ways. Structural changes in inflation and interest rates could affect borrowing and investment incentives for FIs and their customers.

Energy use: AI-related energy consumption – estimated to account at present for about 1% of global energy consumption – is expected to increase further in the future and could have effects on energy demand.[124] While model training has been the focus of attention, inference may be more energy intensive due to increasing end-user interactions with AI-powered services and the development of massive computing clusters.[125,126] Training, developing, and running large AI models and applications require large amounts of reliable and competitive energy, which may compete with other energy consumers to assure the required levels of energy input. To the extent that FIs and financial markets become dependent on AI, their functioning would be exposed to broader energy use and supply issues that could impede their ability to use AI. Furthermore, the sustained growth in AI-related energy consumption could impact climate change risks if it doesn't come from clean energy sources. At the same time, there are potential mitigating factors, including, for example, certain technology firms' commitments to clean energy goals and investments in data centre-centric clean energy innovations[127] as well as the development of more energy efficient model training architecture.

5. Conclusion

Since 2017, the adoption of AI tools in the financial services industry has not only become more widespread but the use cases have also diversified. AI has the potential to deliver significant benefits such as improved operational efficiency, enhanced regulatory compliance, more personalised financial products, and advanced data and analytics capabilities. Although use cases generating new revenue streams are not widely observed at present, the rapid pace of

---

[121] Morgan et al. (2019) *Toward understanding the impact of artificial intelligence on labor*, *Proceedings of the National Academy of Sciences* 116, no. 14 (2019): 6531-6539, April.

[122] Aldasoro et al. (2024), *The impact of artificial intelligence on output and inflation*, *BIS Working Papers* No 1179, April.

[123] Acemoglu and Restrepo (2019), *Artificial intelligence, automation, and work*, The economics of artificial intelligence: An agenda, pp. 197-236. University of Chicago Press, May; Agrawal et al. (2019), *Artificial intelligence: the ambiguous labor market impact of automating prediction*, *Journal of Economic Perspectives* 33, no. 2 (2019): 31-50.

[124] IEA (2024), *Electricity 2024: Analysis and forecast to 2026*, January; Goldman Sachs (2024), *AI is poised to drive 160% increase in data center power demand*, May.

[125] de Vries (2023), *The growing energy footprint of artificial intelligence*, Joule 7(10): 2191-2194, October; IEA (2023), *Data Centres and Data Transmission Networks, Activity*, July.

[126] See, for example, Meta (2022), *Introducing the AI Research SuperCluster — Meta's cutting-edge AI supercomputer for AI research*, January.

[127] Microsoft has pledged to offset all carbon consumption by 2030. Google has set the more ambitious goal that its data centers will run on carbon-free energy sources 24/7 by 2030. See Microsoft (2020), *Microsoft will be carbon negative by 2030*, January; Google (2023), *24/7 carbon-free energy by 2030*, Google Data Centers.

technological advancements and the growing integration of AI into financial sector use cases could change this in the future. RegTech in FIs, e.g. for AML/CFT, and SupTech in the official sector, for more efficient and effective supervision have also seen a notable uptake since 2017.

The use of AI in financial services could amplify certain financial vulnerabilities with potential implications for financial stability. Factors such as a wider uptake of powerful and complex AI methods, novel characteristics of LLMs and GenAI, greater importance of specialised hardware and infrastructure services, and increasing usage of unstructured and opaque data sources have increased the potential systemic impact of AI usage in finance. These developments have the potential to increase vulnerabilities related to third-party dependencies and service provider concentration, market correlations, cybersecurity and fraud, model risk and other emerging vulnerabilities, such as AI-driven disinformation. AI uptake could also drive longer-term changes in macroeconomic conditions, competition in financial markets, and energy use, which could have implications for financial markets and institutions. These vulnerabilities, if not effectively monitored and mitigated, could interact with, and impact, financial stability.

Financial authorities face two key challenges for effective vulnerabilities surveillance: the speed of AI change and the lack of data on AI usage in the financial sector. These developments are not taking place in isolation but rather reinforce existing trends towards greater automaticity and speed in the financial system. They underscore the necessity for authorities to monitor AI developments and related innovations closely and holistically.

Existing financial policy frameworks address many of the vulnerabilities associated with AI adoption, but additional work may be needed to ensure these frameworks are sufficiently comprehensive.[128] Existing regulatory and supervisory frameworks already require FIs to address cyber and operational risks, as well as to manage model and third-party risks.[129] However, AI developments could raise other issues that may require policy consideration. For example, some authorities have adopted or are considering AI-specific guidance to address issues that may go beyond the scope of existing regulations.[130] Finally, it is important to note that future developments could introduce new vulnerabilities and challenges for financial stability. This underscores the importance of continuous monitoring, research, and policy consideration by financial authorities.

In light of the findings of this report and to address potential financial stability risks from AI adoption, the FSB, SSBs and national authorities may wish to:

- Consider ways to address data and information gaps in monitoring developments in AI use in the financial system and assessing their financial stability implications. For example, authorities could consider leveraging periodic and ad-hoc surveys on AI adoption and use cases, reporting from regulated entities, and public disclosures. It may

[128] See OECD (2024), *Regulatory Approaches to Artificial Intelligence in Finance*, October, based on a survey of 49 jurisdictions.

[129] For example, the US Executive Order on AI articulates that AI must be safe and secure and requires that AI systems are compliant with applicable Federal laws and policies. See US White House (2023), *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October. For another example, the FSB's third-party risk management toolkit outlines a range of strategies for monitoring and mitigating concentration risks and supply chain complexities, as well as for identifying critical services and systemic third-party dependencies. See FSB (2023a).

[130] For example, the European Parliament and the Council of the EU reached a political agreement on the AI Act in December 2023 as they believe existing legislation is not sufficient to address the specific challenges AI systems may bring such as issues around transparency and explainability associated with general-purpose AI models. See. EC (2024), *AI Act*, March.

also be beneficial for authorities to intensify their engagement with private sector participants, including FIs, AI developers and other third-party service providers, as well as academics, to stay abreast of developments in this field.

- Assess whether current regulatory and supervisory frameworks adequately address the vulnerabilities identified in this report, both domestically and internationally. The FSB, along with the SSBs and national authorities, could consider the implications of sector-specific regulatory and supervisory frameworks on the level-playing field across sectors, as well as between established firms and new entrants such as fintech firms.

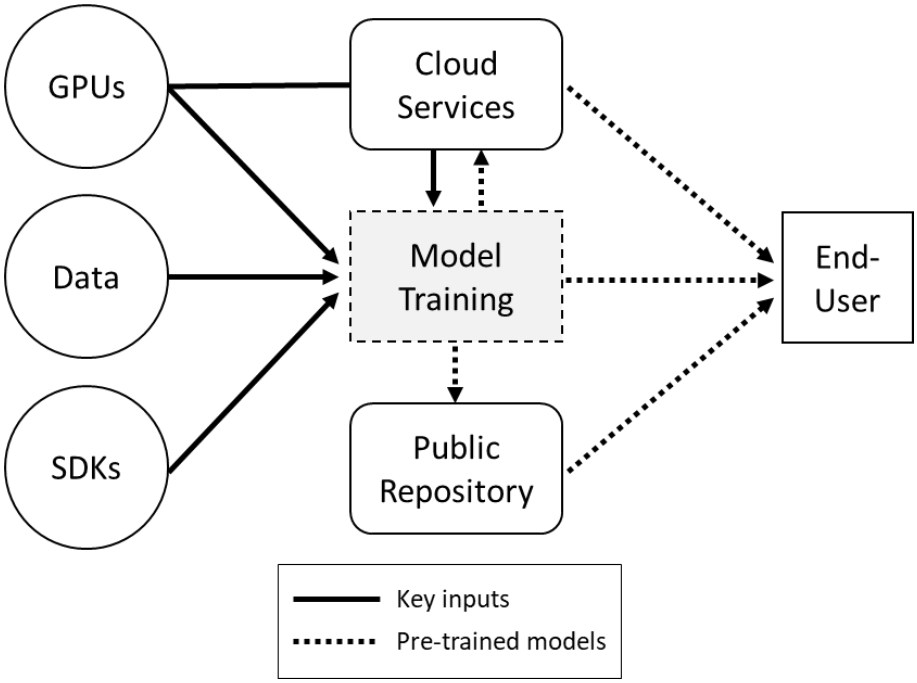
- Consider ways to enhance regulatory and supervisory capabilities for overseeing the policy frameworks related to the application of AI in finance. This may for instance be achieved through international and cross-sectoral coordination. The FSB, coordinating with the relevant SSBs, could consider facilitating international and cross-sectoral cooperation by enhancing the sharing of information and good practices across member jurisdictions. This may require the involvement of non-financial authorities, such as those responsible for data and privacy. In a separate but related effort, financial authorities may consider leveraging AI-powered tools to enhance their supervisory and regulatory capabilities through SupTech and RegTech.

Annex 1: Supply chain for large language models

Figure A1 provides an overview of the current supply chain for LLMs and GenAI. Key inputs to model production include GPUs, data, and software development toolkits (SDKs) that help implement ML architectures. Entities that train LLMs include specialty AI labs, major technology companies, and consortiums of researchers. These firms purchase accelerated computing chips from GPU suppliers or rent them from cloud service providers. The GPU design and fabrication markets are highly concentrated. Key sources of training data that AI firms use include open-source web crawl data, proprietary data, purchased data, and synthetic data.

There are currently three primary channels through which LLMs and GenAI-based products are disseminated: (1) direct to end-user, (2) through open repositories, and (3) via cloud service providers. Table A2 summarises these channels. LLMs can be used in a variety of ways. End users, including FIs, can use curated products, such as chatbots and code generation services. Currently, these products and services are generally affordable and do not require any special computing pre-requisites. Alternatively, developers can use LLMs to build applications. Models can be used as-is or customised ("fine-tuned") with additional data for domain specificity. Another emerging technique is to build retrieval augmented generation (RAG) systems, which involves giving LLMs access to external, authoritative data sources to enable more up-to-date and well-sourced query results. Although computing power needs are less intense for customising LLMs than for training LLMs, GPU access is still advantageous for performance and scalability.

Figure A1: Overview of the LLM supply chain



The figure captures the current supply chain for foundation models and derivative products. Key inputs include GPUs, data, and SDKs. Model developers buy GPUs directly or rent them from cloud service providers. They then train foundation models and distribute them directly to end-users, through cloud services, and through public repositories. Some model developers charge a fee for model access. Source: Author illustration.

Table A1: Primary distribution channels for foundation models and derivative products

Distribution channel	Description
Direct to end-user	• Leading model developers often provide direct access to LLMs through curated products, such as chatbots and code generation tools, as well as through developer-centric methods, such as application programming interfaces (APIs). Some model developers charge end-users a fee for access to premium products.
Open repository	• Some model developers post pre-trained LLMs to open repositories. End-users can download these models and customise them or use them as-is.[131]
Cloud services	• End-users can access some LLMs through cloud services. In addition to offering direct access channels, providers of some of the largest closed models have partnered with specific CSPs to develop cloud-based access channels. Cloud-based channels also offer access to some open-source LLMs.

Three potential sources of concentration risk in the LLM supply chain include model training, cloud services, and hardware. Currently, the most competitive of these is model training. While there are distinct market leaders, several firms are training competitive LLMs. On the second dimension, many end users, including FIs, seeking to build applications with LLMs are likely to use cloud-based access channels for several reasons. First, working with LLMs in the cloud enables more seamless integration with computing resources that are advantageous for fine tuning models and running inference on large models. Second, firms can access some of the most performant closed models via specific CSPs without having to send queries directly to the model providers via API. Finally, many FIs have built institutional capacity and governance structures for vetting cloud security.[132] Currently, the biggest source of concentration risk in the LLM supply chain is in the hardware market, where there are dominant firms in the GPU design and fabrication markets.

[131] As of late April 2024, there were 98 text generation models on Hugging Face with over 100,000 downloads. See Hugging (2024), *Models*. Maslei and others (2024) show that most foundation models developed in 2023 were open. See Maslej et al. (2024), *The AI Index 2024 Annual Report*, AI Index Steering Committee, Institute for Human-Centered AI.

[132] Despite these advantages, there are alternatives. An industry participant from a large financial institution at the FSB-OECD joint roundtable on AI in finance in May 2024 indicated that their institution works with small LLMs using on premises GPUs owned by the firm.

Glossary

This glossary sets out a (non-exhaustive) list of terms used in the report. These terms, commonly used in the field of AI, have been compiled based on their general understanding and usage within the community. These definitions serve as a reference for understanding the specific context in which these terms are used in this report. They may not cover all possible interpretations or uses of these terms in other contexts.

Algorithm: An algorithm is a set of steps to be performed or rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer.

Deep learning: Deep learning is a form of machine learning that uses algorithms that work in 'layers' inspired by the structure and function of the brain. Deep learning algorithms, whose structure are called artificial neural networks, can be used for supervised, unsupervised, or reinforcement learning.

Foundation models: An umbrella term referring to a diversity of models that are usually trained by applying deep learning to massive quantities of data, such as text and images. Because the expertise, time, and computing power involved in training foundation models from scratch are typically prohibitive for most non-specialist firms, these models are usually pre-trained and shared with end-users for further use and refinement.

Generative AI (GenAI): AI that generates new content, such as text, images, and videos, often based on user prompts. GenAI is powered by foundation models, such as LLMs.

Large Language Models (LLMs): A type of foundation model that is trained on and designed to perform tasks with natural language. Most LLMs are trained using the Transformer architecture. Key tasks LLMs perform include text generation, document classification, summarisation, question-and-answer, and sentiment analysis, among other tasks.

Machine learning: Machine learning is a method of designing a sequence of actions to solve a problem, known as algorithms, which optimise automatically through experience and with limited or no human intervention.

Reinforcement learning: 'Reinforcement learning' falls in between supervised and unsupervised learning. In this case, the algorithm is fed an unlabelled set of data, chooses an action for each data point, and receives feedback (perhaps from a human) that helps the algorithm learn. For instance, reinforcement learning can be used in robotics, game theory, and self-driving cars.

Semi-supervised learning: A combination of supervised and unsupervised learning in which some of the input data is labelled.

Supervised learning: In 'supervised learning', the algorithm is fed a set of 'training' data that contains labels on some portion of the observations. For instance, a data set of transactions may contain labels on some data points identifying those that are fraudulent and those that are not fraudulent. The algorithm will 'learn' a general rule of classification that it will use to predict the labels for the remaining observations in the data set.

Traditional AI: Traditional AI models refer to a suite of computational techniques that pre-date recent advances, such as GenAI.

Transformer architecture: Transformer architecture is a type of neural network that feature two key innovations allowing it to improve language understanding and do so efficiently from a computation perspective: self-attention and positional encoding. Self-attention allows each word in a paragraph or text to relate to every other word, which enhances the understanding of context and relationships between words. Positional encoding enables transformers to process data concurrently by applying a 'self-attention' mechanism to better understand the relationship between words in a given text while also using less compute power as compared to other models.

Unsupervised learning: 'Unsupervised learning' refers to situations where the data provided to the algorithm does not contain labels. The algorithm is asked to detect patterns in the data by identifying clusters of observations that depend on similar underlying characteristics. For example, an unsupervised machine learning algorithm could be set up to look for securities that have characteristics similar to an illiquid security that is hard to price. If it finds an appropriate cluster for the illiquid security, pricing of other securities in the cluster can be used to help price the illiquid security.

Abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BoE	Bank of England
CFT	Counter-Terrorist Financing
CSP	Cloud Service Provider
ECB	European Central Bank
EBA	European Banking Authority
EU	European Union
FCA	Financial Conduct Authority
FI	Financial Institution
FSB	Financial Stability Board
FSOC	Financial Stability Oversight Council
FSSCC	Financial Services Sector Coordinating Council
GenAI	Generative Artificial Intelligence
GPU	Graphics Processing Unit
HKMA	Hong Kong Monetary Authority
IAIS	International Association of Insurance Supervisors
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IRB	Internal Ratings-Based
KYC	Know Your Customer

LLM	Large Language Model
ML	Machine Learning
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
PRA	Prudential Regulation Authority
RAG	Retrieval Augmented Generation
RegTech	Regulatory Technology
SDK	Software Development Kit
SSB	Standard Setting Body
SupTech	Supervisory Technology
UK	United Kingdom
US	United States